Short Papers

Secure Beamforming for Cognitive Satellite Terrestrial Networks With Unknown Eavesdroppers

Zhi Lin, Min Lin, *Member, IEEE*, Benoit Champagne, *Senior Member, IEEE*,
Wei-Ping Zhu, *Senior Member, IEEE*, and Naofal Al-Dhahir, *Fellow, IEEE*

***Abstract*—This article proposes a beamforming (BF) scheme for a cognitive satellite terrestrial network, where the base station (BS) and a cooperative terminal (CT) are exploited as green interference resources to enhance the system security performance in the presence of unknown eavesdroppers. Different from the related works, we assume that only imperfect channel information of the mobile user (MU) and earth station (ES) is available. Specifically, we formulate an optimization problem with the objective to degrade the possible wiretap channels within the private signal beampattern region, while imposing constraints on the signal-to-interference-plus-noise ratio (SINR) at the MU, the interference level of the ES and the total transmit power budget of the BS and CT. To solve this mathematically intractable problem, we propose a joint artificial noise generation and cooperative jamming BF scheme to suppress the interception. Finally, the effectiveness and superiority of the proposed BF scheme are confirmed through computer simulations.**

***Index Terms*—Artificial noise (AN), beamforming (BF), cognitive satellite terrestrial networks, cooperative jamming (CJ).**

I. Introduction

Cognitive satellite terrestrial networks (CSTNs), which share frequency resources among satellite and terrestrial subnetworks, are considered as a promising approach to provide seamless connectivity and services not only in densely populated, but also in sparsely populated areas [1]. To enable coexistence of these two subnetworks, the base station (BS) can employ interference management schemes such as transmit beamforming (BF) [2], resource allocation [3], or cooperative scheduling [4], so that the interference affecting the unintended user remains below a certain threshold.

Due to the broadcast nature of wireless communications, CSTN is vulnerable to security threats. During the past decade, physical layer security (PLS), which exploits properties of the wireless channels along with advanced signal processing techniques to achieve secure communication at the physical layer, has attracted considerable research interest [5]–[7]. By exploiting *green* interference, An *et al.* [6] proposed two zero-forcing-based BF schemes to enhance the security of satellite downlink transmission in CSTN. This article is an extension of a more general scenario in [7], where a joint BF scheme was proposed to minimize the total transmit power of the satellite and base station under security constraints.

In most existing PLS works, it is assumed that the transmitter has perfect/partial knowledge of the wiretap channel [8]–[11]. However, due to the passive characteristic of eavesdroppers (Eves), it is difficult to obtain the wiretap channel state information (CSI). To overcome this obstacle, BF design with unknown wiretap CSI has been investigated in [12]–[14], where the transmit power of either the artificial noise (AN) or the cooperative jamming (CJ) signal is maximized to interfere with the unknown Eves under constraint on the signal-to-interference-plus-noise ratio (SINR) of legitimate users. It is worth mentioning that the commonly used secrecy rate objective and constraints are not applicable to the unknown wiretap CSI scenario. In addition, the above-mentioned works aimed at maximizing the transmit power of the interference signal, instead of the received interference power at the unknown Eves, which is not power efficient.

In this article, under the assumption of imperfect knowledge of the angles of departure (AoD) for the mobile user (MU) and earth station (ES), our objective is to degrade the possible wiretap channels within the private signal beampattern region, subject to constraints on the SINR at the MU, the interference level (IL) of the ES, and the total power budget of the BS and cooperative terminal (CT). Specifically, the private signal is processed with the BS transmit beamformer to satisfy the SINR requirement at the MU under the IL constraint. Meanwhile, the AN and CJ beamformers at the BS and CT, respectively, are steered towards the private signal beampattern region to suppress the interception. Simulation results are provided to verify the effectiveness and superiority of the proposed secure BF scheme. Compared with the existing CSTN works [6]-[10], our approach is more practical since it does not require knowledge of the wiretap CSI. Furthermore, in contrast to the transmit AN/CJ power maximization in [12]–[14], we focus on the private signal leakage region and propose a more power efficient scheme to achieve secure communications, which to the best of our knowledge has not been previously investigated in the context of CSTN.

II. System Model

As shown in Fig. 1, we consider a CSTN, where the satellite and cellular subnetwork share the same mmWave frequency band. The

Manuscript received December 24, 2019; revised February 24, 2020; accepted March 18, 2020. Date of publication April 20, 2020; date of current version June 16, 2021. This work was supported in part by the Key International Cooperation Research Project under Grant 61720106003 and in part by Shanghai Aerospace Science and Technology Innovation Foundation under Grant SAST2019-095. *(Corresponding author: Min Lin.)*

Zhi Lin is with the College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China, and also with the Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0G4, Canada (e-mail: linzhi945@163.com).

Min Lin is with the College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: linmin@njupt.edu.cn).

Benoit Champagne is with the Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0G4, Canada (e-mail: benoit.champagne@mcgill.ca).

Wei-Ping Zhu is with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada, and also with the College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: weiping@ece.concordia.ca).

Naofal Al-Dhahir is with the Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: aldhahir@utdallas.edu).

Digital Object Identifier 10.1109/JSYST.2020.2983309

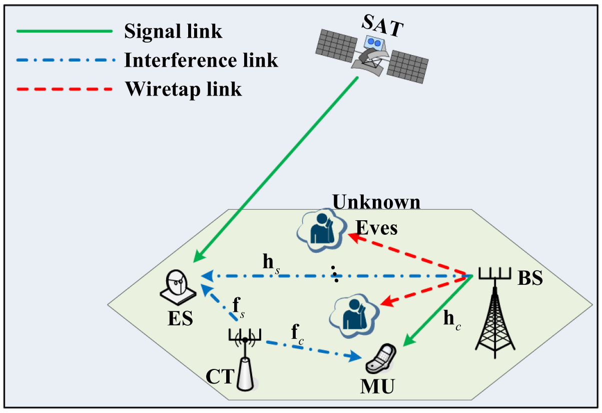

Fig. 1. System model of the considered CSTN.

geostationary orbit satellite serves an ES, while the BS serves a MU in the presence of several unknown Eves. The CT transmits a CJ signal to suppress the interception. The assumption of frequency-flat slow-fading channel model is adopted [15]. It is also assumed that the BS and CT are equipped with uniform linear arrays (ULAs) with N_b and N_c antennas, respectively. Due to the highly directional nature of mmWave transmissions, the terrestrial downlink channel can be modeled as the superposition of a predominant line-of-sight (LoS) propagation component and a sparse set of single-bounce non-LoS (NLoS) components. Hence, the terrestrial downlink channel vector can be expressed as [16]

$$\mathbf{h} = \sqrt{g\left(\theta_0\right)}\rho_0\mathbf{a}\left(\theta_0\right) + \sqrt{\frac{1}{L}}\sum_{l=1}^{L}\sqrt{g\left(\theta_l\right)}\rho_l\mathbf{a}\left(\theta_l\right) \tag{1}$$

where L is the number of NLoS paths, ρ_0 and ρ_l represent the path loss associated with the LoS path and the lth NLoS path, respectively, and $|\rho_0| = \lambda/(4\pi d)$ with λ being the wavelength, and d the transmission distance. The path losses of the NLoS components are typically 5 to 10 dB larger than that of the LoS component [16]. In (1), $g(\theta)$ is the common directivity pattern of the antenna elements, with θ being the AoD. According to the ITU guidelines in [17], the directivity pattern in dB, namely, $g(\theta)$ is described as

$$g\left(\theta\right) = g_{\max} - \min\left\{12(\theta/\theta_{3\mathrm{dB}})^2, \mathrm{SLL}\right\} \tag{2}$$

where $\theta_{3\mathrm{dB}}$ is the antenna array 3 dB beamwidth, SLL stands for the sidelobe level of the array pattern. In addition, $\mathbf{a}(\theta)$ denotes the ULA steering vector, which is expressed as

$$\mathbf{a}\left(\theta\right) = \left[e^{-j\beta((N-1)/2)d\cos\theta}, \cdots, e^{+j\beta((N-1)/2)d\cos\theta}\right]^T. \tag{3}$$

Let s denote the private information signal transmitted by the BS to the MU. Prior to transmission, this signal is normalized as $E[|s|^2] = 1$, and mapped with a BF weight vector $\mathbf{w} \in \mathbb{C}^{N_b\times 1}$. Note that the interference link between the satellite and MU can be neglected [8] since the antenna gain at the MU is much weaker than that at the ES. Meanwhile, the BS and CT send AN $\mathbf{v} \in \mathbb{C}^{N_b\times 1}$ and CJ signal $\mathbf{x} \in \mathbb{C}^{N_c\times 1}$, respectively, to interfere with the unknown Eves. Denote $\{\mathbf{h}_c, \mathbf{h}_s\}$ and $\{\mathbf{f}_c, \mathbf{f}_s\}$ as the channel vectors from the BS and CT to the MU and ES, respectively. Thus, the received signal at the MU is expressed as

$$y_c = \mathbf{h}_c^H\mathbf{w}s + \mathbf{h}_c^H\mathbf{v} + \mathbf{f}_c^H\mathbf{x} + n_c \tag{4}$$

where n_c denotes the complex Gaussian random noise whose variance is $\sigma_c^2 = \kappa BT$ with κ, B and T being the Boltzmann constant, bandwidth, and noise temperature, respectively. Hence, the output SINR at the MU can be written as

$$\gamma_c = \frac{\left|\mathbf{h}_c^H\mathbf{w}\right|^2}{\left|\mathbf{h}_c^H\mathbf{v}\right|^2 + \left|\mathbf{f}_c^H\mathbf{x}\right|^2 + \sigma_c^2} \tag{5}$$

and the interference power to the ES is given by

$$\mathrm{I}_t = \left|\mathbf{h}_s^H\mathbf{w}\right|^2 + \left|\mathbf{h}_s^H\mathbf{v}\right|^2 + \left|\mathbf{f}_s^H\mathbf{x}\right|^2. \tag{6}$$

III. Secure BF Schemes

A. Traditional BF Problem Formulation

In the existing works based on the assumption of unknown wiretap CSI [12]–[14], since no information about the wiretap channels is available, the secrecy rate cannot be evaluated and the commonly used approach is to allocate as much transmit power to the jamming signals as possible, while constraining the SINR of the MU, the IL at the ES and the total power budget. Assuming that the total power budget of the BS and CT is P_{tot}, the optimization problem can be expressed as

$$\begin{aligned} &\max_{\mathbf{w},\mathbf{v},\mathbf{x}} \|\mathbf{v}\|^2 + \|\mathbf{x}\|^2 \\ &\text{s.t.} \quad \gamma_c \geq \Gamma_c \\ &\quad \mathrm{I}_t \leq \Gamma_I \\ &\quad \|\mathbf{w}\|^2 + \|\mathbf{v}\|^2 + \|\mathbf{x}\|^2 \leq P_{\mathrm{tot}}. \end{aligned} \tag{7}$$

The above-mentioned problem can be solved using standard optimization software packages such as CVX, resulting in the AN and CJ signals in the form of isotropically distributed noise within the null space (i.e. orthogonal complement) of $\{\mathbf{h}_c, \mathbf{h}_s, \mathbf{f}_s\}$.

Considering the high directivity of antenna array beampatters in mmWave applications, the interference signals in [12]–[14] were designed by allocating a maximum amount of power within the null space of the private signal, whereas unknown Eves lying in this null space cannot properly receive the private signal and successfully decode it. Therefore, the power maximization of randomly distributed jamming signal within the above-mentioned null space is not power efficient. In the following, we propose an alternative and power efficient BF scheme to suppress the interception in the above-mentioned scenario.

B. Proposed BF scheme

The private signal beampattern can be viewed as a leakage region (i.e., a spatial area) where the private signal is more easily accessible to the unknown Eves. Therefore, in this part, we aim at maximizing the interference signal power in the private signal beampattern region, without affecting the MU. Specifically, the BF vector $\mathbf{w}$ at the BS is designed to satisfy the private signal power constraint at the MU under the IL constraint of the ES. Meanwhile, the AN and CJ beamformers at the BS and CT are steered towards the sidelobes and mainlobe of $\mathbf{w}$, respectively, to suppress the interception.

Due to the mobility of terminals and channel estimation mismatch, perfect knowledge of the CSI is unavailable. To address this issue within the mmWave context, we exploit the angular information based uncertainty model [8], and assume that available channels belong to a given AoD uncertainty set $\mathbb{U} = \{\theta_i \in [\theta_i^L, \theta_i^U], \varphi_i \in [\varphi_i^L, \varphi_i^U]\}$, where θ_i and φ_i denotes the AoD of the BS and CT downlink channels. respectively. By defining $\mathcal{P} = \|\mathbf{v}\|^2 + \|\mathbf{x}\|^2$ as the interference power in the private signal beampattern region, the optimization problem can

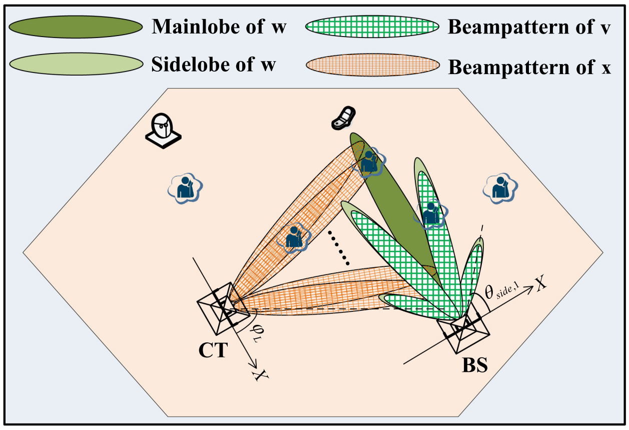

Fig. 2. Proposed BF scheme.

be formulated as

$$\max_{\mathbf{w},\mathbf{v},\mathbf{x}} \mathcal{P} \tag{8a}$$

$$\text{s.t.} \quad \min_{\mathbb{U}} \frac{\mathbf{w}^H\mathbf{H}_c\mathbf{w}}{\mathbf{v}^H\mathbf{H}_c\mathbf{v}+\mathbf{x}^H\mathbf{F}_c\mathbf{x}+\sigma_c^2} \geq \Gamma_c \tag{8b}$$

$$\max_{\mathbb{U}} \mathbf{w}^H\mathbf{H}_s\mathbf{w}+\mathbf{v}^H\mathbf{H}_s\mathbf{v}+\mathbf{x}^H\mathbf{F}_s\mathbf{x} \leq \Gamma_I \tag{8c}$$

$$\|\mathbf{w}\|^2+\|\mathbf{v}\|^2+\|\mathbf{x}\|^2 \leq P_{\text{tot}}. \tag{8d}$$

where $\mathbf{H}_c = \mathbf{h}_c\mathbf{h}_c^H, \mathbf{F}_c = \mathbf{f}_c\mathbf{f}_c^H, \mathbf{H}_s = \mathbf{h}_s\mathbf{h}_s^H$, and $\mathbf{F}_s = \mathbf{f}_s\mathbf{f}_s^H$. Since the constraints (8b) and (8c) are nonconvex due to the AoD uncertainty as per the $\mathbb{U}$, we apply a discretization method to convert these constraints into tractable forms. Specifically, we select *M* + 1 uniformly spaced angles within the AoD uncertainty set as follows:

$$\theta_i^{(j)} = \theta_i^L + j\Delta\theta_i, \quad j = 0,\ldots,M$$

$$\varphi_i^{(j)} = \varphi_i^L + j\Delta\varphi_i, \quad j = 0,\ldots,M \tag{9}$$

where $\theta_i^{(j)}$ and $\varphi_i^{(j)}$ are the *j*th uniformly spaced AoD in $\mathbb{U}$, respectively, and $\Delta\theta_i = (\theta_i^U - \theta_i^L)/M$, $\Delta\varphi_i = (\theta_i^U - \theta_i^L)/M$. Then, we define $\tilde{\mathbf{H}} = \sum_{j=0}^M \mu_j\mathbf{H}^{(j)}$ and $\tilde{\mathbf{F}} = \sum_{j=0}^M \mu_j\mathbf{F}^{(j)}$, where $\mathbf{H}^{(j)} = \mathbf{h}^{(j)}\mathbf{h}^{(j)H}$ and $\mathbf{F}^{(j)} = \mathbf{f}^{(j)}\mathbf{f}^{(j)H}$, and $\mu_j = \frac{1}{M+1}$. This method has been adopted in [16] with satisfactory robustness. Thus, the max and min operations over $\mathbb{U}$ in (8b) and (8c) can be removed.

While problem (8) and (9) remains mathematically challenging, we herein approach it heuristically, based on fundamental and well-proven BF concepts. The private signal beamformer can be obtained as $\mathbf{w} = \sqrt{P_w}\bar{\mathbf{w}} = \sqrt{P_w}\text{eig}(\tilde{\mathbf{H}}_c, \tilde{\mathbf{H}}_s + \mathbf{I}_{N_b})$, where P_w is the transmit power of $\mathbf{w}$, and $\text{eig}(\mathbf{A},\mathbf{B})$ denotes the corresponding eigenvector of the largest generalized eigenvalue of the matrix pair $(\mathbf{A},\mathbf{B})$. As illustrated in Fig. 2, the AN and CJ beamformers at the BS and CT are steered towards the sidelobes and mainlobe of $\mathbf{w}$, i.e., the private signal leakage region. Since the beampattern of $\mathbf{w}$ is available at the BS, the AN beamformer $\mathbf{v}$ is steered towards the N_s sidelobes of $\mathbf{w}$'s beampattern as follows:

$$\mathbf{v} = \sum_{n=1}^{N_s}\left(P_v\frac{P_{\text{side},n}}{\sum_{n=1}^{N_s}P_{\text{side},n}}\right)^{1/2}\mathbf{v}_n \tag{10a}$$

$$\max_{\|\mathbf{v}_n\|=1} \frac{\mathbf{v}_n^H\mathbf{a}\left(\theta_{\text{side},n}\right)\mathbf{a}^H\left(\theta_{\text{side},n}\right)\mathbf{v}_n}{\mathbf{v}_n^H\left(\tilde{\mathbf{H}}_c+\tilde{\mathbf{H}}_s+\mathbf{I}_{N_b}\right)\mathbf{v}_n} \tag{10b}$$

where P_v denotes the AN transmit power, $P_{\text{side},n}$ is the *n*th sidelobe signal strength, $\mathbf{a}(\theta_{\text{side},n})$ denotes the steering vector (SV) of the *n*th sidelobe, and $\mathbf{v}_n$ is steered to suppress the interception in the *n*th sidelobe while avoiding the additional interference on the MU and ES. Since (10b) is in a Rayleigh quotient form, the optimal solution of $\mathbf{v}_n$ can be expressed as

$$\mathbf{v}_n = \text{eig}\left(\mathbf{a}\left(\theta_{\text{side},n}\right)\mathbf{a}^H\left(\theta_{\text{side},n}\right), \tilde{\mathbf{H}}_c+\tilde{\mathbf{H}}_s+\mathbf{I}_{N_b}\right). \tag{11}$$

Then, the CJ beamformer is designed to suppress the interception along the mainlobe of the private signal beampattern. Considering that the leakage area of the $\mathbf{w}$ mainlobe is much wider than the 3 dB beamwidth of the CJ beamformer from the CT perspective, the CT aims at generating several sub-CJ beamformers to cover the $\mathbf{w}$ mainlobe region. The antenna beampattern of the ULA is given by

$$|E(\varphi)| = \left|\frac{\sin\left[N_c(\pi d/\lambda)\sin\varphi\right]}{\sin\left[(\pi d/\lambda)\sin\varphi\right]}\right|. \tag{12}$$

In order to find the 3 dB beamwidth $\varphi_{3\text{dB}}$, the above-mentioned equation should be equated to $1/\sqrt{2}$, leading to the solution for φ given by $0.89\lambda/D$, where *D* is the total aperture length which can be approximated as $N_c d$. For a spacing of $d = \lambda/2$, the 3 dB beamwidth simplifies to $\varphi_{3\text{dB}} = 2/N_c$. By assuming that the angle range of the $\mathbf{w}$ mainlobe is $[\varphi_L, \varphi_U]$ from the perspective of the CT, the coverage of the mainlobe can be achieved with $N_m = [(\varphi_U - \varphi_L)/\varphi_{3\text{dB}}]^+ + 1$ separate beamformers. Similar to (10) and (11), the CJ beamformer $\mathbf{x}$ is expressed as

$$\mathbf{x} = \sum_{m=1}^{N_m}\sqrt{P_x/N_m}\mathbf{x}_m$$

$$\mathbf{x}_m = \text{eig}\left(\mathbf{a}\left(\varphi_{\text{main},m}\right)\mathbf{a}^H\left(\varphi_{\text{main},m}\right), \tilde{\mathbf{F}}_c+\tilde{\mathbf{F}}_s+\mathbf{I}_{N_c}\right) \tag{13}$$

where P_x is the transmit power for the CJ beamformer, and $\mathbf{a}(\varphi_{\text{main},m})$ is the SV towards the *m*th component of $\mathbf{w}$. By assuming that strength of $\mathbf{w}$'s mainlobe is P_{main}, and substituting (11) and (13) into constraint (8b), the power allocation of the AN beamformer can be obtained as

$$P_v = \frac{P_{\text{tot}}\bar{\mathbf{w}}^H\mathbf{H}_c\bar{\mathbf{w}} - \Gamma_c\sigma_c^2}{\left(\Gamma_c\sum\limits_{n=1}^{N_s}\mathbf{v}_n^H\tilde{\mathbf{H}}_c\mathbf{v}_n + \frac{N_m P_{\text{main}}\left(\Gamma_c\sum_{m=1}^{N_m}\mathbf{x}_m^H\tilde{\mathbf{H}}_c\mathbf{x}_m+1\right)}{\sum_{n=1}^{N_s}P_{\text{side},n}}+1\right)} \tag{14}$$

and the power allocation of $\mathbf{x}$ and $\mathbf{w}$ are obtained as $P_x = P_v N_m P_{\text{main}}/\sum_{n=1}^{N_s}P_{\text{side},n}$ and $P_w = P_{tot} - P_v - P_x$.

IV. Numerical Results

We assume that $N_b = N_c = 10$, the number of unknown Eves follows a Poisson distribution, and their locations are uniformly distributed in the cellular coverage region (circular region with 100 m radius). The IL threshold is set as $\Gamma_I = 10$ dBmW and the total power budget as $P_{\text{tot}} = 5$ dBW. Unless otherwise indicated, the SINR threshold of the MU is set as $\Gamma_c = 3$ dB and the AoD uncertainty step size as $\Delta = 6°$. Besides, the BF scheme in [12] is adopted as the benchmark.

Figs. 3 and 4 depict the beampatterns of $\mathbf{w}$, $\mathbf{v}$, $\mathbf{x}$, and $\mathbf{x}_m$ from the perspective of the BS and CT. It can be observed that the mainlobe of $\mathbf{w}$ points to the MU and that the mainlobes of $\mathbf{v}$ are aligned with the sidelobes of $\mathbf{w}$, respectively, while generating nulls with -60 dB depth in the uncertainty region of the ES. The beamformer $\mathbf{x}$, derived from $\mathbf{x}_m$, is designed to suppress the interception in the mainlobe region of $\mathbf{w}$ with at least -10 dB interference. Figs. 3 and 4 verify that the proposed scheme can effectively suppress interception within the private signal region. Fig. 5 plots the maximal SINR of unknown Eves versus the MU SINR threshold. Note that the bounded imperfect CSI assumption of the [12] is replaced with the AoD uncertainty bound for comparison. It is clear that our proposed BF scheme outperforms the benchmark

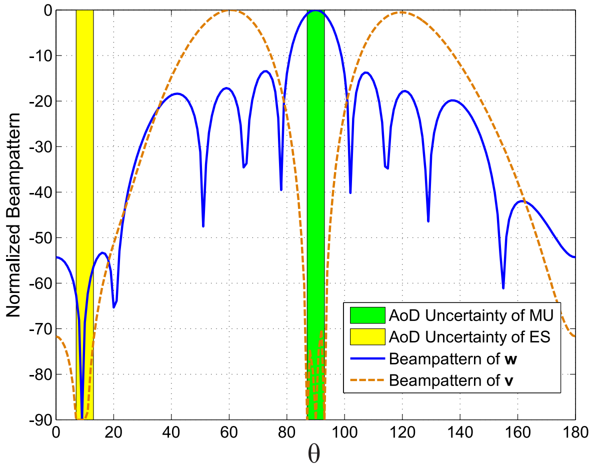

Fig. 3. Beampattern of $\mathbf{w}$ and $\mathbf{v}$.

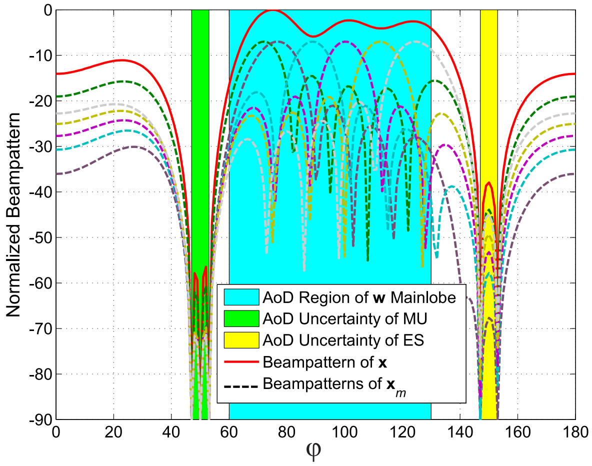

Fig. 4. Beampattern of $\mathbf{x}$.

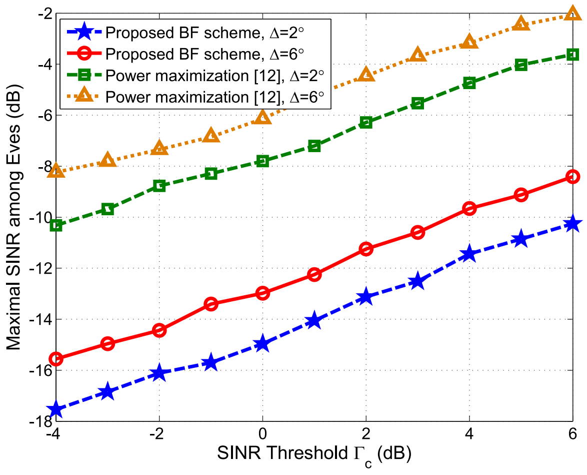

Fig. 5. Maximal SINR among Eves versus Γ_c.

scheme, which is based on interference power maximization. This is due to the fact that the proposed BF scheme exploits the interference to suppress the interception in the private signal leakage area instead of transmitting the interference signal in the null space of the private signal and maximizing the interference power.

V. Conclusion

In this article, we have presented a novel BF design for CSTN operating in the mmWave band. By considering unknown Eves and imperfect knowledge of the AoD for the legitimate users, we have aimed to degrade the possible wiretap channels in the private signal beampattern region, while satisfying constraints on SINR at the MU, IL of the ES and total power budget of the BS and CT. First, we used a discretization method to transform the constraints involving the imperfect channel into tractable ones. Then, the AN and CJ beamformers were steered towards the private signal beampattern region to suppress the interception. Finally, numerical results demonstrated the superiority and effectiveness of the proposed secure BF scheme in comparison with a benchmark scheme.

References

[1] 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, Mar. 2019.

[2] J. Du, C. Jiang, H. Zhang, X. Wang, Y. Ren, and M. Debbah, “Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1367–1382, Jul. 2018.

[3] B. Li, Z. Fei, X. Xu, and Z. Chu, “Resource allocations for secure cognitive satellite-terrestrial networks,” *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 78–81, Jan. 2018.

[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 *Proc. IEEE Int. Conf. Commun.*, Jun. 2015, pp. 1322–1327.

[5] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, “Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918–931, Apr. 2018.

[6] 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.

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

[8] Z. Lin, M. Lin, J.-B. Wang, Y. Huang, and W.-P. Zhu, “Robust secure beamforming for 5G cellular networks coexisting with satellite networks,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 932–945, Apr. 2018.

[9] M. Á. Vázquez, L. Blanco, and A. I. Pérez-Neira, “Spectrum sharing backhaul satellite-terrestrial systems via analog beamforming,” *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 270–281, May 2018.

[10] Z. Lin, M. Lin, J. Ouyang, W. Zhu, A. D. Panagopoulos, and M. Alouini, “Robust secure beamforming for multibeam satellite communication systems,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6202–6206, Jun. 2019.

[11] G. Zheng, P. D. Arapoglou, and B. Ottersten, “Physical layer security in multibeam satellite systems,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[12] J. Xiong, D. Ma, K.-K. Wong, and J. Wei, “Robust masked beamforming for MISO cognitive radio networks with unknown eavesdroppers,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 744–755, Feb. 2016.

[13] H. Ma, J. Cheng, and X. Wang, “Cooperative jamming aided robust beamforming for MISO channels with unknown eavesdroppers,” in *Proc. IEEE Global Commun. (Globecom)*, Dec. 2017, pp. 1–5.

[14] M. Zhang, K. Cumanan, L. Ni, H. Hu, A. G. Burr, and Z. Ding, “Robust beamforming for AN aided MISO SWIPT system with unknown eavesdroppers and non-linear EH model,” in *Proc. IEEE Global Commun. Workshops*, Dec. 2018, pp. 1–7.

[15] M. K. Arti, “Channel estimation and detection in hybrid satellite-terrestrial communication systems,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5764–5771, Jul. 2016.

[16] Z. Lin, M. Lin, J. Wang, T. D. Cola, and J. Wang, “Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access,” *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 657–670, Jun. 2019.

[17] *Guidelines for Evaluation of Radio Interface Technologies for IMT-Advanced*, Tech. Rep. ITU-R M.2135, 2008.