Secure Satellite-Terrestrial Transmission Over Incumbent Terrestrial Networks via Cooperative Beamforming

Jun Du, *Student Member, IEEE*, Chunxiao Jiang, *Senior Member, IEEE*, Haijun Zhang, *Senior Member, IEEE*, Xiaodong Wang, *Fellow, IEEE*, Yong Ren, *Senior Member, IEEE* and Mérouane Debbah, *Fellow, IEEE*

***Abstract*—In this paper, we consider a scenario where the satellite-terrestrial network is overlaid over the legacy cellular network. The established communication system is operated in the millimeter wave (mmWave) frequencies, which enables the massive antennas arrays to be equipped on the satellite and terrestrial base stations (BSs). The secure communication in this coexistence system of the satellite-terrestrial network and cellular network through the physical layer security techniques is studied in this work. To maximize the achievable secrecy rate of the eavesdropped fixed satellite service (FSS), we design a cooperative secure transmission beamforming scheme, which is realized through the satellite's adaptive beamforming, AN and BSs' cooperative beamforming implemented by terrestrial BSs. A non-cooperative beamforming scheme is also designed, according to which BSs implement the maximum ratio transmission (MRT) beamforming strategy. Applying the designed secure beamforming schemes to the coexistence system established, we formulate the secrecy rate maximization problems subjected to the power and transmission quality constraints. To solve the nonconvex optimization problems, we design an approximation and iteration based genetic algorithm, through which the original problems can be transformed into a series of convex quadratic problems. Simulation results show the impact of massive antenna arrays at the mmWave on improving the secure communication. Our results also indicate that through the cooperative and adaptive beamforming, the secrecy rate can be greatly increased. In addition, the convergence and efficiency of the proposed iteration based approximation algorithm are verified by the simulations.**

***Index Terms*—Satellite terrestrial networks, physical layer security, millimeter wave (mmWave) communication, cooperative beamforming.**

I. Introduction

Recently, the fifth generation (5G) of mobile communication is willing to bring an order of magnitude improvement for the network capacity, reliability, availability and security, and to satisfy the current dramatically increasing data traffic demands. To achieve these performance improvements, millimeter wave (mmWave) communication become a potential technology for the future outdoor wireless networks. Many recent studies have demonstrated that the mmWave communication is feasible and effective by using massive antenna arrays in conjunction with the adaptive beamforming technique. Due to its physical properties, the mmWave techniques can solve many problems brought by the high speed broadcast wireless transmission, such as compensating the propagation loss at high frequencies. Specifically, with much smaller wavelengths of mmWave frequencies, the mmWave techniques can reduce the size of the antenna array and enable the large arrays in a given area, and can support the directional beams to the receivers [1], [2].

On the other hand, satellite communication (SatCom) has become an outgrowth of the continuing demand for higher capacity, real-time communication and wider coverage, due to its unique ability to provide seamless connectivity and high data rate. In addition, SatCom is a more economical solution to provide a seamless and high speed connectivity than deploying other terrestrial networks, especially in some remote and sparsely populated locations. To support the higher data rate requirement, SatCom using the mmWave band, especially in Ka band (17.7 – 19.7 GHz for the downlink, and 27.5 – 29.5 GHz for the uplink), has been investigated for many years [3], [3], [4]. However, the Ka band ranged above has been primarily assigned to the terrestrial fixed service (FS) microwave links, according to Decision ECC/DEC/(00)07 adopted by the European Conference of Postal and Telecommunications Administrations (ECPT) [5]. Therefore, in order to share this non-exclusive spectrum, it is necessary to investigate the co-channel interference, cooperation beamforming schemes and many other issues in the coexistence system with SatCom and incumbent terrestrial networks to improve the system performance and efficiency of spectrum utilization, and reduce the energy consumption.

Currently, the on-going development of 5G communication brings an opportunity for ta seamless integration of SatCom with terrestrial networks. In addition, SatCom will play a vital role in the development and full realization of 5G [6]. However, resulting from the immense and open coverage, the transmission security in SatCom with fixed satellite service (FSS) is confronted with an increasing serious challenge,

J. Du is with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, P. R. China, and also with the Electric and Electronic Engineering Department, Imperial College London, South Kensington Campus, London SW7 2AZ, UK (e-mail: blgdujun@gmail.com).

C. Jiang is with Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, P. R. China (e-mail: jchx@tsinghua.edu.cn).

H. Zhang is with the Department of Communications Engineering, University of Science and Technology Beijing, Beijing 100083, P. R. China (e-mail: haijunzhang@ieee.org).

X. Wang is with the Department of Electrical Engineering, Columbia University, New York, NY 10027 USA (e-mail: wangx@ee.columbia.edu).

Y. Ren is with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, P. R. China (e-mail: reny@tsinghua.edu.cn).

M. Debbah is with the Large Networks and System Group (LANEAS), CentraleSupélec, Université Paris-Saclay, Gifsur-Yvette, France, and also with the Mathematical and Algorithmic Sciences Lab, Huawei France, Paris, France (email: merouane.debbah@huawei.com).

especially for the military applications. Therefore, how to minimize the interference between the FSS terminals and terrestrial networks, meanwhile guarantee their transmission quality and security requirements, plays an important role to realize an efficient and secure transmission in the satellite terrestrial networks. In this work, we will consider the downlink communication in a coexistence system with FSS terminals and terrestrial cellular networks sharing the same Ka band. Subjected to the power and transmission quality constraints, we study the cooperation based beamforming schemes among the satellite and terrestrial based stations (BSs) to maximize the achievable secrecy rate of the wiretapped FSS terminals.

A. Related Works

1) Satellite terrestrial networks: Recently, many research efforts have been devoted to the analysis and improvement of the system performance in satellite terrestrial networks by spectrum sharing [7]. In [8], authors considered terrestrial users as the primary users, and studied the optimal power control schemes for real-time applications in cognitive satellite terrestrial networks. Without degrading the communication quality of the primary terrestrial users, the delay-limited capacity and outage capacity can be maximized through the designed power control schemes. Considering the multiple co-channel interferes at both the terrestrial relay and destination, a multiple-antenna hybrid satellite terrestrial relay network was analyzed in [9]. In [10], a multimedia multicast beamforming scheme was investigated for the integrated terrestrial satellite networks, in which the maximum ratio transmission (MRT) based beamforming scheme and the zero-forcing beamforming (ZFBF) scheme were applied by BSs and the satellite, respectively.

However, the transmission security issues are hardly investigated in current studies for satellite terrestrial networks. In [11], although an optimized power allocation strategy was designed to support the secure transmission only for the SatCom scenario, the terrestrial networks were not considered in the system. A secure beamforming scheme was proposed in [12] for a satellite terrestrial network, in which the terrestrial user's capacity was maximized subjected to the power and Signal-to-Interference Plus Noise Ratio (SINR) constraints. Nevertheless, the framework established in [12] has a limited ability to model the current complex and large-scale networks due to its simplified system structure, in which the satellite communicated with only one FSS terminal and there was one terrestrial BS with an associated user. In this work, we will establish a coexistence system of SatCom and terrestrial networks using the mmWave channels, in which the satellite and terrestrial BSs carry multiple antennas. Moreover, the multiple FSS terminals associated to the satellite and mobile users associated to the BSs are equipped with single antenna and are distributed among the terrestrial part of the system.

2) Physical layer security: Using an information theoretic point, physical layer security aims to enable the legitimate destinations to successfully receive the source information and prevent eavesdropping without upper layer data encryption [13]. In the theoretical framework of physical layer security, "secrecy capacity" is defined as the maximum reliable rate of information transmitted from the source to the intended destination, while eavesdroppers are kept as ignorant of this information as possible. As first pioneered in [14], physical layer security has been generalized to the wireless fading channel and communication networks with multiple nodes [15], [16]. In order to maximize the secrecy rate of destinations, cooperative jamming has been studied to increase the SINR at the intended destinations and decrease that at eavesdroppers, through power control, adaptive beamforming and other techniques. In [17], authors studied the secrecy transmission with the assistance of multiple wireless energy harvesting-enabled amplify-and-forward relays, who perform cooperative jamming to ensure the secure transmission of the wireless sensing network. A physical layer security game framework was established and analyzed in [18], in which the source was modeled as a buyer who want to optimize its secrecy capacity minus cost, meanwhile friendly jammers modified their jamming power to maximize their own utility. The study in [18] demonstrated the effectiveness of cooperative jamming on improving the secrecy capacity.

On the other hand, the artificial noise (AN) aided transmission strategy is another efficient method to improve the secrecy rate. In [19], authors introduced AN into multi-antenna wiretap channels, and demonstrated that jointly optimizing the precoder matrix and the portion of power allocated to AN can outperform the solutions which rely on optimizing the precoder only. The power allocation problem was studied in [20] for AN secure precoding systems in MISOSE (MISO, single-eavesdropper), MISOME (MISO, multiple-eavesdropper) and MIMOME (MIMO, multiple-eavesdropper) channels, and the secrecy rate was analyzed and its lower bounds were derived. In this work, we will consider the terrestrial BSs as friendly jammers who operate cooperative beamforming to improve the secrecy rate of FSS terminals. In addition, AN will be introduced into the system to further confuse the eavesdropper, who is located on the ground and wiretapping the information transmitted from the satellite to the FSS terminals.

B. Contributions

The main contributions in this paper can be summarized as follows:

- We establish a coexistence system of FSS and cellular networks, in which one satellite communicating with multiple FSS terminals and multiple terrestrial BSs communicating with their own users are sharing the Ka band. Consider that the satellite and BSs carry multiple antennas, and FSS terminals and BSs' users are equipped with the single antenna. Then a multiple-input-single-output (MISO) channel in mmWave frequency band is modeled. The system model and related assumptions established are reasonable and can be applied to model the current coexistence system of SatCom and terrestrial cellular networks.
- To prevent the eavesdropper from wiretapping the F-SS terminals, we analyze the physical layer security issues. Based on the establish security scenario, the

non-cooperation based secure transmission beamforming and cooperation based security transmission beamforming schemes are designed to ensure the security of SatCom. Simulation results show that the cooperative beamforming scheme can improve the secrecy rate of the eavesdropped FSS terminal greatly by sacrificing the BS users' transmission quality.

- We formulate the physical layer security problem in the established MISO mmWave system. The objective of the security problem is to maximize the achievable secrecy rate of the eavesdropped FSS terminal, subjected to the power and SINR threshold constraints of FSS terminals and BSs' users. In the coexistence system, we consider that the communication of terrestrial network has higher priority and legacy right of protection. This precondition is in conformity with the current regulations and rules of the satellite terrestrial communication.
- To solve the formulated nonlinear and nonconvex optimization problems, we introduce an approximation and iteration based solution to transform the original problem into a series of convex quadratic problems. Our results show that the proposed algorithm can achieve high efficiency and fast convergence to solve the original nonconvex optimization problems.

C. *Organization and Notations*

The remainder of this paper is organized as follows. Section II sets up the system model. In Section III, the secure transmission beamforming schemes are designed, and the corresponding secrecy rate maximization problems are formulated. Iteration based solution for the optimization problems are proposed in Section IV. Simulations are shown in Section V, and conclusions are drawn in Section VI.

Notations: $(\cdot)^H$ and $(\cdot)^T$ demote conjugate transpose and transpose, respectively. $\|\mathbf{x}\|_2$ denotes the Euclidean norm of vector $\mathbf{x}$. $\mathbb{E}\{\cdot\}$ denotes the expectation, $\Re\{\cdot\}$ defines the real operator, and ∇ defines the first order differential operator. Define $\langle \mathbf{x}, \mathbf{y} \rangle \triangleq \mathbf{x}^H \mathbf{y}$.

II. System Model

In a coexistence system of FSS and cellular networks in the mmWave bands, we consider a security scenario as shown in Fig. 1. In particular, in this system, the satellite (Sat), communicating with N FSS terminals distributed within its coverage, is equipped with $N_s > N$ antennas to illustrate beams through beamforming coherently. Considering an interference mmWave scenario, there are M multi-antenna BSs and their associated users within the coverage of the satellite. Assume that there are $N_p \geq M$ antennas at each BS, and BSs' users are equipped with single-antenna. One eavesdropper (EVE), located inside the satellite coverage, intends to wiretap the confidential message transmitted to one FSS terminal, named eavesdropped FSS terminal. Assume that both legitimate FSSs and the eavesdropper are equipped with a single antenna. Therefore, the communications from the sources, i.e., the satellite and terrestrial BSs, to the destinations, which refer to FSS terminals, BSs' uses and the eavesdropper, can be considered as the MISO wiretap channels.

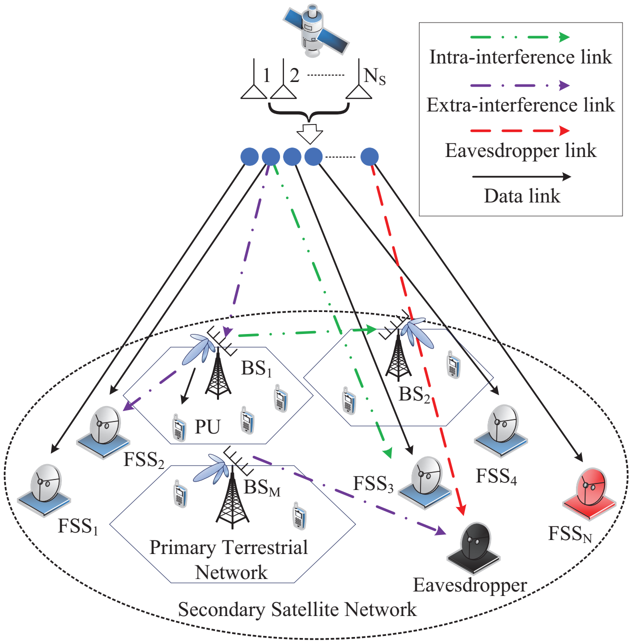


Fig. 1. The coexistence system of SatCom and terrestrial cellular networks.

In this work, we consider that the satellite downlinks and terrestrial BS downlinks are both operating in the Ka band (17.7 – 19.7 GHz). According to Decision ECC/DEC/(00)07 adopted by the ECPT [5], the terrestrial BS links are incumbent links in the 17.7 – 19.7 GHz band, which means that BSs have the higher priority and legacy right to use this specific part of the spectrum. In other words, FSS terminals can be deployed without the right of protection, and their interference bringing to BSs and BS users needs to be limited [3]. Therefore, we define the transmission from BSs to their users as the primary link, while the satellite downlink to its FSS terminals as the secondary links in our work. Before proceeding further, we summarize the main notations used throughout the following sections in Table I for convenience.

A. *Channel Model*

The mmWave channels are expected to have limited scattering [21]. In addition, for the transmission from the satellite to FSS terminals, the line-of-sight (LOS) signal is much stronger than the others. Therefore, we consider a single path link to model the mmWave channel between the satellite and FSS terminals. Specifically, the channel vector $\mathbf{h}_n \in \mathbb{C}^{N_s \times 1}$ of FSS terminal n $(n \in \mathcal{N} \triangleq \{1, 2, \cdots, N\})$ is given by [22], [23]:

$$\mathbf{h}_n = \delta_n \sqrt{N_s} \alpha(\theta_n), \ \forall n \in \mathcal{N}, \tag{1}$$

where δ_n and θ_n are the complex gain and normalized direction of the LOS path for FSS n, respectively. In addition, $\delta_n \sim \mathcal{CN}(0, 1)$ is independent identically distributed (i.i.d.) complex Gaussian distribution with zero-mean and unit covariance, and $\theta_n \sim U[-1, 1]$ is i.i.d. uniformly distributed.

TABLE I
LIST OF MAIN NOTATIONS IN SATELLITE-TERRESTRIAL COMMUNICATIONS WITH CELLULAR NETWORKS.

Parameter	Definition
N	number of FSSs
M	number of BSs
N_s	number of antennas equipped on Sat
N_p	number of antennas equipped on every BS
P_s	total transmit power of Sat
P_p	total transmit power of every BS
$\mathbf{h}_n$	channel vector between Sat and FSS_n
$\mathbf{h}_e$	channel vector between Sat and EVE
$\mathbf{g}_m$	channel vector between BS_m and PU_m
$\mathbf{g}_{j,m}$	channel vector between BS_j and PU_m
$\mathbf{g}_{m,e}$	channel vector between BS_m and EVE
$\mathbf{f}_m$	channel vector between Sat and PU_m
$\mathbf{f}_{m,n}$	channel vector between BS_m and FSS_n
$\mathbf{w}_n$ / $\mathbf{w}$	beamforming vector of Sat for FSS_n / FSSs
$\mathbf{u}_m$ / $\mathbf{u}$	beamforming vector of BS_m / BSs)
$\mathbf{v}$	artificial noise signal generated by Sat
s_n	transmitted data symbols from Sat to FSS_n
s_{ms}	transmitted data symbols from BS_m and PU_m
γ_n	SINR threshold of FSS_n
γ_{ms}	SINR threshold of PU_m

Moreover, when a uniform linear array (ULA) is adopted, the normalized array response $\alpha(\theta)$ is given by

$$\alpha(\theta)=\frac{1}{\sqrt{N_s}}\left[1,e^{-j\frac{2\pi}{\lambda}d\sin(\varphi)},\cdots,e^{-j\frac{2\pi}{\lambda}(N_s-1)d\sin(\varphi)}\right]^T. \quad (2)$$

Here, normalized direction θ_n is related to the physical azimuth angle of departure (AoD) of $\varphi\in[-\pi/2,\pi/2]$ as $\theta=(2d/\lambda)\sin(\varphi)$, where d is the antenna spacing (i.e., the distance between the two adjacent antennas), and λ is the carrier wavelength. In this work, we assume the critically sampled environment, i.e, $d/\lambda=0.5$, considering that the normalized AoD is the sine function of the actual AoD.

For the terrestrial cellular network, we adopt a multi-path channel with L scatters to model the links between BSs and their users and interference links between BSs and FSS terminals. In this work, we assume that there is one associated user for each BS. Then the channel vector $\mathbf{g}_m\in\mathbb{C}^{N_p\times 1}$ ($m\in\mathcal{M}\triangleq\{1,2,\cdots,M\}$) from BS m to its user can be given by

$$\mathbf{g}_m=\sqrt{\frac{N_p}{L_m}}\sum\nolimits_{l=1}^{L_m}\delta_{m,l}\alpha(\theta_{m,l}),\ \forall m\in\mathcal{M}, \quad (3)$$

where $\delta_{m,l}\sim\mathcal{CN}(0,1)$ and $\theta_{m,l}\sim U[-1,1]$ are the path gain and AoD of the lth path of the channel vector $\mathbf{g}_m$, respectively. L_m is the number of multi-path from BS m to its user. Similar to (2), we have

$$\alpha(\theta_{m,l})=\frac{1}{\sqrt{N_p}}\left[1,e^{-j\frac{2\pi}{\lambda}d\sin(\varphi_{m,l})},\cdots,\right.$$
$$\left.e^{-j\frac{2\pi}{\lambda}(N_p-1)d\sin(\varphi_{m,l})}\right]^T \quad (4)$$

where normalized direction $\theta_{m,l}$ are related to the physical AoD $\varphi\in[-\pi/2,\pi/2]$ as $\theta=(2d/\lambda)\sin(\varphi)$.

B. Received Signal Model

Let s_n be the transmitted data symbols to the nth FSS terminal denoted by FSS_n, and s_{ms} be the transmitted data symbols from the mth BS, BS_m, to its user PU_m. The amplitude of the signal is normalized to one, i.e., $\mathbb{E}\left\{|s_n|^2\right\}=\mathbb{E}\left\{|s_{ms}|^2\right\}=1$, $\forall n\in\mathcal{N}$, $m\in\mathcal{M}$. The transmit signals from the satellite and BS_m are mapped onto the antenna array elements by the beamforming vectors $\mathbf{w}_n\in\mathbb{C}^{N_s\times 1}$, $\forall n$ and $\mathbf{u}_m\in\mathbb{C}^{N_p\times 1}$, $\forall m$, respectively. To confuse the eavesdropper, the satellite adds an AN signal, which is denoted by $\mathbf{v}\in\mathbb{C}^{N_s\times 1}$ [24], [25]. The AN signal $\mathbf{v}$ is treated as interference at the eavesdropper, however $\mathbf{v}$ can be known for the legitimate FSS terminals. Therefore, the interference of $\mathbf{v}$ is relatively weak for the legitimate FSS terminals of the SatCom system. Without loss of generality, assume that $\|\mathbf{w}_n\|_2=P_n$, $\|\mathbf{u}_m\|_2=P_{ms}$, $\forall n$, m, and $\|\mathbf{v}\|_2=P_v$. The total transmit power of the satellite is P_s. Assume that the total transmit power of every BS is the same, i.e., P_p. Then $\sum_{n=1}^{N}\|\mathbf{w}_n\|_2+\|\mathbf{v}\|_2\leq P_s$ and $\|\mathbf{u}_m\|_2\leq P_p$, $\forall m$.

Thus, after beamforming, the transmitted signal from the satellite is

$$\mathbf{x}=\sum\nolimits_{n=1}^{N}\mathbf{w}_n s_n+\mathbf{v}, \quad (5)$$

and for each FSS_n, the received signal is

$$\mathbf{x}_n=\mathbf{w}_n s_n+\mathbf{v},\ \forall n\in\mathcal{N}, \quad (6)$$

and the signal received by FSS_n can be expressed

$$\begin{aligned}y_n=&\mathbf{h}_n^H\mathbf{w}_n s_n+\rho_{int}\sum\nolimits_{i=1,i\neq n}^{N}\mathbf{h}_n^H\mathbf{w}_i s_i+\rho_{int}\mathbf{h}_n^H\mathbf{v}\\&+\rho_{ext}\sum\nolimits_{m=1}^{M}\mathbf{f}_{m,n}^H\mathbf{u}_m s_{ms}+n_n,\ \forall n\in\mathcal{N},\end{aligned} \quad (7)$$

where $\mathbf{f}_{m,n}\in\mathbb{C}^{N_p\times 1}$ is the channel vector between the mth BS and nth FSS. $0\leq\rho_{int}<\rho_{ext}\leq 1$ are the interference coefficients of the inter-system and extra-system interference, respectively. $n_n\sim\mathcal{CN}\left(0,\sigma_s^2\right)$ is the i.i.d. noise with a zero-mean complex circular Gaussian distribution with variance σ_s^2.

The signal received by PU_m can be given by

$$\begin{aligned}y_{ms}=&\mathbf{g}_m^H\mathbf{u}_m s_{ms}+\rho_{ext}\sum\nolimits_{n=1}^{N}\mathbf{f}_m^H\mathbf{w}_n s_n+\rho_{ext}\mathbf{f}_m^H\mathbf{v}\\&+\rho_{int}\sum\nolimits_{j=1,j\neq m}^{M}\mathbf{g}_{j,m}^H\mathbf{u}_j s_{js}+n_{ms},\ \forall m\in\mathcal{M},\end{aligned} \quad (8)$$

where $\mathbf{f}_m\in\mathbb{C}^{N_s\times 1}$ is the channel vector between the satellite and PU_m, $\mathbf{g}_{j,m}\in\mathbb{C}^{N_p\times 1}$ is the channel vector between BS_j ($j\in\mathcal{M}\backslash m$) and PU_m, and $n_{ms}\sim\mathcal{CN}\left(0,\sigma_p^2\right)$ is the i.i.d. noise with a zero-mean complex circular Gaussian distribution with variance σ_p^2.

Without loss of generality, we assume that the eavesdropper is wiretapping FSS_N, which is similar to the model in [26]. Therefore, the received signal at the eavesdropper is given by

$$\begin{aligned}y_e=&\mathbf{h}_e^H\mathbf{w}_N s_N+\rho_e\sum\nolimits_{i=1}^{N-1}\mathbf{h}_e^H\mathbf{w}_i s_i+\rho_e\mathbf{h}_e^H\mathbf{v}\\&+\rho_e\sum\nolimits_{m=1}^{M}\mathbf{g}_{m,e}^H\mathbf{u}_m s_{ms}+n_e,\end{aligned} \quad (9)$$

where $\mathbf{h}_e\in\mathbb{C}^{N_s\times 1}$ and $\mathbf{g}_{m,e}\in\mathbb{C}^{N_p\times 1}$ are the channel vectors between the satellite and the eavesdropper and between

BS_m and the eavesdropper, respectively. $0 \leq \rho_e \leq 1$ is the interference coefficient, and $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ is the i.i.d. noise at the eavesdropper. Comparing the expressions in (7) and (9), we can notice that the received signal at eavesdropped FSS_N and the eavesdropper have the similar composition. However, for the eavesdropper, AN signal $\mathbf{v}$ and $\mathbf{w}_i$ ($i = 1, 2, \ldots, N-1$) can hardly known precisely. Therefore, the interference caused by AN and other transmitted signals can bring more serious reduction of the SINR for the eavesdropper.

C. Signal-to-Interference Plus Noise Ratio

Given the received signal formulated in (7), (8) and (9), the SINR of each FSS terminal, BS's user and the eavesdropper can be derived as

$$\Gamma_n = \frac{\mathbf{w}_n^H \mathbf{R}_n \mathbf{w}_n}{\rho_{int} I_{int,n} + \rho_{ext} I_{ext,n} + \rho_{int} I_{AN,n} + \sigma_s^2}, \ \forall n, \quad \text{(10a)}$$

$$\Gamma_{ms} = \frac{\mathbf{u}_m^H \mathbf{G}_m \mathbf{u}_m}{\rho_{ext} I_{ext,ms} + \rho_{int} I_{int,ms} + \rho_{ext} I_{AN,ms} + \sigma_p^2}, \forall m, \quad \text{(10b)}$$

$$\Gamma_{eN} = \frac{\mathbf{w}_N^H \mathbf{R}_e \mathbf{w}_N}{\rho_e I_{s,e} + \rho_e I_{p,e} + \rho_e I_{AN,e} + \sigma_e^2}, \quad \text{(10c)}$$

Respectively. In (10a), $I_{int,n} = \sum_{i=1,i\neq n}^{N} \mathbf{w}_i^H \mathbf{R}_n \mathbf{w}_i$, $I_{ext,n} = \sum_{m=1}^{M} \mathbf{u}_m^H \mathbf{F}_{m,n} \mathbf{u}_m$ and $I_{AN,n} = \mathbf{v}^H \mathbf{R}_n \mathbf{v}$, where $\mathbf{R}_n \triangleq \mathbf{h}_n \mathbf{h}_n^H$ and $\mathbf{F}_{m,n} \triangleq \mathbf{f}_{m,n} \mathbf{f}_{m,n}^H$. In (10b), $I_{ext,ms} = \sum_{n=1}^{N} \mathbf{w}_n^H \mathbf{F}_m \mathbf{w}_n$, $I_{int,ms} = \sum_{j=1,j\neq m}^{M} \mathbf{u}_j^H \mathbf{G}_{j,m} \mathbf{u}_j$ and $I_{AN,ms} = \mathbf{v}^H \mathbf{F}_m \mathbf{v}$, where $\mathbf{G}_m \triangleq \mathbf{g}_m \mathbf{g}_m^H$, $\mathbf{G}_{j,m} \triangleq \mathbf{g}_{j,m} \mathbf{g}_{j,m}^H$ and $\mathbf{F}_m \triangleq \mathbf{f}_m \mathbf{f}_m^H$. In (10c), $I_{s,e} = \sum_{n=1}^{N-1} \mathbf{w}_n^H \mathbf{R}_e \mathbf{w}_n$, $I_{p,e} = \sum_{m=1}^{M} \mathbf{u}_m^H \mathbf{G}_{m,e} \mathbf{u}_m$ and $I_{AN,e} = \mathbf{v}^H \mathbf{R}_e \mathbf{v}$, where $\mathbf{R}_e \triangleq \mathbf{h}_e \mathbf{h}_e^H$ and $\mathbf{G}_{m,e} \triangleq \mathbf{g}_{m,e} \mathbf{g}_{m,e}^H$.

D. Achievable Secrecy Rate

There have been several works that analyzed the MISO and MIMO wiretap channels. For the case of one eavesdropper, an achievable secrecy rate for the eavesdropped FSS_N (the Nth FSS) can be given by [13], [11]:

$$C_{sN} = \max\left\{C_N - C_{eN}, 0\right\}, \quad (11)$$

where

$$C_N = \log\left(1 + \Gamma_N\right), \quad C_{eN} = \log\left(1 + \Gamma_{eN}\right) \quad (12)$$

are the achievable rate of the link between the satellite and the eavesdropped FSS_N, and the achievable rate of the link between the satellite and the eavesdropper, respectively.

III. Secure Transmission Beamforming Schemes for Satellite Terrestrial Networks

In this section, we will design the secure transmission beamforming schemes by introducing AN. In addition, considering the terrestrial BSs distributed within the satellite coverage are performing as friendly jammers, we will also design a cooperative beamforming scheme to further increase the secrecy rate of the eavesdropped FSS terminal. Then we formulate the secrecy rate maximization problems for the designed beamforming schemes in this section.

A. Non-cooperative Beamforming for Secure Transmission

Let us first discuss the beamforming and AN optimization for the satellite transmission without the cooperative jamming from the terrestrial cellular networks. As assumed previously, we consider that FSS_N is wiretapped by the eavesdropper. The optimization goal is to maximize the achievable secrecy rate of FSS_N by modifying the beamforming vectors and AN vector. Meanwhile, the required quality of service (QoS) of the system, i.e., the SINR requirements from both BSs' users and other legitimate FSS terminals, needs to be guaranteed. In addition, the beamforming scheme must meet the power constraint of the satellite. Thus, for the non-cooperative secure transmission beamforming (NCoSTB) scheme, the secrecy rate optimization problem can be formulated as

$$\max_{\mathbf{w}_n, \forall n, \mathbf{v}} \quad C_{sN}(\mathbf{w}, \mathbf{v}) = C_N(\mathbf{w}, \mathbf{v}) - C_{eN}(\mathbf{w}, \mathbf{v}), \quad \text{(13a)}$$

$$\text{s.}t. \quad \sum\nolimits_{n=1}^{N} \left\|\mathbf{w}_n\right\|^2 + \left\|\mathbf{v}\right\|^2 \leq P_s, \quad \text{(13b)}$$

$$\Gamma_n\left(\mathbf{w}, \mathbf{v}\right) \geq \gamma_n, \forall n \in \mathcal{N}, \quad \text{(13c)}$$

$$\Gamma_{ms}\left(\mathbf{w}, \mathbf{v}\right) \geq \gamma_{ms}, \forall m \in \mathcal{M}, \quad \text{(13d)}$$

where $\mathbf{w} = \left\{\mathbf{w}_n\right\}_{n\in\mathcal{N}}$ and $\mathbf{v}$ are the optimization variables, γ_n and γ_{ms} are the SINR threshold required by FSS_n and PU_m, respectively. In this work, we consider that the BSs implement beamforming according to the maximum ratio transmission (MRT) for the NCoSTB scheme, i.e., for each BS,

$$\tilde{\mathbf{u}}_m = \sqrt{P_p} \frac{\mathbf{g}_m}{\left\|\mathbf{g}_m\right\|_2}, \quad m \in \mathcal{M}. \quad (14)$$

B. Cooperative Secure Beamforming for Secure Transmission

In the NCoSTB scheme, BSs implement fixed beaming determined by the channel states. In the coexistence system of the SatCom and terrestrial network when they are sharing the mmWave band, the BSs' transmitted signals after the beamforming can bring the noise and confuse the eavesdropper, which decreases the achievable rate at the eavesdropper according to (9). On the other hand, these signals from the terrestrial network can also influence the received rate at FSS terminals. Therefore, how to minimize the BSs' interference to the FSS terminals as well as to confuse the eavesdropper at the same time, has a significant effect on improving the security and capacity of the SatCom system.

In recent works that study the physical layer security, the cooperative jamming has been employed to reduce the eavesdropper's ability to decode the target receiver's information [27], [28]. Assume that the channel state information can be shared among the satellite terrestrial system. When the BSs transmit to their users, they implement their beamforming according to the channel state information not only of their own but also of the SatCom system. Specifically, BSs can perform as friendly jammers to minimize their interference to FSS terminals, meanwhile, improve the transmission security. Next, we will formulate the secrecy rate optimization problem for this cooperative secure transmission beamforming (CoSTB) scheme above.

Let $\mathbf{u} = \left\{\mathbf{u}_m\right\}_{m\in\mathcal{M}}$. The optimization problem aims to maximize the secrecy rate of the eavesdropped FSS terminal by jointly adjusting the beamforming of satellite and BSs, subjected to the power and SINR constraints of both the satellite and BSs. Thus, we formulate the optimization problem for the CoSTB scheme as

$$\max_{\substack{\mathbf{w}_n,\forall n,\mathbf{v}\\ \mathbf{u}_m,\forall m}} \quad C_{sN}(\mathbf{w},\mathbf{v},\mathbf{u}) = C_N(\mathbf{w},\mathbf{v},\mathbf{u}) - C_{eN}(\mathbf{w},\mathbf{v},\mathbf{u}), \tag{15a}$$

$$\text{s.}t. \quad \sum\nolimits_{n=1}^{N} \|\mathbf{w}_n\|^2 + \|\mathbf{v}\|^2 \leq P_s, \tag{15b}$$

$$\|\mathbf{u}_m\|^2 \leq P_p, \forall m \in \mathcal{M}, \tag{15c}$$

$$\Gamma_n(\mathbf{w},\mathbf{v},\mathbf{u}) \geq \gamma_n, \forall n \in \mathcal{N}, \tag{15d}$$

$$\Gamma_{ms}(\mathbf{w},\mathbf{v},\mathbf{u}) \geq \gamma_{ms}, \forall m \in \mathcal{M}. \tag{15e}$$

So far, we have formulated the secrecy rate optimization problems for the NCoSTB and CoSTB schemes. We can notice that in (13) and (15), the objective fuctions (13a) and (15a) are not concave. For constraints, (13b), (15b) and (15c) are convex. However, constraints (13c), (13d), (15d) and (15e) are not convex in their current forms. In the next section, we will focus on pursuing the solutions of such nonconvex optimization problems approximately but effectively and efficiently.

IV. Solutions of The Optimization Problems

Currently, many works studying the beamforming design focus on solving such complicated and nonconvex optimization problems formulated in the previous section. For instance, the tractable semidefinite technique is introduced to transform the nonconvex problems into a tractable semidefinite program (SDP) [29], [30]. However, when the total dimension of the optimization variables increase explosively in the scenarios where massive antennas are deployed for mmWave communications, the SDP approach will become computationally expensive. Concerning this issue, we will design a path-pursuit iteration based algorithm to solve the secrecy rate maximization problems (13) and (15) with high efficiency. Through the proposed algorithm, (13) and (15) will be decomposed into a series of iterative optimization problems, and each iteration can be formulated as a convex quadratic program in $(\mathbf{w}, \mathbf{v})$ and $(\mathbf{w}, \mathbf{v}, \mathbf{u})$, respectively. In this section, we will first provide a feasible solution to solve the optimization problems in the previous sections. To improve the efficiency and convergence rate of the introduced optimization algorithm, we will design a path-pursuit and iteration based approach later. Then we will prove the feasibility of the designed optimization.

A. Feasible Solution of the Optimization Problems

First, we introduce a classic optimization algorithm to solve the formulated optimization problems in the previous section. As discussed in the previous section, the objective functions of secrecy rate maximization problems (13) and (15) are nonconvex. To find out the approximate solutions, we introduce an efficient and effective stochastic and cooperation based optimization technique, called the cooperative particle swarm optimization (CPSO) algorithm [31]. CPSO was proposed based on the traditional particle swarm optimization (PSO). In PSO, the term of swarm indicates multiple particles, and there is only one swarm with many particles. Each of these particles refers to a possible solution of the optimization problem. PSO is operated with a series of iterations. In each iteration, every particle finds its own best solution and then accelerates in the direction of this position, as well as in the direction of the global best position having been found at present. However, the performance of PSO often deteriorates rapidly as the dimensionality of the problem increases. CPSO can be considered as an improvement of PSO, by expanding the single swarm, aiming to find the optimal S-dimensional vector, into S swarms. Each of these swarms has many particles. Through the cooperative optimization of the one-dimensional vector operated by each of the S swarms, CPSO can achieve a faster convergence to find the optimal solution than PSO.

Algorithm 1 CPSO Algorithm [31].

```
Initialization:
    Create and initialize $S$ one-dimensional PSOs: $P_j$, $j = 1, 2, \cdots, S$;
    Define:
    $g(j, z) \equiv (P_1 \cdot \hat{\mathbf{w}}, P_2 \cdot \hat{\mathbf{w}}, \cdots, P_{j-1} \cdot \hat{\mathbf{w}}, z, P_{j+1} \cdot \hat{\mathbf{w}}, \cdots, P_S \cdot \hat{\mathbf{w}})$;
    Iterations $T$.
for $t \leq T$ do
    for each swarm $j = 1, 2, \cdots, S$ do
        for each particle $i = 1, 2, \cdots, I$ do
            if $C_{sN}(g(j, P_j \cdot \mathbf{x}_i)) < C_{sN}(g(j, P_j \cdot \mathbf{w}_i))$ then
                $P_j \cdot \mathbf{w}_i = P_j \cdot \mathbf{x}_i$
            end if
            if $C_{sN}(g(j, P_j \cdot \mathbf{w}_i)) < C_{sN}(g(j, P_j \cdot \hat{\mathbf{w}}))$ then
                $P_j \cdot \hat{\mathbf{w}} = P_j \cdot \mathbf{w}_i$
            end if
        end for
        Update $P_j$ by PSO with :
            $u_{ij}(t+1) = wu_{ij}(t) + c_1\zeta_{1i}(t)[w_{ij}(t) - x_{ij}(t)] + c_2\zeta_{2i}(t)[\hat{w}_j(t) - x_{ij}(t)],$   (16)
            $\mathbf{x}_i(t+1) = \mathbf{x}_i(t) + \mathbf{u}_i(t+1),$   (17)
        where $j = 1, 2, \cdots, S$, $S$: swarm size;
        $i = 1, 2, \cdots, I$, $I$: number of particles;
        $\mathbf{x}_i = [x_{i1}\ x_{i2} \cdots x_{iS}]$: current position in search space;
        $\mathbf{u}_i = [u_{i1}\ u_{i2}\ \cdots\ u_{iS}]$: current velocity;
        $\mathbf{w}_i = [w_{i1}\ w_{i2}\ \cdots\ w_{iS}]$: local best position;
        $c_1$, $c_2$: acceleration coefficients;
        $\zeta_1$, $\zeta_{2i} \sim U(0, 1)$: random sequences.
    end for
end for
```

In addition, CPSO is an effective and efficient approach to deal with a large range of optimization problems, such as nonconvex, nonsmooth and nonlinear high-dimensional optimization problems [32], [33], [34]. We summarize the main operation of CPSO proposed in [31] as Algorithm 1.

B. Path-pursuit Iteration based Approach

However, sometimes the CPSO algorithm may converge to a local optimal solution when applying it directly to deal with the optimization problems, which depends on the initial feasible values selection. Especially when the objective function and constraints of the optimization problem are nonconvex, the genetic algorithms tend to converge much slower, and are much easier to converge to a local optimal solutions. In response, we will design an iteration based CPSO (ICPSO) to improve the convergence speed and the reliability of the CPSO algorithm in this section.

1) Approximation of optimization problems: To solve the original optimization problems formulated in (13) and (15) with efficiency, we decompose them into a series of iterative optimization problems. In each iteration, the optimization problem will be approximatively formulated into a simple convex quadratic program in $(\mathbf{w},\mathbf{v})$ or $(\mathbf{w},\mathbf{v},\mathbf{u})$. In addition, the solution of the current iterative optimization problem will be set as the initial values of the next iteration. Through the approximation and path-pursuit iteration process above, the optimal point will be evolved and optimized over the iterations.

The approximate and convex transformation mentioned above is the key operation to achieve a feasible and approximate optimal solution after a series of iterations. We can notice that although the objective functions shown in (13a) and (15a) are nonconvex, the components of them, i.e., C_N and C_{eN}, can be transformed into the convex and concave functions, respectively. The proof of the convexity of C_N and concavity of C_{eN} can be found in Appendix A and B, respectively. Additionally, we consider that the Taylor expansion can represent any differentiable nonlinear function as a polynomials with infinite terms, and the coefficient of each term is calculated from the value of this function's relevant order derivative at a given point. If the function is convex (concave), which means that its second derivative is positive (negative), then we can find the lower (upper) bound at a given point when only considering the terms of constant and the first derivative of the Taylor expansion. Furthermore, when the iterative algorithm is implemented, the given point for the Taylor expansion in every iteration can be set as the optimal solution obtained in the last iteration.

According to the analysis above, we can establish the approximate optimization problems of (13) and (15) for every iteration. Denote the approximate objective functions in the tth iteration of the NCoSTB and CoSTB as $C_{sN}^{(t)}(\mathbf{w},\mathbf{v})$ and $C_{sN}^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})$, respectively, which can be given by

$$C_{sN}^{(t)}(\mathbf{w},\mathbf{v}) = C_N^{(t)}(\mathbf{w},\mathbf{v}) - C_{eN}^{(t)}(\mathbf{w},\mathbf{v}), \tag{18a}$$

$$C_{sN}^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u}) = C_N^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u}) - C_{eN}^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u}), \tag{18b}$$

where $C_N^{(t)}(\mathbf{w},\mathbf{v})$ and $C_N^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})$ are the lower bounds of C_N in the tth iteration, which will be provided in Theorem 1, and $C_{eN}^{(t)}(\mathbf{w},\mathbf{v})$ and $C_{eN}^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})$ are the upper bounds of C_{eN} in the tth iteration, which will be provided in Theorem 2.

Theorem 1. *Let* $\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)$ *and* $\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)$ *be the feasible solutions of (13) and (15), respectively, and be the datums in the tth iterative problems. Denote*

$$\begin{aligned}\psi_N(\mathbf{w},\mathbf{v}) &= \rho_{int}\sum\nolimits_{i=1}^{N-1}\mathbf{w}_i^H\mathbf{R}_N\mathbf{w}_i\\ &+\rho_{int}\mathbf{v}^H\mathbf{R}_N\mathbf{v}+\rho_{ext}\sum\nolimits_{m=1}^{M}\tilde{\mathbf{u}}_m^H\mathbf{F}_{m,N}\tilde{\mathbf{u}}_m+\sigma_s^2,\end{aligned} \tag{19a}$$

$$\begin{aligned}\psi_N(\mathbf{w},\mathbf{v},\mathbf{u}) &= \rho_{int}\sum\nolimits_{i=1}^{N-1}\mathbf{w}_i^H\mathbf{R}_N\mathbf{w}_i\\ &+\rho_{int}\mathbf{v}^H\mathbf{R}_N\mathbf{v}+\rho_{ext}\sum\nolimits_{m=1}^{M}\mathbf{u}_m^H\mathbf{F}_{m,N}\mathbf{u}_m+\sigma_s^2,\end{aligned} \tag{19b}$$

where $\tilde{\mathbf{u}}_m$ *in (19a) is obtained by the MRT strategy according to (14). For the NCoSTB scheme, the approximate lower bound of* $C_N(\mathbf{w},\mathbf{v})$ *can be given by*

$$\begin{aligned}&C_N(\mathbf{w},\mathbf{v}) \geq C_N^{(t)}(\mathbf{w},\mathbf{v})\\ &\triangleq C_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)+\frac{2}{\ln 2}\frac{\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N\right\}}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)}\\ &-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\left(\psi_N(\mathbf{w},\mathbf{v})+\mathbf{w}_N{}^H\mathbf{R}_N\mathbf{w}_N\right)}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)\left[\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\right]}\\ &-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)}.\end{aligned} \tag{20}$$

Similarly, for the CoSTB scheme, the approximate lower bound of $C_N(\mathbf{w}_s,\mathbf{v},\mathbf{w}_p)$ *is given by*

$$\begin{aligned}&C_N(\mathbf{w},\mathbf{v},\mathbf{u}) \geq C_N^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})\\ &\triangleq C_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)+\frac{2}{\ln 2}\frac{\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N\right\}}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)}\\ &-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\left(\psi_N(\mathbf{w},\mathbf{v},\mathbf{u})+\mathbf{w}_N{}^H\mathbf{R}_N\mathbf{w}_N\right)}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)\left[\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\right]}\\ &-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}}{\psi_N\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)}.\end{aligned} \tag{21}$$

Proof: See Appendix A.

Remark: As defined in (20) and (21), $C_N^{(t)}(\mathbf{w},\mathbf{v})$ and $C_N^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})$ are concave functions of $(\mathbf{w},\mathbf{v})$ and $(\mathbf{w},\mathbf{v},\mathbf{u})$, respectively.

Theorem 2. *Let*

$$\begin{aligned}\psi_e(\mathbf{w},\mathbf{v}) &= \rho_e\sum\nolimits_{n=1}^{N-1}\mathbf{w}_n^H\mathbf{R}_e\mathbf{w}_n+\rho_e\mathbf{v}^H\mathbf{R}_e\mathbf{v}\\ &+\rho_e\sum\nolimits_{m=1}^{M}\tilde{\mathbf{u}}_m^H\mathbf{G}_{m,e}\tilde{\mathbf{u}}_m+\sigma_e^2,\end{aligned} \tag{22a}$$

$$\begin{aligned}\psi_e(\mathbf{w},\mathbf{v},\mathbf{u}) &= \rho_e\sum\nolimits_{n=1}^{N-1}\mathbf{w}_n^H\mathbf{R}_e\mathbf{w}_n+\rho_e\mathbf{v}^H\mathbf{R}_e\mathbf{v}\\ &+\rho_e\sum\nolimits_{m=1}^{M}\mathbf{u}_m^H\mathbf{G}_{m,e}\mathbf{u}_m+\sigma_e^2.\end{aligned} \tag{22b}$$

Then for the NCoSTB scheme, the approximate upper bound *of* $C_{eN}\left(\mathbf{w},\mathbf{v}\right)$ *can be given by*

$$\begin{aligned} & C_{eN}\left(\mathbf{w},\mathbf{v}\right)\le C_{eN}^{(t)}\left(\mathbf{w},\mathbf{v}\right) \\ \triangleq\; & C_{eN}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)-\frac{1}{\ln 2} \\ +\, & \frac{1}{\ln 2}\frac{\psi_e\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)}{\psi_e\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_e\mathbf{w}_N^{(t)}}\left(\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e^{(t)}\left(\mathbf{w},\mathbf{v}\right)}+1\right), \end{aligned} \tag{23}$$

where

$$\begin{aligned} \psi_e^{(t)}(\mathbf{w},\mathbf{v})=\rho_e\sum\nolimits_{n=1}^{N-1}&\Re\left\{\left\langle\mathbf{h}_e^H\mathbf{w}_n^{(t)},2\mathbf{h}_e^H\mathbf{w}_n-\mathbf{h}_e^H\mathbf{w}_n^{(t)}\right\rangle\right\} \\ &+\rho_e\Re\left\{\left\langle\mathbf{h}_e^H\mathbf{v}^{(t)},2\mathbf{h}_e^H\mathbf{v}-\mathbf{h}_e^H\mathbf{v}^{(t)}\right\rangle\right\} \\ &+\rho_e\sum\nolimits_{m=1}^{M}\tilde{\mathbf{u}}_m^H\mathbf{G}_{m,e}^H\tilde{\mathbf{u}}_m+\sigma_e^2. \end{aligned} \tag{24}$$

Similarly, for CoSTB, the approximate upper bound of $C_{eN}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$ *is given by*

$$\begin{aligned} & C_{eN}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)\le C_{eN}^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right) \\ \triangleq\; & C_{eN}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)-\frac{1}{\ln 2} \\ +\, & \frac{1}{\ln 2}\frac{\psi_e\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)}{\psi_e\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_e\mathbf{w}_N^{(t)}}\left[\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)}+1\right], \end{aligned} \tag{25}$$

where

$$\begin{aligned} \psi_e^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})=\rho_e\sum\nolimits_{n=1}^{N-1}&\Re\left\{\left\langle\mathbf{h}_e^H\mathbf{w}_n^{(t)},2\mathbf{h}_e^H\mathbf{w}_n-\mathbf{h}_e^H\mathbf{w}_n^{(t)}\right\rangle\right\} \\ &+\rho_e\Re\left\{\left\langle\mathbf{h}_e^H\mathbf{v}^{(t)},2\mathbf{h}_e^H\mathbf{v}-\mathbf{h}_e^H\mathbf{v}^{(t)}\right\rangle\right\} \\ &+\rho_e\sum\nolimits_{m=1}^{M}\tilde{\mathbf{u}}_m^H\mathbf{G}_{m,e}^H\tilde{\mathbf{u}}_m+\sigma_e^2. \end{aligned} \tag{26}$$

Proof: See Appendix B.

Remark: As defined in (23) and (25), $C_{eN}^{(t)}(\mathbf{w},\mathbf{v})$ and $C_{eN}^{(t)}(\mathbf{w},\mathbf{v},\mathbf{u})$ are convex functions of $(\mathbf{w},\mathbf{v})$ and $(\mathbf{w},\mathbf{v},\mathbf{u})$, on domains

$$\psi_e^{(t)}\left(\mathbf{w},\mathbf{v}\right)\ge 0, \tag{27a}$$

$$\psi_e^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)\ge 0, \tag{27b}$$

respectively.

According to Theorem 1 and Theorem 2, the secrecy rate maximization problems formulated in (13) and (15) can be transformed into a series of convex quadratic problems, which can be solved and processed with low computational complexity and high efficiency. In order to avoid repeated and similar analysis, in the following parts of this section, we will take the CoSTB scheme as the example to introduce the operation of the path-pursuit iteration approach to find out the approximate solutions of problem (15).

Using (21) and (25), The tth iteration of optimization problem (15) can be approximated as an inner convex program as

$$\max_{\substack{\mathbf{w}_n,\forall n,\mathbf{v}\\ \mathbf{u}_m,\forall m}}\quad C_{sN}^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right), \tag{28a}$$

$$\text{s}.t.\quad \text{(15b), (15c), (15d), (15e) and (27b)}, \tag{28b}$$

where $C_{sN}^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$ is obtained by applying (21) and (25).

Algorithm 2 Path-pursuit iteration based algorithm (ICPSO).

```
Initialization:
    Iterative index: $t = 1$;
    Maximun iterative number: $N_{\text{iter}}$;
    Caculate initial feasible point $(\mathbf{w}^{(1)},\mathbf{v}^{(1)},\mathbf{u}^{(1)})$: Caculate $\tilde{\mathbf{w}}$
    and $\tilde{\mathbf{u}}$ according to MRT, initialize $\tilde{\mathbf{v}} = \mathbf{0}$, and then adjust
    $(\tilde{\mathbf{w}},\tilde{\mathbf{v}},\tilde{\mathbf{u}})$ to meet constraint (28b).
1: for $t \le N_{\text{iter}}$ do
2:     Solve optimization problem in (28),
3:     obtain the optimal solution $(\mathbf{w}^*,\mathbf{v}^*,\mathbf{u}^*)$,
4:     $t = t + 1$,
5:     $\mathbf{w}^{(t)} = \mathbf{w}^*$, $\mathbf{v}^{(t)} = \mathbf{v}^*$, $\mathbf{u}^{(t)} = \mathbf{u}^*$.
6: end for
Output:
    Optimal solution: $(\mathbf{w}^*,\mathbf{v}^*,\mathbf{u}^*)$.
```

2) Path-pursuit iteration based algorithm design: Based on the approximate optimization problem established above, we design a path-pursuit based approach to maximize the secrecy rate of the eavesdropped FSS terminal, as summarized in Algorithm 2. In this part, we still only provide the algorithm for the CoSTB scheme as the example.

To achieve Step 3 in the repeated part of Algorithm 2, apply the CPSO algorithm introduced in section IV-A to obtain the current optimal solution for each iterative optimization problem. After N_{iter} times of iterations, the obtained N_{iter}th $(\mathbf{w}^*,\mathbf{v}^*,\mathbf{u}^*)$ will be considered as the optimal solution of the original optimization problem in (15). Similarly, the iteration based NCoSTB (INCoSTB) can be achieved.

C. Feasibility of Path-pursuit Iteration Based Solution

So far we have provided the path-pursuit iteration based solution to solve the original nonconvex problems by transforming them into a series of convex optimization problems approximately. Next, we will analyze the effectiveness and feasibility of the proposed algorithm, and proof that in the tth iteration, the new optimal point $\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)}\right)$ / $\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)},\mathbf{u}^{(t+1)}\right)$ is a better point than $\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)$ / $\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)$ to get a larger C_{sN}, and that $\lim_{t\to\infty}C_{sN}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)}\right)$ / $\lim_{t\to\infty}C_{sN}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)$ is a Karush-Kuhn-Tucker point of the optimization problem.

We still take the CoSTB scheme as the example to analyze the feasibility of the iteration base approach for the optimization problems. According to the previous definitions in (21) and (25), for the tth iterative optimization problem, we have

$$C_{sN}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)\ge C_{sN}^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right), \tag{29a}$$

$$C_{sN}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)=C_{sN}^{(t)}\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right), \tag{29b}$$

$$C_{sN}\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)},\mathbf{u}^{(t+1)}\right)\ge C_{sN}^{(t)}\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)},\mathbf{u}^{(t+1)}\right), \tag{29c}$$

$\forall\ \mathbf{w},\mathbf{v},\mathbf{u}$. Moreover, consider that both $\left(\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right)$ and $\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)},\mathbf{u}^{(t+1)}\right)$ are feasible points of the tth iterative optimization problem. According to Algorithm 2, $\left(\mathbf{w}^{(t+1)},\mathbf{v}^{(t+1)},\mathbf{u}^{(t+1)}\right)$ is the optimal point of tth iterative optimization problem. Therefore, we have

$$C_{sN}^{(t)}\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) \leq C_{sN}^{(t)}\left(\mathbf{w}^{(t+1)}, \mathbf{v}^{(t+1)}, \mathbf{u}^{(t+1)}\right). \quad (30)$$

Consequently,

$$\begin{aligned} & C_{sN}\left(\mathbf{w}^{(t+1)}, \mathbf{v}^{(t+1)}, \mathbf{u}^{(t+1)}\right) \\ & \geq C_{sN}^{(t)}\left(\mathbf{w}^{(t+1)}, \mathbf{v}^{(t+1)}, \mathbf{u}^{(t+1)}\right) \\ & > C_{sN}^{(t)}\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) = C_{sN}\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right). \end{aligned} \quad (31)$$

Therefore, solution $\left(\mathbf{w}^{(t+1)}, \mathbf{v}^{(t+1)}, \mathbf{u}^{(t+1)}\right)$ in tth optimization is a better point than $\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right)$ as it result to a larger C_{sN} for the original optimization problem in (15).

Consider that sequence $\left\{\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) | t = 1, 2, \cdots, T\right\}$ is constrained by (15b), (15c), (15d) and (15e). Therefore, there must exist a subsequence $\left\{\left(\mathbf{w}^{(t_\tau)}, \mathbf{v}^{(t_\tau)}, \mathbf{u}^{(t_\tau)}\right) | t_\tau \in \{1, 2, \cdots, T\}\right\}$ converging to a limited point $(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*)$, i.e.,

$$\lim_{\tau\to\infty}\left[C_{sN}\left(\mathbf{w}^{(t_\tau)}, \mathbf{v}^{(t_\tau)}, \mathbf{u}^{(t_\tau)}\right) - C_{sN}(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*)\right] = 0. \quad (32)$$

Then for every t, there is τ that $t_\tau \leq t \leq t_{\tau+1}$,

$$\begin{aligned} 0 &= \lim_{\tau\to\infty}\left[C_{sN}\left(\mathbf{w}^{(t_\tau)}, \mathbf{v}^{(t_\tau)}, \mathbf{u}^{(t_\tau)}\right) - C_{sN}(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*)\right] \\ &\leq \lim_{t\to\infty}\left[C_{sN}\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) - C_{sN}\left(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*\right)\right] \\ &\leq \lim_{\tau\to\infty}\left[C_{sN}\left(\mathbf{w}^{(t_\tau+1)}, \mathbf{v}^{(t_\tau+1)}, \mathbf{u}^{(t_\tau+1)}\right) - C_{sN}(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*)\right] = 0. \end{aligned}$$

Therefore, we have

$$\lim_{t\to\infty} C_{sN}\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) = C_{sN}\left(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*\right). \quad (33)$$

As a result, every improved point $(\mathbf{w}^*, \mathbf{v}^*, \mathbf{u}^*)$ is a Karush-Kuhn-Tucker point of sequence $\left\{\left(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{u}^{(t)}\right) | t = 1, 2, \cdots, T\right\}$.

V. Simulation Results

This part provides numerical results to demonstrate and test the validity and effectiveness of designed secure beamforming schemes. In addition, the convergence and efficiency of the proposed iteration based solution for the optimization problem are also verified through the simulation.

First of all, we introduce the scenario setup for simulations. We consider a satellite terrestrial network consisted with one satellite, five FSS terminals and fifteen terrestrial BSs [11], [35]. Assume that the satellite carries fifteen antenna elements and each BS carries sixteen antenna elements [11].

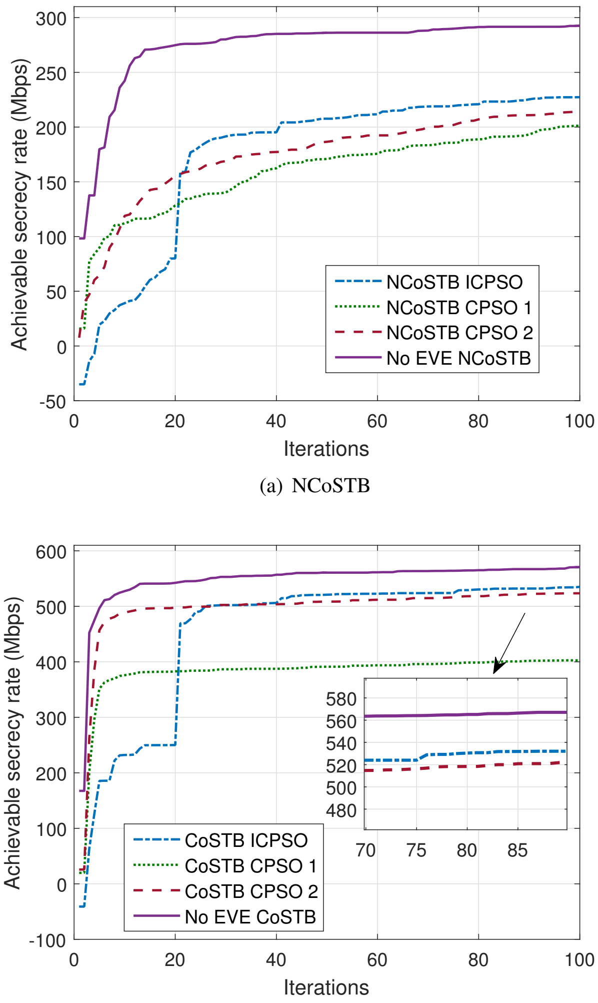
First, we test the convergence of the CPSO algorithm and the proposed ICPSO algorithm when dealing with the optimization problems for the two designed secure beamforming schemes, i.e., NCoSTB and CoSTB. In addition, for the CPSO and ICPSO algorithms, the values of $(\mathbf{w}, \mathbf{v})$ and $(\mathbf{w}, \mathbf{v}, \mathbf{u})$ are initialized randomly and adjusted to satisfy the constraints if the random values are not feasible points of the optimization problems. Moreover, the maximum number of iteration when applying CPSO to solve (15) and (13) directly is set as 100. For ICPSO, let $N_{\text{iter}} = 5$ in Algorithm 2, and for each iterative optimization problem, the maximum number of iteration of CPSO is set as 20. Therefore, the 1st, 21st, 41st, 61st and 81st iterations are the beginnings of the new updated iterative optimization problems formulated in Section IV-B1 and (28), by setting $t = 1, 2, \cdots, 5$. Thus, the total iteration number is 100, the same as that of the contrast experiment above applying CPSO directly. In addition, fix the SINR threshold as $\gamma_n = \gamma_{ms} = 0$ dB, $\forall n,\ m$ [12]. The achievable secrecy rate of FSS_N, the eavesdropped FSS terminal, updated in each iteration when applying the CPSO and ICPSO algorithms for the NCoSTB and CoSTB schemes are shown in Fig. 2(a) and Fig. 2(b), respectively. For both NCoSTB and CoSTB, "CPSO 1" and "CPSO 2" in Fig. 2 indicate two different initial value settings of $(\mathbf{w}, \mathbf{v})$ and $(\mathbf{w}, \mathbf{v}, \mathbf{u})$. To present the influence of the eavesdropper, we test the achievable rates of FSS_N when there is no eavesdropper in the system, and results are shown as the solid lines in Fig. 2(a) and Fig. 2(b).

TABLE II
Detailed System Parameters.

Parameters	**Value**
Terrestrial spanning frequency	17700 $\sim$ 18934 MHz [35], [36]
Satellite spanning frequency	17700 $\sim$ 18895.2 MHz [35], [36]
Terrestrial transmit power	-26 $\sim$ -22 dBW [35]
Satellite transmit power	9.23 dbW [35]
Terrestrial bandwidth	56 MHz [35]
Satellite bandwidth	62.4 MHz [3], [35]
Terrestrial noise power σ_p	-121.52 dBW [35]
FSS terminals noise power σ_s	-126.47 dBW [3], [35]
Eavesdropper noise power σ_e	-121.52 dBW
Number of scatters L_m	3 [8]

Results in Fig. 2 show that through ICPSO, the solutions of the optimization problem can converge to higher secrecy rates than through CPSO, no matter whether applying the NCoSTB or CoSTB scheme. In other words, for the same times of updating iteration, ICPSO tends to produce a better beamforming and AN vectors and bring a higher secrecy rate than CPSO. For both of the secure beamforming schemes, the proposed ICPSO algorithm can achieve a faster convergence to reach the maximum secrecy rate, which results from its convex approximation operation of the original nonconvex objective function. In addition, Fig. 2 also indicates that when the optimization variables are initialized differently, the CPSO algorithm may converge to different optimal values, which might be the local optimal points. Moreover, results in Fig. 2 also reveal that with the assistance of cooperative beamforming from BSs, the achievable secrecy rate of the eavesdropped FSS terminal can be greatly improved, comparing with the beamforming scheme without the BSs' cooperation.

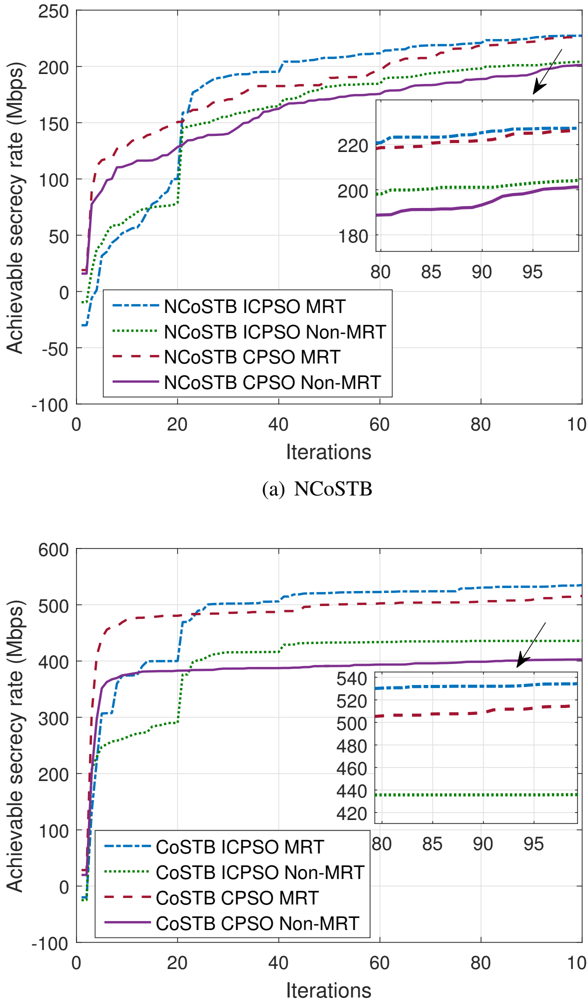
The results shown in Fig. 3 reveal the effect of the optimization variable's initialization on the convergence of the nonconvex optimization problems. In this experiment, the initial values $\left(\mathbf{w}^{(1)}, \mathbf{v}^{(1)}\right)$ and $\left(\mathbf{w}^{(1)}, \mathbf{v}^{(1)}, \mathbf{u}^{(1)}\right)$, of NCoSTB and CoSTB, respectively, are obtained by applying MRT and randomly (denoted by "Non-MRT" in Fig. 3). As shown in Fig. 3(a), for the NCoSTB scheme, the ICPSO algorithm can achieve a faster convergence reaching to a larger secrecy rate than the traditional CPSO, when applying the same initialization strategy. Moreover, no matter whether to apply MRT or



(a) NCoSTB

(b) CoSTB

Fig. 2. Evolution of the achievable secrecy rate of FSS_N and the convergence of CPSO and ICPSO for the NCoSTB and CoSTB schemes.



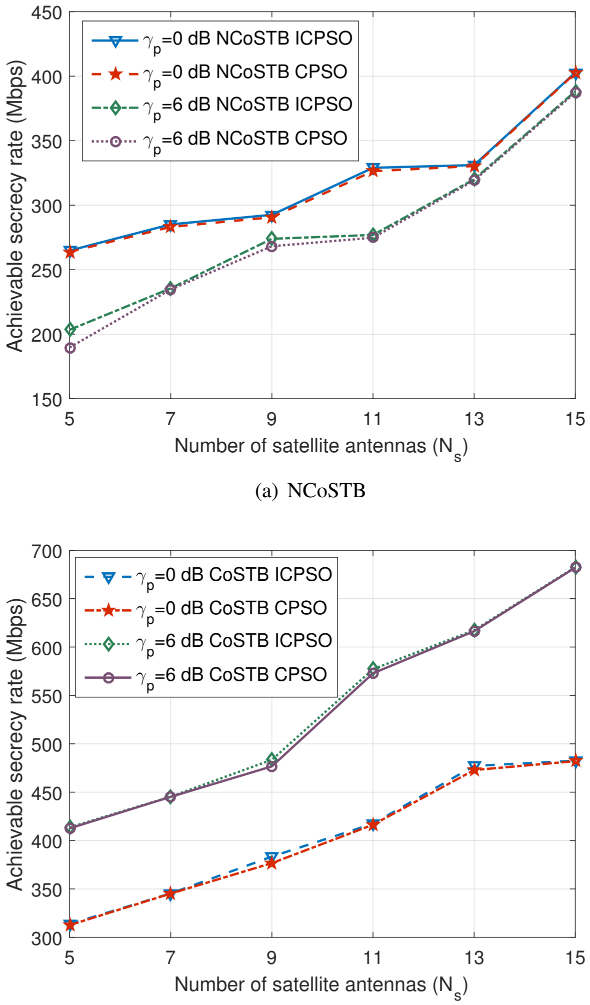
(a) NCoSTB

(b) CoSTB

Fig. 3. Achievable secrecy rate versus optimization variable's initialization.

non-MRT based initialization, we can notice that although the secrecy rates obtained by ICPSO are relatively lower than by CPSO in the beginning of the iterations (from iteration 1 to 20), the rates increase more rapidly and reach higher values in the later iterations than that of CPSO. For the CoSTB scheme, results in Fig. 2(b) present a similar phenomenon. On the other hand, due to the nonconvex characteristic of original objective function and the drawback of CPSO, the convergence points sometimes are not the global optimal solutions, which depends much on the selection of the initial feasible point. Results in Fig. 3 indicate that the initialization obtained through the MRT can achieve a better beamforming and AN vectors to get a higher secrecy rate. Even for the improved ICPSO algorithm, a random initialization may result to a weaker solution than the CPSO algorithm does with a MRT based initialization.

Next, we show the achievable secrecy rate in Fig. 4 when the number of antennas carried on the satellite varies from 5 to 15 and the BSs' SINR threshold are set as $\gamma_{ms} = \gamma_p^1 = 0$ dB and $\gamma_{ms} = \gamma_p^2 = 6$ dB, $\forall\ m \in \mathcal{M}$ [37]. As we can see, as the number of antennas on the satellite increases, the secrecy rate of the eavesdropped FSS terminal increases, no matter whether the terrestrial BSs apply the cooperative beamforming and which optimization algorithm is applied. This result shows that thanks to the mmWave techniques, multiple antennas can greatly improve the transmission capacity and security of the communication network. Moreover, results in Fig. 4 also demonstrate that when the BSs require a higher SINR threshold, the secrecy rate of the eavesdropped FSS terminal will decrease. This dropping of performance results from the fact that the satellite has to lower its transmit power and adjust its beamforming and AN vectors to reduce its interference to BSs' users, which will sacrifice its own transmission rates and secrecy rates. However, with N_s increasing, a higher achievable secrecy rate can be still achieved even when the system is constrained by a higher γ_p. In a real coexistence system of FSSs and cellular networks, the higher priority and legacy right of using some specific part of the spectrum for terrestrial BSs may reduce the capacity and security of the SatCom system. These results shown in Fig. 4 indicate that the communication quality of both FSS terminals and BSs'



(a) NCoSTB

(b) CoSTB

Fig. 4. Achievable secrecy rate versus the number of antennas carried on the satellite N_s and BSs' SINR threshold γ_p.

users can be guaranteed by the multiple antennas (such as massive-MIMO/MISO), which can be realized when using the mmWave spectrum.

To further illustrate the effect of the number of antennas N_s and BSs' SINR threshold γ_{ms} on the system performance, we present the transmit power consumption of the satellite when maximizing the secrecy rate with power and SINR threshold constraints. As the results shown in Fig. 5, for the NCoSTB and CoSTB schemes, the transmit power of satellite decreases with N_s increasing. In addition, when the BSs' SINR threshold is larger, i.e., $\gamma_{ms} = \gamma_p = 6$ dB, satellite will consume less power to guarantee the transmission quality of the BSs. Therefore, results shown in Fig. 4 and Fig. 5 reveal that the multiple antennas can contribute to improve the secure transmission capacity, meanwhile, to reduce the transmit power of the system.

VI. Conclusion

In this paper, we have considered a mmWave and MISO channel based coexistence system of FSS and terrestrial cellular networks. The physical layer security problem is analyzed for the established scenario. To achieve the secure transmission, the adaptive beamforming and AN techniques are introduced to prevent the eavesdropper from receiving and decoding information successfully. We have proposed a non-cooperative beamforming scheme, through which the BSs process precoding through a MRT beamforming. On the other hand, to further improve the secrecy rate, the CoSTB scheme has been designed, according to which BSs implement the cooperative beamforming to decrease the SINR at the eavesdropper and increase the SINR at the eavesdropped FSS terminal, meanwhile ensure the SINR at BSs' users and other legitimate FSS terminals. An iteration based approximate genetic algorithm has been designed to solve the nonconvex secrecy rate maximization problem.

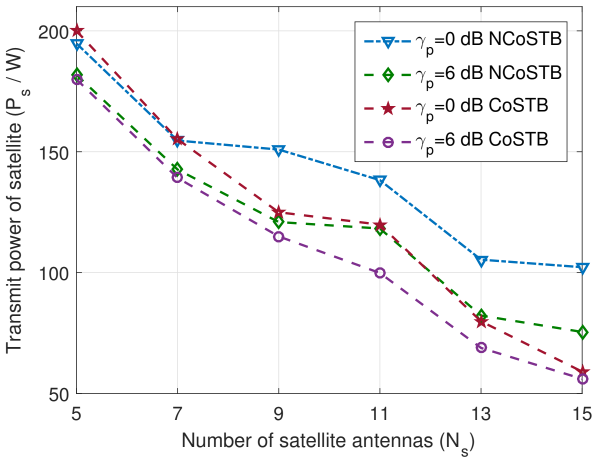


Fig. 5. Transmit power of the satellite versus the number of antennas carried on the satellite N_s and BSs' SINR threshold γ_p.

The simulation results show that massive antenna arrays and the designed secure transmission beamforming schemes can improve the secrecy rate of the eavesdropped terminal, as well as guarantee the transmission quality of the incumbent communication in the coexistence system. In addition, the convergence and efficiency of the proposed iteration based approximation algorithm are verified by the simulation results.

Appendix A
Proof of Theorem 1

For the two security beamforming schemes, i.e., NCoSTB and CoSTB, the analysis and derivation of the lower bound of $C_N(\mathbf{w}, \mathbf{v})$ and $C_N(\mathbf{w}, \mathbf{v}, \mathbf{u})$ are similar, except that the beamforming strategies of SBs are fixed according to MRT under the non-cooperation scheme. In other words, for the NCoSTB, $\mathbf{u}$ is set as a constant vector by (14). Therefore, in this part, we only provide the derivation of the lower bound of $C_N(\mathbf{w}, \mathbf{v}, \mathbf{u})$ for simplification.

As defined in (12), we have

$$\begin{aligned} C_N\left(\mathbf{w},\mathbf{v},\mathbf{u}\right) &= \log_2\left(1+\frac{\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N}{\psi_N\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)}\right)\\ &= -\log_2\left(1-\frac{\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N}{\psi_N\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)+\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N}\right)\\ &\triangleq -\log_2\left(1-\frac{g_1\left(\mathbf{w}_N\right)}{g_2\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)}\right), \end{aligned} \tag{34}$$

where

$$g_1(\mathbf{w}_N)=\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N, \tag{35a}$$

$$g_2(\mathbf{w},\mathbf{v},\mathbf{u})=\psi_N\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)+\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N>g_1\left(\mathbf{w}_N\right). \tag{35b}$$

Consider that $f\left(x\right)=-\log_2\left(1-x\right)$ is an increasing convex function of independent variable x in the domain $\left\{x\left|x<1\right.\right\}$. Thus $f\left(g_1/g_2\right)=-\log_2\left(1-g_1/g_2\right)\triangleq C_N\left(g_1,g_2\right)$ is convex in the domain $\left\{\left(g_1,g_2\right)\left|0<g_1<g_2\right.\right\}$ $\left(g_1/g_2<1\right)$, where $g_1=g_1\left(\mathbf{w}_N\right)$ and $g_2=g_2\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$ are defined as (35). Considering the Taylor expansion and the convexity of $C_N\left(g_1,g_2\right)$ when $0<g_1<g_2$, we have

$$\begin{aligned} C_N\left(g_1,g_2\right) &\geq C_N\left(g_1^{(t)},g_2^{(t)}\right)\\ &\quad+\left\langle\nabla C_N\left(g_1^{(t)},g_2^{(t)}\right),\left(g_1,g_2\right)-\left(g_1^{(t)},g_2^{(t)}\right)\right\rangle. \end{aligned} \tag{36}$$

Denote $\mathbf{x}^{(t)}=\left\{\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right\}$ and $\mathbf{x}=\left\{\mathbf{w},\mathbf{v},\mathbf{u}\right\}$ as simplified representations. Then in (36),

$$\begin{aligned} &\left\langle\nabla C_N\left(g_1^{(t)},g_2^{(t)}\right),\left(g_1,g_2\right)-\left(g_1^{(t)},g_2^{(t)}\right)\right\rangle\\ &=\frac{1}{\ln2}\frac{g_2\left(\mathbf{x}^{(t)}\right)}{g_2\left(\mathbf{x}^{(t)}\right)-g_1\left(\mathbf{x}^{(t)}\right)}\left[\frac{2\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\left(\mathbf{w}_N-\mathbf{w}_N^{(t)}\right)\right\}}{g_2\left(\mathbf{x}^{(t)}\right)}\right]\\ &\quad-\frac{1}{\ln2}\frac{g_2\left(\mathbf{x}^{(t)}\right)}{g_2\left(\mathbf{x}^{(t)}\right)-g_1\left(\mathbf{x}^{(t)}\right)}\left(\frac{g_1\left(\mathbf{x}^{(t)}\right)}{g_2^2\left(\mathbf{x}^{(t)}\right)}\right)\left[g_2\left(\mathbf{x}^{(t)}\right)-g_2(\mathbf{x})\right]\\ &=\frac{2}{\ln2}\frac{\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\left(\mathbf{w}_N-\mathbf{w}_N^{(t)}\right)\right\}}{\psi_N\left(\mathbf{x}^{(t)}\right)}\\ &\quad-\frac{1}{\ln2}\left[\frac{1}{\psi_N\left(\mathbf{x}^{(t)}\right)}-\frac{1}{\psi_N\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}}\right]\left[\psi_N(\mathbf{x})\right.\\ &\quad\left.+\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N-\psi_N\left(\mathbf{x}^{(t)}\right)-\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\right]\\ &=\frac{1}{\ln 2}\frac{\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\left(\mathbf{w}_N-\mathbf{w}_N^{(t)}\right)\right\}}{\psi_N\left(\mathbf{x}^{(t)}\right)}\\ &\quad-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\left(\psi_N\left(\mathbf{x}\right)+\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N\right)}{\psi_N\left(\mathbf{x}^{(t)}\right)\left[\psi_N\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\right]}\\ &\quad+\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}}{\psi_N\left(\mathbf{x}^{(t)}\right)}\\ &=\frac{2}{\ln 2}\frac{\Re\left\{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N\right\}}{\psi_N\left(\mathbf{x}^{(t)}\right)}-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}}{\psi_N\left(\mathbf{x}^{(t)}\right)}\\ &\quad-\frac{1}{\ln 2}\frac{\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\left(\psi_N\left(\mathbf{x}\right)+\mathbf{w}_N^H\mathbf{R}_N\mathbf{w}_N\right)}{\psi_N\left(\mathbf{x}^{(t)}\right)\left[\psi_N\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_N\mathbf{w}_N^{(t)}\right]}. \end{aligned}$$

Substituting the result obtained above into (36), then (21) can be achieved. This completes the proof of Theorem 1.

Appendix B
Proof of Theorem 2

In this part, we will only derive the upper bound of $C_{eN}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$ for the CoSTB scheme. When applying the NCoSTB scheme, the derivation is similar to that of NCoSTB, by considering $\mathbf{u}$ as a constant vector.

According to the definition in (12), we have

$$\begin{aligned} C_{eN}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right) &= \ln\left(1+\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)}\right)\\ &= \log_2\left(1+\Gamma_e\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)\right)\triangleq C_{eN}\left(\Gamma_e\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)\right), \end{aligned} \tag{37}$$

which is an increasing concave function of $\Gamma_e\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$. Denote $\mathbf{x}^{(t)}=\left\{\mathbf{w}^{(t)},\mathbf{v}^{(t)},\mathbf{u}^{(t)}\right\}$ and $\mathbf{x}=\left\{\mathbf{w},\mathbf{v},\mathbf{u}\right\}$. Thus we have

$$\begin{aligned} \log_2\left(1+\Gamma_e\left(\mathbf{x}\right)\right) &\leq \log_2\left(1+\Gamma_e\left(\mathbf{x}^{(t)}\right)\right)\\ &\quad+\left\langle\nabla C_{eN}\left(\Gamma_e\left(\mathbf{x}^{(t)}\right)\right),\Gamma_e^{(t)}\left(\mathbf{x}\right)-\Gamma_e\left(\mathbf{x}^{(t)}\right)\right\rangle, \end{aligned} \tag{38}$$

where

$$\begin{aligned} &\left\langle\nabla C_{eN}\left(\Gamma_e\left(\mathbf{x}^{(t)}\right)\right),\Gamma_e\left(\mathbf{x}\right)-\Gamma_e\left(\mathbf{x}^{(t)}\right)\right\rangle\\ &=\frac{1}{\ln2}\frac{\psi_e\left(\mathbf{x}^{(t)}\right)}{\psi_e\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_e\mathbf{w}_N^{(t)}}\left[\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e^{(t)}\left(\mathbf{x}\right)}-\frac{\left(\mathbf{w}_N^H\right)^{(t)}\mathbf{R}_e\mathbf{w}_N^{(t)}}{\psi_e\left(\mathbf{x}^{(t)}\right)}\right]\\ &=\frac{1}{\ln2}\frac{\psi_e\left(\mathbf{x}^{(t)}\right)}{\psi_e\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_e\mathbf{w}_N^{(t)}}\left[\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e^{(t)}\left(\mathbf{x}\right)}\begin{matrix}+1\\-1\end{matrix}\frac{\left(\mathbf{w}_N^H\right)^{(t)}\mathbf{R}_e\mathbf{w}_N^{(t)}}{\psi_e\left(\mathbf{x}^{(t)}\right)}\right]\\ &=\frac{1}{\ln2}\frac{\psi_e\left(\mathbf{x}^{(t)}\right)}{\psi_e\left(\mathbf{x}^{(t)}\right)+\left(\mathbf{w}_N^{(t)}\right)^H\mathbf{R}_e\mathbf{w}_N^{(t)}}\left[\frac{\mathbf{w}_N^H\mathbf{R}_e\mathbf{w}_N}{\psi_e^{(t)}\left(\mathbf{x}\right)}+1\right]-\frac{1}{\ln 2}, \end{aligned}$$

where $\psi_e^{(t)}\left(\mathbf{w},\mathbf{v},\mathbf{u}\right)$ is defined by (26). Substituting the result obtained above into (38), then (25) can be achieved. This completes the proof of Theorem 2.

References

[1] H. Zhang, S. Huang, C. Jiang, K. Long, V. C. Leung, and H. V. Poor, "Energy efficient user association and power allocation in millimeter wave based ultra dense networks with energy harvesting base stations," *IEEE J. Sel. Areas Commun.*, to be published.

[2] F. Guidolin, M. Nekovee, L. Badia, and M. Zorzi, "A study on the coexistence of fixed satellite service and cellular networks in a mmWave scenario," in *IEEE Int. Conf. on Commun. (ICC 2015)*. London, UK, 8-12 Jun. 2015, pp. 2444–2449.

[3] E. Lagunas, S. K. Sharma, S. Maleki, S. Chatzinotas, and B. Ottersten, "Resource allocation for cognitive satellite communications with incumbent terrestrial networks," *IEEE Trans. Cognitive Commun. and Networking*, vol. 1, no. 3, pp. 305–317, Sept. 2015.

[4] F. Guidolin, M. Nekovee, L. Badia, and M. Zorzi, "A cooperative scheduling algorithm for the coexistence of fixed satellite services and 5g cellular network," in *IEEE Int. Conf. on Commun. (ICC 2015)*. London, UK, 8-12 Jun. 2015, pp. 1322–1327.

[5] ERC/DEC/(00)07, "The shared use of the band 17.7-19.7 GHz by the fixed service and earth stations of the fixed-satellite service (space-to-earth)," in *ECC Report 241*. Electronic Commun. Committee, Copenhagen, Denmark, approved: 19 Oct. 2000, amended: 4 Mar. 2016.

[6] M. Corici, A. Kapovits, S. Covaci, A. Geurtz, I.-D. Gheorghe-Pop, B. Riemer, and A. Weber, "Assessing satellite-terrestrial integration opportunities in the 5G environment," *[On-line] Available: https://artes. esa. int/sites/default/files/Whitepaper*, Sept. 2016.

[7] C. Niephaus, M. Kretschmer, and G. Ghinea, "QoS provisioning in converged satellite and terrestrial networks: A survey of the state-of-the-art," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 4, pp. 2415–2441, Apr. 2016.

[8] S. Shi, G. Li, K. An, Z. Li, and G. Zheng, "Optimal power control for real-time applications in cognitive satellite terrestrial networks," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1815–1818, Aug. 2017.

[9] K. An, M. Lin, T. Liang, J.-B. Wang, J. Wang, Y. Huang, and A. L. Swindlehurst, "Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference," pp. 4390–4404, Nov. 2015.

[10] C. Jiang, X. Zhu, L. Kuang, Y. Qian, and J. Lu, "Multimedia multicast beamforming in integrated terrestrial-satellite networks," in *13th Int. Wireless Commun. and Mobile Computing Conf. (IWCMC 2017)*. Valencia, Spain, 26-30 Jun. 2017, pp. 340–345.

[11] J. Lei, Z. Han, M. Á. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 661–671, Sept. 2011.

[12] 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, Nov. 2016.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[14] A. D. Wyner, "The wire-tap channel," *Bell Lab. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[15] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, May 2008.

[16] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The gaussian wiretap channel with a helping interferer," in *IEEE Int. Symp. on Inform. Theory (ISIT 2008)*. Toronto, ON, Canada, 6-11 Jul. 2008, pp. 389–393.

[17] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec. 2016.

[18] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP J. on Wireless Commun. and Networking*, vol. 2009, no. 452907, pp. 1–10, Jan. 2010.

[19] S. R. Aghdam and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3913–3923, Jun. 2017.

[20] S.-H. L. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–493, Jul. 2014.

[21] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid analog-digital precoding design for secrecy mmWave MISO-OFDM systems," *IEEE Trans. Commun.*, to be published.

[22] G. Lee, Y. Sung, and M. Kountouris, "On the performance of random beamforming in sparse millimeter wave channels," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 560–575, Apr. 2016.

[23] G. Lee, Y. Sung, and J. Seo, "Randomly-directional beamforming in millimeter-wave multiuser MISO downlink," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1086–1100, Feb. 2016.

[24] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, Feb. 2017.

[25] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450–2464, Apr. 2017.

[26] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[27] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1714–1725, Oct. 2016.

[28] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[29] F. Wang, C. Xu, Y. Huang, X. Wang, and X. Gao, "REEL-BF design: Achieving the SDP bound for downlink beamforming with arbitrary shaping constraints," *IEEE Trans. Signal Process.*, vol. 65, no. 10, pp. 2672–2685, Feb. 2017.

[30] F. Zhu and M. Yao, "Improving physical-layer security for crns using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[31] F. Van den Bergh and A. P. Engelbrecht, "A cooperative approach to particle swarm optimization," *IEEE Trans. Evol. Comput.*, vol. 8, no. 3, pp. 225–239, Jun. 2004.

[32] Y. Dong, L. Qiu, and X. Liang, "Energy efficiency maximization for uplink SCMA system using CCPSO," in *IEEE Global Commun. Conf. Workshops (GLOBECOM Wkshps 2016)*. Washington, DC, USA, 4-8 Dec. 2016, pp. 1–5.

[33] M. R. Javan, N. Mokari, F. Alavi, and A. Rahmati, "Resource allocation in decode-and-forward cooperative communication networks with limited rate feedback channel," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 256–267, Jan. 2017.

[34] A. Modiri, X. Gu, A. M. Hagan, and A. Sawant, "Radiotherapy planning using an improved search strategy in particle swarm optimization," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 5, pp. 980–989, May 2017.

[35] E. Lagunas, S. Maleki, L. Lei, C. Tsinos, S. Chatzinotas, and B. Ottersten, "Carrier allocation for hybrid satellite-terrestrial backhaul networks," in *IEEE Int. Conf. on Commun. Workshop (ICC Wkshps 2017) on Satellite Commun.: Challenges and Integration in the 5G ecosystem*, 21–25 May 2017, pp. 1–6.

[36] S. K. Sharma, S. Chatzinotas, J. Grotz, and B. Ottersten, "3D beamforming for spectral coexistence of satellite and terrestrial networks," in *82nd IEEE Veh. Technology Conf. (VTC Fall 2015)*. Boston, MA, USA, 6-9 Sept. 2015, pp. 1–5.

[37] J. Lei, Z. Han, M. Vázquez-Castro, and A. Hjørungnes, "Multibeam SATCOM systems design with physical layer security," in *IEEE Int. Conf. on Ultra-Wideband (ICUWB 2011)*. Bologna, Italy, 14-16 Sept. 2011, pp. 555–559.