Secure and Energy Efficient Transmission for RSMA-Based Cognitive Satellite-Terrestrial Networks

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

***Abstract*—Rate-splitting multiple access (RSMA) has recently received considerable attention due to its high efficiency in both spectral utilization and energy consumption. Inspired by this emerging technique, this letter presents a secure beamforming (BF) scheme for RSMA-based cognitive satellite terrestrial networks in the presence of multiple eavesdroppers. Assuming that the system operates in the millimeter wave band and only imperfect wiretap channel state information is available at the satellite and terrestrial base station, our objective is to maximize the secrecy-energy efficiency of the earth station (ES) while meeting the constraints on the ES secrecy rate, the cellular users' rate requirements, and transmit power budgets of the satellite and base station. As the formulated optimization problem is mathematically intractable, by applying successive convex approximation and Taylor expansion methods, we propose a robust BF scheme to convert the nonconvex objective and constraints into convex ones, which can be iteratively solved. The effectiveness and superiority of the proposed scheme are confirmed through simulation results.**

***Index Terms*—Beamforming, cognitive satellite terrestrial networks, RSMA, secrecy-energy efficiency.**

I. Introduction

With the explosive growth of wireless services, future wireless networks will need to support drastically increasing data traffic and provide reliable user access in remote areas. To meet these challenges, the cognitive satellite-terrestrial network (CSTN) offers an effective architecture for providing seamless connectivity in both densely and sparsely populated areas, where satellite and terrestrial subnetworks adopt cognitive radio techniques to share the limited frequency resources [1], [2]. To solve the inevitable inter-subnetwork interference issue in CSTN, the base station (BS) can employ interference management schemes, such as beamforming (BF) and resource allocation methods, to guarantee that the inter-subnetwork interference remains below a certain level [3], [4].

Rate-splitting multiple access (RSMA), that uses linearly precoded rate splitting at the transmitter and successive interference cancellation (SIC) at the terminals, is viewed as a powerful framework to increase spectral efficiency by bridging the commonly used space-division multiple access and non-orthogonal multiple access, where the former treats the interference as noise and the latter decodes the interference. In RSMA, the transmitted signal is split into common and private parts, where the common part is decoded by all the receivers and removed using SIC before decoding the private part. Authors of [5] presented a survey on recent advances in RSMA, highlighting the benefits of RSMA in terms of spectral and energy efficiencies, and pointing out the challenges and necessary standardization efforts to make RSMA a reality.

Physical layer security (PLS), as a complement to cryptographic approaches, has been thoroughly investigated in terrestrial networks [6]. However, the characteristics of CSTN present new challenges for PLS. Specifically, due to the high altitude of the satellite, its 3dB beamwidth angle is extremely narrow, which makes the legitimate and wiretap downlink channels highly correlated. Thus, it is difficult to implement BF onboard to simultaneously guarantee the quality-of-service (QoS) of the legitimate earth station (ES) and restrict the private signal exposure to eavesdroppers (Eves). The authors of [7]–[10] exploited the *green* interference from BS to achieve satellite secure communication under different wiretap channel assumptions. Recently, the secrecy-energy efficiency (SEE), defined as the ratio between the secrecy rate and the consumed power, has been introduced as a key metric from both secrecy and ecological perspectives for the design of future communication networks in order to achieve the best trade-off between security and energy consumption [11].

To take advantage of the improved spectral efficiency and transmission security respectively offered by RSMA and PLS technologies in the context of CSTN, we consider a more practical scenario where only imperfect wiretap channel state information (CSI) is available at the transmitters. Our goal is to maximize the SEE, while satisfying the secrecy rate constraint

Manuscript received August 3, 2020; revised September 9, 2020; accepted September 17, 2020. Date of publication September 25, 2020; date of current version February 9, 2021. This work was supported in part by the Key International Cooperation Research Project under Grant 61720106003, and in part by the Shanghai Aerospace Science and Technology Innovation Foundation under Grant SAST2019-095. The associate editor coordinating the review of this article and approving it for publication was I. Krikidis. *(Corresponding author: Min Lin.)*

Zhi Lin is with the Institute of Electronic Countermeasure, National University of Defense Technology, Hefei 230037, China (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, University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: aldhahir@utdallas.edu).

Digital Object Identifier 10.1109/LWC.2020.3026700

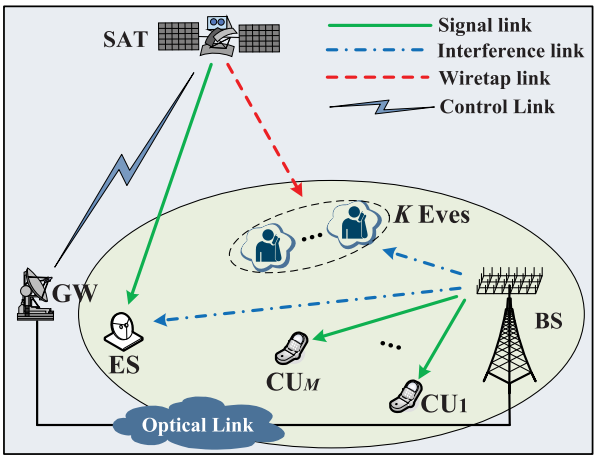

Fig. 1. System model of the considered CSTN.

at the ES, rate requirements for the cellular users (CUs), and transmit power budgets at the satellite and BS. Since the formulated optimization problem is mathematically intractable, we propose a robust BF design scheme wherein successive convex approximation (SCA) and Taylor expansion methods are combined to transform the fractional objective function and nonconvex constraints into convex ones, allowing us to obtain solutions efficiently. Compared to existing works [3]–[10], the exploitation of interference to achieve security and maximize SEE in RSMA-based CSTN with imperfect CSI is a new and challenging topic, which features our contributions in this letter.

II. System Model

We consider a CSTN communication scenario, where a geostationary orbit (GEO) satellite serves an ES in the presence of K Eves. Besides, the BS serves M CUs and employs RSMA to achieve high spectral efficiency, while the satellite and BS share the same frequency band. Moreover, the BS is connected to a gateway (GW) through optical links. The GW operates as a cloud processing center, so that the total network resources can be allocated centrally and dynamically through cloud computing. It is assumed that the satellite and BS are equipped with array fed reflector antennas with N_s feeds and a uniform planar array (UPA) with N_b antennas, respectively. For the UPA, we let $N_b = N_1 \times N_2$ with N_1 and N_2 being the number of antennas along the azimuth and elevation axes, respectively.

By taking into account the effects of path loss, rain attenuation and satellite beam gains, the satellite downlink channel model is given by [12]

$$\mathbf{g} = \sqrt{C_L}\xi^{-\frac{1}{2}}\mathbf{b}^{\frac{1}{2}} \odot e^{j\boldsymbol{\theta}}, \tag{1}$$

where $C_L = (\lambda/4\pi d_s)^2$ denotes the free space path loss, with λ being the wavelength and d_s the satellite transmission distance, ξ represents the rain attenuation fading coefficient, with $\xi_{\text{dB}} = 20\log_{10}(\xi)$ satisfying $\ln(\xi_{\text{dB}}) \sim \mathcal{N}(\mu, \sigma^2)$ where μ and σ are the rain fading statistics, $\mathbf{b}$ is the beam gain vector [12], and $\boldsymbol{\theta}$ denotes the phase vector with entries uniformly distributed over $[0, 2\pi)$.

Considering the highly directional characteristic of mmWave communications, the terrestrial downlink channel can be modeled as the superposition of a predominant line-of-sight (LoS) component and a sparse set of single-bounce non-LoS (NLoS) components. Then, the terrestrial downlink channel vector can be expressed as [13]

$$\begin{aligned}\mathbf{h} = &\sqrt{g(\theta_0,\varphi_0)}\rho_0\mathbf{a}_a(\theta_0,\varphi_0)\otimes\mathbf{a}_e(\theta_0,\varphi_0)\\ &+\sqrt{\frac{1}{L}}\sum_{l=1}^{L}\sqrt{g(\theta_l,\varphi_l)}\rho_l\mathbf{a}_a(\theta_l,\varphi_l)\otimes\mathbf{a}_e(\theta_l,\varphi_l).\end{aligned} \tag{2}$$

where L is the number of NLoS paths, ρ_0 and ρ_l represent the path losses associated with the LoS path and the l-th NLoS path, respectively. The parameters θ_i and ϕ_i for $i = 0, \ldots, L$ represent the azimuth and elevation angles of departure (AoD) of the corresponding paths. The path losses of the NLoS components are typically 5 to 10 dB larger than that of the LoS component [13]. In addition, $g(\theta_i, \varphi_i)$ is the directivity pattern of the antenna elements, while $\mathbf{a}_a(\theta, \varphi)$ and $\mathbf{a}_e(\theta, \varphi)$ represent the azimuth and elevation steering vectors, which are expressed as

$$\begin{aligned}\mathbf{a}_a(\theta,\varphi) = &\left[e^{-j\beta((N_1-1)/2)d_1\sin\theta\cos\varphi},\ldots,\right.\\ &\left.e^{+j\beta((N_1-1)/2)d_1\sin\theta\cos\varphi}\right]^T,\\ \mathbf{a}_e(\theta,\varphi) = &\left[e^{-j\beta((N_2-1)/2)d_2\cos\theta},\ldots,\right.\\ &\left.e^{+j\beta((N_2-1)/2)d_2\cos\theta}\right]^T.\end{aligned} \tag{3}$$

where d_1 and d_2 denote the inter-element spacing along the azimuth and elevation axes of the UPA. Let x denote the private multicast signal transmitted from the satellite to the ES, which is mapped with BF weight vector $\mathbf{v} \in \mathbb{C}^{N_s\times 1}$ prior to transmission. Using the rate-splitting technique at the BS, the unicast signal s_m intended for the m-th CU is split into a common sub-signal s_c and a private sub-signal $s_{p,m}$. The common sub-signals are jointly encoded into a common signal s_c using a codebook shared by all the CUs. Besides, it is assumed that the signals x, s_c and $s_{p,m}$ are uncorrelated with zero-mean and unit variance. Denote by $\mathbf{w}_c \in \mathbb{C}^{N_b\times 1}$ and $\mathbf{w}_m \in \mathbb{C}^{N_b\times 1}$ the BF weight vectors of the common signal s_c and private sub-signal $s_{p,m}$, respectively. Thus, the received signals at the ES, k-th Eve and m-th CU are expressed as

$$\begin{aligned}y_s &= \mathbf{g}^H\mathbf{v}x + \mathbf{h}_s^H\mathbf{w}_c s_c + \sum_{m=1}^{M}\mathbf{h}_s^H\mathbf{w}_m s_{p,m} + n_s,\\ y_{s,k} &= \mathbf{g}_{e,k}^H\mathbf{v}x + \mathbf{h}_{e,k}^H\mathbf{w}_c s_c + \sum_{m=1}^{M}\mathbf{h}_{e,k}^H\mathbf{w}_m s_{p,m} + n_{e,k},\\ y_{c,m} &= \mathbf{h}_{c,m}^H\mathbf{w}_c s_c + \sum_{m=1}^{M}\mathbf{h}_{c,m}^H\mathbf{w}_m s_{p,m} + \mathbf{g}_{c,m}^H\mathbf{v}x + n_{c,m},\end{aligned} \tag{4}$$

where $n_s, n_{e,k}$ and $n_{c,m}$ denote i.i.d. complex Gaussian random noises with noise variances $\sigma_s^2, \sigma_{e,k}^2$ and $\sigma_{c,m}^2$, respectively. At the m-th CU, the common sub-signal s_c is firstly decoded by treating private sub-signals as interference. By using SIC, s_c is re-encoded, precoded, and subtracted from the received signal, such that the m-th CU can decode its

private sub-signal $s_{p,m}$ by treating other private sub-signals as interference. The achievable rate of the ES, k-th Eve, common signal s_c and private sub-signal of the m-th CU can be expressed as

$$\begin{aligned}
R_s &= \log_2(1+\frac{\left|\mathbf{g}^H\mathbf{v}\right|^2}{\left|\mathbf{h}_s^H\mathbf{w}_c\right|^2+\sum_{m=1}^{M}\left|\mathbf{h}_s^H\mathbf{w}_m\right|^2+\sigma_s^2}),\\
R_{s,k} &= \log_2(1+\frac{\left|\mathbf{g}_{e,k}^H\mathbf{v}\right|^2}{\left|\mathbf{h}_{e,k}^H\mathbf{w}_c\right|^2+\sum_{m=1}^{M}\left|\mathbf{h}_{e,k}^H\mathbf{w}_m\right|^2+\sigma_{e,k}^2}),\\
R_{c,m} &= \log_2(1+\frac{\left|\mathbf{h}_{c,m}^H\mathbf{w}_c\right|^2}{\sum_{m=1}^{M}\left|\mathbf{h}_{c,m}^H\mathbf{w}_m\right|^2+\left|\mathbf{g}_{c,m}^H\mathbf{v}\right|^2+\sigma_{c,m}^2}),\\
R_{p,m} &= \log_2(1+\frac{\left|\mathbf{h}_{c,m}^H\mathbf{w}_m\right|^2}{\sum_{i\neq m}^{M}\left|\mathbf{h}_{c,m}^H\mathbf{w}_i\right|^2+\left|\mathbf{g}_{c,m}^H\mathbf{v}\right|^2+\sigma_{c,m}^2})
\end{aligned} \tag{5}$$

Considering that Eves are not authenticated users of the satellite sub-network, we assume that the channel uncertainty of $\mathbf{h}_{e,k}$ and $\mathbf{g}_{e,k}$ follow the Euclidean norm bounded error models $\mathbf{g}_{e,k}=\tilde{\mathbf{g}}_{e,k}+\mathbf{e}_{g,k}$ and $\mathbf{h}_{e,k}=\tilde{\mathbf{h}}_{e,k}+\mathbf{e}_{h,k}$, where $\tilde{\mathbf{g}}_{e,k}$ and $\tilde{\mathbf{h}}_{e,k}$ denotes the estimated CSI at the satellite and BS, $\|\mathbf{e}_{g,k}\|\leq\delta_g$ and $\|\mathbf{e}_{h,k}\|\leq\delta_h$.

To achieve both secure and energy efficient transmission, we will maximize the SEE while satisfying the secrecy rate constraint for the ES, the minimum rate constraints for the CUs and the power budgets of the satellite and BS. Mathematically, the optimization problem can be formulated as

$$\begin{aligned}
\max_{\mathbf{v},\mathbf{w}_c,\mathbf{w}_m}\ & \min_{\mathbf{e}_{g,k},\mathbf{e}_{h,k}} \frac{R_s-\max R_{s,k}}{\mu_1\|\mathbf{v}\|^2+\mu_2\left(\|\mathbf{w}_c\|^2+\sum_{m=1}^{M}\|\mathbf{w}_m\|^2\right)+P_c}\\
\text{s.t.}\ & \min_{\mathbf{e}_{g,k},\mathbf{e}_{h,k}} R_s-R_{s,k}\geq\Gamma_s,\ \forall k\\
& R_{c,m}\geq\Gamma_c,\ \forall m,\\
& R_{p,m}\geq\Gamma_p,\ \forall m,\\
& \|\mathbf{v}\|^2\leq P_s,\ \|\mathbf{w}_c\|^2+\sum_{m=1}^{M}\|\mathbf{w}_m\|^2\leq P_b,
\end{aligned} \tag{6}$$

where μ_1 and μ_2 are the power amplifier inefficiencies of the satellite and that of the BS, P_c, P_s and P_b denote the constant circuit power consumption, power budget of the satellite and of the BS, respectively. In addition, Γ_s represents the secrecy rate threshold of the ES, while Γ_c and Γ_p are the data rate thresholds for the common and private parts of the CUs, respectively.

III. BF Scheme Based on SEE Maximization

Since the optimization problem in (6) is mathematically intractable, we propose a robust BF scheme to obtain suboptimal solutions to the SEE maximization. This is done by transforming the nonconvex objective function and constraints into convex ones and iteratively obtaining the rank-1 solutions.

Let $\mathbf{H}_\ell=\mathbf{h}_\ell\mathbf{h}_\ell^H$ and $\mathbf{G}_\ell=\mathbf{g}_\ell\mathbf{g}_\ell^H$ denote the terrestrial and satellite channel matrices, respectively, where ℓ stands for the index identifying the particular link under consideration. To evaluate the channel uncertainty error of the wiretap channel matrices, we can rewrite $|\mathbf{g}_{e,k}^H\mathbf{v}|^2$ as

$$\begin{aligned}
\left|\mathbf{g}_{e,k}^H\mathbf{v}\right|^2 &= \mathbf{v}^H\left(\tilde{\mathbf{g}}_{e,k}\tilde{\mathbf{g}}_{e,k}^H+\tilde{\mathbf{g}}_{e,k}\mathbf{e}_{g,k}^H+\mathbf{e}_{g,k}\tilde{\mathbf{g}}_{e,k}^H+\mathbf{e}_{g,k}\mathbf{e}_{g,k}^H\right)\mathbf{v}\\
&= \mathbf{v}^H\left(\tilde{\mathbf{G}}_{e,k}+\Delta_{g,k}\right)\mathbf{v}
\end{aligned} \tag{7}$$

where $\tilde{\mathbf{G}}_{e,k}=\tilde{\mathbf{g}}_{e,k}\tilde{\mathbf{g}}_{e,k}^H$. It can be verified that the error matrix $\Delta_{g,k}$ is also norm-bounded as follows

$$\begin{aligned}
\|\Delta_{g,k}\| &\leq \left\|\tilde{\mathbf{g}}_{e,k}\mathbf{e}_{g,k}^H\right\|+\left\|\mathbf{e}_{g,k}\tilde{\mathbf{g}}_{e,k}^H\right\|+\left\|\mathbf{e}_{g,k}\mathbf{e}_{g,k}^H\right\|\\
&\leq \|\tilde{\mathbf{g}}_{e,k}\|\left\|\mathbf{e}_{g,k}^H\right\|+\|\mathbf{e}_{g,k}\|\left\|\tilde{\mathbf{g}}_{e,k}^H\right\|+\|\mathbf{e}_{g,k}\|^2\delta\\
&\leq \delta_g^2+2\delta_g\|\tilde{\mathbf{g}}_{e,k}\|=\varepsilon_{g,k}
\end{aligned} \tag{8}$$

Noting that the above inequalities are also applicable to $\mathbf{h}_{e,k}$, we assume that $\mathbf{H}_{e,k}=\tilde{\mathbf{H}}_{e,k}+\Delta_{h,k}$ and $\|\Delta_{h,k}\|\leq\varepsilon_{h,k}$. By defining $\mathbf{V}=\mathbf{v}\mathbf{v}^H$, $\mathbf{W}_c=\mathbf{w}_c\mathbf{w}_c^H$ and $\mathbf{W}_m=\mathbf{w}_m\mathbf{w}_m^H$, we can obtain upper and lower bounds as follows

$$\max_{\mathbf{e}_{g,k}}\ \mathrm{Tr}\big(\mathbf{G}_{e,k}\mathbf{V}\big)=\mathrm{Tr}\Big(\Big(\tilde{\mathbf{G}}_{e,k}+\varepsilon_{g,k}\mathbf{I}_{N_s}\Big)\mathbf{V}\Big), \tag{9a}$$

$$\min_{\mathbf{e}_{g,k}}\ \mathrm{Tr}\big(\mathbf{G}_{e,k}\mathbf{V}\big)=\mathrm{Tr}\Big(\Big(\tilde{\mathbf{G}}_{e,k}-\varepsilon_{g,k}\mathbf{I}_{N_s}\Big)\mathbf{V}\Big). \tag{9b}$$

The nonconvex secrecy constraint of (6) can be rewritten as

$$AB\geq\frac{a}{a-1}\mathrm{Tr}(\mathbf{G}\mathbf{V})\mathrm{Tr}\big(\mathbf{G}_{e,k}\mathbf{V}\big), \tag{10}$$

where $a=2^{\Gamma_s}$ and

$$\begin{aligned}
A &= \mathrm{Tr}(\mathbf{G}\mathbf{V})+(1-a)(\mathrm{Tr}(\mathbf{H}_s(\mathbf{W}_c+\sum_{m=1}^{M}\mathbf{W}_m))+\sigma_s^2),\\
B &= \mathrm{Tr}(\mathbf{H}_{e,k}(\mathbf{W}_c+\sum_{m=1}^{M}\mathbf{W}_m))+\sigma_{e,k}^2+\frac{a}{a-1}\mathrm{Tr}\big(\mathbf{G}_{e,k}\mathbf{V}\big).
\end{aligned} \tag{11}$$

Then, the right side of inequality (10) can be transformed as [14]

$$\mathrm{Tr}(\mathbf{G}\mathbf{V})\mathrm{Tr}\big(\mathbf{G}_{e,k}\mathbf{V}\big)=[\mathrm{Tr}(\mathbf{G}_k\mathbf{V})]^2, \tag{12}$$

where $\mathbf{G}_k=\mathbf{g}\mathbf{g}_{e,k}^H$. Thus, we can further rewrite (9) in the form of a second order cone (SOC), that is,

$$\left\|\begin{matrix}2\sqrt{\frac{a}{a-1}}\mathrm{Tr}(\mathbf{G}_k\mathbf{V})\\ B-A\end{matrix}\right\|_2\leq B+A \tag{13}$$

By considering the channel uncertainty and substituting (9) into (13), the secrecy constraint can be reformulated as

$$\left\|\begin{matrix}2\sqrt{\frac{a}{a-1}}\mathrm{Tr}\Big(\Big(\mathbf{g}\tilde{\mathbf{g}}_{e,k}^H+\delta_g\mathbf{I}_{N_s}\Big)\mathbf{V}\Big)\\ B_1-A\end{matrix}\right\|_2\leq B_2+A \tag{14}$$

where B_1 and B_2 are found by replacing $\mathbf{G}_{e,k}$ in B from (11) with (9a) and (9b), respectively.

By introducing auxiliary variables $\Phi=\{t,x,y,z,p_k,q_k\}$ into the objective function in (6), we obtain

$$\max_{\mathbf{V},\mathbf{W}_c,\mathbf{W}_m,\Phi}\ t \tag{15a}$$

$$\text{s.t. } x-y-z\geq t\varsigma, \tag{15b}$$

$$\mu_1\mathrm{Tr}(\mathbf{V})+\mu_2(\mathrm{Tr}(\mathbf{W}_c)+\sum_{m=1}^{M}\mathbf{W}_m)+P_c\leq\varsigma, \tag{15c}$$

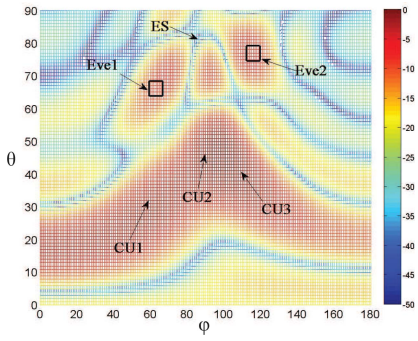

Fig. 2. Beampattern of $\mathbf{w}_c$.

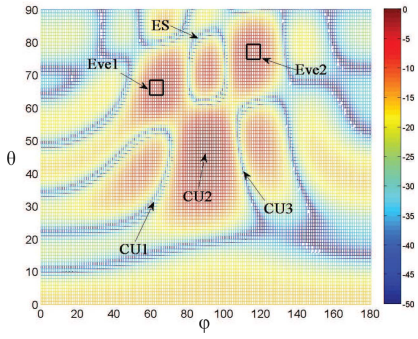

Fig. 3. Beampattern of $\mathbf{w}_2$.

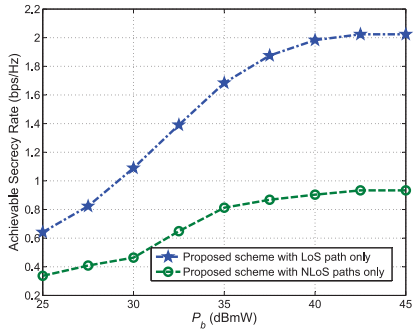

Fig. 4. Achievable secrecy rate versus P_b.

$$\mathrm{Tr}(\mathbf{GV}) + \mathrm{Tr}(\mathbf{H}_s(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_s^2 \geq e^x \quad (15d)$$

$$\mathrm{Tr}(\mathbf{H}_s(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_s^2 \leq e^y, \quad (15e)$$

$$\mathrm{Tr}((\tilde{\mathbf{H}}_{e,k} + \varepsilon_{h,k}\mathbf{I}_{N_b})(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_{e,k}^2 \leq e^{q_k}, \ \forall k, \quad (15f)$$

$$\mathrm{Tr}((\tilde{\mathbf{G}}_{e,k} - \varepsilon_{g,k}\mathbf{I}_{N_s})\mathbf{V}) + \mathrm{Tr}((\tilde{\mathbf{H}}_{e,k} - \varepsilon_{h,k}\mathbf{I}_{N_b})(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_{e,k}^2 \geq e^{p_k}, \ \forall k, \quad (15g)$$

$$\mathrm{Tr}\big(\mathbf{H}_{c,m}\mathbf{W}_c\big) - 2^{\Gamma_c - 1}\Big(\sum_{m=1}^{M} \mathrm{Tr}\big(\mathbf{H}_{c,m}\mathbf{W}_m\big) + \mathrm{Tr}\big(\mathbf{G}_{c,m}\mathbf{V}\big) + \sigma_{c,m}^2\Big) \geq 0, \ \forall m, \quad (15h)$$

$$\mathrm{Tr}\big(\mathbf{H}_{c,m}\mathbf{W}_m\big) - 2^{\Gamma_p - 1}\Big(\sum_{i \neq m}^{M} \mathrm{Tr}\big(\mathbf{H}_{c,m}\mathbf{W}_i\big) + \mathrm{Tr}\big(\mathbf{G}_{c,m}\mathbf{V}\big) + \sigma_{c,m}^2\Big) \geq 0, \ \forall m, \quad (15i)$$

$$\mathrm{Tr}(\mathbf{V}) \leq P_s, \quad \mathrm{Tr}(\mathbf{W}_c) + \sum_{m=1}^{M} \mathbf{W}_m \leq P_b, \quad (15j)$$

$$p_k - q_k \leq z, \ \forall k, \quad (15k)$$

$$\mathrm{rank}(\mathbf{V}) = \mathrm{rank}(\mathbf{W}_c) = \mathrm{rank}(\mathbf{W}_m) = 1, \ \forall m, \quad (15l)$$

$$(14) \quad (15m)$$

It can be observed that the constraints (15b), (15e), (15f) and (15l) are still nonconvex. By introducing auxiliary variable τ into (15b), the latter can be rewritten as

$$x - y - z \geq \tau^2, \quad \tau^2/\varsigma \geq t \quad (16)$$

Using the first order Taylor series expansion around $\tau^{(n)}$ and $\varsigma^{(n)}$, (16) can be further transformed into the following SOC and inequality

$$\frac{x - y - z + 1}{2} \geq \left\| \left[\frac{x - y - z - 1}{2}, \tau \right]^T \right\|_2, \quad 2\Big(\tau^{(n)}/\varsigma^{(n)}\Big)\tau - \Big(\tau^{(n)}/\varsigma^{(n)}\Big)^2 \varsigma \geq t \quad (17)$$

Next, applying the first order Taylor series expansion around $y^{(n)}$ and $q_k^{(n)}$ to the constraints (15e) and (15f), the latter can be approximated at the n-th iteration as

$$\mathrm{Tr}(\mathbf{H}_s(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_s^2 \leq e^{y^{(n)}}\Big(y - y^{(n)} + 1\Big),$$

$$\mathrm{Tr}((\tilde{\mathbf{H}}_{e,k} + \varepsilon_{h,k}\mathbf{I}_{N_b})(\mathbf{W}_c + \sum_{m=1}^{M} \mathbf{W}_m)) + \sigma_{e,k}^2 \leq e^{q_k^{(n)}}\Big(q_k - q_k^{(n)} + 1\Big). \quad (18)$$

To address the rank-1 constraint, let us denote by $\mathbf{v}^{(n)}, \mathbf{w}_c^{(n)}, \mathbf{w}_m^{(n)}$ the values of $\mathbf{v}, \mathbf{w}_c, \mathbf{w}_m$ at the n-th iteration. We can then approximate the BF matrix variables as

$$\begin{aligned} \mathbf{V} &= \mathbf{v}^{(n)}\mathbf{v}^H + \mathbf{v}\mathbf{v}^{(n)H} - \mathbf{v}^{(n)}\mathbf{v}^{(n)H}, \\ \mathbf{W}_c &= \mathbf{w}_c^{(n)}\mathbf{w}_c^H + \mathbf{w}_c\mathbf{w}_c^{(n)H} - \mathbf{w}_c^{(n)}\mathbf{w}_c^{(n)H}, \\ \mathbf{W}_m &= \mathbf{w}_m^{(n)}\mathbf{w}_m^H + \mathbf{w}_m\mathbf{w}_m^{(n)H} - \mathbf{w}_m^{(n)}\mathbf{w}_m^{(n)H}. \end{aligned} \quad (19)$$

Thus, the original problem (6) is converted to

$$\max_{\mathbf{v},\mathbf{w}_c,\mathbf{w}_m,\Phi} \quad t \quad \text{s.t.} \quad (14), (15c), (15d), (15g) - (15k), (17), (18). \quad (20)$$

which can be iteratively solved by means of a standard convex optimization software package such as CVX.

IV. Numerical Results

We consider a CSTN with $M = 3$ CUs and $K = 2$ Eves. The other parameter values are set as follows: the central frequency, $f_c = 18$ GHz; signal bandwidth, $B = 500$ KHz; number of

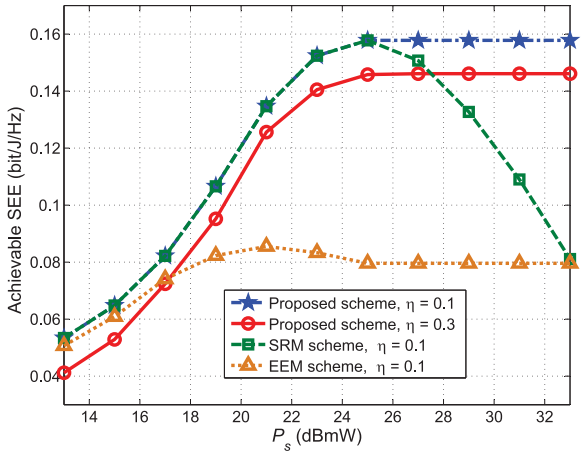

Fig. 5. Achievable SEE versus P_s.

antennas at satellite and BS, $N_s = 7$ and $N_b = 8 \times 8$; rain fading statistics, $\mu = -3.125$, $\sigma = 1.591$; secrecy rate constraint, $\Gamma_s = 0.2$ bit/s/Hz; rate constraints of common and private sub-signals, $\Gamma_c = \Gamma_p = 1$ bit/s/Hz; BS transmit power budget, $P_b = 12$ dBmW; and power amplifier inefficiencies of satellite and BS, $\mu_1 = \mu_2 = 1/0.39$. To better demonstrate the effect of channel uncertainty, we define the error ratio as $\eta = \delta_h/\|\tilde{\mathbf{h}}_{e,k}\| = \delta_g/\|\tilde{\mathbf{g}}_{e,k}\|$. The secrecy rate maximization (SRM) and energy-efficiency maximization (EEM) schemes in [11] are considered as benchmarks.

Figures 2 and 3 illustrate the beampattern of $\mathbf{w}_c$ and $\mathbf{w}_m$ for $m = 2$. It can be observed that the mainlobe of $\mathbf{w}_c$ covers the locations of the CUs. In addition, two secondary lobes point to the uncertainty region of the Eves creating interference at -10 dB level, while a -60 dB null is generated toward the ES. The mainlobe of beamformer $\mathbf{w}_2$ points to the 2nd CU while the interference to the other CUs and ES is well restrained. In addition, $\mathbf{w}_2$ also generates -10 dB interference towards Eves. Defining the achievable secrecy rate as $R_{sec} = R_s - \max R_{s,k}$, Fig. 4 plots R_{sec} of the proposed scheme versus the BS transmit power budget P_b for two extreme situations, i.e., when only the LoS path is available, and when only NLoS paths exist. The satellite transmit power is fixed to 25 dBmW while the NLoS paths number is set as $L = 5$. It can be observed that the achievable secrecy rate increases monotonically with the transmit power budget. Furthermore, when the transmit power budget reaches 42.5 dBmW, the proposed scheme approaches a constant secrecy rate performance. These observations demonstrate that our proposed scheme can achieve secure transmission by using the green interference from BS even if the LoS path between the BS and Eve is blocked.

Figure 5 plots the achievable SEE versus the BS power budget. It can be observed that the proposed scheme outperforms the other two schemes and achieves satisfying robust performance with increasing error ratio η. Also, the SEE performance of both the proposed and SRM schemes increases as P_s increases until the latter reaches 25 dBmW. Beyond this value, however, the proposed scheme approaches a constant SEE performance, while the SRM scheme degrades rapidly. When $P_s = 29$ dBW, the achievable SEE of the proposed robust BF scheme with channel error ratio $\eta = 0.1$ is 8% more than the one with channel error ratio $\eta = 0.3$, and 98% more than the EEM scheme. These observations demonstrate that our proposed scheme not only maximizes the SEE by exploiting the green interference from the BS, but also achieves satisfactory performance for the cellular users.

V. Conclusion

In this letter, we studied secure communication in RSMA-based CSTN. We maximized the achievable SEE of the ES under imperfect wiretap CSI, while satisfying a secrecy constraint on the ES, data rate requirements for the CUs and power budgets of the satellite and BS. To solve the intractable optimization problem, SCA and Taylor expansion methods were adopted to transform the nonconvex objective and constraints into convex ones, allowing the BF weight vectors to be iteratively calculated. The simulation results verified the superiority of the proposed BF scheme compared to two benchmark schemes.

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] K. An and T. Liang, "Hybrid satellite-terrestrial relay networks with adaptive transmission," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12448–12452, Dec. 2019.

[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, Feb. 2018.

[4] Q. Huang, M. Lin, J.-B. Wang, T. A. Tsiftsis, and J. Wang, "Energy efficient beamforming schemes for satellite-aerial-terrestrial networks," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3863–3875, Jun. 2020.

[5] B. Clerckx, H. Joudeh, C. Hao, M. Dai, and B. Rassouli, "Rate splitting for MIMO wireless networks: A promising PHY-layer strategy for LTE evolution," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 98–105, May 2016.

[6] 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.

[7] 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.

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

[9] Z. Lin, M. Lin, W.-P. Zhu, J.-B. Wang, and J. Cheng, "Robust secure beamforming for wireless powered cognitive satellite-terrestrial networks," *IEEE Trans. Cogn. Commun. Netw.*, early access, Aug. 12, 2020, doi: 10.1109/TCCN.2020.3016096.

[10] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure beamforming for cognitive satellite terrestrial networks with unknown eavesdroppers," *IEEE Syst. J.*, early access, Apr. 20, 2020, doi: 10.1109/JSYST.2020.2983309.

[11] J. Ouyang, M. Lin, Y. Zou, W.-P. Zhu, and D. Massicotte, "Secrecy energy efficiency maximization in cognitive radio networks," *IEEE Access*, vol. 5, pp. 2641–2650, 2017.

[12] 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.

[13] 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.

[14] 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.