Physical Layer Security in Cybertwin-Enabled Integrated Satellite-Terrestrial Vehicle Networks

Zhisheng Yin, *Member, IEEE*, Nan Cheng, *Member, IEEE*, Tom H. Luan, *Senior Member, IEEE*,
and Ping Wang, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the secure vehicle communications in cybertwin-enabled integrated satellite-terrestrial networks, where the digital twins (DTs) in the cybertwin space reflects the physical entities (i.e., satellite, terrestrial base station (BS), and vehicles). Particularly, considering the channel similarity between different satellite links versus the randomness difference in terrestrial links, it is challenging to reach the secure transmission in satellite and terrestrial links independently with limited resources. Considering the information exchange in the cybertwin space can support an information sharing between such physical entities, the secure transmission design by using the heterogeneous satellite-terrestrial resources can be conducted from a global perspective. With the channel feedback information of vehicles gathered at the cybertwin, the co-channel interference caused by the spectrum sharing is leveraged to assist the implementation of secure transmissions in the integrated satellite-terrestrial vehicle network. Specifically, the problems of maximizing the secrecy rate of satellite-to-vehicle link and the terrestrial BS-to-vehicle link are formulated, respectively. To solve such two problems, we propose two corresponding beamforming optimization approaches, where semi-definite relaxation (SDR) and semi-definite programming (SDP) are adopted due to the non-convexity. In addition, the tightness of SDR is proved and the complexity of proposed approaches is also analyzed. Finally, extensive numerical simulations are carried out and results show the effectiveness of our proposed approach.**

***Index Terms*—Integrated satellite-terrestrial networks, cybertwin, digital twin, secure transmission, beamforming.**

I. Introduction

SPACE-AIR-GROUND integrated network (SAGIN) expands the coverage range, increases the access capacity, and provides comprehensive and diverse services, which has been attracted great attention in 6G [1]–[3]. Recently, digital twins (DTs) as the precise virtual copy of a physical machine or system mirrors almost every facet of a product, process or service, which has been applied in the manufacture, aviation, transport, and healthcare etc., and is revolutionizing industry [4]. By digitally representing humans or things, the cybertwin-driven network architecture for 6 G is first proposed in [5], [6], where the cybertwin serves as a communications assistant, network behavior logger, and digital asset owner. With the cybertwin, the heterogeneous satellite-terrestrial resources could be orchestrated globally and uniformly. Particularly, the basic DT communication models are first presented in [7], including inter-twin and intra-twin communication models, and a case study of DT system for autonomous vehicles is conducted, which potentially directs the vehicle-to-everything (V2X) applications with high mobility in integrated satellite-terrestrial networks. Inspired by the previous works, we design the cybertwin-enabled integrated satellite-terrestrial vehicle networks shown in Fig. 1, where the cybertwin space consists of Sat-DT, BS-DT, and Veh-DT which virtually reflect the physical entities of integrated satellite-terrestrial networks.

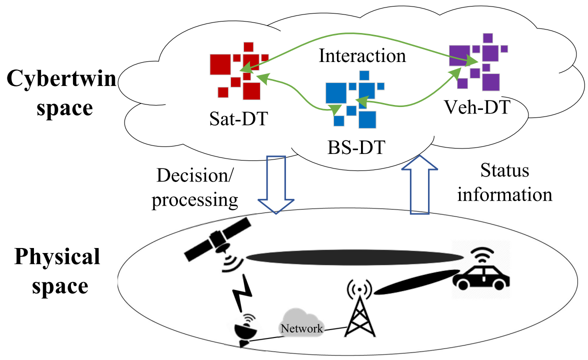

Fig. 1. Cybertwin-enabled integrated satellite-terrestrial networks.

Due to the spectrum scarcity of space information networks, Internet service providers (ISPs) have considered sharing the same frequency bands for many different kinds of communications [8]. By spectrum sharing, the spectrum utilization can be improved in the integrated satellite-terrestrial communications [9]. However, due to co-channel and the inherent broadcast nature of wireless mediums, satellite and terrestrial communication links are vulnerable to eavesdropping threats [10], [11]. In addition, malicious threats are easy to occur in heterogeneous vehicular networks [12].

Different from the traditional encryption algorithms in the upper layer, physical layer security can achieve secure transmissions based on the randomness difference of wireless channels,

Manuscript received July 22, 2021; revised October 17, 2021; accepted November 26, 2021. Date of publication December 9, 2021; date of current version May 20, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62071356, and in part by the Fundamental Research Funds for the Central Universities under Grant JB210113. The review of this article was coordinated by the Guest Editors of the Special Section on Cybertwin-Driven 6G for V2X Applications. *(Corresponding authors: Nan Cheng; Tom H. Luan.)*

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

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

Ping Wang is with the Department of Electrical Engineering and Computer Science, Lassonde School of Engineering, York University, Toronto, ON M3J 1P3, Canada (e-mail: pingw@yorku.ca).

Digital Object Identifier 10.1109/TVT.2021.3133574

which has been well studied in terrestrial 5 G networks [13]–[16]. Particularly, the physical layer security techniques can be roughly classified into three categories according to where they are implemented in the transmission chain, i.e., at channel, signal, or coding level [17]. Compared with terrestrial communications, limited resources can be exploited to assist physical layer security in satellite-terrestrial communications, such as power, multi-antenna, and the computation resource, etc. Furthermore, the main and wiretap channels are similar with weak randomness difference when the distance difference from satellite to legitimate user and eavesdropper (Eve) can be negligible [18]. All these pose a great challenge to implement the physical layer security in satellite-terrestrial communications.

To overcome these challenges, several related works have explored to use the green interference generated by cooperative users or terrestrial base stations (BSs) to enhance the difference between the main and wiretap channels [18]–[20]. Without the assistance of terrestrial resources, the inter-user interference serves as the green interference to increase the difference of similar satellite channels [18]. However, only the secure transmission of satellite link is considered. For the coexisting satellite and terrestrial networks, the BS serves as a green interference resource, which is designed for unequally damaging the main and wiretap channels through optimizing the beamforming (BF) at the BS [19], and jointly optimizing the BF vector of the BS and satellite [20]. However, only the secure transmission of satellite link is considered and the BS makes some sacrifices. Besides, it is challenging to integrating heterogeneous resources to conduct a joint optimization with global information. The green interference introduced in the previous exploration works shows potential benefit for secure transmissions, which motivates us to investigate the use of green interference for guaranteeing the secrecy in both satellite-to-vehicle and terrestrial BS-to-vehicle links in integrated satellite-terrestrial networks.

In this paper, we consider a cybertwin-enabled secure transmissions for vehicles in integrated satellite-terrestrial networks, where the legitimate vehicle users connected to satellite (SU) and to terrestrial BS (GU) coexist within the common coverage of satellite and terrestrial networks. Particularly, a passive Eve is considered to wiretap such two vehicles, i.e., SU and GU, simultaneously. Considering the channel similarity from satellite to SU and Eve, the inherent co-channel interference caused by spectrum sharing, serving as the green interference, is leveraged to assist the implementation of physical layer security for both satellite and terrestrial links. Our main contributions can be summarized as follows.

- We propose a framework of cybertwin-enabled physical layer security in the integrated satellite-terrestrial vehicle communications. The cybertwin enables a global information sharing and directs a heterogeneous collaboration between satellite and terrestrial networks. Particularly, the secrecy requirements of vehicles associated with satellite and BS are gathered and managed at the cybertwin, where the terrestrial BS has access to global information through the cybertwin to carry out a BF design.
- To maximize the secrecy rate of the satellite-to-vehicle link, the interference from terrestrial BS serves as the green interference to damage the wiretap channel of SU and the BF vector at BS is optimized with the perfect and imperfect channel state information (CSI) of Eve. Particularly, the predefined secrecy rate of the terrestrial BS-to-vehicle link is simultaneously guaranteed. To solve this non-convex optimization problem, we first convert it into a bi-convex problem by introducing an auxiliary variable, and then propose an iterative BF optimization approach to optimize the BF at the terrestrial BS. In addition, the semi-definite relaxation (SDR) is adopted to relax the rank-one constraint of BF and the tightness of this relaxation is proved. The complexity of this proposed BF approach is also analyzed.
- To maximize the secrecy rate of the terrestrial BS-to-vehicle link, the interference from satellite serves as the green interference to damage the wiretap channel of GU and the main channel of GU is enhanced by the BF optimization at BS. Besides, the secrecy rate constraint of SU is taken into consideration. Similarly, SDR is adopted to relax the rank-one constraint of BF matrix and an iterative alternating BF optimization approach is proposed to obtain the solution. Specifically, an one-dimension search is first adopted and an alternating semi-definite programming (SDP) and single variable optimization is executed in each search. In addition, the tightness of relaxation is proved and the complexity of our proposed BF approach is analyzed and extensive simulations are carried out to verify the effectiveness of our proposed approach.

The remainder of this paper is organized as follows. Related works are summarized in Section II. In Section III, the system model of cybertwin-enabled secure transmissions for vehicles in the integrated satellite-terrestrial networks is illustrated. In Section IV, we formulate an optimization problem to maximize secrecy rate for the vehicle associated with satellite network. An iterative BF optimization approach is proposed to solve this problem, and some reformulations are presented to simplify the primal problem. In Section V, a problem to maximize the secrecy rate for vehicle associated with terrestrial network is formulated, where some reformulations are presented to convert this intractable problem to a bi-convex problem and an iterative alternating BF optimization approach is proposed to solve it. In Section VI, extensive simulations are carried out to evaluate the secrecy rate performance of both satellite-to-vehicle and terrestrial BS-to-vehicle links. Finally, we conclude this paper and direct our future work in Section VII.

II. Related Works

A comprehensive survey of DT networks is presented in [21], where it points out that the DT introduces innovative transport services such as traffic information reporting, vehicles secure access and data sharing, which shows potential applications of DT in intelligent transportation. The mathematical model of service delay for a cybertwin based multi-access edge computing system is proposed in [22]. To against cyber attackers, an Internet-of-things (IoT) based DT of cyber-physical system for the resilience of interconnected microgrids is designed in [23]. With the DTs of edge servers and mobile edge computing (MEC), a mobile offloading scheme is proposed to minimize the offloading latency [24], where the user mobility and

TABLE I
SUMMARY OF NOTATIONS AND DEFINITIONS

Notation	Definition
N	number of BS transmit antennas
$h_{su} \in \mathbb{C}^{N\times 1}$	channel vector from satellite to SU
$h_{gu} \in \mathbb{C}^{N\times 1}$	channel vector from satellite to GU
$h_{e} \in \mathbb{C}^{N\times 1}$	channel vector from satellite to Eve
$\mathbf{g}_{su} \in \mathbb{C}^{M\times 1}$	channel vector from BS to SU
$\mathbf{g}_{gu} \in \mathbb{C}^{M\times 1}$	channel vector from BS to GU
$\mathbf{g}_{e} \in \mathbb{C}^{M\times 1}$	channel vector from BS to Eve
$\mathbf{w} \in \mathbb{C}^{N\times 1}$	BF vector of BS
$\mathcal{R}_s$	predefined secrecy rate constraint of GU
$\mathcal{R}_s^{'}$	predefined secrecy rate constraint of SU
ε	the norm-bounded channel estimate error

unpredictable MEC environment are considered. Considering an aerial-assisted Internet of vehicles (IoV), the DT-driven resource allocation is proposed to maximize the satisfaction of vehicles and improve the energy efficiency [25]. A multisource model driven DT system based on the geometric, physics, and sequential rule description is demonstrated in [26]. The DT and edge networks are integrated and the DT empowered reinforcement learning scheme is proposed to allocate spectrum resources in resource-limited IoT networks [27]. Particularly, the DT reflection model and its corresponding security architecture is investigated and the DT-driven security requirements for DT are designed based on the data sharing and control [28].

Recently, the investigations of physical layer security have shown growing interests in satellite-terrestrial networks. To improve the secrecy rate of satellite downlink communications, the inter-user interference caused by frequency domain non-orthogonal multiple access (FD-NOMA) is leveraged to degrade the Eve [18], and a multi-user cooperation scheme is proposed to enhance the main channel of legitimate satellite users. An intelligent reflecting surface (IRS) is deployed to reflect the green interference from the terrestrial network to secure the satellite communication [29]. An unmanned aerial vehicle (UAV) assisted physical layer security in multi-beam satellite-enabled vehicle communications is investigated in [30]. However, the DT has not been investigated with respect to physical layer security and only the single-link secure transmission is addressed in the integrated satellite-terrestrial networks.

Notations: $(\cdot)^H$ denote the Hermitian transpose, respectively. $|\cdot|$ and $\|\cdot\|$ stand for the absolute value and Euclidean norm of a vector. $\mathrm{Tr}(\cdot)$ and $rank(\cdot)$ denote the trace and rank of a matrix, respectively. $\mathbb{C}^{N\times M}$ denotes a complex space of $N \times M$. $\mathcal{N}(\mu, \delta^2)$ denotes the normal distribution with mean μ and variance δ^2. Other notations are defined in Table I.

III. System Model

We design a cybertwin model for the integrated satellite-terrestrial networks as shown in Fig. 1, where the cybertwin space consists of Sat-DT, BS-DT, and Veh-DT which virtually reflect physical entities of the integrated satellite-terrestrial networks. The DTs are deployed at the same network connected to Internet and they can exchange with each other in the cybertwin. To enable an integrated framework of satellite and terrestrial networks, we deploy the Sat-DT in the gateway and it can interact with the BS-DT and the Veh-DT in the edge network. Particularly, the Sat-DT and the BS-DT represent DTs of satellite and terrestrial BS, respectively, which manages the heterogeneous resources of radio access networks. The Veh-DT represents the DT of a vehicle, which is the agent of the vehicle in cybertwin space, and it supervises and records the activity information of the vehicle and facilitates the decision-making for the vehicle. In this work, focusing on the physical layer security, we simplify the system model as shown in Fig. 2, where the interactions between DTs are implemented in the cybertwin. Particularly, the satellite transmit power, the secrecy requirements of vehicles respectively associated with satellite and BS, and the CSI from satellite to vehicles are required by the BS to execute the beamforming for implement the secure vehicle communications. Thus, by the interactions between DTs in the cybertwin space, the BS is assumed to have such information of satellite and vehicles.

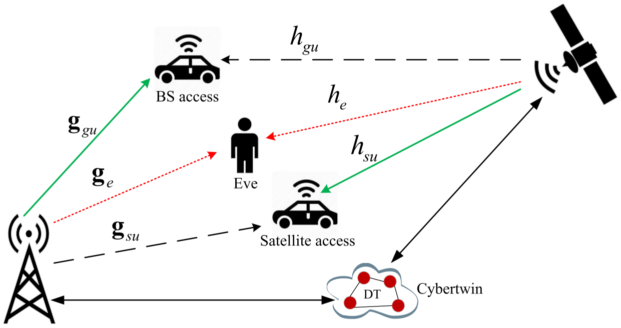

Fig. 2. Secure vehicle communications in cybertwin-enabled integrated satellite-terrestrial networks.

Particularly, we consider secure vehicle communications in a cybertwin-enabled integrated satellite-terrestrial network shown in Fig. 2, where the downlink spectrum is shared between satellite and terrestrial networks. Vehicles in the common coverage of satellite and terrestrial BS can alternatively access to satellite and the terrestrial BS. To enable secure vehicle communications in the integrated satellite-terrestrial network, we consider a framework of wiretapping scenario as shown in Fig. 2. Specifically, two legitimate vehicles with different access selections (alternative satellite and BS) are considered under the common coverage of satellite and BS, and they can receive signals from satellite and BS simultaneously by spectrum sharing. Particularly, we assume that a passive Eve exists in the common coverage and has the potential to wiretap vehicles due to the common-channel with the vehicles. In addition, we assume that satellite and terrestrial BS can be connected to Internet and there is an integrated control and management center in the cybertwin.

A. Channel Models

According to the ITU-R P.618 [31], the free space path loss (FSPL), rain attenuation, and satellite beam gain are considered to construct the satellite channel model, which is given by

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

where C_L denotes the FSPL, b denotes the beam gain, β denotes the channel gain due to rain attenuation, and θ is the phase variable with uniform distribution over $[0, 2\pi)$. Specifically,

$$C_L = \left(\lambda/4\pi\right)^2 / \left(d^2 + h^2\right), \tag{2}$$

where λ denotes signal wavelength, d denotes the distance from the beam center to the center of satellite coverage, and h accounts for the height of satellite [19], [20]. The beam gain is defined by [20]

$$b = G\left(\frac{J_1\left(u_0\right)}{2u_0} - 36\frac{J_3\left(u_0\right)}{u_0^2}\right)^2, \tag{3}$$

where G denotes the maximum satellite antenna gain, $u_0 = 2.07123\frac{\sin(\alpha)}{\sin(\alpha_{3\text{dB}})}$ with α being the elevation angle between the beam center and SU and $\alpha_{3\text{dB}}$ being the 3 dB angle of satellite beam. Additionally, $J_1(\cdot)$ and $J_3(\cdot)$ are the first-kind Bessel functions of order 1 and 3, respectively. β is modeled as a log-normal random variable, i.e., $\beta_{dB} \sim \mathcal{N}(u, \delta^2)$ with β_{dB} being the dB form of β [20]. Particularly, h_{su}, h_{gu}, and h_e denote the channel coefficients from satellite to SU, 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. Additionally, $\mathbf{g}_0$ denotes the small-scale fading which undergoes Nakagami-m fading with fading severity m and average power Ω. Particularly, $\mathbf{g}_{su} \in \mathbb{C}^{N\times 1}$, $\mathbf{g}_{gu} \in \mathbb{C}^{N\times 1}$, and $\mathbf{g}_e \in \mathbb{C}^{N\times 1}$ denote the channel vectors between BS and SU, GU, and Eve, respectively.

Similar to related works [19], the CSI of Eve is assumed to be imperfect in this work, i.e., $h_e = \hat{h}_e + \Delta h_e$ and $\mathbf{g}_e = \hat{\mathbf{g}}_e + \Delta\mathbf{g}_e$, where $\hat{h}_e$ and $\hat{\mathbf{g}}_e$ denote the channel estimate of Eve which are known at BS, Δh_e and $\Delta\mathbf{g}_e$ correspond to the norm-bounded estimate errors. To facilitate the analysis, we assume $\|\Delta h_e\| = \|\Delta\mathbf{g}_e\| \leq \varepsilon$ in this work.

B. Signal Models

Denoting the transmission signals of satellite and BS by x_{su} and x_{gu}, respectively, the signal received by SU and GU can be respectively expressed as

$$y_{su} = h_{su}\sqrt{P_S}x_{su} + \mathbf{g}_{su}^H\mathbf{w}x_{gu} + n_{su}, \tag{4}$$

$$y_{gu} = \mathbf{g}_{gu}^H\mathbf{w}x_{gu} + h_{gu}\sqrt{P_S}x_{su} + n_{gu}, \tag{5}$$

where P_S denotes the satellite transmit power, $\mathbf{w} \in \mathbb{C}^{N\times 1}$ is the BF of BS, and n_{su} and n_{gu} denote the noise received by SU and GU, respectively. The received signal at Eve is given by

$$y_e = h_e\sqrt{P_S}x_{su} + \mathbf{g}_e^H\mathbf{w}x_{gu} + n_e, \tag{6}$$

where n_e denotes the noise received at Eve. Based on (4) and (5), the received SINR of SU and GU can be obtained as

$$\gamma_{su} = \frac{P_S|h_{su}|^2}{\|\mathbf{g}_{su}^H\mathbf{w}\|^2 + \delta_{su}^2}, \tag{7}$$

$$\gamma_{gu} = \frac{\|\mathbf{g}_{gu}^H\mathbf{w}\|^2}{P_S|h_{gu}|^2 + \delta_{gu}^2}. \tag{8}$$

From (6), the received SINR to wiretap SU is expressed as

$$\gamma_{se} = \frac{P_S|h_e|^2}{\|\mathbf{g}_e^H\mathbf{w}\|^2 + \delta_e^2}, \tag{9}$$

and the SINR of Eve to wiretap GU can be written as

$$\gamma_{ge} = \frac{\|\mathbf{g}_e^H\mathbf{w}\|^2}{P_S|h_e|^2 + \delta_e^2}. \tag{10}$$

Based on the definition of secrecy rate [32], [33], and using (7)–(10), the secrecy rate of SU and GU can be respectively given by

$$R_s^{S2V} = \left[\log_2\left(1 + \gamma_{su}\right) - \log_2\left(1 + \gamma_{se}\right)\right]^+, \tag{11}$$

$$R_s^{B2V} = \left[\log_2\left(1 + \gamma_{gu}\right) - \log_2\left(1 + \gamma_{ge}\right)\right]^+. \tag{12}$$

To facilitate the analysis, we assume that the noise power is normalized, i.e., $\delta_{su}^2 = \delta_{gu}^2 = \delta_e^2 = 1$. Substituting (7) and (9) into (11) and meanwhile substituting (8) and (10) into (12), the secrecy rate R_s^{S2V} and R_s^{B2V} can be further expressed as shown in (13) and (14) at the bottom of the next page, respectively.

IV. Maximizing Secrecy Rate for the Vehicle Associated With Satellite Network

To maximize the secrecy rate of SU and guarantee a secrecy rate constraint ($\mathcal{R}_s$) of GU, the formulated problem can be written as

$$\mathcal{P}1: \quad \max_{\mathbf{w}} \quad R_s^{S2V} \tag{15a}$$

$$\text{s.t.:} \quad R_s^{B2V} \geq \mathcal{R}_s, \tag{15b}$$

$$\|\mathbf{w}\|^2 \leq P_B, \tag{15c}$$

where (15b) assures a predefined secrecy rate of the terrestrial BS-to-vehicle link, (15c) constraints the maximum transmit power (P_B) of the terrestrial BS, and the optimization variable $\mathbf{w}$ is solved in the cybertwin space and which is carried out at the terrestrial BS. From (15), it is observed that the objective function is non-convex due to its form of logarithmic subtraction. Besides, we can see a constraint condition of another secrecy rate (logarithmic subtraction) included, where its non-linearity and non-convexity increases the challenge of the problem maximizing the secrecy rate to find solutions.

By introducing an auxiliary variable ξ and using (11)–(12), the problem $\mathcal{P}1$ can be rewritten as

$$\mathcal{P}2: \quad \max_{\mathbf{w},\xi} \quad \log_2\left(1 + \gamma_{su}\right) - \log_2\left(\xi^{-1}\right) \tag{16a}$$

$$\text{s.t.:} \quad \log_2\left(1 + \gamma_{se}\right) \leq \log_2\left(\xi^{-1}\right), \tag{16b}$$

$$\log_2\left(1+\gamma_{gu}\right) - \log_2\left(1+\gamma_{ge}\right) \ge \mathcal{R}_s, \tag{16c}$$

$$\|\mathbf{w}\|^2 \le P_B. \tag{16d}$$

Substituting (7)–(10) into problem $\mathcal{P}2$, it can be equivalently reformulated as

$$\mathcal{P}3: \max_{\mathbf{w},\xi} \quad \xi + \xi\frac{P_S|h_{su}|^2}{\mathbf{w}^H\mathbf{g}_{su}\mathbf{g}_{su}^H\mathbf{w}+1} \tag{17a}$$

$$\text{s.t.:} \quad \left(1-\xi^{-1}\right)\left(\mathbf{w}^H\left(\hat{\mathbf{g}}_e\hat{\mathbf{g}}_e^H+\varepsilon\right)\mathbf{w}\right) \le \xi^{-1}-1 - P_S(|\hat{h}_e|^2+\varepsilon), \tag{17b}$$

$$\frac{\mathbf{w}^H\mathbf{g}_{gu}\mathbf{g}_{gu}^H\mathbf{w}}{P_S|h_{gu}|^2+1} - 2^{\mathcal{R}_s}\frac{\mathbf{w}^H\left(\hat{\mathbf{g}}_e\hat{\mathbf{g}}_e^H+\varepsilon\right)\mathbf{w}}{P_S(|\hat{h}_e|^2+\varepsilon)+1} \ge 2^{\mathcal{R}_s}-1, \tag{17c}$$

$$\|\mathbf{w}\|^2 \le P_B. \tag{17d}$$

It is observed that $\mathcal{P}_3$ is nonconvex, due to the fractional polynomial in the objective function. By replacing the optimizing variable with $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ and adopting SDR to ignore the rank-one constraint of $\mathbf{W}$, the problem $\mathcal{P}3$ can be reformulated as

$$\mathcal{P}4: \max_{\mathbf{W},\xi} \quad \xi\left(1+\frac{P_S|h_{su}|^2}{\mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}\right)+1}\right) \tag{18a}$$

$$\text{s.t.:} \left(1-\xi^{-1}\right)\mathrm{Tr}\left(\left(\mathbf{G}_e+\varepsilon\right)\mathbf{W}\right) \le \xi^{-1}-1-P_S(|\hat{h}_e|^2+\varepsilon), \tag{18b}$$

$$\mathrm{Tr}((\frac{\mathbf{G}_{gu}}{P_S|h_{gu}|^2+1} - \frac{2^{\mathcal{R}_s}(\mathbf{G}_e+\varepsilon)}{P_S(|\hat{h}_e|^2+\varepsilon)+1})\mathbf{W}) \ge 2^{\mathcal{R}_s}-1, \tag{18c}$$

$$\mathrm{Tr}\left(\mathbf{W}\right) \le P_B, \tag{18d}$$

$$\mathbf{W} \succeq \mathbf{0}, \tag{18e}$$

where $\mathbf{G}_{gu} = \mathbf{g}_{gu}\mathbf{g}_{gu}^H$ and $\mathbf{G}_e = \hat{\mathbf{g}}_e\hat{\mathbf{g}}_e^H$. We can see that $\mathcal{P}_4$ is a bi-convex problem. To solve $\mathcal{P}_4$, we propose an approach that iteratively and alternately optimizes ξ and $\mathbf{w}$. Particularly, we reformulate $\mathcal{P}_4$ as two subproblems to optimize $\mathbf{w}$ and ξ, respectively.

When ξ is fixed, the maximizing problem in (18a) can be equivalently transformed into minimizing $\mathrm{Tr}(\mathbf{G}_{su}\mathbf{W})$. Thus, a subproblem to optimize $\mathbf{W}$ can be formulated as

$$\mathcal{P}4 - A: \min_{\mathbf{W}} \quad \mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}\right) \tag{19a}$$

$$\text{s.t.:} \quad (18b) - (18e). \tag{19b}$$

It is observed that the problem $\mathcal{P}4 - A$ is convex which can be solved by semi-definite programing (SDP). Since the rank-one constraint of $\mathbf{W}$ is relaxed by adopting SDR from $\mathcal{P}3$ to $\mathcal{P}4$, the following Theorem is given to prove the tightness of rank-one relaxation.

Theorem 1: For any feasible ξ, the solution of $\mathbf{W}$ is rank-one.

Proof: Please see Appendix A. ■

After obtaining a feasible $\mathbf{W}^\circ$ by solving $\mathcal{P}4 - A$, the objective function in (18a) can be reduced to maximizing ξ, where the constant satisfies

$$1+\frac{P_S|h_{su}|^2}{\mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}^\circ\right)+1} > 0. \tag{20}$$

Thus, the subproblem to optimize ξ can be equivalently formulated as

$$\mathcal{P}4 - B: \max_{\xi} \quad \xi \tag{21a}$$

$$\text{s.t.:} \left(1-\xi^{-1}\right)\mathrm{Tr}\left(\left(\mathbf{G}_e+\varepsilon\right)\mathbf{W}^\circ\right) \le \xi^{-1}-1-P_S(|\hat{h}_e|^2+\varepsilon), \tag{21b}$$

$$\xi_{min} \le \xi \le \xi_{max}, \tag{21c}$$

where ξ_{min} and ξ_{max} are determined by the following Lemma.

$$\begin{aligned} R_s^{S2V} &= \log_2\left(1+\frac{P_S|h_{su}|^2}{\|\mathbf{g}_{su}^H\mathbf{w}\|^2+\delta_{su}^2}\right) - \log_2\left(1+\frac{P_S|h_e|^2}{\|\mathbf{g}_e^H\mathbf{w}\|^2+\delta_e^2}\right) \\ &= \log_2\left(\frac{P_S|h_{su}|^2+\left\|\mathbf{g}_{su}^H\mathbf{w}\right\|^2+1}{\|\mathbf{g}_{su}^H\mathbf{w}\|^2+1}\right) - \log_2\left(\frac{P_S|h_e|^2+\left\|\mathbf{g}_e^H\mathbf{w}\right\|^2+1}{\|\mathbf{g}_e^H\mathbf{w}\|^2+1}\right) \\ &= \log_2\left(\frac{P_S|h_{su}|^2+\mathbf{w}^H\mathbf{g}_{su}\mathbf{g}_{su}^H\mathbf{w}+1}{\mathbf{w}^H\mathbf{g}_{su}\mathbf{g}_{su}^H\mathbf{w}+1}\right) - \log_2\left(\frac{P_S|h_e|^2+\mathbf{w}^H\mathbf{g}_e\mathbf{g}_e^H\mathbf{w}+1}{\mathbf{w}^H\mathbf{g}_e\mathbf{g}_e^H\mathbf{w}+1}\right). \end{aligned} \tag{13}$$

$$\begin{aligned} R_s^{B2V} &= \log_2\left(1+\frac{\left\|\mathbf{g}_{gu}^H\mathbf{w}\right\|^2}{P_S|h_{gu}|^2+1}\right) - \log_2\left(1+\frac{\left\|\mathbf{g}_e^H\mathbf{w}\right\|^2}{P_S|h_e|^2+1}\right) \\ &= \log_2\left(1+\frac{\mathbf{w}^H\mathbf{g}_{gu}\mathbf{g}_{gu}^H\mathbf{w}}{P_S|h_{gu}|^2+1}\right) - \log_2\left(1+\frac{\mathbf{w}^H\mathbf{g}_e\mathbf{g}_e^H\mathbf{w}}{P_S|h_e|^2+1}\right) \\ &= \log_2\left(\frac{1+P_S|h_{gu}|^2+\mathbf{w}^H\mathbf{g}_{gu}\mathbf{g}_{gu}^H\mathbf{w}}{P_S|h_{gu}|^2+1}\right) - \log_2\left(\frac{1+P_S|h_e|^2+\mathbf{w}^H\mathbf{g}_e\mathbf{g}_e^H\mathbf{w}}{P_S|h_e|^2+1}\right). \end{aligned} \tag{14}$$

Algorithm 1: Iterative BF Optimization Approach.

```
   Input: $P_S, P_B, \mathcal{R}_s, h_{su}, h_{gu}, \hat{h}_e, \mathbf{g}_{su}, \mathbf{g}_{gu}, \hat{\mathbf{g}}_e$.
   Result: $\mathbf{W}^\star$.
1  Initialization: $\xi_0$ $(0 \le \xi_0 \le 1)$.
2  Set $n = 1$.
3  repeat
4      Execute SDP by CVX tool to solve $\mathcal{P}4 - A$;
       Output: $\mathbf{W}_n^\circ$.
5      Calculate the secrecy rate:
         $R_s^{A(n)} = \log_2 \left( \xi_n^\circ + \frac{\xi_n^\circ P_S |h_{su}|^2}{\mathrm{Tr}(\mathbf{G}_{su}\mathbf{W}_n^\circ)+1} \right)$;
6      Obtain $\xi_{n+1}^\circ$ according to (24);
7      Calculate the secrecy rate:
         $R_s^{B(n)} = \log_2 \left( \xi_{n+1}^\circ + \frac{\xi_{n+1}^\circ P_S |h_{su}|^2}{\mathrm{Tr}(\mathbf{G}_{su}\mathbf{W}_n^\circ)+1} \right)$;
8      Return $\xi_{n+1}^\circ$ to step 4;
9  until $\left| R_s^{B(n+1)} - R_s^{A(n)} \right| \le \epsilon$;
10 Obtain the optimal $\mathbf{w}_n^\star$ by the singular value
     decomposition (SVD) of the optimal $\mathbf{W}^\star$.
11 Procedure End
```

Lemma 1: Given P_S, the value range of ξ is determined by

$$\frac{1}{1 + P_S |h_{su}|^2} \le \xi \le 1. \tag{22}$$

Proof: Since the positive secrecy rate is required, the objective function in (16a) indicates $1 + \gamma_{su} \ge \xi^{-1}$. Substituting (7) into (22), we have

$$\xi \ge \frac{1}{1 + \frac{P_S |h_{su}|^2}{\|\mathbf{g}_{su}^H \mathbf{w}\|^2 + 1}} \ge \frac{1}{1 + P_S |h_{su}|^2}. \tag{23}$$

From (16b), it indicates that $0 \le \xi \le 1$. Thus, (22) is obtained and the proof is completed. ■

Using (21b) and Lemma 1, the optimal solution of $\mathcal{P}4 - B$ can be obtained as

$$\xi^\circ = \frac{1 + \mathrm{Tr}\left(\mathbf{G}_e \mathbf{W}^\circ\right)}{1 + \mathrm{Tr}\left(\mathbf{G}_e \mathbf{W}^\circ\right) + P_S |\hat{h}_e|^2}. \tag{24}$$

Based on the solutions of $\mathcal{P}4 - A$ and $\mathcal{P}4 - B$, the bi-convex problem $\mathcal{P}4$ can be solved by the iterative alternating approach. Specifically, given an initialized ξ_0 at the beginning of procedure, a feasible $\mathbf{W}^\circ$ can be found by adopting SDP to solve $\mathcal{P}4 - A$. Based on $\mathbf{W}^\circ$, the optimal ξ° can be obtained by using (24). Returning ξ° to $\mathcal{P}4 - A$, the next iteration is started. Additionally, a convergence tolerance ϵ is predefined to terminate the procedure. Particularly, the rank-one of $\mathbf{W}$ has been proved, which guarantees the solution of $\mathcal{P}4$ is optimal for the primal $\mathcal{P}3$. Finally, the details of the proposed iterative BF optimization approach is given in Algorithm 1.

Computational complexity: The main complexity of Algorithm 1 can be calculated by the iteration number multiplying the complexity in each iteration. For each iteration, the SDP for solving $\mathcal{P}4 - A$ 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, the complexity of solving $\mathcal{P}4 - A$ in each iteration is $\mathcal{O}(N^4)$. For solving $\mathcal{P}4 - B$, the complexity can be calculated based on (24) which is $\mathcal{O}(N^3)$. Thus, the total complexity can be calculated as $log(1/\epsilon)(\mathcal{O}(N^4) + \mathcal{O}(N^3))$.

V. Maximizing Secrecy Rate for the Vehicle Associated With Terrestrial Network

For the vehicle associated with the terrestrial network, we formulate a problem to maximize the secrecy rate of the vehicle as follows.

$$\mathcal{P}5: \quad \max_{\mathbf{w}} \quad R_s^{B2V} \tag{25a}$$

$$\text{s.t.:} \quad R_s^{S2V} \ge \mathcal{R}_s', \tag{25b}$$

$$\|\mathbf{w}\|^2 \le P_B, \tag{25c}$$

where a predefined secrecy rate of the vehicle connected to satellite is guaranteed and the BS transmit power is also constrained. However, it is observed that $P5$ is non-convex and intractable to be solved.

Similarly, we introduce another auxiliary variable φ for facilitating the reformulation of the objective function in (25a), which holds the following constraint

$$\log_2 \left(\frac{1 + P_S \left(|\hat{h}_e|^2 + \varepsilon \right) + \mathbf{w}^H \left(\hat{\mathbf{g}}_e \hat{\mathbf{g}}_e^H + \varepsilon \right) \mathbf{w}}{P_S \left(|\hat{h}_e|^2 + \varepsilon \right) + 1} \right) \le \log_2 \left(\varphi^{-1} \right). \tag{26}$$

Particularly, according to the monotonicity of $\log_2(\cdot)$, the constraint in (26) can be represented as

$$\varphi \left(1 + P_S \left(|\hat{h}_e|^2 + \varepsilon \right) + \mathbf{w}^H \left(\mathbf{g}_e \mathbf{g}_e^H + \varepsilon \right) \mathbf{w} \right) \le P_S \left(|\hat{h}_e|^2 + \varepsilon \right) + 1. \tag{27}$$

In addition, (25b) can be represented as

$$\frac{P_S |h_{su}|^2}{\mathbf{w}^H \mathbf{g}_{su} \mathbf{g}_{su}^H \mathbf{w} + 1} \ge 2^{\mathcal{R}_s'} \frac{P_S \left(|\hat{h}_e|^2 + \varepsilon \right)}{\mathbf{w}^H \left(\hat{\mathbf{g}}_e \hat{\mathbf{g}}_e^H + \varepsilon \right) \mathbf{w} + 1} + 2^{\mathcal{R}_s'} - 1. \tag{28}$$

To address the fractional polynomial in (28), we make the following replacement

$$\eta = \frac{1}{\mathbf{w}^H \left(\hat{\mathbf{g}}_e \hat{\mathbf{g}}_e^H + \varepsilon \right) \mathbf{w} + 1}. \tag{29}$$

Thus, (28) can be further simplified as

$$\left(2^{\mathcal{R}_s'} \eta \left(P_S \left(|\hat{h}_e|^2 + \varepsilon \right) \right) + 2^{\mathcal{R}_s'} - 1 \right) \left(\mathbf{w}^H \mathbf{g}_{su} \mathbf{g}_{su}^H \mathbf{w} + 1 \right) \le P_S |h_{su}|^2. \tag{30}$$

Finally, $P5$ can be equivalently reformulated as

$$\mathcal{P}6: \quad \max_{\mathbf{w}, \varphi} \quad \varphi + \varphi \frac{\mathbf{w}^H \mathbf{g}_{gu} \mathbf{g}_{gu}^H \mathbf{w}}{P_S |h_{gu}|^2 + 1}, \tag{31a}$$

$$\text{s.t.:} \quad (27), (30), (25c). \tag{31b}$$

Nevertheless, it can be seen that $\mathcal{P}6$ is still non-convex due to the fractional polynomial in the objective function and constraints. By replacing the optimizing variables with $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, $\mathbf{G}_{gu} = \mathbf{g}_{gu}\mathbf{g}_{gu}^H$, and $\mathbf{G}_e = \hat{\mathbf{g}}_e\hat{\mathbf{g}}_e^H$, and adopting SDR to ignore the rank-one constraint of $\mathbf{W}$, the problem $\mathcal{P}6$ can be represented as

$$\mathcal{P}7: \max_{\mathbf{W},\varphi,\eta} \quad \varphi\left(1 + \frac{\mathrm{Tr}\left(\mathbf{G}_{gu}\mathbf{W}\right)}{P_S|h_{gu}|^2 + 1}\right), \tag{32a}$$

$$\text{s.t.:} \quad \varphi\left(1 + P_S\left(\left|\hat{h}_e\right|^2 + \varepsilon\right) + \mathrm{Tr}\left(\mathbf{G}_e\mathbf{W}\right) + \mathrm{Tr}\left(\varepsilon\mathbf{W}\right)\right) \le P_S\left(\left|\hat{h}_e\right|^2 + \varepsilon\right) + 1. \tag{32b}$$

$$\left(2^{\mathcal{R}'_s}\eta P_S|h_e|^2 + 2^{\mathcal{R}'_s} - 1\right)\left(\mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}\right) + 1\right) \le P_S|h_{su}|^2, \tag{32c}$$

$$\mathrm{Tr}\left(\mathbf{W}\right) \le P_B, \tag{32d}$$

$$\mathbf{W} \succeq \mathbf{0}. \tag{32e}$$

It can be seen that $\mathcal{P}7$ is a bi-convex problem. To solve $\mathcal{P}7$, we propose an iterative alternating BF optimization approach demonstrated in Algorithm 2. Specifically, the algorithm 2 consists of an inner and outer stages. In the outer stage, a one-dimension search is adopted to find the solution of η. Within each search in the inner stage, we first fix the optimization variable φ, then an SDP is executed to obtain a feasible $\mathbf{W}_n^\circ$. In addition, the tightness of rank-one relaxation is proved through the following Theorem.

Theorem 2: For any feasible ϕ and η, the solution of $\mathbf{W}$ in $\mathcal{P}7$ is rank-one.

Proof: Please see Appendix B. ■

Lemma 2: For any feasible $\mathbf{W}_n^\circ$, the optimal φ can be obtained as

$$\varphi_n = \frac{P_S\left(|\hat{h}_e|^2 + \varepsilon\right) + 1}{1 + P_S(|\hat{h}_e|^2 + \varepsilon) + \mathrm{Tr}\left(\mathbf{G}_e\mathbf{W}_n^\circ\right) + \mathrm{Tr}\left(\varepsilon\mathbf{W}_n^\circ\right)} \tag{33}$$

Proof: Given $\mathbf{W}_n^\circ$, the objective function in (32a) is monotonically increasing with ϕ. Since $\mathbf{W}_n^\circ$ is the feasible solution of $\mathcal{P}7$, it satisfies constraints in (32b)–(32e). Particularly, based on (32b), the maximum value of ϕ can be obtained when (32b) holds the equal sign. Since $1 + P_S(|\hat{h}_e|^2 + \varepsilon) + \mathrm{Tr}(\mathbf{G}_e\mathbf{W}_n^\circ) + \mathrm{Tr}(\varepsilon\mathbf{W}_n^\circ) > 0$, thus (33) is achieved.

Computational complexity: The main complexity of Algorithm 2 can be calculated by the one-dimension search number (N_s) multiplying the complexity in each search. For each search, the SDP for solving $\mathbf{w}_n^\circ$ 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, the complexity of SDP in each search is $\mathcal{O}(N^4)$. Besides, the complexity for solving ϕ_n can be calculated based on (33) which is $\mathcal{O}(N^3)$. Thus, the total complexity can be calculated as $N_s log(1/\epsilon)(\mathcal{O}(N^4) + \mathcal{O}(N^3))$.

Algorithm 2: Iterative Alternating BF Optimization Approach.

```
   Input: $P_S, P_B, \mathcal{R}'_s, h_{su}, h_{gu}, \hat{h}_e, \mathbf{g}_{su}, \mathbf{g}_{gu}, \hat{\mathbf{g}}_e$.
   Result: $\mathbf{W}^\star$.
1  Initialization: $\phi_0$, $\eta_0$.
2  Set $n = 1$.
3  Initialization: $\eta_0$
4  while Searching $\eta_n$ do
5      while clause repeat
6          Execute SDP by CVX tool to solve $\mathcal{P}7$;
           Output: $\mathbf{W}_n^\circ$.
7          Calculate the secrecy rate:
           $R_s^{B2V(n)} = \log_2\left(\varphi_n + \frac{\varphi_n \mathrm{Tr}(\mathbf{G}_{gu}\mathbf{W}_n^\circ)}{P_S|h_{gu}|^2+1}\right)$;
8          Obtain $\varphi_n$ according to (33);
9          Return $\varphi_n$ to step 4;
10         Calculate the secrecy rate:
11         $R_s^{B2V(n+1)} = \log_2\left(\varphi_{n+1} + \frac{\varphi_{n+1} \mathrm{Tr}(\mathbf{G}_{gu}\mathbf{W}_n^\circ)}{P_S|h_{gu}|^2+1}\right)$;
12     until $\left|R_s^{B2V(n+1)} - R_s^{B2V(n)}\right| \le \epsilon$;
13     Update $\eta_n$.
14 Obtain the optimal $\mathbf{w}_n^\star$ by the singular value
     decomposition (SVD) of the optimal $\mathbf{W}^\star$.
15 Procedure End
```

In addition, we can see the inputs of algorithm 1 and algorithm 2 consist of parameters from satellite, SU, GU, and the BS, which is hard to be gathered at one device generally and a joint optimization is hard to reached in such heterogeneous network. Benefit from the cybertwin deployment, a global information exchange for carrying out the secure BF optimization to implement the physical layer security in both satellite and terrestrial vehicle communications is realized.

VI. Performance Evaluations

In this section, simulations are carried out to evaluate the secrecy rate performance of the cybertwin-driven integrated satellite-terrestrial vehicle transmissions. The system parameters are specifically set as follows. The low earth orbit (LEO) satellite is employed and the height of satellite orbit is 600 Km, the maximum beam gain is 52 dB, and the 3-dB angle of satellite beam is set to 0.4°. The rain attenuation parameters of satellite-terrestrial channel are set to -3.152 dB and 1.6. The carrier frequency of the integrated satellite-terrestrial transmissions is 2 GHz. In addition, the distances from BS to the SU and Eve are set to 90 m and 100 m, respectively. The terrestrial channel power gain at the reference distance of 1 m is set to -38.46 dB. The Nakagami-m channel parameters are $m = 2$ and $\Omega = 1$. System parameters are set in Table II.

Benchmark: We consider the widely used MRT/ZF-based BF schemes as the benchmark in this section, which is designed as the fixed BF scheme at BS for secure transmission. The MRT/ZF-based BF vector can be respectively given by [30], [34]

$$\mathbf{w}_{MRT} = \mathbf{g}_{su}/\|\mathbf{h}_{rd}\|, \tag{34}$$

$$\mathbf{w}_{ZF} = \mathbf{f}_0/\|\mathbf{f}_0\|, \tag{35}$$

TABLE II
SYSTEM PARAMETERS SETTING

System parameters	Numerical value
Satellite channel parameters	
Satellite height	600 Km
Carrier frequency	2 GHz
Maximum beam gain	52 dB
3 dB angle (for all beams)	0.4°
Rain attenuation parameters	$\mu_{\zeta_{dB}}$ = -3.152, $\delta^2 = 1.6$
BS channel parameters	
Channel power gain	-38.46 dB
Nakagami-m channel parameters	$m = 2$ and $\Omega = 1$
Distance from BS to GU, SU and Eve	80m, 90m, 100m

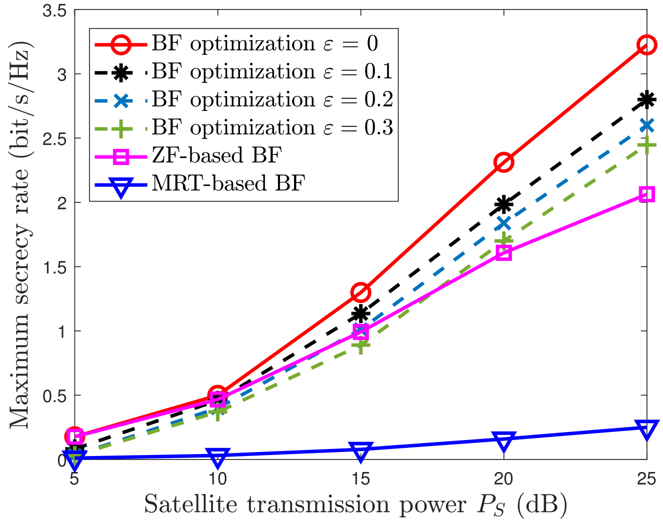

Fig. 3. The impact of the satellite transmission power on the maximum secrecy rate of SU. ($P_B = 30$ dB, $\mathcal{R}_s = 2$ bit/s/Hz, $N = 4$).

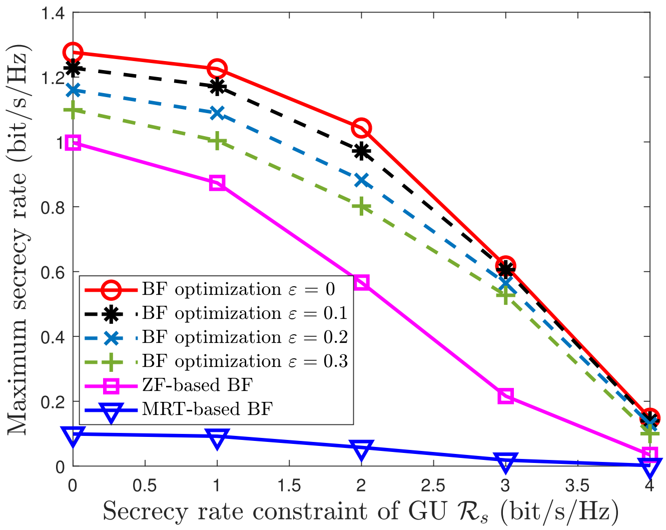

Fig. 4. The impact of the secrecy rate constraint of GU on the maximum secrecy rate of SU. ($P_S = 15$ dB, $P_B = 30$ dB, $N = 4$).

where $\mathbf{f}_0 = (\mathbf{I}_M - \mathbf{g}_e(\mathbf{g}_e^H\mathbf{g}_e)^{-1}\mathbf{g}_e^H)\mathbf{g}_{su}$. Fig. 3 shows the impact of satellite transmission power on the maximum secrecy rate of SU, where the secrecy rate of GU is constrained by $\mathcal{R}_s = 2$ bit/s/Hz and the number of transmit antennas at BS is set to $N = 4$. We can see that the maximum secrecy rate of SU increases as the satellite transmission power increases, and the proposed BF optimization approach outperforms the ZF/MRT-based BF approaches. This is because the secrecy rate of SU is monotonically increasing with P_S based on (17a). For the ZF-based BF approach, the green interference from BS only degrades the wiretap channel of SU. The main channel quality of SU is enhanced when P_S increases, which leads to an increasing secrecy rate of SU. However, the signal quality of the main channel of GU is degraded due to the signal loss [20], which conflicts with the secrecy constraint of GU. Compared with the ZF-based BF approach, the rest power of BS can completely serve as the green interference for the secure transmission of SU when the secrecy constraint of GU is satisfied based on our BF optimization approach. For the MRT-based BF scheme, insufficient interference can be leveraged to increase the channel difference from satellite to SU and Eve, thus the secrecy performance of SU cannot be improved significantly. In addition, the larger CSI uncertainty (ε) results in the worse secrecy rate performance due to the increasing channel estimation errors as ε becomes larger. Fig. 4 shows the impact of the secrecy constraint of GU on the maximum secrecy rate of SU increases, where $P_S = 15$ dB, $P_B = 30$ dB, and $N = 4$. From Fig. 4, we can observe that the maximum secrecy rate of SU decreases as the secrecy rate constraint of GU. With the increasing $\mathcal{R}_s$, more BS power is required for the secure BS link based on (18c) and (19a), which indicates that less green interference from the BS can be used for the secure transmission of SU, as consequently the secrecy rate of SU decreases. For the ZF-based BF approach, i.e., $\mathrm{Tr}(\mathbf{G}_{su}\mathbf{W}) = 0$, $\mathrm{Tr}(\mathbf{G}_e\mathbf{W})$ decreases as $\mathcal{R}_s$ increases based on (12). The secrecy rate of SU is determined by (24), which is a monotonically increasing function of $\mathrm{Tr}(\mathbf{G}_e\mathbf{W})$. Thus, the secrecy rate of SU decreases as $\mathcal{R}_s$ increases. The proposed BF optimization approach outperforms the ZF-based BF approach, since the damage of Eve by ZF-based BF is lighter. Since the BS power focuses more on the main channel of GU by MRT-based BF as $\mathcal{R}_s$ increases, few green interference could be used for damaging the wiretap channel of SU. Fig. 5 shows the impact of the number of transmit antennas at BS on the maximum secrecy rate of SU, where $P_S = 15$ dB, $P_B = 30$ dB, and $\mathcal{R}_s = 2$ bit/s/Hz. From Fig. 5, we can see that the maximum secrecy rate of SU increases with the number of BS antennas. This is because the BF focuses more on its intended directions, and thus BF gain increases when the number of BS antennas increases, which controls the signal leakage and interference better. In addition, we can see our proposed BF optimization approach outperforms the ZF/MRT-based BF approaches, which indicates that it can improve the secrecy performance of SU when the additional BS resource serves as the green interference to degrades the Eve.

Fig. 6 shows the impact of the BS transmission power on the maximum secrecy rate of GU, where $P_S = 10$ dB and $\mathcal{R}_s = 0.2$ bit/s/Hz. From Fig. 6, we can see that the maximum secrecy rate of GU increases with the BS transmission power. This is because the main channel capacity of GU increases as the BS

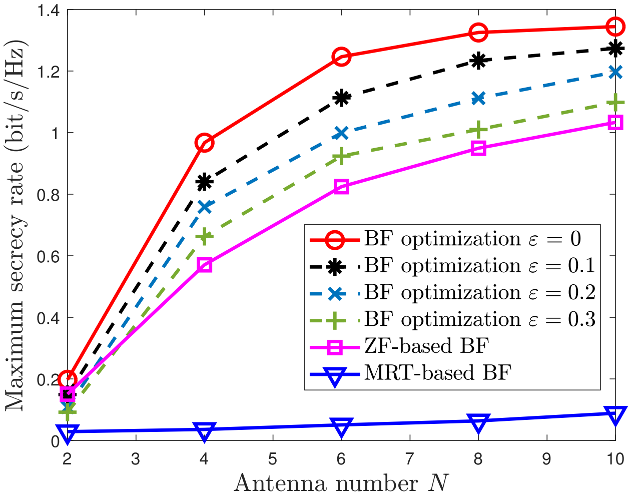

Fig. 5. The impact of the number of BS transmit antennas on the maximum secrecy rate of SU. ($P_S = 15$ dB, $P_B = 30$ dB, $\mathcal{R}_s = 2$ bit/s/Hz).

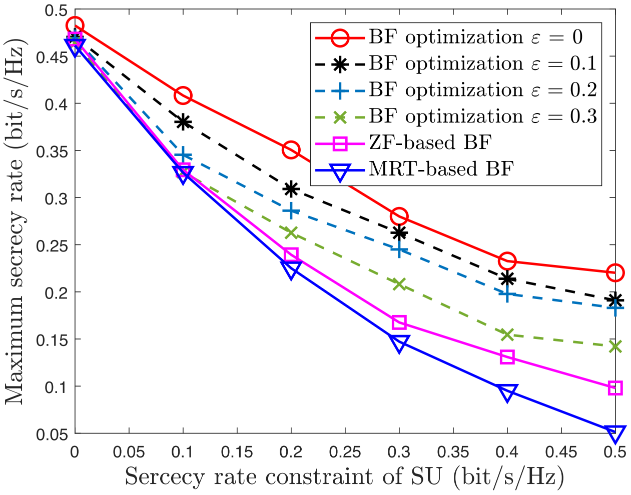

Fig. 7. The impact of secrecy rate constraint of SU on the maximum secrecy rate of GU. ($P_S = 15$ dB, $P_B = 20$ dB, $N = 4$).

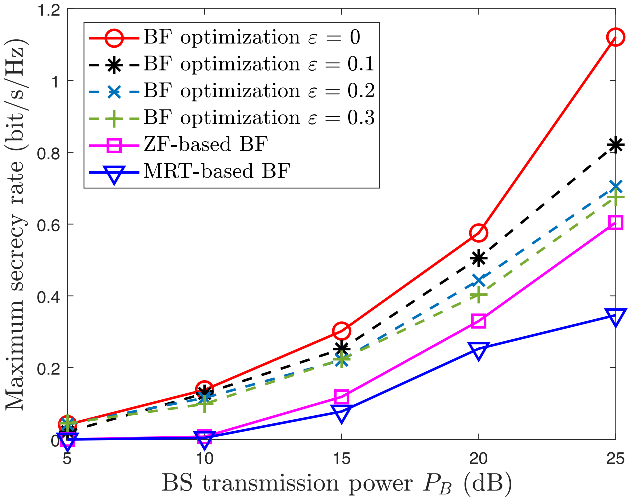

Fig. 6. The impact of BS transmission power on the maximum secrecy rate of GU. ($P_S = 10$ dB, $\mathcal{R}'_s = 0.2$ bit/s/Hz, $N = 4$).

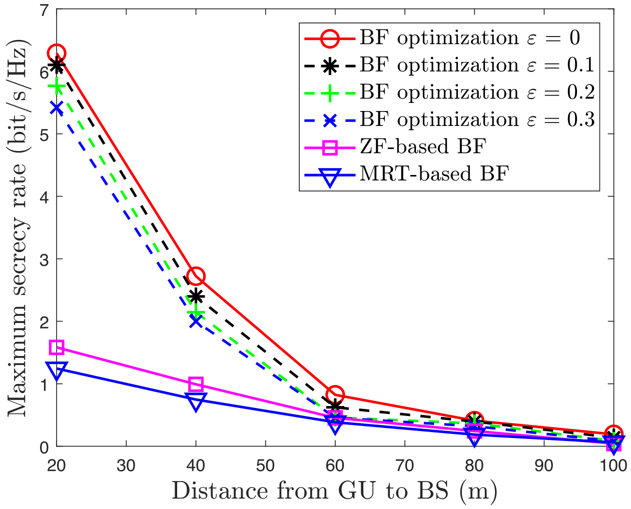

Fig. 8. The impact of the distance from GU to BS on the maximum secrecy rate of SU. ($P_B = 20$ dB, $P_S = 15$ dB, $\mathcal{R}_s = 0.2$ bit/s/Hz, $N = 4$).

transmission power increases, and thus the secrecy rate of GU increases. From (32a), the objective function is monotonically increasing with P_B, thus the secrecy rate of GU increases as the rest BS transmission power increases when a fixed part of BS transmission power for guaranteeing the secrecy constraint of SU is satisfied. Particularly, our proposed BF optimization approach in Algorithm 2 outperforms the ZF- and MRT-based BF schemes.

Fig. 7 shows the impact of the secrecy rate constraint of SU on the maximum secrecy rate of GU, where $P_S = 15$ dB, $P_B = 20$ dB, and $N = 4$. From Fig. 7, it can be observed that the maximum secrecy rate of GU decreases as the secrecy rate constraint of GU. This is because the BF focuses more on the wiretap channel of SU as the secrecy rate constraint of SU increases, as a result the damage to the GU's wiretap channel and the secrecy enhancement of the GU's main channel are weakened. Comparing to the ZF/MRT-based BF scheme, by our proposed BF optimization approach the green interference from BS degrades the Eve and the main channel capacity of GU also has the enhancement. Fig. 8 shows the impact of the distance from GU to BS on the maximum secrecy rate of GU increases, where $P_B = 20$ dB, $P_S = 15$ dB, $\mathcal{R}_s = 0.2$ bit/s/Hz, and $N = 4$. From Fig. 8, it can be observed that the maximum secrecy rate of GU decreases as the distance from GU to BS. This is because the channel attenuation between the BS and GU increases as the GU moves away from the BS. The main channel capacity of GU decreases as the distance from GU to BS increases and thus the maximum secrecy of GU decreases. Particularly, we can see our proposed BF optimization approach outperforms the ZF- and MRT-based BF schemes.

VII. Conclusion

In this paper, we have investigated physical layer security in the cybertwin-driven integrated satellite-terrestrial vehicle communications, where both the secure transmissions of satellite and BS downlinks are considered. Particularly, the co-channel interference serving as the green interference is leveraged to conduct the secure transmissions by optimizing the BF at the terrestrial BS. The cybertwin provides the satellite-terrestrial information interaction platform, and directs the BF optimization of the terrestrial BS with the satellite/BS transmission power, the satellite/BS-to-vehicle channel feedback information, and the secrecy constraint of the satellite/BS link from the Sat-DT, BS-DT, and Veh-DT. Then the BS-DT delivers the optimal BF to the physical terrestrial BS. Specifically, to maximize the secrecy rate of SU while guaranteeing the secrecy rate constraint of GU, we have formulated a problem to optimize the BF of BS, which has been solved by the proposed iterative BF optimization approach. Besides, to maximize the secrecy rate of GU while the secrecy rate of SU is constrained, another iterative alternating BF optimization approach has been proposed. Moreover, the SDR and SDP have been adopted to reformulate these two non-convex problems. The tightness of relaxation has been proved and the complexity of our proposed approaches has been also analyzed. Simulation results have revealed that the co-channel interference due to spectrum sharing can effectively improve the secrecy performance of the integrated satellite-terrestrial communications. For the future work, we will investigate the cybertwin-enabled dynamical secure access selection in satellite-terrestrial integrated networks.

Appendix A
Proof of Theorem 1

Proof: The Lagrangian function of $\mathcal{P}4 - A$ can be obtained, which is shown in (36) at the bottom of this page, where $\lambda \geq 0$, $\rho \geq 0$, $\phi \geq 0$, and $\mathbf{U} \succeq \mathbf{0}$.

Taking the partial derivative of the Lagrangian function with respect to $\mathbf{W}$ and applying the karush-kuhn-tucker (KKT) conditions, we have

$$\mathbf{A} - \rho \frac{\mathbf{G}_{gu}}{P_S |h_{gu}|^2 + 1} + \lambda \left(1 - \xi^{-1}\right) \mathbf{G}_e - \mathbf{U} = \mathbf{0}, \tag{37}$$

$$\mathbf{U}\mathbf{W} = \mathbf{0}, \tag{38}$$

$$\mathbf{W} \succeq \mathbf{0}, \tag{39}$$

where $\mathbf{A}$ can be represented as

$$\mathbf{A} = \left(\phi + \frac{\varepsilon \rho 2^{\mathcal{R}_s}}{P_S \left(|\hat{h}_e|^2 + \varepsilon\right) + 1} + \lambda \varepsilon \left(1 - \xi^{-1}\right)\right) \mathbf{I}_N + \mathbf{G}_{su} + \frac{\rho 2^{\mathcal{R}_s}}{P_S \left(|\hat{h}_e|^2 + \varepsilon\right) + 1} \mathbf{G}_e. \tag{40}$$

Due to $\phi \geq 0$, $\lambda \geq 0$, and $\rho \geq 0$, we can obtain

$$\phi + \frac{\varepsilon \rho 2^{\mathcal{R}_s}}{P_S \left(|\hat{h}_e|^2 + \varepsilon\right) + 1} + \lambda \varepsilon \left(1 - \xi^{-1}\right) > 0, \tag{41}$$

and thus it can be observed that $\mathbf{A}$ is with full rank.

Based on (37) and denoting as

$$\mathbf{Z} = \mathbf{A} - \rho \frac{\mathbf{G}_{gu}}{P_S |h_{gu}|^2 + 1}, \tag{42}$$

the rank of matrix $\mathbf{Z}$ has

$$N - 1 \leq rank\left(\mathbf{Z}\right) \leq N, \tag{43}$$

where $\mathbf{G}_{gu} = \mathbf{g}_{gu}\mathbf{g}_{gu}^H$ with rank one. By post-multiplying both sides of (37) with $\mathbf{W}$ and using (39), (37) can be rewritten as

$$\mathbf{Z}\mathbf{W} = \lambda \left(\xi^{-1} - 1\right) \mathbf{G}_e \mathbf{W}. \tag{44}$$

Thus, we have

$$rank\left(\mathbf{Z}\mathbf{W}\right) = rank\left(\lambda \left(\xi^{-1} - 1\right) \mathbf{G}_e \mathbf{W}\right) \leq rank\left(\mathbf{G}_e\right) = 1. \tag{45}$$

Using the Sylvester inequality, we can obtain

$$rank\left(\mathbf{Z}\right) + rank\left(\mathbf{W}\right) \leq rank\left(\mathbf{Z}\mathbf{W}\right) + N. \tag{46}$$

It indicates that $rank(\mathbf{W}) = N$ if $rank(\mathbf{Z}\mathbf{W}) = 1$.

However, it yields $rank(\mathbf{Z}) \leq 1$, which conflicts with the result in (43). Thus, $rank(\mathbf{Z}\mathbf{W}) = 0$ and we have

$$rank\left(\mathbf{Z}\right) + rank\left(\mathbf{W}\right) \leq N. \tag{47}$$

Recall (43), $rank(\mathbf{W}) \leq 1$ is obtained from (47). With the rank-one constraint, $\mathbf{W} = \mathbf{0}$ can not be a solution, thus $rank(\mathbf{W}) = 1$. The proof is completed. ■

Appendix B
Proof of Theorem 2

Proof: Similar to the proof of Theorem 1, we first derive the Lagrangian function of $\mathcal{P}7$ shown in (48) at the bottom of this page, where $\varsigma \geq 0, \ell \geq 0, \vartheta \geq 0, \mathbf{\Theta} \succeq \mathbf{0}$.

Taking the partial derivative of (48) with respect to $\mathbf{W}$ and applying the karush-kuhn-tucker (KKT) conditions, we have

$$\mathbf{G}_{gu} + \ell \left(2^{\mathcal{R}'_s} \eta P_S |h_e|^2 + 2^{\mathcal{R}'_s} - 1\right) \mathbf{G}_{su} + \varsigma \varphi \left(\mathbf{G}_e + \varepsilon\right) + \vartheta \mathbf{I} - \mathbf{\Theta} = \mathbf{0}, \tag{49}$$

$$\mathbf{\Theta}\mathbf{W} = \mathbf{0}, \tag{50}$$

$$\mathbf{W} \succeq \mathbf{0}. \tag{51}$$

$$\mathrm{L}\left(\mathbf{W}, \lambda, \rho, \phi, \mathbf{U}\right) = \mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}\right) + \phi\left(\mathrm{Tr}\left(\mathbf{W}\right) - P_B\right) - \mathbf{U}\mathbf{W} + \lambda \left(\left(1 - \xi^{-1}\right) \mathrm{Tr}\left(\left(\mathbf{G}_e + \varepsilon\right)\mathbf{W}\right) - \xi^{-1} + 1 - P_S\left(|\hat{h}_e|^2 + \varepsilon\right)\right) - \rho \left(\mathrm{Tr}\left(\left(\frac{\mathbf{G}_{gu}}{P_S|h_{gu}|^2 + 1} - \frac{2^{\mathcal{R}_s}\left(\mathbf{G}_e + \varepsilon\right)}{P_S\left(|\hat{h}_e|^2 + \varepsilon\right) + 1}\right)\mathbf{W}\right) - 2^{\mathcal{R}_s} + 1\right). \tag{36}$$

$$\mathrm{L}\left(\mathbf{W}, \varsigma, \ell, \vartheta, \mathbf{\Theta}\right) = \mathrm{Tr}\left(\mathbf{G}_{gu}\mathbf{W}\right) + \vartheta\left(\mathrm{Tr}\left(\mathbf{W}\right) - P_B\right) + \ell\left(\left(2^{\mathcal{R}'_s}\eta P_S|h_e|^2 + 2^{\mathcal{R}'_s} - 1\right)\left(\mathrm{Tr}\left(\mathbf{G}_{su}\mathbf{W}\right) + 1\right) - P_S|h_{su}|^2\right) + \varsigma\left(\varphi\left(1 + P_S(|\hat{h}_e|^2 + \varepsilon) + \mathrm{Tr}\left(\mathbf{G}_e\mathbf{W}\right) + \mathrm{Tr}\left(\varepsilon\mathbf{W}\right)\right) - P_S\left(|\hat{h}_e|^2 + \varepsilon\right) - 1\right) - \mathbf{\Theta}\mathbf{W}. \tag{48}$$

Based on (29), it indicates that $0 < \eta \leq 1$. Then, it is easy to obtain $\ell(2^{\mathcal{R}'_s}\eta P_S|h_e|^2 + 2^{\mathcal{R}'_s}) \geq 0$. We make the following definition

$$\mathbf{B} = \vartheta\mathbf{I} + \mathbf{G}_{gu} + \ell\left(2^{R}\eta P_S|h_e|^2 + 2^{R}\right)\mathbf{G}_{su} + \varsigma\varphi\left(\mathbf{G}_e + \varepsilon\right), \tag{52}$$

and $\mathbf{B} \succ \mathbf{0}$ can be reached, which indicates $\mathbf{B}$ is with full rank.

By post-multiplying both sides of (49) with $\mathbf{W}$ and using (50), we have $\mathbf{BW} = \mathbf{G}_{su}\mathbf{W}$. Thus,

$$rank\left(\mathbf{BW}\right) = rank\left(\mathbf{G}_{su}\mathbf{W}\right) \leq rank\left(\mathbf{G}_{su}\right) = 1. \tag{53}$$

Based on (53), we have $rank(\mathbf{W}) = rank(\mathbf{BW}) \leq 1$. Particularly, $\mathbf{W} = \mathbf{0}$ can not be a solution which should be discarded, thus $rank(\mathbf{W}) = 1$. The proof is completed. ■

REFERENCES

[1] N. Cheng *et al.*, "A comprehensive simulation platform for space-air-ground integrated network," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 178–185, Feb. 2020.

[2] M. Matthaiou, O. Yurduseven, H. Q. Ngo, D. Morales-Jimenez, S. L. Cotton, and V. F. Fusco, "The road to 6G: Ten physical layer challenges for communications engineers," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 64–69, Jan. 2021.

[3] S. Zhou, G. Wang, S. Zhang, Z. Niu, and X. Shen, "Bidirectional mission offloading for agile space-air-ground integrated networks," *IEEE Wireless Commun.*, vol. 26, no. 2, pp. 38–45, Apr. 2019.

[4] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019.

[5] 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, Dec. 2019.

[6] Q. Yu, J. Ren, H. Zhou, and W. Zhang, "A cybertwin based network architecture for 6G," in *Proc. 2nd 6G Wireless Summit*, 2020, pp. 1–5.

[7] T. H. Luan, R. Liu, L. Gao, R. Li, and H. Zhou, "The paradigm of digital twin communications," May 2021, *arXiv:2105.07182*.

[8] N. Kato *et al.*, "Optimizing space-air-ground integrated networks by artificial intelligence," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 140–147, Aug. 2019.

[9] B. Qian, H. Zhou, T. Ma, K. Yu, Q. Yu, and X. Shen, "Multi-operator spectrum sharing for massive IoT coexisting in 5G/B5G wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 3, pp. 881–895, Mar. 2021.

[10] Y. Liu *et al.*, "Physical layer security assisted computation offloading in intelligently connected vehicle networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3555–3570, Jun. 2021.

[11] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[12] Y. Hui *et al.*, "Secure and personalized edge computing services in 6G heterogeneous vehicular networks," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2021.3065970.

[13] Y. Liu *et al.*, "Secrecy rate maximization via radio resource allocation in cellular underlaying V2V communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7281–7294, Jul. 2020.

[14] W. Wang, N. Cheng, Y. Liu, H. Zhou, X. Lin, and X. Shen, "Content delivery analysis in cellular networks with aerial caching and mmWAVE backhaul," *IEEE Trans. Veh. Tech.*, vol. 70, no. 5, pp. 4809–4822, May 2021.

[15] Z. Yin, M. Jia, W. Wang, N. Cheng, F. Lyu, and X. Shen, "Max-min secrecy rate for NOMA-based UAV-assisted communications with protected zone," in *Proc. IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.

[16] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.

[17] Á. Vázquez-Castro and M. Hayashi, "Physical layer security for RF satellite channels in the finite-length regime," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 981–993, Apr. 2019.

[18] Z. Yin *et al.*, "Secrecy rate analysis of satellite communications with frequency domain NOMA," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 11 847–11858, Dec. 2019.

[19] B. Li, Z. Fei, Z. Chu, F. Zhou, K. Wong, and P. Xiao, "Robust chance-constrained secure transmission for cognitive satellite-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4208–4219, May 2018.

[20] M. Lin, Z. Lin, W. Zhu, and J. Wang, "Joint beamforming for secure communication in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 5, pp. 1017–1029, May 2018.

[21] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: A survey," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13789–13804, Sep. 2021.

[22] T. K. Rodrigues, J. Liu, and N. Kato, "Application of cybertwin for offloading in mobile multi-access edge computing for 6G networks," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16231–16242, Nov. 2021.

[23] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5138–5150, Nov. 2020.

[24] W. Sun, H. Zhang, R. Wang, and Y. Zhang, "Reducing offloading latency for digital twin edge networks in 6G," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12240–12 251, Oct. 2020.

[25] W. Sun, P. Wang, N. Xu, G. Wang, and Y. Zhang, "Dynamic digital twin and distributed incentives for resource allocation in aerial-assisted Internet of Vehicles," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2021.3058213.

[26] X. Li, B. He, Y. Zhou, and G. Li, "Multisource model-driven digital twin system of robotic assembly," *IEEE Syst. J.*, vol. 15, no. 1, pp. 114–123, Mar. 2021.

[27] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, Feb. 2021.

[28] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 669–680, Jan. 2020.

[29] 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, Feb. 2021.

[30] Z. Yin *et al.*, "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2021.3090017.

[31] P. Series, *Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems*, *Recommendation ITU-R*, International Telecommunication Union, pp. 618–12, 2015.

[32] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[33] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[34] E. P. Simon, J. Farah, and P. Laly, "Performance evaluation of massive MIMO with beamforming and nonorthogonal multiple access based on practical channel measurements," *IEEE Antennas Wireless Propag. Lett.*, vol. 18, no. 6, pp. 1263–1267, Jun. 2019.

Zhisheng Yin (Member, IEEE) received the B.E. degree from the Wuhan Institute of Technology, Wuhan, China, the B.B.A. degree from the Zhongnan University of Economics and Law, Wuhan, China, in 2012, the M.Sc. degree from the Civil Aviation University of China, Tianjin, China, in 2016, and the Ph.D. degree from the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China, in 2020. From September 2018 to September 2019, he visited to the BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is currently an Assistant Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include space-air-ground integrated networks, wireless communications, cybertwin, and physical layer security.

Nan Cheng (Member, IEEE) received the B.E. and M.S. degrees from the Department of Electronics and Information Engineering, Tongji University, Shanghai, China, in 2009 and 2012, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2016. From 2017 to 2019, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. He is currently a Professor with the State Key Laboratory of ISN and with School of Telecommunication Engineering, Xidian University, Shaanxi, China. His current research interests include B5G/6G, space-air-ground integrated network, Big Data in vehicular networks, self-driving system, performance analysis, MAC, opportunistic communication, and application of AI for vehicular networks.

Tom H. Luan (Senior Member, IEEE) received the B.Eng. degree from Xi'an Jiaotong University, Xi'an, China, in 2004, the M.Phil. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2007, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2012. He is currently a Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. He has authored or coauthored more than 40 journal articles and 30 technical articles in conference proceedings. His research interests include content distribution and media streaming in vehicular ad hoc networks, peer-to-peer networking, and the protocol design and performance evaluation of wireless cloud computing and edge computing. Dr. Luan was the recipient of one U.S. patent. He was the TPC Member of the IEEE Global Communications Conference, IEEE International Conference on Communications, and IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, and Technical Reviewer for multiple IEEE Transactions, including the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.

Ping Wang (Fellow, IEEE) received the bachelor's and master's degrees in electrical and computer engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1994 and 1997, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. She is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, York University, Toronto, ON, Canada. Prior to that from 2008 to 2018, she was with Nanyang Technological University, Singapore. Her research interests mainly include wireless communication networks, cloud computing, and the Internet of Things. Her scholarly works have been widely disseminated through top-ranked IEEE journals/conferences and was the recipient of the best paper awards from IEEE Wireless Communications and Networking Conference (WCNC) in 2020 and 2012, from IEEE Communication Society, Green Communications & Computing Technical Committee in 2018, and from IEEE International Conference on Communications (ICC) in 2007. She is a Distinguished Lecturer of the IEEE Vehicular Technology Society.