DT-Assisted Multi-point Symbiotic Security in Space-air-ground Integrated Networks

Zhisheng Yin, *Member IEEE,* Nan Cheng, *Member IEEE*, Tom H. Luan, *Senior Member IEEE*, Yunchao Song, *Member IEEE*, and Wei Wang, *Member IEEE*

***Abstract*—In this paper, we investigate the secure transmission of multi-resource heterogeneous radio access networks (RANs) in space-air-ground integrated network (SAGIN) from the perspective of physical layer security. Considering the network heterogeneity, resource constrain, and channel similarity, it is challenging to implement the physical layer security in SAGIN. Particularly, digital twin (DT) is considered in the cyberspace of SAGIN to reflect the physical network entities (i.e., satellite, unmanned aerial vehicle (UAV), and terrestrial base station), which is assumed to comprehensively control and manage the heterogeneous RANs' resources. To ensure secure transmissions of multi-tier heterogeneous downlink communications in SAGIN, a multi-point symbiotic security scheme is proposed through DT-assisted multi-dimensional domain synergy precoding, where the co-channel interference due to spectrum sharing among these heterogeneous RANs is recast to unevenly corrupt the main and wiretap channels of each legitimate user. Specifically, to realize the multi-point symbiotic security, a max-min problem is formulated to maximize the minimum secrecy rate of three heterogeneous downlinks. Since this problem is non-convex and challenging, a list of mathematical reformulations is derived and the successive convex approximation (SCA) based multi-dimensional domain synergy precoding algorithm is proposed to solve it. Moreover, the computational complexity of our proposed approach is analyzed and meaningful discussions are made. In addition, extensive simulations are carried out to evaluate the secrecy rate performance and verify the efficiency of our proposed approach.**

***Index Terms*—SAGIN, digital twin, symbiotic security, secrecy rate, multi-dimensional domain precoding.**

I. Introduction

SPACE-air-ground integrated network (SAGIN) is promising to enable new services and requirements such as ubiquitous artificial intelligence (AI), integrated cloud-edge-end, and integrated sensing-communication-computing etc. In sixth generation (6G) networks since its seamless coverage, random access and strong resistance to damage [1]–[3]. To fullfill such anticipated potentials, the architecture of SAGIN for on-demand service has been ambitiously investigated in academia and industry, where the resource orchestration and security in SAGIN is still an open issue and poses key challenges since its multi-tier heterogeneity, dynamic, and differentiated properties [3]–[5]. Currently, the emerging digital twin (DT) technology is trying to create a revolution in industrial manufacturing and network infrastructure, which has attracted frontier attentions in both military and civilian networks [6]–[8]. Particularly, DT has also been introduced into 6G to support flexible management and control, which shows a potential solution to deeply integrate and efficiently orchestrate multi-source heterogeneous resources in SAGIN [3], [4], [6], [9].

Due to the open connectivity, dynamic topology, and compatible and concurrent air-interface protocols, the wireless transmissions in SAGIN are susceptible to eavesdropping threats and the threat penetration between different secure domains [11], [12]. Different from cryptographic security in the upper layer, physical layer security places emphasis on the secure transmission via wireless channels, which is a lightweight information-theoretic approach and generally realized through signal processing and secure coding [13]–[16]. Particularly, the absolute security can be realized when the main channel capacity is better than the eavesdropping capacity, according to the Wyner eavesdropping channel model [17], [18]. Based on this, extensive studies on physical layer security have been well conducted in terrestrial communications, where abundant randomness difference of terrestrial wireless channels could be utilized for carrying out physical layer security techniques [19], [20]. Recently it also has attracted great attention on physical layer security towards SAGIN [21], [22]. However, different from traditional terrestrial networks, the non-terrestrial channels in SAGIN experience similarity since the strong line-of-sight path is dominant and the distance difference between source and destination can be neglected. Besides, the non-terrestrial segments are well known as resource-constrained, such as power and antenna, etc. Besides, these multi-tier resources in SAGIN are heterogeneous and thus it is hard to conduct the synergy signal processing comprehensively. Considering the above challenges, the secure transmissions in SAGIN have not been well addressed, which motivates this work.

In this paper, we investigate the multi-point symbiotic security in SAGIN with assistance of DT, where the secure transmissions in multiple heterogeneous links are synchronously achieved and reciprocally benefit from each other. Particularly, a typical model in SAGIN where three heterogeneous communication links, i.e., satellite-to-ground link, air-to-ground link, and terrestrial link, are comprehensively considered to

Z. Yin and Tom H. Luan are with State Key Lab. of ISN and School of Cyber Engineering, Xidian University, Xi'an, 710071, China (e-mail: {zsyin,tom.luan}@xidian.edu.cn).

N. Cheng is with State Key Lab. of ISN and School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China (e-mail: dr.nan.cheng@ieee.org).

Y. Song is with the College of Electronic and Optical Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China (e-mail: songyc@njupt.edu.cn).

W. Wang is with the College of Electronic Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, 211106, China (e-mail: wei_wang@nuaa.edu.cn).

Corresponding authors: N. Cheng and Tom H. Luan.

conduct the symbiotic secure transmissions, where the spectrum sharing is adopted between these links. Our concerned mobile agents coexist in the overlapping coverage of radio access networks (RANs) respectively associated with satellite, the unmanned aerial vehicle (UAV), and the terrestrial base station (BS). An eavesdropper (Eve) is assumed to hide in that overlapping coverage and thus it holds the threat of eavesdropping on the three communication links. Considering the channel similarity, limited resource, and heterogeneity in SAGIN, we comprehensively and synchronously guarantee the secure transmission in satellite link, air-to-ground link, and terrestrial link, by an idea of symbiosis, in this work. Specifically, main contributions of this paper are summarized as follows.

- A framework of DT-assisted symbiotic secure transmissions in SAGIN is proposed, where the heterogeneous resources are cooperatively managed by the DTs of satellite, UAV, and BS in both the core and edge cloud. The real-time link information is reflected at the corresponding DT and the interaction between heterogeneous links is established through the inter- and intra-twin communication. Based on this framework, the signal processing within multi-dimensional domains can be conducted in SAGIN, which directs the symbiotic secure transmissions in this work.
- To realize the multi-point symbiotic secure transmission, the co-channel interference among links of satellite, UAV, and BS caused by spectrum sharing is leveraged to unevenly affect the main and eavesdropping channels. To preferably shape such interference for improving the secrecy rate performance, we formulate a max-min problem to maximize the minimum secrecy rate of downlinks from satellite, UAV, and BS, where the synergy precoding within multi-dimensional domains is executed. Since the formulated max-min problem is non-convex and challenging, a list of ingenious mathematical manipulations are made and the successive convex approximation (SCA) based synergy precoding algorithm is proposed to find the near-optimal solutions.
- To ensure the tightness of relaxation from the rank-one matrix optimization to the semidefinite optimization in the above solving process, the rank-one of output precoding matrix of our proposed algorithm is proved. Also the computational complexity of the SCA-based synergy precoding for multi-point symbiotic security is analyzed. In addition, extensive simulations for the performance evaluation are carried out to verify the efficiency of our proposed approach and some interesting insights are found.

The remainder of this paper is organized as follows. Related works are summarized in Section II. In Section III, the system model of DT-assisted symbiotic secure transmissions in SAGIN is illustrated and the problem formulation is conducted. In Section IV, the approach of multi-dimensional domains synergy precoding is proposed for symbiotic secure transmissions. In Section V, extensive simulations are carried out to verify the secrecy rate performance in SAGIN. Finally, we conclude this paper and direct future work in Section VII.

II. Related Works

DT can accurately reflect the physical entity in the digital domain, where the DT monitors the status of physical system through the real-time sensing interaction between the physical entity and its DT [2]. In DT edge networks, the edge nodes can acquire the real-time behavior information of physical entities and a virtual dynamical environment can be built by DT [23]. Moreover, considering the more complex network architecture in 6G such as SAGIN, the DTs of network components can be distributed over the cloud and edges and they can overall orchestrate resource [24], [25]. Particularly, DT enables an intelligent offloading and resource allocation in [26], where an optimization problem is solved in the digital domain of edge networks. DT-enabled edge-cloud collaborative architecture with clock synchronization is developed to improve the overall system efficiency for heterogeneous networks [27]. DT-enabled the heterogeneous resource integration has shown great potential and keen attention, and the functions of DT in network applications can be summarized as prediction, data logging, model training, information exchange, and decision making, etc. [9], [25].

For the investigation of physical layer security in SAGIN, there are literates contributing secure transmission technologies in satellite networks, UAV netowrks, and satellite-terrestrial hybrid/integrated networks, respectively. In fact, a few works focus on the independent satellite network, and the channel similarity between satellite channels is first pointed out in [28], which is much different from the case in conventional terrestrial networks. Under constrained transmission power of satellite. Researches on secure transmissions related to UAV networks are comparatively extensive, but most of it has not been included in SAGIN, only as an independent scenario [29], [30]. Due to the high mobility and flexible deployment of UAV, it is also adopted to serve as a relay or jammer to facilitate the secure transmission in other networks [31]–[35], e.g., satellite networks, cellular networks, and IoT networks, etc. However, the aforementioned studies have only considered scenarios involving individual networks such as satellite networks or drone networks. They have focused solely on the secure transmission of individual links, neglecting to address scenarios that involve the integration of multilayer heterogeneous networks.

Whereas, in satellite-terrestrial hybrid/integrated networks, the secure transmissions of satellite link and terrestrial link are respectively explored independently. To guarantee the secure transmission of terrestrial link, the system secrecy energy efficiency (SEE) is maximized by secure beamforming and the common rate requirements of cellular users are satisfied in cognitive satellite-terrestrial networks where satellite and BS share the same frequency band [36]. Based on non-orthogonal multiple access (NOMA), the effect of hardware impairments on the secrecy performance of integrated satellite multiple-terrestrial relay networks is studied and the secrecy outage probability (SOP) for both colluding and non-colluding cases is analyzed [37]. By exploiting an intelligent reflecting surface, the signal-to-interference-plus-noise-ratio (SINR) at Eve

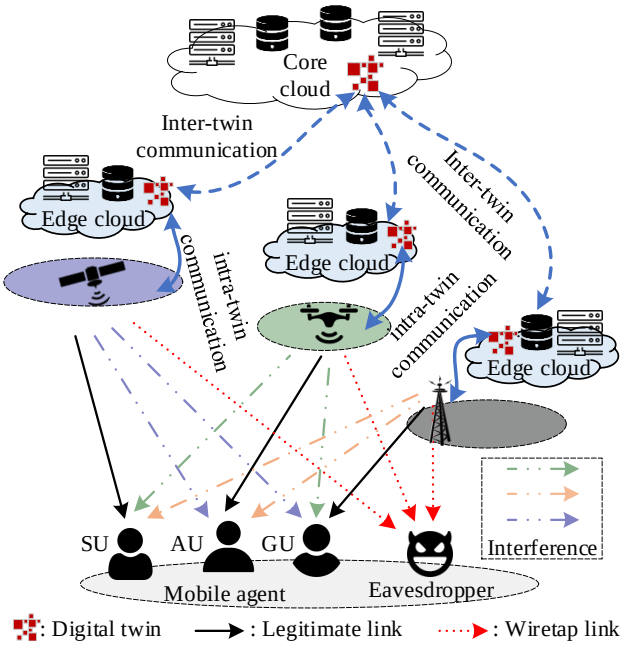

Fig. 1. DT-assisted symbiotic secure transmissions in SAGIN.

targeting satellite downlink is minimized and meanwhile the reliable communication of terrestrial link is guaranteed [38]. The relay-user pairing and the relay-user pairing approaches are proposed to secure the confidential signals from both satellite and terrestrial relays [39], where the secrecy outage probability is analyzed. The beamforming scheme is proposed at secondary network served by terrestrial BS to suppress Eve for eavesdropping primary link [40], and a joint beamforming design at both satellite and terrestrial BS is proposed for maximizing the sum secrecy rate of satellite users while meeting the rate requirements of terrestrial users and transmit power constraints [41]. However, the existing studies, despite considering scenarios involving the coexistence of satellite and terrestrial networks, have only addressed the secure transmission of individual links. They also depend on resources external to the secure link for functions such as interference mechanisms or cooperative signal processing. Different from these existing studies, this paper addresses the issue of secure transmission over multi-tier heterogeneous links within SAGIN. This means achieving simultaneous secure transmission over multiple access links at the space, air, and ground layers without relying on external system resources. It takes into account the reciprocal influences between heterogeneous access networks with the objective of establishing mutually beneficial secure transmission links.

Notations: $(\cdot)^{\dagger}$ denotes the Hermitian transpose, respectively. $\|\cdot\|$ stands for the Euclidean norm of a vector. $tr(\cdot)$ and $rank(\cdot)$ denote the trace and rank of a matrix, respectively. $\mathbb{C}^{N\times M}$ denotes a complex space of $N \times M$. $\mathcal{N}\left(\mu, \delta^2\right)$ denotes the normal distribution with mean μ and variance δ^2. $[x]^{+} = \max(x, 0)$. e is the natural constant. Other notations are defined in Table I.

TABLE I
SUMMARY OF NOTATIONS AND DEFINITIONS

Notation	Definition
N_S	Number of satellite transmit antennas
N_U	Number of UAV transmit antennas
N_B	Number of BS transmit antennas
P_S	Satellite transmission power
P_U	UAV transmission power
P_B	BS transmission power
$\mathbf{h}_{su} \in \mathbb{C}^{N\times 1}$	Channel vector from satellite to SU
$\mathbf{h}_{au} \in \mathbb{C}^{N_S\times 1}$	Channel vector from satellite to AU
$\mathbf{h}_{gu} \in \mathbb{C}^{N_S\times 1}$	Channel vector from satellite to GU
$\mathbf{h}_{e} \in \mathbb{C}^{N_S\times 1}$	Channel vector from satellite to Eve
$\mathbf{a}_{su} \in \mathbb{C}^{N_U\times 1}$	Channel vector from UAV to SU
$\mathbf{a}_{au} \in \mathbb{C}^{N_U\times 1}$	Channel vector from UAV to AU
$\mathbf{a}_{gu} \in \mathbb{C}^{N_U\times 1}$	Channel vector from UAV to GU
$\mathbf{a}_{e} \in \mathbb{C}^{N_U\times 1}$	Channel vector from UAV to Eve
$\mathbf{g}_{su} \in \mathbb{C}^{M\times 1}$	Channel vector from BS to SU
$\mathbf{g}_{au} \in \mathbb{C}^{M\times 1}$	Channel vector from BS to AU
$\mathbf{g}_{gu} \in \mathbb{C}^{M\times 1}$	Channel vector from BS to GU
$\mathbf{g}_{e} \in \mathbb{C}^{M\times 1}$	Channel vector from BS to Eve
$\mathbf{w} \in \mathbb{C}^{N_S\times 1}$	Precoding vector of satellite downlink transmission
$\mathbf{f} \in \mathbb{C}^{N_U\times 1}$	Precoding vector of UAV downlink transmission
$\mathbf{v} \in \mathbb{C}^{N_G\times 1}$	Precoding vector of BS downlink transmission
R_{su}	Instantaneous secrecy rate of SU
R_{au}	Instantaneous secrecy rate of AU
R_{gu}	Instantaneous secrecy rate of GU
Δ	Norm-bounded channel estimate error
ϵ	Predefined tolerance for the termination of procedure

III. SYSTEM MODEL

Due to the multi-source heterogeneity, DT is considered to assist the deep integration in SAGIN in this work, where the resource orchestration and the heterogeneous access are assumed to be controlled and managed by DTs of networking entities. Fig. 1 shows the architecture of DT-enabled symbiotic secure transmissions in SAGIN, where a satellite, an UAV, and a terrestrial BS are deployed for constituting a basic SAGIN model. Respectively, the DTs of satellite, UAV, or BS are constructed in both core and edge cloud sides. The intra-twin communication refers to the information exchange between a specific entity in the network and its DT, accurately reflecting the real-time status information of the entity. On the other hand, inter-twin communication denotes the communication among different DTs in the cloud, involving information exchange between heterogeneous networks. Particularly, we consider multi-source heterogeneous access network providers, i.e., satellite, UAV, and BS, share the spectrum to improve the utilization, which is a general consideration in research field of 6G SAGIN and institution operators. Without loss of generality, three kinds of mobile agents, i.e., satellite user (SU), aerial user (AU), and ground user (GU), are assumed

to associate with satellite, UAV, and BS, respectively. Considering an eavesdropping scenario in SAGIN, an Eve exists within the overlapping coverage of among satellite, UAV, and BS, where the Eve works with the same spectrum as legitimate users, e.g., SU, AU, and GU, thus the legitimate signals would leak out to the Eve. In addition, multiple antennas are assumed at satellite, UAV, and BS to transmit downlink signals, where the number of transmit antennas are denoted by N_S, N_U, N_B, respectively.

Considering this typical heterogeneous secure transmission scenario, to achieve integrated secure transmission among multi-tier heterogeneous networks, necessary interactions are required to form a global optimization model based on the resource information of the heterogeneous links. Therefore, intra-twin communication is responsible for conveying key information to its corresponding DT. Subsequently, the exchange of parameters needed for executing a global optimization is conducted through the inter-twin communication link.

A. Physical Layer Channel Models

In Fig. 1, the communication links between SAGIN RAN and mobile agents involve satellite-to-ground channel, air-to-ground channel, and terrestrial channel.

For the satellite-to-ground channel, the impact of free space path loss (FSPL), rain attenuation, and satellite beam gain [42] can be modeled as

$$\mathbf{h} = \sqrt{C_L b \beta} \exp\left(-j\boldsymbol{\theta}\right), \tag{1}$$

where $C_L = \left(\lambda/4\pi\right)^2 / \left(d^2 + h^2\right)$ denotes the FSPL from satellite to ground with λ denoting the signal wavelength, d being the distance from the beam center to the center of satellite coverage, and h accounting for the height of satellite; β denotes the channel gain due to rain attenuation and β is modeled as a log-normal random variable, i.e., $\ln\left(\beta_{dB}\right) \sim \mathcal{N}\left(u, \delta^2\right)$ with β_{dB} being the dB form of β; $\boldsymbol{\theta}$ is the phase vector with uniform distribution over $[0, 2\pi)$; and b denotes the satellite beam gain, which is defined by

$$b = G_{max}\left(\frac{J_1\left(u_0\right)}{2u_0} - 36\frac{J_3\left(u_0\right)}{u_0^2}\right)^2, \tag{2}$$

where G_{max} denotes the maximum satellite antenna gain, $u_0 = 2.07123 \sin\left(\alpha\right)/\sin\left(\alpha_{3\mathrm{dB}}\right)$ with α being the elevation angle between the beam center and SU, and $\alpha_{3\mathrm{dB}}$ being the 3 dB angle of satellite beam. Additionally, $J_1\left(\cdot\right)$ and $J_3\left(\cdot\right)$ are the first-kind Bessel functions of order 1 and 3, respectively. Particularly, $\mathbf{h}_{su} \in \mathbb{C}^{N_S \times 1}$, $\mathbf{h}_{au} \in \mathbb{C}^{N_S \times 1}$, $\mathbf{h}_{gu} \in \mathbb{C}^{N_S \times 1}$, $\mathbf{h}_e \in \mathbb{C}^{N_S \times 1}$ are assumed to be the channel vectors from satellite to SU, AU, GU, and Eve, respectively.

The channel of air-to-ground dominantly involves both path loss and small-scale fading, which is given by [43]

$$\mathbf{a} = \sqrt{G_L}\left(\sqrt{\frac{K}{K+1}}\mathbf{a}_{\mathrm{LoS}} + \sqrt{\frac{1}{K+1}}\mathbf{a}_{\mathrm{Ray}}\right), \tag{3}$$

where $G_L = g_0 / \left(U_d^2 + U_h^2\right)$ denotes the path loss with g_0 being the channel power gain at a reference distance of 1 m, U_d being the horizontal distance from UAV to the destination, and U_h being the UAV altitude; the small-scale fading adopts Rician channel model, where K is the Rician factor ($K_B = 10log_{10}(K)$ in dB), $\mathbf{a}_{\mathrm{LoS}} \in \mathbb{C}^{N_U \times 1}$ denotes the line-of-sight (LoS) component, and $\mathbf{a}_{\mathrm{Ray}} \in \mathbb{C}^{N_U \times 1}$ represents the non-line-of-sight (NLoS) Rayleigh fading component. Particularly, $\mathbf{a}_{su} \in \mathbb{C}^{N_U \times 1}$, $\mathbf{a}_{au} \in \mathbb{C}^{N_U \times 1}$, $\mathbf{a}_{gu} \in \mathbb{C}^{N_U \times 1}$, $\mathbf{a}_e \in \mathbb{C}^{N_U \times 1}$ are assumed to be the channel vectors from the UAV to SU, AU, GU, and Eve, respectively.

Whereas, we adopt the channel model for terrestrial links as $\mathbf{g} = \sqrt{\alpha}\mathbf{g}_0$, where α denotes the large-scale fading, $\alpha = C_0 r^{-4}$ with C_0 being the channel power gain at the reference distance of 1 m and r denoting the distance from BS to the destination [44]. Additionally, $\mathbf{g}_0$ denotes the small-scale fading which undergoes Nakagami-m fading with fading severity m and average power Ω. Particularly, $\mathbf{g}_{su} \in \mathbb{C}^{N_G \times 1}$, $\mathbf{g}_{au} \in \mathbb{C}^{N_G \times 1}$, $\mathbf{g}_{gu} \in \mathbb{C}^{N_G \times 1}$, and $\mathbf{g}_e \in \mathbb{C}^{N_G \times 1}$ denote the channel vectors from BS to SU, AU, GU, and Eve, respectively.

B. SAGIN Downlink Signal Models

In the downlink communication in SAGIN, we consider the heterogeneous links request satellite, UAV, and BS for the transmission of confidential signals, i.e., s_{su}, s_{au}, and s_{gu}, respectively. Therefore, the signals received at SU, AU, and GU can be respectively expressed as

$$y_{su} = \mathbf{h}_{su}^{\dagger}\mathbf{w}s_{su} + \mathbf{a}_{su}^{\dagger}\mathbf{f}s_{au} + \mathbf{g}_{su}^{\dagger}\mathbf{v}s_{gu} + n_{su}, \tag{4}$$

$$y_{au} = \mathbf{h}_{au}^{\dagger}\mathbf{w}s_{su} + \mathbf{a}_{au}^{\dagger}\mathbf{f}s_{au} + \mathbf{g}_{au}^{\dagger}\mathbf{v}s_{gu} + n_{au}, \tag{5}$$

$$y_{gu} = \mathbf{h}_{gu}^{\dagger}\mathbf{w}s_{su} + \mathbf{a}_{gu}^{\dagger}\mathbf{f}s_{au} + \mathbf{g}_{gu}^{\dagger}\mathbf{v}s_{gu} + n_{gu}, \tag{6}$$

where $\mathbf{w} \in \mathbb{C}^{N_S \times 1}$, $\mathbf{f} \in \mathbb{C}^{N_U \times 1}$, and $\mathbf{v} \in \mathbb{C}^{N_G \times 1}$ are the precoding vectors of satellite, UAV, and BS downlink transmission, respectively, and n_{su}, n_{au}, and n_{gu} denote the noise received by SU, AU, and GU, respectively.

The received signal at the Eve is given by

$$y_e = \mathbf{h}_e^{\dagger}\mathbf{w}x_{su} + \mathbf{a}_e^{\dagger}\mathbf{f}x_{au} + \mathbf{g}_e^{\dagger}\mathbf{v}x_{gu} + n_e, \tag{7}$$

where n_e denotes the noise received at Eve.

From (4–6), it can be seen that the legitimate user, e.g., SU, AU, and GU, receives their corresponding expected signal and the co-channel interference is also received, which indicates that the three heterogeneous legitimate links in Fig. 1 constitute a multi-point self-interfere system due to the spectrum sharing among multi-resource RAN in SAGIN. From (7), the Eve wiretaps legitimate signals of both SU, AU, and GU, and their modulation and demodulation schemes are assumed to be known at Eve. Thus, the Eve has an opportunistic access to the confidential information from either satellite, UAV, or BS indiscriminatingly.

Based on (4–6), the received SINRs of SU, AU, and GU can be respectively obtained as

$$\gamma_{su} = \frac{\left|\mathbf{h}_{su}^{\dagger}\mathbf{w}\right|^2}{\left|\mathbf{a}_{su}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{su}^{\dagger}\mathbf{v}\right|^2 + \delta_{su}^2}, \tag{8}$$

$$\gamma_{au} = \frac{\left|\mathbf{a}_{au}^{\dagger}\mathbf{f}\right|^2}{\left|\mathbf{h}_{au}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{au}^{\dagger}\mathbf{v}\right|^2 + \delta_{au}^2}, \tag{9}$$

$$\gamma_{gu} = \frac{\left|\mathbf{g}_{gu}^{\dagger}\mathbf{v}\right|^2}{\left|\mathbf{h}_{gu}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{gu}^{\dagger}\mathbf{f}\right|^2 + \delta_{gu}^2}, \tag{10}$$

where the δ_{su}^2, δ_{au}^2, and δ_{gu}^2 denote the noise power received by SU, AU, and GU.

Observing (7), the SINRs of Eve for wiretapping SU, AU, and GU can be respectively calculated as

$$\gamma_{se} = \frac{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2}{\left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + \delta_{e}^2}, \tag{11}$$

$$\gamma_{ae} = \frac{\left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2}{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + \delta_{e}^2}, \tag{12}$$

$$\gamma_{ge} = \frac{\left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2}{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + \delta_{e}^2}. \tag{13}$$

From (8-13), the co-channel interference affects the SINRs of both legitimate users and Eve simultaneously, which brings a drawback for common communication performance of legitimate users but it is expected to benefit the secure transmission. We design the inherent interference due to spectrum sharing as a reciprocal interference for assisting secure transmissions of SU, AU, and GU.

C. Problem Formulation

In this work, we aim at the physical layer security of SAGIN and focus on the secrecy rate performance of both satellite, UAV, and BS downlink. By using (8)–(13), the secrecy rates of SU, AU, and GU can be respectively given by

$$R_{su} = \left[\log_2\left(1+\gamma_{su}\right) - \log_2\left(1+\gamma_{se}\right)\right]^+, \tag{14}$$

$$R_{au} = \left[\log_2\left(1+\gamma_{au}\right) - \log_2\left(1+\gamma_{ae}\right)\right]^+, \tag{15}$$

$$R_{gu} = \left[\log_2\left(1+\gamma_{gu}\right) - \log_2\left(1+\gamma_{ge}\right)\right]^+. \tag{16}$$

For easy analysis and reformulation, we make the following facilitation, i.e., $\delta_{su}^2 = \delta_{au}^2 = \delta_{gu}^2 = \delta_{e}^2 = \delta_{e}^2 = 1$, and (17)–(19) can be further represented as shown at the top of this page.

To realize secure transmissions in multi-source RANs of SAGIN and improve the secrecy rate performance of both SU, AU, and GU, a max-min problem is formulated as shown in $\mathcal{P}1$ in (20).

$$\mathcal{P}1: \quad \underset{\mathbf{w},\mathbf{f},\mathbf{v}}{\text{Max}}\, \text{Min}\left\{R_{su}, R_{au}, R_{gu}\right\} \tag{20a}$$

$$\text{s.t.:} \quad \left\|\mathbf{w}\right\|^2 \le P_S, \tag{20b}$$

$$\left\|\mathbf{f}\right\|^2 \le P_U, \tag{20c}$$

$$\left\|\mathbf{v}\right\|^2 \le P_B, \tag{20d}$$

where (20b), (20c), and (20d) represent the constrained-power of satellite, UAV, and BS, respectively. From $\mathcal{P}1$, it is observed that the problem is non-convex since it has a non-convex objective function with some fractions of quadratic terms, and non-convex constraints. Therefore, it is intractable to solve $\mathcal{P}1$ directly.

Remark 1. *By solving $\mathcal{P}1$, the SU, AU, and GU can reach the symbiotic security. Addressing the insufficient channel difference, the inherent co-channel interference caused by spectrum sharing in SAGIN serves as the reciprocal interference, which is leveraged to design for unevenly damaging both the main and wiretap channels associated with satellite, UAV, and BS downlink, respectively. Therefore, the approach that achieves secure transmission between heterogeneous links through the intrinsic security mechanisms of system, which we refer to as "symbiotic security," displays a unique method of design. Importantly, this technique eschews dependence on external resources such as jamming devices or cooperative entities, highlighting its self-sufficient character within the context of security protocol implementation.*

IV. Multi-dimensional Domains Synergy Precoding for Symbiotic Secure Transmissions

In this section, we first make a list of reformulations to convert the problem $\mathcal{P}1$ into a solvable form, and then the multi-dimensional domain synergy precoding is carried out to solve it. The connotation of the multi-dimensional domains synergy precoding is to synergistically execute the precoding at satellite, UAV, and BS for designing the co-channel interference among multi-RANs, which is leveraged to increase the difference of signal transmission quality via both main and wiretapping channels in satellite-to-SU link, UAV-to-AU link, and BS-to-GU link, respectively. Thereby, the positive secrecy rates in (17), (18), and (19) can be guaranteed. On this basis, the secrecy performance of theses transmissions in SAGIN can be further improved with solving the problem $\mathcal{P}1$.

By introducing an auxiliary variable φ to represent the minimum secrecy rate of R_{su}, R_{au}, R_{gu}, thus we have

$$\varphi \le R_{su}, \tag{21}$$

$$\varphi \le R_{au}, \tag{22}$$

$$\varphi \le R_{gu}. \tag{23}$$

Remark 2. *With the introduction in (21–23), we assume a feasible solution φ° from the following reconstructed problem*

$$\mathcal{P}: \quad \underset{\mathbf{w},\mathbf{f},\mathbf{v}}{\text{Max}}\, \varphi$$
$$\textit{s.t.:} \quad (20b) - (23).$$

Therefore, $\varphi^\circ \le R_{su}$, $\varphi^\circ \le R_{au}$, and $\varphi^\circ \le R_{gu}$ are satisfied and then $\varphi^\circ \le \min\left\{R_{su}, R_{au}, R_{gu}\right\}$ is also achieved. We assume the feasible precoding vectors $\left\{\mathbf{w}^\circ, \mathbf{f}^\circ, \mathbf{v}^\circ\right\}$ are obtained when the φ° is achieved. Since the constraints in primal $\mathcal{P}1$ are all satisfied in the reconstructed $\mathcal{P}$, $\left\{\mathbf{w}^\circ, \mathbf{f}^\circ, \mathbf{v}^\circ\right\}$ are also feasible for $\mathcal{P}1$. It can be seen that the maximum φ^* is achieved when $\varphi^* = \min\left\{R_{su}, R_{au}, R_{gu}\right\}$, thus

$$\left\{\mathbf{w}^*, \mathbf{f}^*, \mathbf{v}^*\right\} = \arg\max \min\left\{R_{su}, R_{au}, R_{gu}\right\}$$

which is achieved when φ^* is obtained, and it is proved to be equivalent to the primal problem.

$$R_{su} = \log_2\left(\frac{\left|\mathbf{h}_{su}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{su}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{su}^{\dagger}\mathbf{v}\right|^2 + 1}{\left|\mathbf{a}_{su}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{su}^{\dagger}\mathbf{v}\right|^2 + 1}\right) - \log_2\left(\frac{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + 1}{\left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + 1}\right)$$
$$= \log_2\left(\frac{\mathbf{h}_{su}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{su} + \mathbf{a}_{su}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{su} + \mathbf{g}_{su}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{su} + 1}{\mathbf{a}_{su}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{su} + \mathbf{g}_{su}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{su} + 1}\right) - \log_2\left(\frac{\mathbf{h}_{e}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{e} + \mathbf{a}_{e}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{e} + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + 1}{\mathbf{a}_{e}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{e} + \mathbf{g}_{e}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{e} + 1}\right), \quad (17)$$

$$R_{au} = \log_2\left(\frac{\left|\mathbf{a}_{au}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{h}_{au}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{au}^{\dagger}\mathbf{v}\right|^2 + 1}{\left|\mathbf{h}_{au}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{au}^{\dagger}\mathbf{v}\right|^2 + 1}\right) - \log_2\left(\frac{\left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + \left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + 1}{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + 1}\right)$$
$$= \log_2\left(\frac{\mathbf{a}_{au}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{au} + \mathbf{h}_{au}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{au} + \mathbf{g}_{au}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{au} + 1}{\mathbf{h}_{au}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{au} + \mathbf{g}_{au}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{au} + 1}\right) - \log_2\left(\frac{\mathbf{a}_{e}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{e} + \mathbf{h}_{e}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{e} + \mathbf{g}_{e}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{e} + 1}{\mathbf{h}_{e}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{e} + \mathbf{g}_{e}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{e} + 1}\right), \quad (18)$$

$$R_{gu} = \log_2\left(\frac{\left|\mathbf{g}_{gu}^{\dagger}\mathbf{v}\right|^2 + \left|\mathbf{h}_{gu}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{gu}^{\dagger}\mathbf{f}\right|^2 + 1}{\left|\mathbf{h}_{gu}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{gu}^{\dagger}\mathbf{f}\right|^2 + 1}\right) - \log_2\left(\frac{\left|\mathbf{g}_{e}^{\dagger}\mathbf{v}\right|^2 + \left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + 1}{\left|\mathbf{h}_{e}^{\dagger}\mathbf{w}\right|^2 + \left|\mathbf{a}_{e}^{\dagger}\mathbf{f}\right|^2 + 1}\right)$$
$$= \log_2\left(\frac{\mathbf{a}_{gu}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{gu} + \mathbf{h}_{gu}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{gu} + \mathbf{g}_{gu}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{gu} + 1}{\mathbf{h}_{gu}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{gu} + \mathbf{a}_{gu}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{gu} + 1}\right) - \log_2\left(\frac{\mathbf{a}_{e}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{e} + \mathbf{h}_{e}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{e} + \mathbf{g}_{e}^{\dagger}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{g}_{e} + 1}{\mathbf{h}_{e}^{\dagger}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{h}_{e} + \mathbf{a}_{e}^{\dagger}\mathbf{f}\mathbf{f}^{\dagger}\mathbf{a}_{e} + 1}\right). \quad (19)$$

Particularly, we first make the following replacements:

$$\mathbf{H}_{su} = \mathbf{h}_{su}\mathbf{h}_{su}^{\dagger}, \mathbf{H}_{au} = \mathbf{h}_{au}\mathbf{h}_{au}^{\dagger}, \mathbf{H}_{gu} = \mathbf{h}_{gu}\mathbf{h}_{gu}^{\dagger}, \mathbf{H}_{e} = \hat{\mathbf{h}}_{e}\hat{\mathbf{h}}_{e}^{\dagger};$$
$$\mathbf{A}_{su} = \mathbf{a}_{su}\mathbf{a}_{su}^{\dagger}, \mathbf{A}_{au} = \mathbf{a}_{au}\mathbf{a}_{au}^{\dagger}, \mathbf{A}_{gu} = \mathbf{a}_{gu}\mathbf{a}_{gu}^{\dagger}, \mathbf{A}_{e} = \hat{\mathbf{a}}_{e}\hat{\mathbf{a}}_{e}^{\dagger};$$
$$\mathbf{G}_{su} = \mathbf{g}_{su}\mathbf{g}_{su}^{\dagger}, \mathbf{G}_{au} = \mathbf{g}_{au}\mathbf{g}_{au}^{\dagger}, \mathbf{G}_{gu} = \mathbf{g}_{gu}\mathbf{g}_{gu}^{\dagger}, \mathbf{G}_{e} = \hat{\mathbf{g}}_{e}\hat{\mathbf{g}}_{e}^{\dagger};$$
$$\mathbf{W} = \mathbf{w}\mathbf{w}^{\dagger}, \mathbf{F} = \mathbf{f}\mathbf{f}^{\dagger}, \mathbf{V} = \mathbf{v}\mathbf{v}^{\dagger}.$$

Note that the CSI of Eve is hard to figure out and thus the imperfect CSI model of Eve is generally adopted [21], i.e., $\mathbf{h}_e = \hat{\mathbf{h}}_e + \Delta\mathbf{h}_e$, $\mathbf{a}_e = \hat{\mathbf{a}}_e + \Delta\mathbf{a}_e$, $\mathbf{g}_e = \hat{\mathbf{g}}_e + \Delta\mathbf{g}_e$, where $\Delta\mathbf{h}_e, \Delta\mathbf{a}_e$, and $\Delta\mathbf{g}_e$ denote the corresponding norm-bounded estimate errors.

By using (17-19), (21–23) can be further rewritten as shown in (24)–(26).

$$\varphi \le \log\left(\frac{tr\left(\mathbf{H}_{su}\mathbf{W}\right) + tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1}{tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1}\right) - \log\left(\frac{tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1}{tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1}\right), \quad (24)$$

$$\varphi \le \log\left(\frac{tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{A}_{au}\mathbf{F}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1}{tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1}\right) - \log\left(\frac{tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1}{tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1}\right), \quad (25)$$

$$\varphi \le \log\left(\frac{tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + tr\left(\mathbf{G}_{gu}\mathbf{V}\right) + 1}{tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + 1}\right) - \log\left(\frac{tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1}{tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + 1}\right). \quad (26)$$

From (24-26), it can be seen that the co-channel interference affects the secrecy rate of both SU, AU, and GU, as well as the value of φ. For instance, in (24), the main channel from satellite to SU is affected by the interference from both UAV and BS, i.e., the interference level is determined by $tr\left(\mathbf{A}_{su}\mathbf{F}\right)$ and $tr\left(\mathbf{G}_{su}\mathbf{V}\right)$ respectively. Whereas, the eavesdropping channel from satellite to Eve is also damaged by the interference from both UAV and BS, i.e., the interference level is determined by $tr\left(\mathbf{A}_{e}\mathbf{F}\right)$ and $tr\left(\mathbf{G}_{e}\mathbf{V}\right)$ respectively. It indicates that the secrecy rate of SU is leveraged by such co-channel interference. In particular, an insight is proposed for the variation of the secrecy rate with transmission power in the following proposition.

Proposition 1. *When the co-channel interference from other coexisting legitimate links damages the Eve more sharply than it affects the legitimate one in SAGIN, the secrecy rate of SU, AU, and GU monotonously increases as its transmission power, respectively.*

Proof. Please see Appendix A. ■

Therefore, the problem $\mathcal{P}1$ can be equivalently reformulated as

$$\mathcal{P}2: \quad \underset{\mathbf{W},\mathbf{F},\mathbf{V}}{\text{Max}}\ \varphi \quad (27a)$$
$$\text{s.t.:} \quad (24) - (26) \quad (27b)$$
$$tr\left(\mathbf{W}\right) \le P_S, \quad (27c)$$
$$tr\left(\mathbf{F}\right) \le P_U, \quad (27d)$$
$$tr\left(\mathbf{V}\right) \le P_B, \quad (27e)$$
$$rank\left(\mathbf{W}\right) = 1, rank\left(\mathbf{F}\right) = 1, rank\left(\mathbf{V}\right) = 1. \quad (27f)$$

Since the fractional polynomial of optimization variables exist in (24)–(26), the constraints in (24)–(26) is non-convex. Besides, the rank-one constraint in (27f) is also non-convex. Therefore, the problem $\mathcal{P}2$ is still non-convex. For the rank-one constrains of $\mathbf{W}$, $\mathbf{F}$, and $\mathbf{V}$, a general transformation is adopted by semi-definite relaxation. Whereas, the constraints in (24)–(26) can be further reshaped by introducing auxiliary

variables, i.e., x_{su}, x_{au}, x_{gu}, y_{su}, y_{au}, y_{gu}, z_{su}, z_{au}, z_{gu}, and t, such as

$$e^{x_{su}} = tr\left(\mathbf{H}_{su}\mathbf{W}\right) + tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1, \quad (28)$$

$$e^{y_{su}} = tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1, \quad (29)$$

$$e^{z_{su}} = tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (30)$$

$$e^{t} = tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1. \quad (31)$$

By substituting (28-31) into (24), (24) can be represented as

$$\varphi \ln 2 - x_{su} + y_{su} - z_{su} + t \leq 0, \quad (32)$$

$$e^{x_{au}} = tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{A}_{au}\mathbf{F}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1, \quad (33)$$

$$e^{y_{au}} = tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1, \quad (34)$$

$$e^{z_{au}} = tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (35)$$

$$\varphi \ln 2 - x_{au} + y_{au} - z_{au} + t \leq 0, \quad (36)$$

$$e^{x_{gu}} = tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + tr\left(\mathbf{G}_{gu}\mathbf{V}\right) + 1, \quad (37)$$

$$e^{y_{gu}} = tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + 1, \quad (38)$$

$$e^{z_{gu}} = tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + 1, \quad (39)$$

$$\varphi \ln 2 - x_{gu} + y_{gu} - z_{gu} + t \leq 0. \quad (40)$$

Thus, the reformulated problem can be written as

$$\mathcal{P}3: \max_{\mathbf{W},\mathbf{F},\mathbf{V}} \varphi \quad (41)$$

$$\text{s.t.:} \quad (32, 36, 40, 27c, 27d, 27e), \quad (41a)$$

$$e^{x_{su}} \leq tr\left(\mathbf{H}_{su}\mathbf{W}\right) + tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1, \quad (41b)$$

$$e^{x_{au}} \leq tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{A}_{au}\mathbf{F}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1, \quad (41c)$$

$$e^{x_{gu}} \leq tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + tr\left(\mathbf{G}_{gu}\mathbf{V}\right) + 1, \quad (41d)$$

$$e^{y_{su}} \geq tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1, \quad (41e)$$

$$e^{y_{au}} \geq tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1, \quad (41f)$$

$$e^{y_{gu}} \geq tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + 1, \quad (41g)$$

$$e^{z_{su}} \leq tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (41h)$$

$$e^{z_{au}} \leq tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (41i)$$

$$e^{z_{gu}} \leq tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + 1, \quad (41j)$$

$$e^{t} \geq tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (41k)$$

$$\mathbf{W} \succeq \mathbf{0}, \mathbf{F} \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, . \quad (41l)$$

Remark 3. *For any feasible solution, the equivalences in constraints of (41b-41k) are satisfied simultaneously. From (32, 36, and 40), it is observed that φ increases monotonically with $x_{su,au,gu}$ and $z_{su,au,gu}$, and decreases monotonically with $g_{su,au,gu}$ and t, respectively. It indicates that $e^{x_{su}}, e^{x_{au}}, e^{x_{gu}}, e^{z_{su}}, e^{z_{au}}$, and $e^{z_{gu}}$ take the maximum value and $e^{y_{su}}, e^{y_{au}}, e^{y_{gu}}$, and t take the minimum value simultaneously when maximizing φ.*

For the constraints (41e-41g, 41k) in $\mathcal{P}3$, the first-order Taylor expansion is adopted to recast it, which can be written as

$$e^{\tilde{y}_{su}}\left(y_{su} - \tilde{y}_{su} + 1\right) \geq tr\left(\mathbf{A}_{su}\mathbf{F}\right) + tr\left(\mathbf{G}_{su}\mathbf{V}\right) + 1, \quad (42)$$

$$e^{\tilde{y}_{au}}\left(y_{au} - \tilde{y}_{au} + 1\right) \geq tr\left(\mathbf{H}_{au}\mathbf{W}\right) + tr\left(\mathbf{G}_{au}\mathbf{V}\right) + 1, \quad (43)$$

$$e^{\tilde{y}_{gu}}\left(y_{gu} - \tilde{y}_{gu} + 1\right) \geq tr\left(\mathbf{H}_{gu}\mathbf{W}\right) + tr\left(\mathbf{A}_{gu}\mathbf{F}\right) + 1, \quad (44)$$

$$e^{\tilde{t}}\left(t - \tilde{t} + 1\right) \geq tr\left(\mathbf{H}_{e}\mathbf{W}\right) + tr\left(\mathbf{A}_{e}\mathbf{F}\right) + tr\left(\mathbf{G}_{e}\mathbf{V}\right) + 1, \quad (45)$$

where $\tilde{y}_{su}$ is a constant. Replacing by (42-45) into $\mathcal{P}3$, for any feasible $\{\tilde{y}_{su}, \tilde{y}_{au}, \tilde{y}_{gu}, \tilde{t}\}$ the problem $\mathcal{P}3$ turns into convex and solvable, which can be finally solved based on a SCA algorithm. Specifically, in each iterative update, the SDP is executed for matrix optimization by MATLAB CVX tool, the output feasible solutions are denoted by $\mathbf{W}^*, \mathbf{F}^*, \mathbf{V}^*$ and the procedure is terminated by a predefined tolerance ϵ, i.e., $\left|\varphi_i\left(\mathbf{W}_i^*, \mathbf{F}_i^*, \mathbf{V}_i^*\right) - \varphi_{i-1}\left(\mathbf{W}_{i-1}^*, \mathbf{F}_{i-1}^*, \mathbf{V}_{i-1}^*\right)\right| < \epsilon$. In addition, the algorithm is concluded as shown in Algorithm Table 1. In the DT-assisted framework, SCA-based synergy precoding is performed in the digital domain. Parameters from multiple heterogeneous access networks within the SAGIN are integrated into the DT domain. The DTs then compute the output precoding vectors based on Algorithm 1. These vectors are subsequently transferred to the corresponding network entity for further operations.

Considering a multi-user access technique prevalently employed in satellite communication systems and UAV downlink scenarios, e.g., frequency division multiple access (FDMA), provides an appropriate foundation for applying the coexistence security strategy developed in this study. This strategy, premised on the principle of synergy precoding, can be seamlessly applied to each resource block, offering considerable scope for extension to multi-user transmission scenarios. The crux of our proposed approach lies in its design of reciprocal interference, a byproduct of spectrum sharing, enabling the simultaneous satisfaction of secure transmission requisites across an array of heterogeneous links. The extensibility of this symbiotic secure transmission mechanism, therefore, becomes apparent when one considers its applicability to communication contexts where reciprocal interference is available. This provides opportunities for enhancing secrecy performance through joint optimization, highlighting the broad-ranging applicability of our proposed methodology.

Algorithm 1: SCA-based Synergy Precoding for Multi-point Symbiotic Security.

Input: P_S, P_U, P_B.
Result: $\mathbf{W}^*, \mathbf{F}^*, \mathbf{V}^*$.
Initialization: $\tilde{y}_{su}, \tilde{y}_{au}, \tilde{y}_{gu}, \tilde{t}$.
Set $i = 1$.
repeat
  Execute SDP solver by CVX tool to solve $\mathcal{P}3$;
  Output: $\mathbf{W}^*, \mathbf{F}^*, \mathbf{V}^*, \varphi_i^*, \tilde{x}_{su}^*, \tilde{x}_{au}^*, \tilde{x}_{gu}^*, \tilde{z}_{su}^*, \tilde{z}_{au}^*, \tilde{z}_{gu}^*$.
  Update parameters:
  $\tilde{y}_{su} = \tilde{y}_{su}^*, \tilde{y}_{au} = \tilde{y}_{au}^*, \tilde{y}_{gu} = \tilde{y}_{gu}^*, \tilde{t} = \tilde{t}^*$;
  Return to step 4;
until
  $\left|\varphi_i\left(\mathbf{W}_i^*, \mathbf{F}_i^*, \mathbf{V}_i^*\right) - \varphi_{i-1}\left(\mathbf{W}_{i-1}^*, \mathbf{F}_{i-1}^*, \mathbf{V}_{i-1}^*\right)\right| < \epsilon$;
Obtain precoding vectors $\mathbf{w}_n^\star, \mathbf{f}_n^\star, \mathbf{v}_n^\star$ by the singular value decomposition (SVD) of the final output $\mathbf{W}^*, \mathbf{F}^*, \mathbf{V}^*$.
Calculate the secrecy rate: Obtain R_{su}, R_{au}, R_{gu} according to (17-19);
Procedure End

Since semidefinite relaxation is used for the transformation

of (27f) $\mathcal{P}2$ into (41l) in $\mathcal{P}3$, the following Proposition and Theorem are given to prove the tightness of rank-one relaxation which guarantees that precoding vectors can be obtained by taking the SVD of $\mathbf{W}^*, \mathbf{F}^*$, and $\mathbf{V}^*$, respectively. For easy analysis, we fire provide an power-minimization problem defined in Proposition2 which is equivalent to $\mathcal{P}3$ and then Theorem 1 proves its rank-one condition to complete the proof the tightness of semidefinite relaxation.

Proposition 2. *Assuming φ^* to be the optimal objection value of $\mathcal{P}3$, an equivalent power-minimization problem is constructed as follows*

$$\mathcal{P}4: \min_{\{\mathbf{W},\mathbf{F},\mathbf{V},\varphi\}} tr(\mathbf{W}) + tr(\mathbf{F}) + tr(\mathbf{V}), \tag{46a}$$

$$s.t.: \quad \varphi \geq \varphi^*, \tag{46b}$$

$$(41a - 41l), \tag{46c}$$

which has the same solution as $\mathcal{P}3$.

Proof. We assume $\mathbf{W}^\star, \mathbf{F}^\star, \mathbf{V}^\star$, and $\varphi^\star$ to be the optimal solution for the power-minimization problem, thus $\varphi^\star \geq \varphi^*$ is satisfied based on (46b). It is clear to observe that any feasible solution in Proposition 2 is optimal for $\mathcal{P}3$, and the maximum φ^* is achieved at $\varphi^\star$. Therefore, $\mathbf{W}^\star, \mathbf{F}^\star, \mathbf{V}^\star$, and $\varphi^\star$ are also optimal for $\mathcal{P}3$. ■

Based on Proposition 2, it is equivalent to prove the rank-one constraint in $\mathcal{P}3$ by proving that in the power-minimization problem given in the following Theorem 1.

Theorem 1. *For solving $\mathcal{P}3$, any feasible $\mathbf{W}^\star, \mathbf{F}^\star$, or $\mathbf{V}^\star$ output from* Algorithm 1 holds rank-one.

Proof. Please see Appendix B. ■

Computational complexity: The main complexity of Algorithm 1 can be calculated by the iteration number multiplying the complexity in each iteration. In each iteration, the SDP for solving $\mathcal{P}3$ by using an interior-point algorithm can be calculated by $\mathcal{O}(max\{m,n\}^4 n^{1/2})$, where m and n are the constraint order and the dimension of equality constraints for SDP, respectively. Thus, given a considerable solution accuracy $\epsilon > 0$, the Algorithm 1 can be solved with a worst-case complexity of $\mathcal{O}(I(16^{4.5} log(1/\epsilon) + 3N^3))$ with I denoting the iteration number.

V. Performance Evaluations

In this section, we first establish a simulation platform of DT-assisted space-air-ground integrated networks with wire-tapping model and then extensive simulations are carried out to evaluate the secrecy rate performance of heterogeneous users in SAGIN, i.e., SU, AU, and GU. Specifically, system parameters are set as shown in Tab. II. A LEO satellite with multi-antenna is employed where its orbit height is set to 600 Km, the maximum beam gain is 46 dB, and the 3-dB angle of satellite beam is set to 0.4°. The log-normal attenuation parameters of satellite channel gain are set to $\mathcal{N}(-3.152\text{dB}, 1.6)$. The air-to-ground channel power gain at the reference distance of 1 m is set to -40 dB and the Rician factor of small-scale fading is 10 dB. The channel power gain of BS downlink is set to -38.46 dB. The carrier frequency of satellite, UAV, and BS downlink is 2.4 GHz. Particularly, the impacts of transmit power and number of transmit antennas of satellite, UAV, and BS on the secrecy rate performance are evaluated, respectively. Besides the impact of UAV altitude on the secrecy rate performance is also evaluated. In addition, fixed precoding schemes, i.e., zero-forcing (ZF) and maximum ratio transmission (MRT), are considered as the benchmarks, where such fixed precoding schemes are set for benefiting its corresponding secure transmission [21], [45], [46] and the primal max-min optimization problem is still succeeded with the power optimization of satellite, UAV, and BS.

TABLE II
System Parameters Setting

System parameters	Numerical value
Satellite-ground channel parameters	
Satellite height	600 Km
Carrier frequency	2.4 GHz
Maximum beam gain	46 dB
3 dB angle (for all beams)	0.4°
Rain attenuation parameters	$\mu_{\zeta_{dB}}$ = -3.152, $\delta^2 = 1.6$
Air-to-ground channel parameters	
Channel reciean factor,	10 dB
Channel power gain	-40 dB
BS channel parameters	
Channel power gain	-38.46 dB
Nakagami-m channel parameters	$m = 2$, $\Omega = 1$

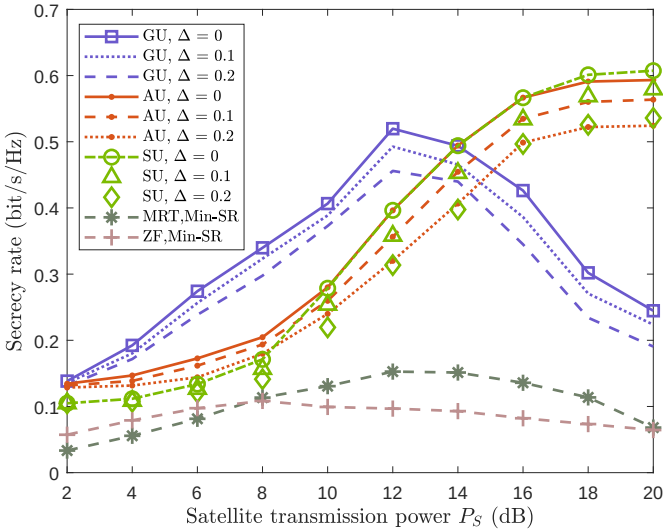

Fig. 2. The impact of satellite transmit power on the secrecy rates of SU, AU, and GU. ($P_U = 5$ dB, $P_B = 15$ dB, $N_S = 4$, $N_U = 4$, $N_B = 4$)

Fig. 2 shows the impact of satellite transmission power on the secrecy rates of SU, AU, and GU, where the transmission powers of UAV and BS are $P_U = 5$ dB and $P_B = 15$ dB, respectively, and the transmit antennas of satellite, UAV, and BS are all set to 4, i.e., $N_S = 4$, $N_U = 4$, $N_B = 4$. From

Fig. 2, it can be seen that the symbiotic secure transmissions among SU, AU, and GU is realized, where the secrecy rates of SU and AU increase monotonically with the satellite transmission power by our proposed multi-dimensional domains synergy precoding approach, and the secrecy rate of GU firstly increases monotonically and then decreases with the satellite transmission power. Particularly, the impact of satellite transmission power on the secrecy rate of SU has been proved in Proposition 1, which is verified by the simulation. Whereas to the secrecy rate of the GU, the interference from satellite on GU increases with the satellite's transmission power, which benefits the secrecy rate of the GU in a moderate range and turns into a drawback as it grows persistently. The secrecy rate performance is also evaluated in the presence of channel estimate error, i.e., $\Delta = 0.1, 0.2$ and it can be seen that the secrecy rate degrades as the channel estimation error increases. This is because the calculated precoding vectors focus on the direction with channel estimation errors which leads to signal leakage. It is obvious that the secrecy rates of AU and SU are closely equal, this is because the security in both satellite and UAV links mainly relies on the assistance from BS. By the proposed synergy precoding, the max-min secrecy rate is achieved when the secrecy rates of AU and SU are closely equal. In addition, compared with the minimum secrecy rate among SU, AU, and GU obtained by heterogeneous MRT/ZF based precoding schemes, our proposed approach shows improved max-min secrecy performance.

Fig. 3 shows the impact of UAV transmission power on the secrecy rates of SU, AU, and GU, where the transmission powers of satellite and BS are set to $P_S = 10$ dB and $P_B = 15$ dB, respectively, and the transmit antennas of satellite, UAV, and BS are all set to 4, i.e., $N_S = 4$, $N_U = 4$, $N_B = 4$. From Fig. 3, it can be seen that the secrecy rate of AU increases monotonically with the UAV transmission power based on our proposed approach, which verifies the analysis in Proposition 1; For the secrecy rates of SU and GU, they

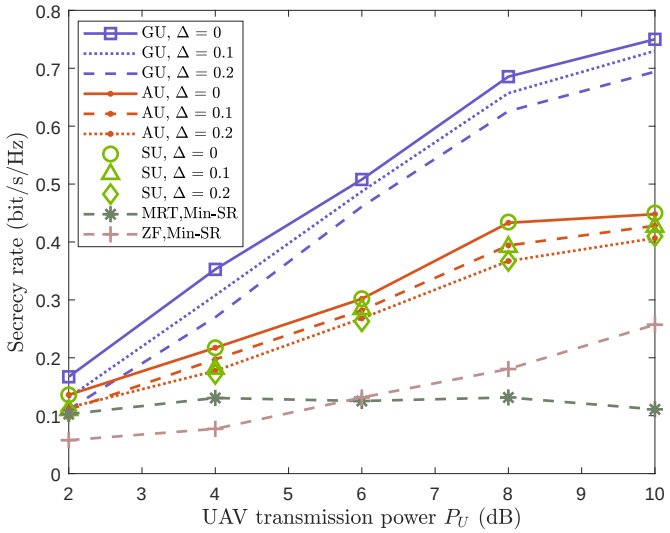

Fig. 3. The impact of UAV transmission power on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_B = 15$ dB, $N_S = 4$, $N_U = 4$, $N_B = 4$)

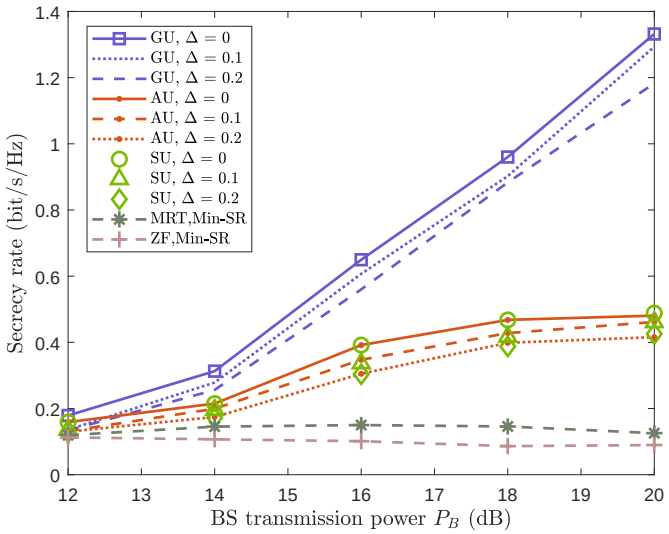

Fig. 4. The impact of BS transmission power on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_U = 5$ dB, $N_S = 4$, $N_U = 4$, $N_B = 4$)

are also increasing monotonically of the UAV transmission power. This is because the interference from UAV damages the Eve more heavily than it interferes with SU and GU, respectively. In addition, the efficiency of multi-dimensional domains synergy precoding approach is verified by comparing to the MRT/ZF-based precoding schemes.

Fig. 4 shows the impact of BS transmission power on the secrecy rates of SU, AU, and GU, where the transmission powers of satellite and UAV are set to $P_S = 10$ dB and $P_U = 5$ dB, respectively, and the transmit antennas of satellite, UAV, and BS are $N_S = 4$, $N_U = 4$, $N_B = 4$, respectively. From Fig. 4, it can be seen that the secrecy rate of GU increases monotonically with the BS transmission power, which has been verified in Proposition 1; For the impact of BS transmission power on the secrecy rate of SU or GU which also increases monotonically with the BS transmission power, this is because the interference from BS damages the Eve for eavesdropping SU and GU more heavily than it interferes with SU and GU, respectively. Besides, when the BS transmission power increases much enough, the secrecy rates of SU and GU grow slowly and reach a platform, which indicates that the BS transmission power focuses more on GU and the legitimated interference to both SU and GU is well controlled.

Fig. 5 shows the impact of number of satellite transmit antennas on the secrecy rates of SU, AU, and GU, where the transmission powers of satellite, UAV and BS are set to $P_S = 10$ dB, $P_U = 5$ dB, and $P_B = 15$ dB, respectively, and the number of transmit antennas at UAV and BS are $N_U = 4$ and $N_B = 4$, respectively. From Fig. 5, we can see that the secrecy rate of GU increases monotonically with the number of satellite transmit antennas by our proposed approach and outperforms the secrecy rates of SU and GU. This is because that the matrix dimensions of satellite precoding increases as the number of satellite transmit antennas, which can direct the signal direction better. Besides, the synergy precoding shows improved secrecy rate performance compared to traditional fixed MRT/ZF precodings.

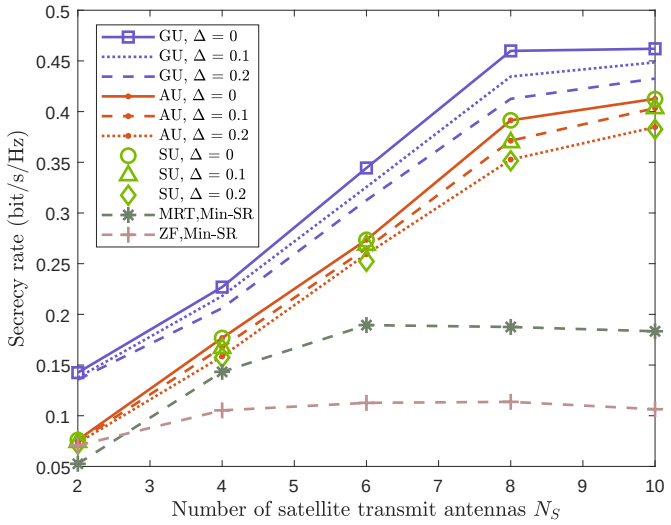

Fig. 5. The impact of number of satellite transmit antennas on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_U = 5$ dB, $P_B = 15$ dB, $N_U = 4$, $N_B = 4$)

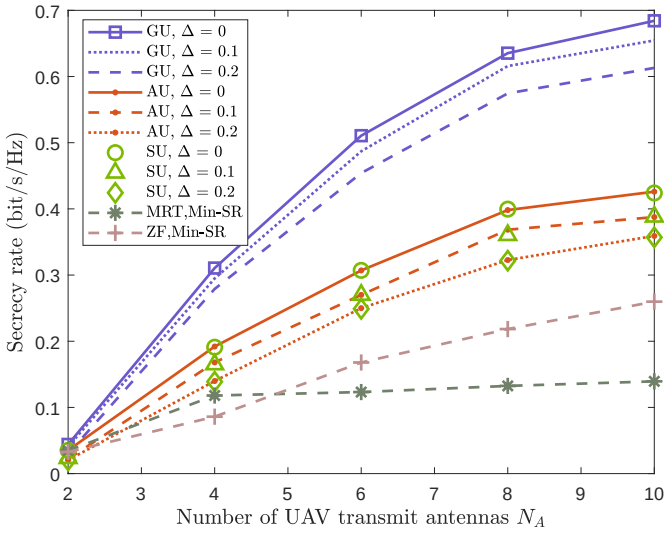

Fig. 6. The impact of number of UAV transmit antennas on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_U = 5$ dB, $P_B = 15$ dB, $N_S = 4$, $N_G = 4$)

Fig. 6 and Fig. 7 show the impact of the number of UAV transmit antennas and the number of BS transmit antennas on the secrecy rates of SU, AU, and GU, respectively. In Fig. 6 and Fig. 7, the transmission powers of satellite, UAV, and BS are set to $P_S = 10$ dB, $P_U = 5$ dB, and $P_B = 15$ dB, respectively. The number of transmit antennas of satellite and BS are $N_S = 4$ and $N_G = 4$ in Fig. 6, respectively. Whereas in Fig. 7, the number of transmit antennas of satellite and BS are $N_S = 4$ and $N_A = 4$, respectively. From Fig. 6 and Fig. 7, we can that the secrecy rates of SU, AU, and GU increase monotonically with the number of UAV transmit antenna and also with the number of BS transmit antenna. This is because, as the number of transmit antennas at UAV or BS increases, the signal direction is accordingly more concentrated at AU or GU. Besides, the channel difference in air-to-ground and terrestrial links can be better utilized to distinguish the main and eavesdropping channels through the precoding before the signal transmitting. Particularly, in Fig. 6, it can be seen that the SU and GU also benefit from the increasing number of UAV transmit antennas. Fig. 7 shows that the SU and AU can also benefit from the increasing number of BS transmit antennas. In addition, our proposed synergy precoding approach outperforms the traditional MRT/ZF schemes.

We also investigate the impact of UAV altitude on the secrecy rates of SU, AU, and GU in Fig. 8, where the transmission powers of satellite, UAV, and BS are set to $P_S = 10$ dB, $P_U = 5$ dB, and $P_B = 15$ dB, respectively, and the number of transmit antennas at satellite, UAV, and BS are set to $N_S = 4$, $N_U = 4$, and $N_G = 4$, respectively. From Fig. 8, it can be seen that the secrecy rates of SU, AU, and GU decrease as the UAV altitude increases. This is because the air-to-ground channel quality degrades as the increasing UAV altitude and the channel difference between the channels from UAV to AU and Eve becomes weaker. Therefore, as the UAV altitude increases, the secrecy rate of AU decreases and the available interference from UAV for SU and GU becomes

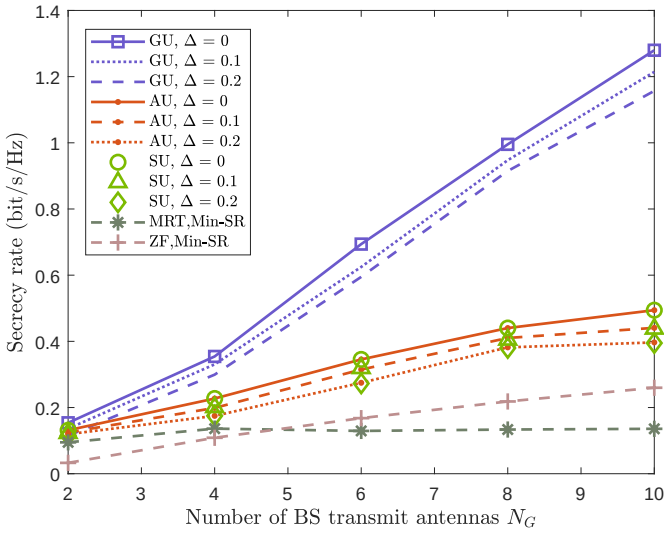

Fig. 7. The impact of number of BS transmit antennas on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_U = 5$ dB, $P_B = 15$ dB, $N_S = 4$, $N_U = 4$)

weaker which degrades the secrecy rates of SU and GU. In addition, the impact of channel estimation errors agrees with the analysis we given previously.

VI. Conclusions

In this paper, we have investigated the DT-assisted multi-point symbiotic security in space-air-ground integrated network. The framework of DT-assisted symbiotic secure transmissions in SAGIN is first established, where heterogeneous secure transmissions are conducted simultaneously in SAGIN. The co-channel interference due to spectrum sharing among downlinks of satellite, UAV, and BS has been considered as a reciprocal interference for benefiting the symbiotic secure transmission. To realize the symbiotic security with assistance of reciprocal interference, a problem is formulated to max-

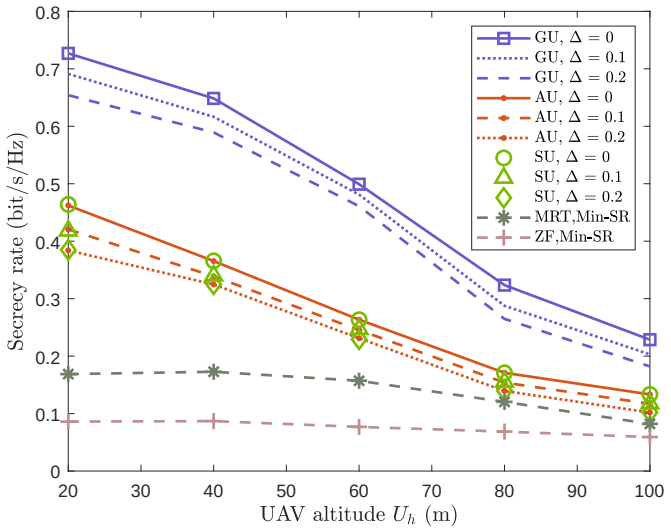

Fig. 8. The impact of UAV altitude on the secrecy rates of SU, AU, and GU. ($P_S = 10$ dB, $P_U = 5$ dB, $P_B = 15$ dB, $N_S = 4$, $N_U = 4$, $N_G = 4$)

imize the minimum secrecy rate among satellite, UAV, and terrestrial links. Particularly, the multi-dimensional domains synergy precoding scheme is proposed to optimize the reciprocal interference at SU, AU, and GU, which unevenly corrupts the main and eavesdropping channel capacity to improve the secrecy performance. In addition, the impact of such reciprocal interference on the secrecy rate of SU, AU, and GU has been analyzed. To solve the formulated problem, a list of efficient transformations and a SCA-based synergy precoding algorithm for multi-point symbiotic security have been provided to find near-optimal solutions. Besides, the complexity is analyzed and the rank-one relaxation is proved. Finally, extensive numerical results have verified the efficiency of our proposed approach. For future work, we will investigate the case that multiple eavesdroppers collude with symbiotic security transmission mechanism.

Appendix A: Proof of Proposition 1

Proof. Considering the channel similarity between both legitimate and wiretap satellite channels, it indicates that $tr\left(\mathbf{H}_{su}\mathbf{W}\right) \approx tr\left(\mathbf{H}_{e}\mathbf{W}\right)$ with any feasible solution of $\mathbf{W}$. Therefore, the secrecy rate of SU can be further approximatively expressed as

$$\begin{aligned} R_{su} &= \log\left(\frac{tr\left(\mathbf{H}_{su}\mathbf{W}\right)+tr\left(\mathbf{A}_{su}\mathbf{F}\right)+tr\left(\mathbf{G}_{su}\mathbf{V}\right)+1}{tr\left(\mathbf{A}_{su}\mathbf{F}\right)+tr\left(\mathbf{G}_{su}\mathbf{V}\right)+1}\right) \\ &\quad - \log\left(\frac{tr\left(\mathbf{H}_{e}\mathbf{W}\right)+tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+1}{tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+1}\right) \\ &\approx \log\left(\frac{tr\left(\mathbf{A}_{su}\mathbf{F}\right)+tr\left(\mathbf{G}_{su}\mathbf{V}\right)+\alpha}{tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+\alpha}\right) \\ &\quad - \log\left(\frac{tr\left(\mathbf{A}_{su}\mathbf{F}\right)+tr\left(\mathbf{G}_{su}\mathbf{V}\right)+1}{tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+1}\right), \end{aligned} \tag{47}$$

where $\alpha = tr\left(\mathbf{H}_{su}\mathbf{W}\right)+1 \approx tr\left(\mathbf{H}_{e}\mathbf{W}\right)+1$. Observing the form of expression in (47), we define two constant variables to simplify (47), which can be represented as

$$\vartheta\left(\alpha\right) = \log\left(\frac{r+\alpha}{s+\alpha}\right) - \log\left(\frac{r+1}{s+1}\right), \tag{48}$$

where $r = tr\left(\mathbf{A}_{su}\mathbf{F}\right)+tr\left(\mathbf{G}_{su}\mathbf{V}\right)$ and $s = tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)$.

Based on (48), we take the derivative of $\vartheta\left(\alpha\right)$ with respect to α, which is given as

$$\nabla_{\alpha}\vartheta\left(\alpha\right) = \log e\left(\frac{1}{r+\alpha}-\frac{1}{s+\alpha}\right). \tag{49}$$

Thus, when $r \leqslant s$, it achieves $\nabla_{\alpha}\vartheta\left(\alpha\right) \geqslant 0$, which is proved as the co-channel interference from UAV and BS damages the Eve more sharply than that affects SU. In this case, R_{su} monotonously increases as α and thus it increases as satellite transmission power.

For the secrecy rate of AU, we take the derivative of R_{au} with respect to $\mathbf{F}$, which is given as

$$\nabla_{\mathbf{F}}R_{au} = \log e\left(\frac{\nabla_{\mathbf{F}}tr\left(\mathbf{A}_{au}\mathbf{F}\right)}{\beta_f}-\frac{\nabla_{\mathbf{F}}tr\left(\mathbf{A}_{e}\mathbf{F}\right)}{\theta_f}\right), \tag{50}$$

where

$$\beta_f = tr\left(\mathbf{H}_{au}\mathbf{W}\right)+tr\left(\mathbf{A}_{au}\mathbf{F}\right)+tr\left(\mathbf{G}_{au}\mathbf{V}\right)+1, \tag{51}$$

and

$$\theta_f = tr\left(\mathbf{H}_{e}\mathbf{W}\right)+tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+1. \tag{52}$$

Since the UAV primarily concentrates its signal power on the direction of AU with precoding matrix $\mathbf{F}$, it is clear to obtain that $tr\left(\mathbf{A}_{au}\mathbf{F}\right) \geqslant tr\left(\mathbf{A}_{e}\mathbf{F}\right)$, thus $\nabla_{\mathbf{F}}tr\left(\mathbf{A}_{au}\mathbf{F}\right) \geqslant \nabla_{\mathbf{F}}tr\left(\mathbf{A}_{e}\mathbf{F}\right)$ is satisfied. Recalling (50), it can be observed that $\nabla_{\mathbf{F}}R_{au} \geqslant 0$ when $tr\left(\mathbf{H}_{au}\mathbf{W}\right)+tr\left(\mathbf{G}_{au}\mathbf{V}\right) \leqslant tr\left(\mathbf{H}_{e}\mathbf{W}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)$, which is proved as the co-channel interference from satellite and BS damages the Eve more sharply than that affects AU. Thus we prove that R_{au} increases as UAV transmission power.

For taking the derivative of R_{gu} with respect to $\mathbf{V}$, we have

$$\nabla_{\mathbf{V}}R_{gu} = \log e\left(\frac{\nabla_{\mathbf{V}}tr\left(\mathbf{G}_{gu}\mathbf{V}\right)}{\beta_v}-\frac{\nabla_{\mathbf{V}}tr\left(\mathbf{G}_{e}\mathbf{V}\right)}{\theta_v}\right), \tag{53}$$

where

$$\beta_v = tr\left(\mathbf{H}_{gu}\mathbf{W}\right)+tr\left(\mathbf{A}_{gu}\mathbf{F}\right)+tr\left(\mathbf{G}_{gu}\mathbf{V}\right)+1, \tag{54}$$

and

$$\theta_v = tr\left(\mathbf{H}_{e}\mathbf{W}\right)+tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right)+1. \tag{55}$$

Similarly, keeping in mind that the co-channel interference from satellite and UAV damages the Eve more sharply than that affects GU, i.e.,

$$tr\left(\mathbf{A}_{gu}\mathbf{F}\right)+tr\left(\mathbf{G}_{gu}\mathbf{V}\right) \leq tr\left(\mathbf{A}_{e}\mathbf{F}\right)+tr\left(\mathbf{G}_{e}\mathbf{V}\right), \tag{56}$$

thus $\beta_v \leq \theta_v$ is achieved. In addition, $\nabla_{\mathbf{V}}tr\left(\mathbf{G}_{gu}\mathbf{V}\right) \geq \nabla_{\mathbf{V}}tr\left(\mathbf{G}_{e}\mathbf{V}\right)$ is a basic guarantee to ensure the positive secrecy rate. Thus, $\nabla_{\mathbf{V}}R_{gu} \geq 0$ is achieved which proves that R_{gu} increases as BS transmission power. Thus the proof is completed. ■

$$
\begin{aligned}
&L\left\{\lambda,\rho_{au},\rho_{su},\rho_{gu},\tau_{su},\tau_{au},\tau_{gu},\zeta_{su},\zeta_{au},\zeta_{gu},\ell_{su},\ell_{au},\ell_{gu},\mu,\sigma_w,\sigma_f,\sigma_v,\mathbf{U},\mathbf{L},\mathbf{V}\right\}=\\
&tr\left(\mathbf{W}\right)+tr\left(\mathbf{F}\right)+tr\left(\mathbf{V}\right)-\lambda\left(\varphi-\varphi^{*}\right)+\rho_{au}\left(\varphi\ln 2-x_{au}+y_{au}-z_{au}+t\right)+\rho_{su}\left(\varphi\ln 2-x_{su}+y_{su}-z_{su}+t\right)\\
&+\rho_{gu}\left(\varphi\ln 2-x_{gu}+y_{gu}-z_{gu}+t\right)+\tau_{su}\left(e^{x_{su}}-tr\left(\mathbf{H}_{su}\mathbf{W}\right)-tr\left(\mathbf{A}_{su}\mathbf{F}\right)-tr\left(\mathbf{G}_{su}\mathbf{V}\right)-1\right)-\mathbf{UW}-\mathbf{LF}-\mathbf{TV}\\
&+\tau_{au}\left(e^{x_{au}}-tr\left(\mathbf{H}_{au}\mathbf{W}\right)-tr\left(\mathbf{A}_{au}\mathbf{F}\right)-tr\left(\mathbf{G}_{au}\mathbf{V}\right)-1\right)+\tau_{gu}\left(e^{x_{gu}}-tr\left(\mathbf{H}_{gu}\mathbf{W}\right)-tr\left(\mathbf{A}_{gu}\mathbf{F}\right)-tr\left(\mathbf{G}_{gu}\mathbf{V}\right)-1\right)\\
&-\zeta_{su}\left(e^{\tilde{y}_{su}}\left(y_{su}-\tilde{y}_{su}+1\right)-tr\left(\mathbf{A}_{su}\mathbf{F}\right)-tr\left(\mathbf{G}_{su}\mathbf{V}\right)-1\right)-\zeta_{au}\left(e^{\tilde{y}_{au}}\left(y_{au}-\tilde{y}_{au}+1\right)-tr\left(\mathbf{H}_{au}\mathbf{W}\right)-tr\left(\mathbf{G}_{au}\mathbf{V}\right)-1\right)\\
&-\zeta_{gu}\left(e^{\tilde{y}_{gu}}\left(y_{gu}-\tilde{y}_{gu}+1\right)-tr\left(\mathbf{H}_{gu}\mathbf{W}\right)-tr\left(\mathbf{A}_{gu}\mathbf{F}\right)-1\right)+\ell_{su}\left(e^{z_{su}}-tr\left(\mathbf{A}_{e}\mathbf{F}\right)-tr\left(\mathbf{G}_{e}\mathbf{V}\right)-1\right)\\
&+\ell_{au}\left(e^{z_{au}}-tr\left(\mathbf{H}_{e}\mathbf{W}\right)-tr\left(\mathbf{G}_{e}\mathbf{V}\right)-1\right)+\ell_{gu}\left(e^{z_{gu}}-tr\left(\mathbf{H}_{e}\mathbf{W}\right)-tr\left(\mathbf{A}_{e}\mathbf{F}\right)-1\right)+\sigma_w\left(tr\left(\mathbf{W}\right)-P_S\right)\\
&-\mu\left(e^{\tilde{t}}\left(t-\tilde{t}+1\right)-tr\left(\mathbf{H}_{e}\mathbf{W}\right)-tr\left(\mathbf{A}_{e}\mathbf{F}\right)-tr\left(\mathbf{G}_{e}\mathbf{V}\right)-1\right)+\sigma_f\left(tr\left(\mathbf{F}\right)-P_U\right)+\sigma_v\left(tr\left(\mathbf{V}\right)-P_B\right).
\end{aligned}
\tag{57}
$$

Appendix B: Proof of Theorem 1

Proof. Based on (46a-46c), we can obtain the Lagrangian function of $\mathcal{P}4$ as shown in (57) at the top of this page.

By taking the partial derivative of the Lagrangian function in (57) with respect to $\mathbf{W}$, we have the following KKT conditions

$$
\begin{aligned}
\left(1+\sigma_w\right)\mathbf{I}-\tau_{su}\mathbf{H}_{su}-\left(\tau_{au}-\zeta_{au}\right)\mathbf{H}_{au}-\left(\tau_{gu}-\zeta_{gu}\right)\mathbf{H}_{gu}&\\
-\left(\ell_{au}+\ell_{gu}-\mu\right)\mathbf{H}_{e}-\mathbf{U}=\mathbf{0},&\quad(58)\\
\mathbf{UW}=\mathbf{0},&\quad(59)\\
\mathbf{W}\succeq\mathbf{0}.&\quad(60)
\end{aligned}
$$

Due to the channel matrix is figured out by a column vector multiplying by a row vector, the channel matrices in (58) hold rank-one. Therefore, denoting by

$$
\mathbf{A}=\left(1+\sigma_w\right)\mathbf{I}+\left(\zeta_{au}-\tau_{au}\right)\mathbf{H}_{au}+\left(\zeta_{gu}-\tau_{gu}\right)\mathbf{H}_{gu}+\mu\mathbf{H}_{e},\tag{61}
$$

the rank of $\mathbf{A}$ is satisfied with $N-2\leq rank\left(\mathbf{A}\right)\leq N$, since $\sigma_w,\zeta_{au},\tau_{au},\zeta_{gu},\tau_{gu},\mu\geq 0$. Then, by post-multiplying $\mathbf{W}$ at both sides of (58), it can be achieved as

$$
\mathbf{AW}=\left(\ell_{au}+\ell_{gu}\right)\mathbf{H}_{e}\mathbf{W}+\tau_{su}\mathbf{H}_{su}\mathbf{W},\tag{62}
$$

and the rank condition is

$$
\begin{aligned}
rank\left(\mathbf{AW}\right)&=rank\left(\left(\ell_{au}+\ell_{gu}\right)\mathbf{H}_{e}\mathbf{W}+\tau_{su}\mathbf{H}_{su}\mathbf{W}\right)&(63)\\
&\approx rank\left(\left(\ell_{au}+\ell_{gu}+\tau_{su}\right)\mathbf{H}_{su}\mathbf{W}\right)&(64)\\
&\leq rank\left(\mathbf{H}_{su}\right)=1.&(65)
\end{aligned}
$$

Keeping the following in mind,

$$
rank\left(\mathbf{AW}\right)\leq\min\left\{rank\left(\mathbf{A}\right),rank\left(\mathbf{W}\right)\right\},\tag{66}
$$

the $rank\left(\mathbf{W}\right)\leq 1$ can be obtained where the $rank\left(\mathbf{W}\right)=0$ could not be a solution obviously which is discarded. Thus the proof of $rank\left(\mathbf{W}\right)=1$ is completed.

In addition, the partial derivative of the Lagrangian function in (57) with respect to $\mathbf{F}$ can be calculated as

$$
\begin{aligned}
\left(1+\sigma_f\right)\mathbf{I}+\left(\zeta_{su}-\tau_{su}\right)\mathbf{A}_{su}+\left(\zeta_{gu}-\tau_{gu}\right)\mathbf{A}_{gu}-\tau_{au}\mathbf{A}_{au}&\\
-\left(\ell_{su}+\ell_{gu}-\mu\right)\mathbf{A}_{e}-\mathbf{L}=\mathbf{0},&\quad(67)\\
\mathbf{LF}=\mathbf{0},&\quad(68)\\
\mathbf{F}\succeq\mathbf{0}.&\quad(69)
\end{aligned}
$$

The partial derivative of the Lagrangian function in (57) with respect to $\mathbf{V}$ can be calculated as

$$
\begin{aligned}
\left(1+\sigma_v\right)\mathbf{I}+\left(\zeta_{su}-\tau_{su}\right)\mathbf{G}_{su}+\left(\zeta_{au}-\tau_{au}\right)\mathbf{G}_{au}-\tau_{gu}\mathbf{G}_{gu}&\\
+\mu\mathbf{G}_{e}-\left(\ell_{su}+\ell_{au}\right)\mathbf{G}_{e}-\mathbf{T}=\mathbf{0},&\quad(70)
\end{aligned}
$$

and $\mathbf{TV}=\mathbf{0}$, and $\mathbf{V}\succeq\mathbf{0}$. Based on the derivatives of Lagrangian function with respect to $\mathbf{F}$ and $\mathbf{V}$, the $rank\left(\mathbf{F}\right)=1$ and $rank\left(\mathbf{V}\right)=1$ can be proved similarly. Thus the proof is completed. ■

References

[1] N. Cheng, W. Quan, W. Shi, H. Wu, Q. Ye, H. Zhou, W. Zhuang, X. Shen, and B. Bai, "A comprehensive simulation platform for space-air-ground integrated network," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 178–185, 2020.

[2] F. Tang, H. Hofner, N. Kato, K. Kaneko, Y. Yamashita, and M. Hangai, "A deep reinforcement learning-based dynamic traffic offloading in space-air-ground integrated networks (SAGIN)," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 276–289, 2022.

[3] N. Cheng, J. He, Z. Y. Yin, C. Z. Zhou, H. W. Wu, F. Lyu, H. Zhou, and X. Shen, "6G service-oriented space-air-ground integrated network: A survey," *Chin. J. Aeronaut.*, vol. 35, no. 9, pp. 1–18, 2022.

[4] X. Fang, Z. Du, X. Yin, L. Liu, X. Sha, and H. Zhang, "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, 2022.

[5] F. Tang, C. Wen, M. Zhao, and N. Kato, "Machine learning for space–air–ground integrated network assisted vehicular network: A novel network architecture for vehicles," *IEEE Veh. Technol. Mag.*, vol. 17, no. 3, pp. 34–44, 2022.

[6] H. X. Nguyen, R. Trestian, D. To, and M. Tatipamula, "Digital twin for 5G and beyond," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 10–15, 2021.

[7] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: A survey," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13 789–13 804, 2021.

[8] W. Quan, M. Liu, N. Cheng, X. Zhang, D. Gao, and H. Zhang, "Cybertwin-driven drl-based adaptive transmission scheduling for software defined vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4607–4619, 2022.

[9] Q. Yu, J. Ren, Y. Fu, Y. Li, and W. Zhang, "Cybertwin: An origin of next generation network architecture," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 111–117, 2019.

[10] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Comput. Networks*, 2022, early access.

[11] M. G. Schraml, R. T. Schwarz, and A. Knopp, "Multiuser MIMO concept for physical layer security in multibeam satellite systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1670–1680, 2021.

[12] F. Tang, C. Wen, L. Luo, M. Zhao, and N. Kato, "Blockchain-based trusted traffic offloading in space-air-ground integrated networks (sagin): A federated reinforcement learning approach," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3501–3516, 2022.

[13] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Select. Areas Inform. Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[14] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted MIMOME system," *IEEE Trans. Wireless Commun.*, 2022, early access.

[15] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3480–3495, 2021.

[16] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1470–1482, 2017.

[17] Y. Chen, D. He, C. Ying, and Y. Luo, "Strong secrecy of arbitrarily varying wiretap channel with constraints," *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4700–4722, 2022.

[18] F. R. Ghadi and G. A. Hodtani, "Copula-based analysis of physical layer security performances over correlated rayleigh fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 431–440, 2020.

[19] X. Jiang, P. Li, Y. Zou, B. Li, and R. Wang, "Physical layer security for cognitive multiuser networks with hardware impairments and channel estimation errors," *IEEE Trans. Commun.*, pp. 1–1, 2022.

[20] J. Pfeiffer and R. F. Fischer, "Multilevel coding for physical-layer security," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1999–2009, 2022.

[21] Z. Yin, N. Cheng, T. H. Luan, Y. Hui, and W. Wang, "Green interference based symbiotic security in integrated satellite-terrestrial communications," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9962–9973, 2022.

[22] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Netw.*, vol. 36, no. 3, pp. 98–104, 2022.

[23] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning for digital twin edge networks in industrial iot," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5709–5718, 2020.

[24] H. Ahmadi, A. Nag, Z. Khar, K. Sayrafian, and S. Rahardja, "Networked twins and twins of networks: An overview on the relationship between digital twins and 6G," *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 154–160, 2021.

[25] Z. Yin, T. H. Luan, N. Cheng, Y. Hui, and W. Wang, "Cybertwin-enabled 6G space-air-ground integrated networks: Architecture, open issue, and challenges," *arXiv preprint arXiv:2204.12153*, 2022.

[26] K. Peng, H. Huang, M. Bilal, and X. Xu, "Distributed incentives for intelligent offloading and resource allocation in digital twin driven smart industry," *IEEE Trans. Ind. Informat.*, 2022, early access.

[27] P. Jia, X. Wang, and X. Shen, "Digital-twin-enabled intelligent distributed clock synchronization in industrial iot systems," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4548–4559, 2021.

[28] Z. Yin, M. Jia, W. Wang, N. Cheng, F. Lyu, Q. Guo, and X. Shen, "Secrecy rate analysis of satellite communications with frequency domain noma," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 11 847–11 858, 2019.

[29] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in uav systems: Challenges and opportunities," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 40–47, 2019.

[30] H.-M. Wang, X. Zhang, and J.-C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 32–39, 2019.

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

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

[33] 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, 2022.

[34] Y. Zhou, P. L. Yeoh, C. Pan, K. Wang, Z. Ma, B. Vucetic, and Y. Li, "Caching and UAV friendly jamming for secure communications with active eavesdropping attacks," *IEEE Trans. Veh. Technol.*, 2022, early access.

[35] P. K. Sharma and D. I. Kim, "Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2770–2784, 2020.

[36] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 251–255, 2021.

[37] K. Guo, K. An, F. Zhou, T. A. Tsiftsis, G. Zheng, and S. Chatzinotas, "On the secrecy performance of noma-based integrated satellite multiple-terrestrial relay networks with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3661–3676, 2021.

[38] S. Xu, J. Liu, Y. Cao, J. Li, and Y. Zhang, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 2007–2011, 2021.

[39] W. Cao, Y. Zou, Z. Yang, B. Li, Y. Lin, Y. Li, W. Wu, and L. Liu, "Secrecy outage analysis of relay-user pairing for secure hybrid satellite-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8906–8918, 2022.

[40] X. Li, Y. Fan, R. Yao, P. Wang, N. Qi, N. I. Miridakis, and T. A. Tsiftsis, "Rate-splitting multiple access-enabled security analysis in cognitive satellite terrestrial networks," *IEEE Trans. Veh. Technol.*, pp. 1–16, 2022.

[41] H. Li, S. Zhao, Y. Li, and C. Peng, "Sum secrecy rate maximization in noma-based cognitive satellite-terrestrial network," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2230–2234, 2021.

[42] P.-. Series, "Propagation model for IF77," *ITU-R Report*, pp. 1–72, 2020. [Online]. Available: http://www.itu.int/publ/R-REP/en

[43] P. S. Bithas, V. Nikolaidis, A. G. Kanatas, and G. K. Karagiannidis, "UAV-to-ground communications: Channel modeling and UAV selection," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5135–5144, 2020.

[44] A. M. Magableh, T. Aldalgamouni, O. Badarneh, S. Mumtaz, and S. Muhaidat, "Performance of non-orthogonal multiple access (noma) systems over n-nakagami-m multipath fading channels for 5G and beyond," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 11 615–11 623, 2022.

[45] H. Fu, S. Feng, W. Tang, and D. W. K. Ng, "Robust secure beamforming design for two-user downlink MISO rate-splitting systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 8351–8365, 2020.

[46] Z. Lin, K. An, H. Niu, Y. Hu, S. Chatzinotas, G. Zheng, and J. Wang, "SLNR-based secure energy efficient beamforming in multibeam satellite systems," *IEEE Trans. Aerosp. Electron. Syst.*, pp. 1–4, 2022.