Multi-domain Resource Multiplexing Based Secure Transmission for Satellite-Assisted IoT: AO-SCA Approach

Zhisheng Yin, *Member IEEE*, Nan Cheng, *Member IEEE*, Yilong Hui, *Member IEEE*, Wei Wang, *Member IEEE*, Lian Zhao, *Senior Member IEEE*, Khalid Aldubaikhy, *Member IEEE*, and Abdullah Alqasir, *Member IEEE*

***Abstract*—Due to the wireless broadcasting and broad coverage in satellite-supported Internet of things (IoT) networks, the IoT nodes are susceptible to eavesdropping threats. Considering the distance difference between satellite and nearby destinations is negligible, the main and wiretapping channels between satellite and IoT node are similar, it poses great challenges to reach physical layer security in satellite-assisted IoT networks. In this paper, to guarantee secure transmissions for satellite-assisted IoT downlink communications, the multi-domain resource multiplexing based secure approach is proposed. Particularly, the self-induced co-channel interference between adjacent nodes is leveraged to increase the difference of signal transmission quality over both main and wiretapping channels. By comprehensively optimizing multi-domain resources, i.e., frequency, power, and spatial domains, secure transmissions from satellite to IoT nodes are reached. Specifically, the problem to maximize the sum secrecy rate of IoT nodes is formulated with a constraint of common communication rate of IoT nodes. To solve this non-convex problem, an alternating optimization (AO) algorithm with two inner successive convex approximation (SCA) algorithms are executed to solve the power allocation, spectral multiplexing, and precoding. In addition, simulation results are carried out to evaluate the secrecy rate performance and verify the efficiency of our proposed approach.**

***Index Terms*—LEO satellite, IoT, physical layer security, sum secrecy rate, multi-domain resource multiplexing.**

I. Introduction

Due to the wide broadcasting and full coverage, satellite communication has attracted great attention towards 6G networks [1]–[3]. Especially, low earth orbit (LEO) satellite network is involving in constructing satellite-air-ground integrated networks, since its low latency and attenuation, flexible deployment, and strong resistance to natural disaster [4], [5], which has potential advantages in providing mobile broadband for applications in complex geographical environment service, such as Internet of things (IoT) [6], [7], vehicle networks [8], navigation and monitoring [9], etc. Particularly, we summarize the benefits of satellite-supported networks such as cost-effectiveness, low latency, wider range, greater reliability, transformation of infrastructure, etc [4]. Recently, IoT applications have been booming in the industry with the number of IoT connected devices being increasing [10]. For the large-scale distributed IoT nodes, satellite networks have shown unique advantages in offering ubiquitous connectivity with limited or no access to terrestrial networks [11]–[13]. Therefore, LEO satellite can be a great option for IoT applications. However, massive data created from IoT nodes requires effective spectral efficient technologies to meet the high-speed data transmission [14], [15]. Besides, lightweight security is urgent due to the limited resource at satellite and the low-power consumption of IoT [16].

To improve the utilization of spectrum resource, frequency multiplexing or spectrum sharing is generally adopted in multi-beam satellite networks [17]–[19]. Whereas, co-channel interference is also introduced, which brings a drawback for system performance and abundant works have been investigated addressing on the topic of interference cancellation [20]–[22]. Interestingly, it has been verified in [23] that the detrimental co-channel interference actually benefits the secure transmission, as it facilitates the implementation of physical layer security. Based on the information theory, the physical layer security relies on the randomness difference of wireless channel. However, different from terrestrial communications, the line-of-sight is dominant in satellite networks, leading to similarity in the downlink channels. Besides, satellite beam is widely broadcasting and passive eavesdropping threats are hard to avoid. This poses challenges to implement physical layer security for the downlink of satellite-supported IoT networks.

To resist the eavesdropping threats, physical layer security approach as the lightweight way has been widely studied in wireless communications, which is carried out through signal processing, e.g., secure coding, beamforming, and relaying, etc. [24]–[26]. In satellite communications, physical layer security has attracted great research interests in recent years. An overview on physical layer security in LEO satellite system

This work was supported in part by the National Natural Science Foundation of China (No. 62201432, 62071356, and 62071398), the Fundamental Research Funds for the Central Universities of Ministry of Education of China under Grant XJS221501, the National Natural Science Foundation of Shaanxi Province under Grant 2022JQ-602, and in part by the Guangzhou Science and Technology Program under Grant 202201011732.

Z. Yin is with State Key Lab. of ISN and School of Cyber Engineering, Xidian University, Xi'an, 710071, China (e-mail: zsyin@xidian.edu.cn).

N. Cheng (*corresponding author*) and Y. Hui are with State Key Lab. of ISN and School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China (e-mail: dr.nan.cheng@ieee.org; ylhui@xidian.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).

L. Zhao is with the Department of Electrical, Computer and Biomedical Engineering, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada (e-mail: l5zhao@ryerson.ca).

K. Aldubaikhy and A. Alqasir are with the Department of Electrical Engineering, College of Engineering, Qassim University, Qassim, Saudi Arabia (e-mail: {khalid, a.alqasir}@qec.edu.sa).

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2023.3250227

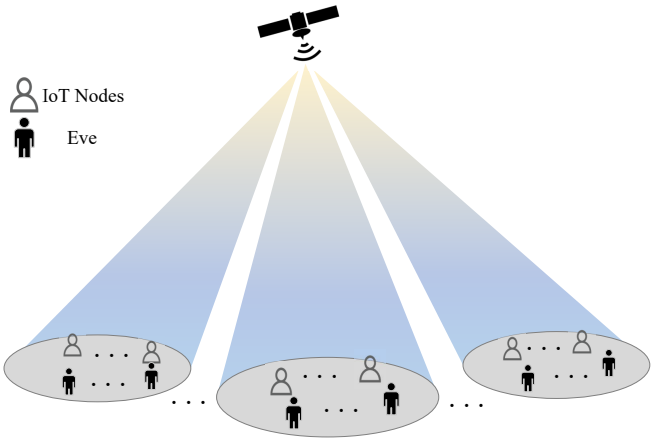

Fig. 1. Downlink eavesdropping scenario in satellite supporting IoT networks.

is investigated in [25]. It is studied that the fundamental ability of physical layer security leads the encryption to code and to provide a positive secrecy capacity. In the downlink hybrid satellite-terrestrial network, an opportunistic user-relay selection criteria is proposed in [27] to guarantee the secure transmission, where the secrecy outage probability (SOP) is quantitatively analyzed. Considering an integrated satellite-terrestrial network, the interference between satellite and terrestrial downlinks is used to implement the physical layer security in both satellite and terrestrial links by beamforming [28], [29]. The Unmanned Aerial Vehicle (UAV) is exploited as a relay to improve the secure multi-beam satellite communications in [30], where the artificial noise (AN) is created by UAV to confuse Eve. Particularly, satellite beamforming (BF) and UAV power allocation (PA) are jointly optimized to maximize the secrecy rate performance of satellite users. It reveals that the secure transmission can be achieved with the assistance of external infrastructure to satellite system. In addition, several investigations have focused on independent satellite communications, where more resource with multiple dimensions can be utilized to conduct signal processing. For both the colluded and collaborated eavesdropping scenarios, a threshold-based scheduling scheme is proposed in [31] and the closed-form expression for the average secrecy capacity (ASC) is derived based on the proposed user scheduling scheme, where the asymptotic analysis for the SOP is given at high signal-to-noise ratio (SNR) regions. The secrecy rate performance is analyzed in satellite communications based on frequency domain non-orthogonal multiple access (FD-NOMA) and the impact of the level of spectral overlapping on secrecy rate performance is also analyzed in [32].

Appreciating to previous related works, however the available resources vehemently address on the security issue to complete the signal processing while the sacrifice of common communication performance has not been investigated. It is still challenging to implement physical layer security in satellite networks without additional assistance. In this paper, we investigate the secure transmission in the downlink of satellite-supported IoT networks in areas without terrestrial networks shown in Fig. 1, where the multi-beam satellite service is provided and multiple IoT nodes are within each beam. The frequency division multiplexing (FDM) scheme is adopted in the downlink access for multiple IoT nodes within a beam. Particularly, the spectral partially overlapping among IoT nodes is considered, thus the co-channel interference can be leveraged to assist the implementation of physical layer security. Specifically, we aim to jointly optimize the level of spectral overlapping, the power allocation to each IoT node, and the spatial precoding for designing the interference to strengthen secure communication. We summarize the contributions of this paper as follows.

- Considering the similarity among satellite channels, we conduct a framework to realize secure transmissions in satellite-supported IoT networks with multi-domain resource multiplexing. On this basis, the self-induced co-channel interference among IoT nodes can be designed to unevenly damage a pair of main and wiretapping channels where the secure transmission between satellite and IoT nodes can be realized. Particularly, the interference can be handled by the signal processing from multi-domain, i.e., frequency domain, power domain, spatial domain, which facilitates the implementation of physical layer security in case of channel similarity and limited resource at satellite.
- The problem to maximize the sum secrecy rate of satellite downlink transmissions is formulated, where the communication achievable rate of each IoT node is constrained. Since the mixed multiplications of quadratic terms exist in the objective function and constraints, reformulations by Taylor expansion and semidefinite relaxation (SDR) are made to transform the problem into a bi-convex problem, which can be solved by a two-stage alternation optimization approach. Besides, the tightness of the relaxation is proved by the proof of rank-one.
- To find the solutions of multi-resource optimization, an alternating optimization with successive convex approximation (AO-SCA) approach is proposed to solve the reformulated bi-convex problem. Performance of the reference algorithms in the open literature is also given for comparisons. In addition, simulations are carried out to verify the efficiency of our proposed approach and evaluate the impact of system parameters on the sum secrecy rate performance.

The reminder of this work is organized as follows. In Section II, the system design and problem formulation are first depicted, the multi-domain resource multiplexing based secure transmission approach is conducted in Section III. Extensive simulations are carried out in Section IV to evaluate the sum secrecy rate performance of satellite downlinks. Finally, this paper is concluded in Section V. In addition, main notations are defined as shown in Table I.

Notations: $(\cdot)^{\dagger}$ denotes the complex conjugate transpose. $|\cdot|$ and $\|\cdot\|$ stand for the absolute value and Euclidean norm of a vector, respectively. $\mathrm{Tr}\,(\cdot)$ and $\mathrm{rank}\,(\cdot)$ denote the trace and rank of a matrix, respectively. $\mathbb{C}^{n\times m}$ denotes a complex space of $n \times m$. $[x]^{+} = \max(x, 0)$. e is the natural constant.

TABLE I
SUMMARY OF MAIN NOTATIONS AND DEFINITIONS

Notation	Definition
M	Number of IoT nodes in each satellite beam
N	Number of satellite beams
P_S	Satellite transmit power
G	Maximum satellite antenna gain
α	Spectral overlapping factor
$\mathrm{IN}_{n,k}$	The k^{th} IoT node in n^{th} satellite beam
$P_{n,k}$	Power allocation to $\mathrm{IN}_{n,k}$
$\mathbf{w}_{n,k} \in \mathbb{C}^{N\times 1}$	Precoding vector for $\mathrm{IN}_{n,k}$
$\mathbf{h}_{n,k} \in \mathbb{C}^{N\times 1}$	Channel vector between satellite and $\mathrm{IN}_{n,k}$
$\mathbf{g}_{n,k} \in \mathbb{C}^{N\times 1}$	Wiretapping channel vector targeting $\mathrm{IN}_{n,k}$
$R_{n,k}$	Secrecy rate from satellite to $\mathrm{IN}_{n,k}$
$\gamma^b_{n,k}$	SINR received at $\mathrm{IN}_{n,k}$ from the main channel
$\gamma^e_{n,k}$	SINR received at Eve targeting $\mathrm{IN}_{n,k}$
c_i	Correlation coefficient among received signals
e	The natural constant
$\mathcal{C}_{n,k}$	Constraint of communication rate of $\mathrm{IN}_{n,k}$
$\mathbf{w}^{mrt}_{n,k}$	MRT-based precoding vector
$\mathbf{w}^{zf}_{n,k}$	ZF-based precoding vector
Δ	Channel estimate error
ε	Error margin

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a downlink eavesdropping scenario in satellite supporting IoT networks illustrated in Fig. 1, where a multi-beam satellite with N beams is deployed and M IoT nodes are assumed in each satellite beam. In each beam, we adopt frequency division non-orthogonal multiplexing (FD-NOM) for IoT nodes getting access to satellite downlink. In Fig. 2, the adjacent bandwidths between two IoT nodes have the proportion α of its spectral overlapped, where $\alpha = \frac{\Delta f}{B}$ and Δf denotes the overlapping spectral between two nodes and B is the bandwidth of each node. We define α as the spectral overlapping factor (SOF). The power domain is also divided and these M nodes are allocated different signal transmit power. Besides, spatial precoding is considered which introduces another domain of multiplexing in the spatial domain. Thus, a framework of multi-domain resource multiplexing among a FD-NOM frame with M nodes is realized. In addition, we assume multiple Eves hide in the coverage of multi-satellite targeting to wiretap the downlink transmissions for IoT nodes. The IoT node and Eve are equipped with single receive antenna, and the multi-beam of satellite is formed by adopting the single feed per beam (SFPB) architecture [30].

The signal received by the k^{th} IoT node in n^{th} beam ($\mathrm{IN}_{n,k}$) can be represented as

$$y^b_{n,k} = \sqrt{P_{n,k}}\mathbf{h}^\dagger_{n,k}\mathbf{w}_{n,k}s_{n,k} + n_{n,k} + \underbrace{\frac{1}{M}\mathbf{h}^\dagger_{n,k}\sum_{m=0}^{M-1}\sum_{i\neq k,i=0}^{M-1}\sqrt{P_{n,i}}\mathbf{w}_{n,k}s_{n,i}e^{j2\pi\frac{(i-k)m}{M}\alpha}}_{\text{IUI}}, \quad (1)$$

where $s_{n,k}$ and $s_{n,i}$ are the transmit signals from satellite to $\mathrm{IN}_{n,k}$ and $\mathrm{IN}_{n,i}$ respectively, $P_{n,k}$ denotes the transmit power allocated to $\mathrm{IN}_{n,k}$, $\mathbf{h}_{n,k} \in \mathbb{C}^{N\times 1}$ denotes the channel vector between satellite and this node, $\dagger$ is the operator of complex conjugate transpose, $\mathbf{w}_{n,k} \in \mathbb{C}^{N\times 1}$ is the precoding vector for $\mathrm{IN}_{n,k}$, and $n_{n,k}$ is the additive white Gaussian noise (AWGN) received at $\mathrm{IN}_{n,k}$. In (1), the received signal from satellite of each IoT node is disturbed by other nodes in a FD-NOM frame shown in Fig. 2 and the inter-user-interference (IUI) is resulted in when $\alpha \neq 1$. Based on the multi-domain resource multiplexing model in Fig. 2, the SOF α can also be seen as the inter-carrier interval and the IUI can be calculated as in (1).

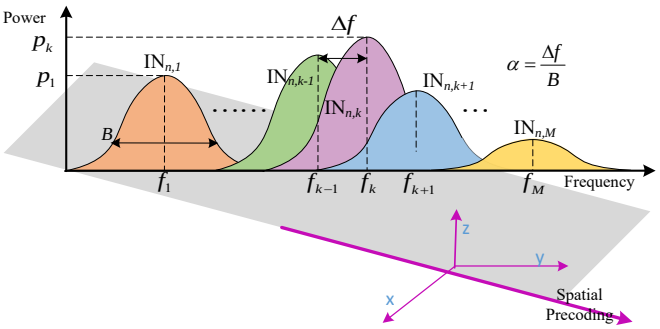

Fig. 2. Multi-domain Resource Multiplexing in satellite supporting IoT networks (Frequency, power, and spatial domains).

Particularly, the free space path loss (FSPL), rain attenuation, and satellite beam gain are generally considered to construct the channel model. Thus the channel vector from satellite to the k^{th} IoT $\mathbf{h}_{n,k}$ is defined by [28], [33]

$$\mathbf{h}_{n,k} = \sqrt{C_L b\beta}\exp\left(-j\boldsymbol{\theta}\right), \quad (2)$$

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

$$C_L = (\lambda/4\pi)^2/\left(d^2 + h^2\right), \quad (3)$$

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. Besides, the beam gain is defined by

$$b = G\left(\frac{J_1(u_0)}{2u_0} - 36\frac{J_3(u_0)}{u_0^2}\right)^2, \quad (4)$$

where G denotes the maximum satellite antenna gain, $u_0 = 2.07123\frac{\sin(a)}{\sin(a_{3\mathrm{dB}})}$ with a being the elevation angle between the beam center and $\mathrm{IN}_{n,k}$, and $a_{3\mathrm{dB}}$ 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., $\ln(\beta_{dB}) \sim \mathcal{N}(u, \delta^2)$ with β_{dB} being the dB form of β.

Considering a pessimistic eavesdropping scenario, an Eve targeting to wiretap $\mathrm{IN}_{n,k}$ works with the same spectral as $\mathrm{IN}_{n,k}$. Therefore, M Eves are assumed to wiretap a FD-NOM frame with M nodes in a beam. Without loss of generality, the received signal by Eve targeting $\mathrm{IN}_{n,k}$ can be expressed as

$$y^e_{n,k} = \sqrt{P_{n,k}}\mathbf{g}^\dagger_{n,k}\mathbf{w}_{n,k}s_{n,k} + n_e + \underbrace{\frac{1}{M}\mathbf{g}^\dagger_{n,k}\sum_{m=0}^{M-1}\sum_{i\neq k,i=0}^{M-1}\sqrt{P_{n,i}}\mathbf{w}_{n,k}s_{n,i}e^{j2\pi\frac{(i-k)m}{M}\alpha}}_{\text{IUI}}, \quad (5)$$

where $\mathbf{g}^\dagger_{n,k}$ is the wiretapping channel vector targeting $\mathrm{IN}_{n,k}$ and it follows the same statistical property as $\mathbf{h}^\dagger_{n,k}$.

Based on the Eqns. (1) and (5), the signal-to-interference-plus-noise-ratio (SINR) of both main channel and wiretapping channel of $\mathrm{IN}_{n,k}$ can be respectively calculated as

$$\gamma^b_{n,k} = \frac{P_{n,k}\mathbf{w}^\dagger_{n,k}\mathbf{h}_{n,k}\mathbf{h}^\dagger_{n,k}\mathbf{w}_{n,k}}{\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{w}^\dagger_{n,k}\mathbf{h}_{n,k}\mathbf{h}^\dagger_{n,k}\mathbf{w}_{n,k}c_i + 1}, \quad (6)$$

$$\gamma^e_{n,k} = \frac{P_{n,k}\mathbf{w}^\dagger_{n,k}\mathbf{g}_{n,k}\mathbf{g}^\dagger_{n,k}\mathbf{w}_{n,k}}{\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{w}^\dagger_{n,k}\mathbf{g}_{n,k}\mathbf{g}^\dagger_{n,k}\mathbf{w}_{n,k}c_i + 1}, \quad (7)$$

where

$$c_i = \left|\frac{\mathrm{sinc}(\alpha(i-k))}{\mathrm{sinc}(\alpha(i-k)/M)}e^{j\alpha\frac{M-1}{M}(i-k)}\right|^2, \quad (8)$$

with the SOF α being defined by $\alpha = \frac{\Delta f}{B}$ (Δf denotes the overlapping spectral between two nodes and B is the bandwidth of each node). Thus c_i represents the correlation coefficient among received signals.

According to the information security theory with Wyner wiretap channel model [34], the secure transmission can be reached when the main channel capacity is greater than the eavesdropping capacity. By using the SINRs in (6) and (7), the secrecy rate of $\mathrm{IN}_{n,k}$ can be calculated as [24], [35]

$$R_{n,k} = \left[\log_2\left(1+\gamma^b_{n,k}\right) - \log_2\left(1+\gamma^e_{n,k}\right)\right]^+, \quad (9)$$

where $[x]^+ = \max(x, 0)$.

To improve the secrecy performance, we formulate a problem to maximize the sum secrecy rate of legitimate IoT nodes in each satellite beam, which can be mathematically written as

$$\mathcal{P}1: \max_{\mathbf{w}_{n,k},\alpha,P_{n,k}} \sum_k R_{n,k} \quad (10)$$

$$\text{s.t.:} \quad C_{n,k} \geq \mathcal{C}_{n,k}, \quad (10a)$$

$$\|\mathbf{w}_{n,k}\|^2 \leq P_S, \quad (10b)$$

$$\sum_k P_{n,k} = 1, \quad (10c)$$

$$0 < P_{n,k} < 1, \quad (10d)$$

$$0 < \alpha < 1, \quad (10e)$$

where the constraint in (10a) ensures a predefined common communication rate ($\mathcal{C}_{n,k}$) for each IoT nodes to guarantee a minimum transmission requirement, and $C_{n,k} = \log_2\left(1+\gamma^b_{n,k}\right)$ is the achieved communication rate of $\mathrm{IN}_{n,k}$; (10b) constrains the maximum transmission power in each satellite beam where $\|\cdot\|$ stands for the Euclidean norm of a vector; the power allocation to IoT nodes in the beam is constrained by (10c); with the transmit power of satellite beam $\|\mathbf{w}_{n,k}\|^2$, the power allocation of $\mathrm{IN}_{n,k}$ is constrained by $P_{n,k}$ in (10d); and the bandwidth overlapping factor is constrained by (10e). Based on (6) and (7), we can see that there exists the product of multiple variables and fractional polynomials in the objective function and constraints in problem $\mathcal{P}1$. Therefore, $\mathcal{P}1$ is obviously non-convex and it is intractable.

III. Multi-domain Resource Multiplexing Based Secure Transmission

Considering the channel similarity among satellite channels, it is hard to guarantee a positive capacity difference between both main and eavesdropping capacity and reach a secure transmission. However, based on (6) and (7), it can be found that the IUI power can be leveraged to obtain a positive capacity difference. Moreover, the formulated $\mathcal{P}1$ can guarantee the secure transmission of each node. Particularly, the IUT power is designed by the multi-domain resource multiplexing, which directs a solution with multi-domain resource optimization for solving $\mathcal{P}1$. Therefore, the main connotation of multi-domain resource multiplexing is to introduce the IUT and design its power from frequency, power, and spatial domains for increasing the SINR difference between both main and eavesdropping satellite channels.

In this section, to solve such intractable problem, the subsequent reformulations are made to facilitate the exploration of solutions. Particularly, the Taylor expansion and SDR are adopted to reformulate the primal problem to a solvable form and then the AO-SCA approach for multi-resource optimization is proposed to maximize the sum secrecy rate of the downlink of satellite-supporting IoT networks. In addition, for the reference propose, the approach that joint optimization of power allocation and spectral multiplexing and the approach that joint optimization of power allocation and precoding are carried out, respectively.

A. Problem Reformulations

To replace the quadratic terms in $\mathcal{P}1$, we first make the following definitions: $\mathbf{H}_{n,k} = \mathbf{h}_{n,k}\mathbf{h}^\dagger_{n,k}$, $\mathbf{W}_{n,k} = \mathbf{w}_{n,k}\mathbf{w}^\dagger_{n,k}$,

$$R_{n,k} = \log_2\Big(\frac{1+(1-c_i)\,P_{n,k}\mathbf{H}_{n,k}\mathbf{W}_{n,k}+\sum\limits_{i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}c_i}{1+\sum\limits_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}c_i}\Big)-\log_2\Big(\frac{1+\big(1-c_i\big)P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k}+\sum\limits_{i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,i}c_i}{1+\sum\limits_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,i}c_i}\Big). \tag{11}$$

and $\mathbf{G}_{n,k} = \mathbf{g}_{n,k}\mathbf{g}_{n,k}^{\dagger}$. Based on ($\mathcal{P}1$), only the positive secrecy rate of all the nodes will indicate a feasible solution. For easy analysis, we remove the $[\cdot]^+$ in (9).

By substituting (6) and (7) into (9) and using the above definitions, the secrecy rate of of $\mathrm{IN}_{n,k}$ can be reformulated as shown in (11) at the top of this page.

By introducing exponential functions, we have following replacements

$$e^{x_{n,k}} = 1+(1-c_i)\,P_{n,k}\mathbf{H}_{n,k}\mathbf{W}_{n,k}+\sum_{i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,k}c_i, \tag{12}$$

$$e^{y_{n,k}} = 1+\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,k}c_i, \tag{13}$$

$$e^{z_{n,k}} = 1+(1-c_i)\,P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k}+\sum_{i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i, \tag{14}$$

$$e^{v_{n,k}} = 1+\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i. \tag{15}$$

By using (12–15), the objective function can be rewritten as

$$\sum_k R_{n,k} = \log_2 e\cdot\big(\sum_k x_{n,k}-y_{n,k}-z_{n,k}+v_{n,k}\big). \tag{16}$$

To reformulate the non-convex constraints, we introduce new optimization variables to reformulate the objective function and constraints. Particularly, the exponential variables have introduced corresponding constraints, which can be written as

$$e^{x_{n,k}} \leq 1+(1-c_i)\,P_{n,k}\mathbf{H}_{n,k}\mathbf{W}_{n,k}+\sum_{i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,k}c_i, \tag{17}$$

$$e^{y_{n,k}} \geq 1+\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,k}c_i, \tag{18}$$

$$e^{z_{n,k}} \geq 1+(1-c_i)\,P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k}+\sum_{i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i, \tag{19}$$

$$e^{v_{n,k}} \leq 1+\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i. \tag{20}$$

Since the exponential function is monotonously increasing, it can be observed that (18) and (19) are obviously non-convex. By using the first-order Taylor expansion of $y_{n,k}$ and $v_{n,k}$, (18) and (20) can be respectively reformulated as

$$e^{\tilde{y}_{n,k}}\,(y_{n,k}-\tilde{y}_{n,k}+1) \geq 1+\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}c_i, \tag{21}$$

$$e^{z_{n,k}}\,(z_{n,k}-\tilde{z}_{n,k}+1) \geq 1+(1-c_i)\,P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k}+\sum_{i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i, \tag{22}$$

where $\tilde{y}_{n,k}$ and $\tilde{z}_{n,k}$ are initial constants which can be updated with an update step.

Besides, the constraint (10a) can be rewritten as

$$\big(2^{\mathcal{C}_{n,k}}-1\big)\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_k c_i - P_{n,k}\mathbf{H}_{n,k}\mathbf{W}_k \leq 1-2^{\mathcal{C}_{n,k}}. \tag{23}$$

In (23), the common communication capacity is constrained, which ensures the communication system has a basic performance rather than burns it out for security. From (23), we can see that the capacity of IoT node is concerned with the power allocation, satellite transmit precoding, and the level of spectral overlapping. Particularly, in these domain, i.e., power domain, frequency domain, and spatial domain, the secrecy rate performance is also affected by their distribution in these domain based on the above. To address the secrecy rate performance of satellite downlink and guarantee its common communication capacity, the framework of multi-domain resource optimization can be conducted.

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

$$\mathcal{P}2: \quad \max_{\mathbf{W}_{n,k},c_i} \log_2 e\cdot\sum_k\left(x_{n,k}-y_{n,k}-z_{n,k}+v_{n,k}\right) \tag{24}$$

$$\text{s.t.:} \quad (10c, 10d, 10e, 17, 20, 21, 22, 23) \tag{24a}$$

$$\mathrm{Tr}\left(\mathbf{W}_{n,k}\right) \leq P_S, \tag{24b}$$

$$\mathbf{W}_{n,k} \succeq \mathbf{0}. \tag{24c}$$

From $\mathcal{P}2$, it can be observed that there is a term of multi-variable product in the constraints of $\mathcal{P}2$, which indicates $\mathcal{P}2$ is still non-convex. To address the non-convexity due to the form of multi-variable product, we propose an alternating iterative optimization approach to conduct the joint optimization of beamforming, bandwidth overlapping, and power allocation. In addition, since $\mathbf{W}_{n,k} = \mathbf{w}_{n,k}\mathbf{w}_{n,k}^{\dagger}$, thus $\mathrm{rank}(\mathbf{W}_{n,k}) = 1$, however which is relaxed by the SDR in $\mathcal{P}2$ and it is a general operation for optimizing quadratic polynomials.

B. AO-SCA Approach For Multi-resource Optimization

To carry out the algorithm for solving $\mathcal{P}2$, the optimization variables are first merged. To replace both the optimization variables $P_{n,i}$ and $\mathbf{W}_k$, we define

$$\omega_{n,i} = P_{n,i}\mathbf{W}_{n,k}, \tag{25}$$

and keep (24b) in mind, (25) is constrained by

$$\sum_i \mathrm{Tr}\left(\omega_i\right) \leq P_S. \tag{26}$$

Considering the precoding vector Implies a condition represented as

$$\left\|\mathbf{W}_{n,k}\right\|^2 = 1, k = 1, ..., M. \tag{27}$$

(10b) and (10c), the merged variable ω_i can be constrained by $\sum_i \mathrm{Tr}\left(\omega_i\right) \leq P_S$.

Since the product term of $\omega_{n,i}$ and c_i still exists, thus a two-stage alternating iteration optimization approach can be conducted to find the solutions. For the first stage, the problem for solving $\omega_{n,i}$ can be represented as

$$\mathcal{P}3: \quad \max_{\omega_{n,i}} \log_2 e \cdot \big(\sum_k x_{n,k} - y_{n,k} - z_{n,k} + v_{n,k}\big) \tag{28}$$

$$\text{s.t.:} \quad \left(2^{\mathcal{C}_{n,k}} - 1\right) \sum_{i\neq k, i=0}^{M-1} \omega_{n,i}\mathbf{H}_{n,k}c_i - \omega_{n,k}\mathbf{H}_{n,k} \leq 1 - 2^{\mathcal{C}_{n,k}}, \tag{28a}$$

$$e^{x_n} \leq 1 + \left(1 - c_i\right)\omega_{n,k}\mathbf{H}_{n,k} + \sum_{i=0}^{M-1} \omega_{n,i}\mathbf{H}_{n,k}c_i, \tag{28b}$$

$$e^{\tilde{y}_{n,k}}\left(y_{n,k} - \tilde{y}_{n,k} + 1\right) \geq \sum_{i\neq k, i=0}^{M-1} \omega_{n,i}\mathbf{H}_{n,k}c_i + 1, \tag{28c}$$

$$e^{z_{n,k}}\left(z_{n,k} - \tilde{z}_{n,k} + 1\right) \geq 1 + \left(1 - c_i\right)\omega_{n,k}\mathbf{G}_{n,k} + \sum_{i=0}^{M-1} \omega_{n,i}\mathbf{G}_{n,k}c_i, \tag{28d}$$

$$e^{v_{n,k}} \leq 1 + \sum_{i\neq k, i=0}^{M-1} \omega_{n,i}\mathbf{G}_{n,k}c_i, \tag{28e}$$

$$\sum_i \mathrm{Tr}\left(\omega_i\right) \leq P_S, \tag{28f}$$

$$\omega_i \succeq \mathbf{0}. \tag{28g}$$

Theorem 1. *For any feasible solution of $\mathcal{P}3$, the rank of ω_i is 1.*

Proof. The proof of Theorem 1 can be seen in appendix A. ■

It can be found that $\mathcal{P}3$ is convex and it can be solved by CVX tool when c_i is given, and $\tilde{y}_{n,k}$ and $\tilde{z}_{n,k}$ are initialized. We assume $\omega_{n,i}^{\circ}$ to be the solution of $\mathcal{P}3$ and it can be substituted into $\mathcal{P}2$ to conduct the second stage optimization for solving c_i. Particularly, with $\omega_{n,i}^{\circ}$ output from the first stage, $\mathcal{P}2$ can be rewritten as

$$\mathcal{P}4: \quad \max_{c_i} \log_2 e \cdot \big(\sum_k x_{n,k} - y_{n,k} - z_{n,k} + v_{n,k}\big) \tag{29}$$

$$\text{s.t.:} \quad \left(2^{\mathcal{C}_{n,k}} - 1\right) \sum_{i\neq k, i=0}^{M-1} \mathbf{H}_{n,k}\omega_{n,i}^{\circ}c_i - \mathbf{H}_{n,k}\omega_{n,k}^{\circ} \leq 1 - 2^{\mathcal{C}_{n,k}}, \tag{29a}$$

$$e^{x_n} \leq 1 + \left(1 - c_i\right)\omega_{n,k}^{\circ}\mathbf{H}_{n,k} + \sum_{i=0}^{M-1} \omega_{n,i}\mathbf{H}_{n,k}c_i, \tag{29b}$$

$$e^{\tilde{y}_{n,k}}\left(y_{n,k} - \tilde{y}_{n,k} + 1\right) \geq 1 + \sum_{i\neq k, i=0}^{M-1} \omega_{n,i}\mathbf{H}_{n,k}c_i, \tag{29c}$$

$$e^{z_{n,k}}\left(z_{n,k} - \tilde{z}_{n,k} + 1\right) \geq 1 + \left(1 - c_i\right)\omega_{n,k}^{\circ}\mathbf{G}_{n,k} + \sum_{i=0}^{M-1} \omega_{n,i}\mathbf{G}_{n,k}c_i, \tag{29d}$$

$$e^{v_{n,k}} \leq 1 + \sum_{i\neq k, i=0}^{M-1} \omega_{n,i}^{\circ}\mathbf{G}_{n,k}c_i, \tag{29e}$$

$$0 \leq c_i \leq 1, \tag{29f}$$

where (29f) can be obtained by using (8)

$$0 \leq c_i \leq \left|\frac{\mathrm{sinc}\left(\alpha\left(i-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(i-k\right)/M\right)}\right|^2 \leq 1. \tag{30}$$

Therefore, $\mathcal{P}4$ is also convex and which can be solved by CVX tool. Particularly, we conduct the completed algorithm as shown in Algorithm 1 at the top of the next page. Particularly, a two-stage SCA-based optimization algorithm is executed, where in each iteration the $\mathcal{P}3$ is solved for obtaining feasible $\omega_{n,i}^{\circ}$ in the first stage and the $\mathcal{P}4$ is solved for obtaining feasible c_i° in the second stage with the input of feasible $\omega_{n,i}^{\circ}$. The tolerance ϵ is set in the two-stage optimization procedure to find near-optimal solutions. Then the output c_i° from the second stage updates the inputs in next iteration. Thus an alternating optimization between both two-stage optimizations is realized and our proposed AO-SCA based multi-domain resource optimization approach is carried out completely. Finally, we have $P_{n,i}^* = \left\|\omega_{n,i}^*\right\|^2$ and $\mathbf{w}_{n,i}^* = \frac{\omega_{n,i}^*}{P_{n,i}^*}$.

Complexity analysis: The AO-SCA based multi-domain resource optimization algorithm is carried out by two-stage optimizations for solving $\mathcal{P}3$ and $\mathcal{P}4$ alternatively. To solve $\mathcal{P}3$, we adopt the cvx tool and carry out the SCA based approach, where the main computational complexity is solving the convex approximation problem in each iteration. Considering the semi-definite programming solver for solving $\omega_{n,i}^{\circ}$ in each iteration, the computational complexity 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 the first stage can be calculated as $t \cdot (\mathcal{O}((6MN+N)^4) + log(1/\epsilon))$, where t is the iteration number in this stage. Whereas for solving $\mathcal{P}4$ with obtaining c_i°, the complexity of the first stage can be calculated as $\mu \cdot (\mathcal{O}(6MNlog(1/\epsilon)))$. Finally, the total complexity of AO-SCA can be calculated as $I^{\max}[t \cdot (O((6MN+N)^4) +$

Algorithm 1: AO-SCA based Multi-domain Resource Optimization

Input: $\{\mathcal{C}_{n,k}\}, P_S$.
Result: $\{\mathbf{w}^{\star}_{n,i}\}$, $\{c_i\}$,$\{P_{n,i}\}$.
Initialization: initial values for $\tilde{y}_{n,k}, \tilde{z}_{n,k}, c_i$: $\left\{\tilde{y}_k^0\right\}, \left\{\tilde{z}_k^0\right\}, \left\{\tilde{c}_i^0\right\}$.
repeat
  Set step $t = 1$;
  repeat
    Using the CVX solver sedumi to solve $\mathcal{P}3$;
    Output: $\left\{x^{\circ}_{n,k}\right\}, \left\{y^{\circ}_{n,k}\right\}, \left\{z^{\circ}_{n,k}\right\}, \left\{v^{\circ}_{n,k}\right\}, \left\{\omega^{\circ}_{n,k}\right\}$;
    Obtain $R^t_{s,sum} = \sum_{k=1}^{M} x^{\circ}_{n,k} - y^{\circ}_{n,k} - z^{\circ}_{n,k} + v^{\circ}_{n,k}$.
    Update $\left\{\tilde{y}^t_{n,k} = y^{\circ}_{n,k}, \tilde{z}^t_{n,k} = z^{\circ}_{n,k}\right\}$.
  until $\left|R^t_{s,sum} - R^{t-1}_{s,sum}\right| < \epsilon$;
  Set step $\mu = 1$;
  repeat
    Using the CVX solver sedumi to solve $\mathcal{P}4$;
    Output: $\left\{x^{\circ}_{n,k}\right\}, \left\{y^{\circ}_{n,k}\right\}, \left\{z^{\circ}_{n,k}\right\}, \left\{v^{\circ}_{n,k}\right\}, \{c_i^{\circ}\}$;
    Obtain $R^{\mu}_{s,sum} = \sum_{k=1}^{M} x^{\circ}_{n,k} - y^{\circ}_{n,k} - z^{\circ}_{n,k} + v^{\circ}_{n,k}$.
    Update $\left\{\tilde{y}^{\mu}_{n,k} = y^{\circ}_{n,k}, \tilde{z}^{\mu}_{n,k} = z^{\circ}_{n,k}\right\}$.
  until $\left|R^{\mu}_{s,sum} - R^{\mu-1}_{s,sum}\right| < \epsilon$;
until $\left|R^t_{s,sum} - R^{\mu}_{s,sum}\right| \leq \varepsilon$;
Procedure End

$log(1/)) + \mu \cdot (O(6MNlog(1/)))]log(1/\varepsilon)$, and $I^{\max}$ is the number of alternating iteration between these two stages of optimizations.

C. Joint Optimization of Power Allocation and Spectral Multiplexing

MRT and ZF based precoding as fixed precoding schemes have been widely used to enhance the link transmission or suppress the signal leakage in multi-antenna systems, which are usually adopted as benchmarks in researches with beamforming and precoding [36], [37]. However, by using the fixed precoding scheme, our formulated problem is still not easy to find the optimal solution. In this section, we aim to fix the spatial dimension and another multi-domain optimization is carried out to address the primal problem in other dimensions, i.e., power domain and frequency domain.

For the reference propose, we first adopt MRT/ZF-based precoding and jointly optimize the power allocation and the bandwidth multiplexing to solve the primal problem to maximize the sum secrecy rate of IoT nodes. Particularly, MRT/ZF-based precoding vectors are represented as $\mathbf{w}^{mrt}_{n,k} = \mathbf{h}_{n,k}/\left\|\mathbf{h}_{n,k}\right\|$, and $\mathbf{w}^{zf}_{n,k} = \mathbf{f}_0/\|\mathbf{f}_0\|$, where $\mathbf{f}_0 = \left(\mathbf{I}_M - \mathbf{g}_{n,k}\left(\mathbf{g}^{\dagger}_{n,k}\mathbf{g}_{n,k}\right)^{-1}\mathbf{g}^{\dagger}_{n,k}\right)\mathbf{h}_{n,k}$, respectively, [38]–[40].

When the $\mathbf{W}_k$ is fixed and a new variable $\beta_k = P_{n,k}c_k$ is introduced, $\mathcal{P}2$ can be reformulated as

$$\mathcal{P}5: \max_{p_{n,k},\beta_k} \quad \log_2 e \cdot \Big(\sum_k x_{n,k} - y_{n,k} - z_{n,k} + v_{n,k}\Big) \quad (31)$$

$$\text{s.t.: } \left(2^{\mathcal{C}_{n,k}} - 1\right)\left(1 + \sum_{i\neq k, i=0}^{M-1} \mathbf{H}_{n,k}\mathbf{W}_{n,i}\beta_i\right) \leq P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}, \quad (31a)$$

$$e^{x_{n,k}} \leq 1 + P_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,k} + \sum_{i=0, i\neq k}^{M-1} \beta_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}, \quad (31b)$$

$$e^{\tilde{y}_{n,k}}\left(y_{n,k} - \tilde{y}_{n,k} + 1\right) \geq 1 + \sum_{i\neq k, i=0}^{M-1} \beta_{n,i}\mathbf{H}_{n,k}\mathbf{W}_{n,i}, \quad (31c)$$

$$e^{z_{n,k}}\left(z_{n,k} - \tilde{z}_{n,k} + 1\right) \geq$$
$$1 + P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k} + \sum\nolimits_{i=0, i\neq k}^{M-1} \beta_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,i}, \quad (31d)$$

$$e^{v_{n,k}} \leq 1 + \sum_{i\neq k, i=0}^{M-1} \beta_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,i}, \quad (31e)$$

$$\sum_k P_{n,k} \leq Ps, \quad (33f)$$

$$0 \leq \beta_k \leq P_{n,k}. \quad (31g)$$

By using the MRT/ZF-based precoding vectors, two approaches that jointly optimize the power allocation and the bandwidth multiplexing with MRT and ZF based precoding can be carried out to solve $\mathcal{P}5$. Particularly, it can be seen that β_k and $P_{n,k}$ can be simultaneously optimized. Since the Taylor expansion is adopted, similarly the SCA-based joint optimization of power allocation and bandwidth multiplexing is proposed to realized these two approaches and the algorithm is depicted as shown in the following Algorithm 2.

Algorithm 2: SCA-based Joint Optimization of Power Allocation and Spectral Multiplexing

Input: $\{\mathcal{C}_{n,k}\}, P_S, \{\mathbf{w}_{n,i}\}$.
Result: $\{c_i\}$,$\{P_{n,i}\}$.
Initialization: initial values for $\tilde{y}_{n,k}, \tilde{z}_{n,k}$: $\left\{\tilde{y}_k^0\right\}, \left\{\tilde{z}_k^0\right\}$.
Set step $t = 1$;
repeat
  Using the CVX solver sedumi to solve $\mathcal{P}5$;
  Output: $\left\{x^{\circ}_{n,k}, y^{\circ}_{n,k}, z^{\circ}_{n,k}, v^{\circ}_{n,k}, \beta^{\circ}_{n,k}, P^{\circ}_{n,k}\right\}$;
  Obtain $R^t_{s,sum} = \sum_{k=1}^{M} x^{\circ}_{n,k} - y^{\circ}_{n,k} - z^{\circ}_{n,k} + v^{\circ}_{n,k}$.
  Update $\left\{\tilde{y}^t_{n,k} = y^{\circ}_{n,k}, \tilde{z}^t_{n,k} = z^{\circ}_{n,k}\right\}$.
until $\left|R^t_{s,sum} - R^{t-1}_{s,sum}\right| < \epsilon$;
Procedure End

D. Joint Optimization of Power Allocation and Precoding

We fix the multiplexing scheme to conduct the joint optimization of power allocation and precoding for solving the problem of sum secrecy rate. Without loss of generality, orthogonal multiplexing access (OMA) [41], [42], is adopted

in this section, then we have $\alpha = 0$ and $c_i = 0$. In this case, the equivalent optimization problem can be formulated as

$$\mathcal{P}6: \quad \max_{\omega_{n,k}} \log_2 e \cdot \Big(\sum_k x_{n,k} - y_{n,k} - z_{n,k} + v_{n,k}\Big) \tag{32}$$

$$\text{s.t.:} \quad -\omega_{n,k}\mathbf{H}_{n,k} \le 1 - 2^{\mathcal{C}_{n,k}}, \tag{32a}$$

$$e^{x_n} \le 1 + \omega_{n,k}\mathbf{H}_{n,k}, \tag{32b}$$

$$e^{\tilde{y}_{n,k}}\left(y_{n,k} - \tilde{y}_{n,k} + 1\right) \ge 1, \tag{32c}$$

$$e^{z_{n,k}}\left(z_{n,k} - \tilde{z}_{n,k} + 1\right) \ge 1 + \omega_{n,k}\mathbf{G}_{n,k}, \tag{32d}$$

$$e^{v_{n,k}} \le 1, \tag{32e}$$

$$\sum_i \mathrm{Tr}\left(\omega_i\right) \le P_S, \tag{32f}$$

$$\omega_i \succeq \mathbf{0}. \tag{32g}$$

To solve the problem $\mathcal{P}6$, the algorithm of SCA-based joint optimization of power allocation and precoding can be carried out as shown in Algorithm 3.

Algorithm 3: SCA-based Joint Optimization of Power Allocation and Precoding

Input: $\{\mathcal{C}_{n,k}\}, P_S, \alpha$.
Result: $\{\mathbf{W}_{n,k}\}$,$\{P_{n,i}\}$.
Initialization: initial values for $\tilde{y}_{n,k}, \tilde{z}_{n,k}$: $\left\{\tilde{y}_k^0\right\}, \left\{\tilde{z}_k^0\right\}$.
Set step $t = 1$;
repeat
  Using the CVX solver sedumi to solve $\mathcal{P}6$;
  Output: $\left\{x_{n,k}^\circ, y_{n,k}^\circ, z_{n,k}^\circ, v_{n,k}^\circ, \beta_{n,k}^\circ, P_{n,k}^\circ\right\}$;
  Obtain $R_{s,sum}^t = \sum_{k=1}^{M} x_{n,k}^\circ - y_{n,k}^\circ - z_{n,k}^\circ + v_{n,k}^\circ$.
  Update $\left\{\tilde{y}_{n,k}^t = y_{n,k}^\circ, \tilde{z}_{n,k}^t = z_{n,k}^\circ\right\}$.
until $\left|R_{s,sum}^t - R_{s,sum}^{t-1}\right| < \epsilon$;
Procedure End

IV. Numerical Results

In this section, we carry out extensive simulations to evaluate the secrecy rate performance of multi-domain resource multiplexing based secure transmission for satellite supporting IoT networks. Particularly, the impact of satellite transmission power, number of satellite transmit antenna, number of IoT nodes in a beam, and correlation coefficient on the maximum sum secrecy rate are evaluated, respectively. Besides, the convergence of our proposed algorithm is also evaluated. In addition, the system parameters are set in Table II, where the satellite channel model and main parameters setting reference related works in [31], [33]. Specifically, the height of LEO satellite is 600 Km, carrier frequency is 2 GHz, the maximum beam gain is set to 46.6 dB, and the rain attenuation parameter $\mu_{\zeta_{dB}}$ = -3.152 and $\delta^2 = 1.6$, and the 3 dB angle (for all beams) is set to 0.4°.

In Fig. 3, the impact of satellite transmission power on the maximum sum secrecy rate is evaluated. From Fig. 3, it can be seen that the sum secrecy rate monotonously increases as satellite transmission power and our proposed multi-resource optimization scheme outperforms the benchmarks. This is because that more power can be used to design the co-channel interference by the AO-SCA algorithm as the satellite transmission power increases, where more interference can be designed to damage the Eve. Since the ZF-based precoding scheme results in signal leakage, the received SINR of wire-tapping channel is damaged and meanwhile the signal quality of main channel is weakened. Whereas, for the MRT-based precoding scheme, the signal quality in the main channel is enhanced, as well as it in the wiretapping channel due to the channel similarity. Besides, comparing with the approach that jointly optimizes both power allocation and precoding based on OMA, it indicates that the interference due to spectral overlapping benefits the secrecy rate performance, and the gain of sum secrecy rate increases as satellite transmission power. In addition, the larger the maximum sum secrecy rate is achieved when the channel estimation error is smaller. This is because the precoding vector from AO-SCA algorithm would lead to the leakage of legitimate signal and the IUI could not suppress the Eve well when the channel estimation is error.

Fig. 4 shows the impact of satellite transmit antenna number on the maximum sum secrecy rate, which shows the sum secrecy rate monotonously increases as the number of transmit antennas. This is because our proposed approach can focus

TABLE II
Simulation Parameters

System Parameters	Numerical Value
Satellite height	600 Km
Carrier frequency	2 GHz
Maximum beam gain	46.6 dB
3 dB angle (for all beams)	0.4°
Rain attenuation parameters	$\mu_{\zeta_{dB}}$ = -3.152, $\delta^2 = 1.6$
Channel estimation error	0, 0.2, 0.5
Speed of wave	$3 * 10^8$ m/s
Noise power spectral density	-174 dBm/Hz

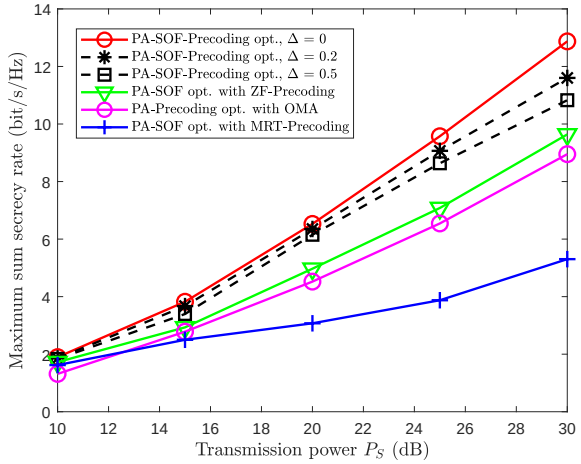

Fig. 3. The impact of satellite transmission power on the maximum sum secrecy rate. ($N = 4, M = 2, \mathcal{C}_{n,k}$ = 1bit/s/Hz)

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2023.3250227

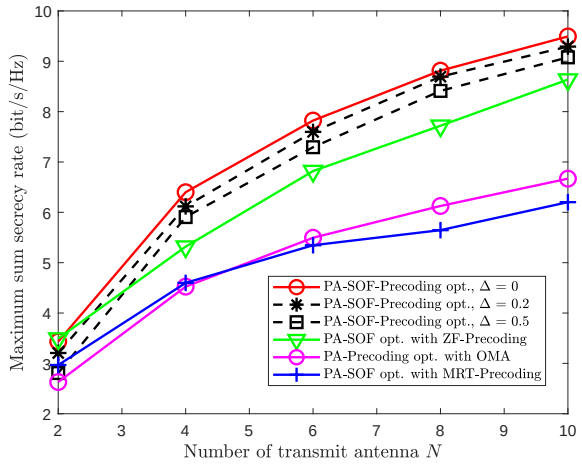

Fig. 4. The impact of satellite transmit antenna number on the maximum sum secrecy rate. ($P_S = 20$dB, $M = 2, \mathcal{C}_{n,k} = 2$bit/s/Hz)

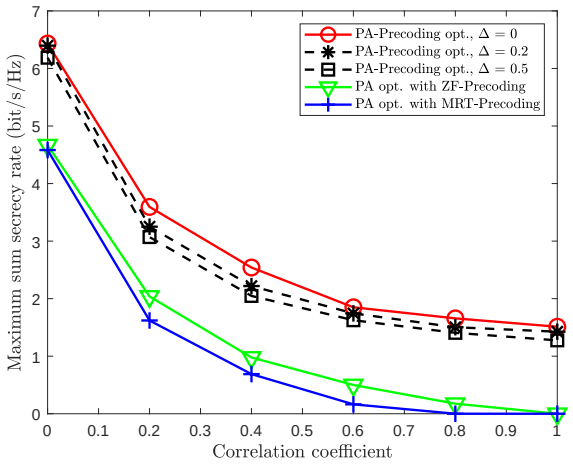

Fig. 6. The impact of correlation coefficient on the maximum sum secrecy rate. ($P_S = 20$dB, $N = 4, M = 2, \mathcal{C}_{n,k} = 1$bit/s/Hz)

more centralized to confuse the Eve and enhance the main satellite links as the number of transmit antennas, where the interference can be well designed to confuse the Eve. For the fixed precoding approaches, although the signal leakage can be suppressed to a certain extent with ZF-based precoding and the signal of main channel can be strengthened with MRT-based precoding as the number of transmit antennas increases, respectively, however the interference for damaging the Eve is not well controlled.

Fig. 5 and Fig. 6 show the impact of the number of IoT nodes and the correlation coefficient due to bandwidth overlapping on the maximum sum secrecy rate, respectively. From Fig. 5, it can be seen that the sum secrecy rate is monotonously increasing of the number of IoT nodes. Particularly, our proposed approach shows superior advantages in the sum secrecy rate performance. This is because the more inter-user interference can be used to damage the Eves as the number of IoT nodes increases. In Fig. 6, the correlation coefficient reflects the level of spectral overlapping between adjacent channels from satellite to IoT nodes, where we can see that the sum secrecy rate decreases as the correlation coefficient. This is because the capacity of main channel is affected by the co-channel interference and this effect surpasses it on the wiretapping channel. In addition, it is observed that sum secrecy rate performance decreases as the channel estimation error increases. Similarly, our proposed approach outperforms the benchmarks, since the signal leakage by the ZF-based precoding and the received signal of wiretapping channel can be also strengthened by the MRT-based precoding, while slight interference can be used to confuse the Eve based on OMA.

In addition, the convergence of our proposed AO-SCA approach for maximizing the secrecy rate is evaluated in Fig. 7. From Fig. 7, it can be seen that the AO-SCA algorithm has fast convergence speed, which indicates low complexity. The convergences in each stage of alternating procedures are also evaluated in Fig. 7, where both the SCA-based joint optimization of power allocation and precoding and the SCA-

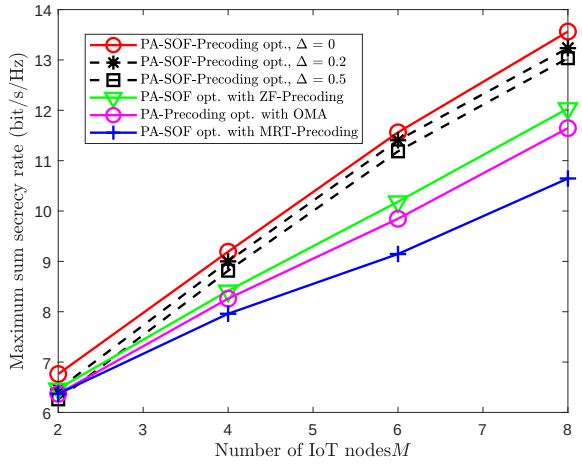

Fig. 5. The impact of number of IoT nodes on the maximum sum secrecy rate. ($P_S = 20$dB, $N = 4, \mathcal{C}_{n,k} = 2$bit/s/Hz)

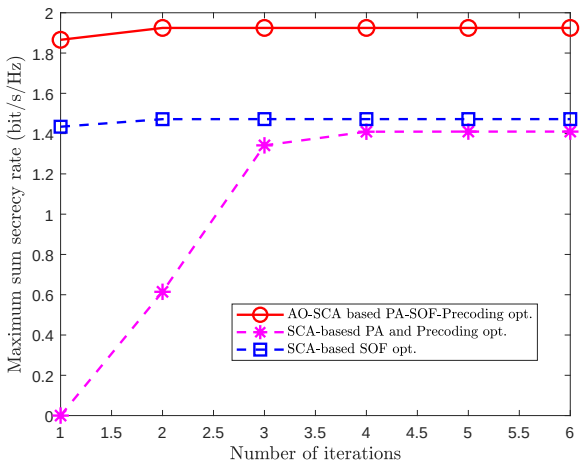

Fig. 7. The convergence of AO-SCA for maximizing the sum secrecy rate.

based spectral multiplexing optimization have good convergence performance.

V. Conclusions

In this work, the secure transmission in satellite-supported IoT networks has been investigated. To address the channel similarity between satellite downlinks and the limited resource at satellite side, the multi-domain resource multiplexing scheme has been proposed to achieve the physical layer security. Particularly, the co-channel interference is created by the spectral overlapping among satellite downlink multichannel in frequency domain, which is leveraged to be designed for confusing the Eve. Based on this, the multi-domain resource optimization has been conducted to maximize the sum secrecy rate of IoT nodes, where the power allocation of downlink transmission, the level of spectral overlapping, and the multi-antenna precoding are jointly optimized. To solve the formulated problem, the Taylor expansion and SDR have been adopted to reformulate it into a solvable bi-convex problem and a two-stage AO-SCA approach has been proposed to find the near-optimal solution. To verify the efficiency of our proposed approach, extensive simulations have been carried out and the performance of sum secrecy rate has been evaluated. Results reveal that the multi-domain resource multiplexing scheme can assist the implementation of physical layer security in satellite-supported IoT networks. For future work, the dimension of multi-domain can be extended, e.g., time domain and code domain, and a new framework addressing secure transmission could be realized.

Appendix A
Proof of Theorem 1

Proof. The Lagrangian function of $\mathcal{P}3$ can be obtained as shown in (33) at the bottom of this page. Based on (33), we take the partial derivative of $\mathcal{L}(\cdot)$ with respect to $\omega_{n,k}$ and apply KKT conditions as follows

$$\mathbf{A}-\mathbf{U}=\ell\mathbf{H}_{n,k}+\rho\sum_{i\neq k,i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i, \tag{34}$$

$$\mathbf{U}\omega_i=\mathbf{0}, \tag{35}$$

$$\mathbf{U}\succeq\mathbf{0}, \tag{36}$$

where

$$\ell=\lambda+(1-c_i)\,\theta+\theta\sum\nolimits_i c_i, \tag{37}$$

and

$$\mathbf{A}=\tau\mathbf{I}+\left(\lambda\left(2^{C_{n,k}}-1\right)+\varphi\right)\sum_{i\neq k,i=0}^{M-1}\mathbf{H}_{n,k}c_i + (1-c_i)\,\xi\mathbf{G}_{n,k}+\xi\sum_{i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i, \tag{38}$$

and we can see that $\mathbf{A}\succ\mathbf{0}$.

By post-multiplying ω_i at both sides of (34), we have

$$\mathbf{A}\omega_k=\big(\ell\mathbf{H}_{n,k}+\rho\sum_{i\neq k,i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i\big)\omega_k. \tag{39}$$

Thus,

$$\begin{aligned}rank\left(\omega_k\right)&=rank\left(\mathbf{A}\omega_k\right)\\&\leq rank\left(\mathbf{H}_{n,k}\right)+rank\left(\mathbf{G}_{n,k}\right)\\&\leq 2,\end{aligned} \tag{40}$$

Besides, by denoting

$$\mathbf{B}=\mathbf{A}-\big(\lambda+\big(1-c_i\big)\theta+\theta\sum_{i=0}^{M-1}c_i\big)\mathbf{H}_{n,k}, \tag{41}$$

based on (34), we have

$$\mathbf{B}\omega_k=\rho\sum_{i\neq k,i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i\omega_k. \tag{42}$$

From (42), the rank of matrix can be obtained as

$$\begin{aligned}rank\left(\mathbf{B}\omega_k\right)&=rank\big(\rho\sum_{i\neq k,i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i\omega_k\big)\\&\leq rank\left(\mathbf{G}_{n,k}\right)=1,\end{aligned} \tag{43}$$

and if the following is achieved, i.e.,

$$rank\left(\mathbf{B}\omega_k\right)=rank\left(\rho\sum_{i\neq k,i=0}^{M-1}\frac{P_{n,i}}{P_{n,k}}\mathbf{G}_{n,k}c_i\omega_k\right)=1, \tag{44}$$

we have

$$rank\left(\mathbf{B}\right)\leq 1. \tag{45}$$

$$\begin{aligned}\mathcal{L}\left(\lambda,\theta,\varphi,\xi,\tau\right)&=\log_2 e\cdot\Big(\sum_k x_{n,k}-y_{n,k}-z_{n,k}+v_{n,k}\Big)+\lambda\big(\big(2^{C_{n,k}}-1\big)\sum_{i\neq k,i=0}^{M-1}\omega_{n,i}\mathbf{H}_{n,k}c_i-\omega_{n,k}\mathbf{H}_{n,k}-1+2^{C_{n,k}}\big)\\&-\varphi(e^{\tilde{y}_{n,k}}\left(y_{n,k}-\tilde{y}_{n,k}+1\right)-1-\sum_{i\neq k,i=0}^{M-1}\omega_{n,i}\mathbf{H}_{n,k}c_i)+\theta(e^{x_n}-1-(1-c_i)\omega_{n,k}\mathbf{H}_{n,k}-\sum_{i=0}^{M-1}\omega_{n,i}\mathbf{H}_{n,k}c_i)-\mathbf{U}\omega_i\\&-\xi(e^{z_{n,k}}\left(z_{n,k}-\tilde{z}_{n,k}+1\right)-1-\left(1-c_i\right)P_{n,k}\mathbf{G}_{n,k}\mathbf{W}_{n,k}-\sum_{i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i)+\tau(\sum_i\mathrm{Tr}\left(\omega_i\right)-P_S)\\&+\rho(e^{v_{n,k}}-1-\sum_{i\neq k,i=0}^{M-1}P_{n,i}\mathbf{G}_{n,k}\mathbf{W}_{n,k}c_i).\end{aligned} \tag{33}$$

According to the following property of inequality

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

However, based on (41), the constraint is

$$N - 1 \leq rank\left(\mathbf{B}\right) \leq N, \tag{47}$$

which conflicts with (45). Therefore, in (43)

$$rank\left(\mathbf{B}\omega_k\right) = 0, \tag{48}$$

and (46) is rewritten as

$$rank\left(\mathbf{B}\right) + rank\left(\omega_k\right) \leq N. \tag{49}$$

By considering (49) and (47), the rank of ω_k indicates

$$rank\left(\omega_k\right) = 1. \tag{50}$$

Thus, the proof is completed. ■

REFERENCES

[1] N. Cheng, J. He, Z. Yin, C. Zhou, H. 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, 2021.

[2] B. Mao, F. Tang, Y. Kawamoto, and N. Kato, "Optimizing computation offloading in satellite-UAV-served 6G IoT: A deep learning approach," *IEEE Netw.*, vol. 35, no. 4, pp. 102–108, 2021.

[3] Q. Wu, W. Wang, Z. Li, B. Zhou, Y. Huang, and X. Wang, "Spectrum-chain: A disruptive dynamic spectrum-sharing framework for 6G," *Sci. China Inf. Sci.*, vol. 66, no. 130302, pp. 1–14, 2023.

[4] T. Chen, J. Liu, Q. Ye, Q. Tang, W. Zhang, T. Huang, and Y. Liu, "Efficient uplink transmission in ultra-dense leo satellite networks with multiband antennas," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1373–1377, 2022.

[5] R. Deng, B. Di, H. Zhang, L. Kuang, and L. Song, "Ultra-dense LEO satellite constellations: How many LEO satellites do we need?" *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4843–4857, 2021.

[6] N. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, and X. Shen, "Space/aerial-assisted computing offloading for IoT applications: A learning-based approach," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1117–1129, 2019.

[7] D. A. Tubiana, J. Farhat, G. Brante, and R. D. Souza, "Q-learning NOMA random access for IoT-satellite terrestrial relay networks," *IEEE Wireless Commun. Lett.*, 2022.

[8] N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. Shen, "Big data driven vehicular networks," *IEEE Netw.*, vol. 32, no. 6, pp. 160–167, 2018.

[9] H. Yang, M. Hernández-Pajares, W. Jarmołowski, P. Wielgosz, S. L. Vadas, O. L. Colombo, E. Monte-Moreno, A. Garcia-Rigo, V. Graffigna, A. Krypiak-Gregorczyk, B. Milanowska, P. Bofill-Soliguer, G. Olivares-Pulido, Q. Liu, and R. Haagmans, "Systematic detection of anomalous ionospheric perturbations above LEOs from GNSS POD data including possible tsunami signatures," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, pp. 1–23, 2022.

[10] W.-B. Sun, W.-X. Meng, J.-C. Guo, and C. Li, "Fairness-based resource allocation for multiple weights opportunistic beamforming in internet of things networks," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10 022–10 035, 2022.

[11] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, and R. Prasad, "Satellite communications supporting internet of remote things," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 113–123, 2016.

[12] B. Manzoor, A. Al-Hourani, and B. A. Homssi, "Improving iot-over-satellite connectivity using frame repetition technique," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 736–740, 2022.

[13] Z. Zhang, Y. Li, C. Huang, Q. Guo, L. Liu, C. Yuen, and Y. L. Guan, "User activity detection and channel estimation for grant-free random access in leo satellite-enabled internet of things," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8811–8825, 2020.

[14] V. Nallarasan and K. Kottilingam, "Spectrum management analysis for cognitive radio iot," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1–5.

[15] A. Rana, A. Taneja, and N. Saluja, "Accelerating IoT applications new wave with 5G: A review," *Mater. Today:. Proc.*, 2021.

[16] J. Zhang, C. Shen, H. Su, M. T. Arafin, and G. Qu, "Voltage over-scaling-based lightweight authentication for iot security," *IEEE Trans. Comput.*, vol. 71, no. 2, pp. 323–336, 2021.

[17] N. Cassiau, G. Noh, S. Jaeckel, L. Raschkowski, J.-M. Houssin, L. Combelles, M. Thary, J. Kim, J.-B. Doré, and M. Laugeois, "Satellite and terrestrial multi-connectivity for 5G: making spectrum sharing possible," in *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2020, pp. 1–6.

[18] F. Guidolin and M. Nekovee, "Investigating spectrum sharing between 5G millimeter wave networks and fixed satellite systems," in *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2015, pp. 1–7.

[19] P. Gu, R. Li, C. Hua, and R. Tafazolli, "Dynamic cooperative spectrum sharing in a multi-beam LEO-GEO co-existing satellite system," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 1170–1182, 2022.

[20] N. F. Kiyani, V. Sridharan, and G. Dolmans, "Co-channel interference mitigation technique for non-coherent ook receivers," *IEEE Wireless Commun. Lett.*, vol. 3, no. 2, pp. 189–192, 2014.

[21] S. W. Kim, Y. J. Chun, and S. Kim, "Co-channel interference cancellation using single radio frequency and baseband chain," *IEEE Trans. Commun.*, vol. 58, no. 7, pp. 2169–2175, 2010.

[22] M. Velez, P. Angueira, D. De La Vega, A. Arrinda, and J. Ordiales, "Dvb-t ber measurements in the presence of adjacent channel and co-channel analogue television interference," *IEEE Trans. Broadcast.*, vol. 47, no. 1, pp. 80–84, 2001.

[23] Z. Sheng, H. D. Tuan, A. A. Nasir, H. V. Poor, and E. Dutkiewicz, "Physical layer security aided wireless interference networks in the presence of strong eavesdropper channels," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3228–3240, 2021.

[24] Y. Liu, W. Wang, H.-H. Chen, F. Lyu, L. Wang, W. Meng, and X. Shen, "Physical layer security assisted computation offloading in intelligently connected vehicle networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3555–3570, 2021.

[25] C.-Y. Yang, J.-F. J. Yao, C.-E. Yen, and M.-S. Hwang, "Overview on physical layer security in low earth orbit (leo) satellite system," in *2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. IEEE, 2021, pp. 1–2.

[26] 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.*, vol. 22, no. 2, pp. 1374–1387, Feb. 2023.

[27] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2488–2501, 2019.

[28] Z. Yin, N. Cheng, T. H. Luan, and P. Wang, "Physical layer security in cybertwin-enabled integrated satellite-terrestrial vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4561–4572, 2021.

[29] K. An, M. Lin, J. Ouyang, and W.-P. Zhu, "Secure transmission in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 3025–3037, 2016.

[30] 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, 2021.

[31] K. Guo, K. An, B. Zhang, Y. Huang, X. Tang, G. Zheng, and T. A. Tsiftsis, "Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5129–5141, 2020.

[32] 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.

[33] P. Series, "Propagation data and prediction methods required for the design of earth-space telecommunication systems," *Recommendation ITU-R*, pp. 618–12, 2015.

[34] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[36] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the miso downlink channel," *IEEE Trans. Signal Proce.*, vol. 63, no. 9, pp. 2239–2252, 2015.

[37] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 760–773, 2022.

[38] L. Wei, C. Huang, G. C. Alexandropoulos, C. Yuen, Z. Zhang, and M. Debbah, "Channel estimation for ris-empowered multi-user miso

wireless communications," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4144–4157, 2021.
[39] Z. Yin, N. Cheng, T. H. Luan, Y. Hui, and W. Wang, "Green interference based symbiotic security in integrated satellite-terrestrial communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9962–9973, 2022.
[40] F. Sohrabi, K. M. Attiah, and W. Yu, "Deep learning for distributed channel feedback and multiuser precoding in FDD massive MIMO," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4044–4057, 2021.
[41] Q. Zhang, K. Luo, W. Wang, and T. Jiang, "Joint C-OMA and C-NOMA wireless backhaul scheduling in heterogeneous ultra dense networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 874–887, 2020.
[42] N. Nomikos, T. Charalambous, D. Vouyioukas, G. K. Karagiannidis, and R. Wichman, "Hybrid NOMA/OMA with buffer-aided relay selection in cooperative networks," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 524–537, 2019.

Zhisheng Yin (M'20) received his Ph.D. degree from the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China, in 2020, and the B.E. degree from the Wuhan Institute of Technology, the B.B.A. degree from the Zhongnan University of Economics and Law, Wuhan, China, in 2012, and the M.Sc. degree from the Civil Aviation University of China, Tianjin, China, in 2016. From Sept. 2018 to Sept. 2019, Dr. Yin visited in BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently an Assistant Professor with School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include space-air-ground integrated networks, wireless communications, digital twin, and physical layer security.

Nan Cheng (M'16) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo in 2016, and B.E. degree and the M.S. degree from the Department of Electronics and Information Engineering, Tongji University, Shanghai, China, in 2009 and 2012, respectively. He worked as a Post-doctoral fellow with the Department of Electrical and Computer Engineering, University of Toronto, from 2017 to 2019. He is currently a professor with State Key Lab. of ISN and with School of Telecommunications Engineering, Xidian University, Shaanxi, China. His current research focuses on B5G/6G, space-air-ground integrated network, big data in vehicular networks, and self-driving system. His research interests also include performance analysis, MAC, opportunistic communication, and application of AI for vehicular networks.

Yilong Hui (M'18) received the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 2018. He is currently an Associate Professor with the State Key Laboratory of Integrated Services Networks, and with the School of Telecommunications Engineering, Xidian University, China. He has published over 50 scientific articles in leading journals and international conferences. His research interests include wireless communication, mobile edge computing, vehicular networks, intelligent transportation systems and autonomous driving. He was a recipient of the Best Paper Award Aof the International Conference WiCon2016 and IEEE Cyber-SciTech2017.

Wei Wang (M'19) received the PhD degree in Electrical and Electronic Engineering from Nanyang Technological University (NTU), Singapore, in 2018. From Sep. 2018 to Aug. 2019, he was a postdoctoral fellow at the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Currently, he is a Professor at Nanjing University of Aeronautics and Astronautics. His research interests include wireless communications, space-air-ground integrated networks, wireless security, and blockchain.

Lian Zhao (S'99-M'03-SM'06) received the Ph.D. degree from the Department of Electrical and Computer Engineering (ELCE), University of Waterloo, Canada, in 2002. She joined the Department of Electrical and Computer Engineering at Toronto Metropolitan University (formerly Ryerson University), Canada, in 2003. Her research interests are in the areas of wireless communications, resource management, mobile edge computing, caching and communications, and IoV networks.

She has been an IEEE Communication Society (ComSoc) and IEEE Vehicular Technology (VTS) Distinguished Lecturer (DL); received the Best Land Transportation Paper Award from IEEE Vehicular Technology Society in 2016, Top 15 Editor Award in 2016 for IEEE Transaction on Vehicular Technology, Best Paper Award from the 2013 International Conference on Wireless Communications and Signal Processing (WCSP), and the Canada Foundation for Innovation (CFI) New Opportunity Research Award in 2005.

She has been serving as an Editor for IEEE Transactions on Wireless Communications, IEEE Internet of Things Journal, and IEEE Transactions on Vehicular Technology (2013-2021). She served as a co-Chair of Wireless Communication Symposium for IEEE Globecom 2020 and IEEE ICC 2018; Finance co-Chair for 2021 ICASSP; Local Arrangement co-Chair for IEEE VTC Fall 2017 and IEEE Infocom 2014; co-Chair of Communication Theory Symposium for IEEE Globecom 2013. She has been a Board of Governor (BoG) committee member since 2023. She has severed as a panel expert in various federal, provincial, and international evaluation committees. She is a licensed Professional Engineer in the Province of Ontario and a senior member of the IEEE Communication Society and Vehicular Technology Society.

Khalid Aldubaikhy (S'10-M'19) is currently an assistant professor at Qassim University, Buraydah, Al-Qassim, Saudi Arabia. He received the B.E. degree from Qassim University, Saudi Arabia, in 2008, the M.A.Sc. degree in electrical and computer engineering from Dalhousie University, Halifax, NS, Canada, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2019. His research interests include millimeter-wave wireless networks, medium access control, impulse radio ultra-wideband, and millimeter-wave 5G cellular networks.

Abdullah Alqasir (M'22) received the Ph.D. degree in electrical engineering and computer engineering from Iowa State University, Ames, IA, USA, in 2019. He is currently an Assistant Professor with the Department of Electrical Engineering, Qassim University, Qassim, Saudi Arabia. His research interests include wireless networks, green communication, Internet of Things, and energy harvesting.