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

Zhi Lin\textsuperscript{\textcircled{a}}, Min Lin\textsuperscript{\textcircled{a}}, Member, IEEE, Benoit Champagne\textsuperscript{\textcircled{b}}, Senior Member, IEEE, Wei-Ping Zhu\textsuperscript{\textcircled{a}}, 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

\textsuperscript{2162-2345 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.}
Consider 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]

\[
\mathbf{h} = \sqrt{g(\theta_0, \varphi_0)}\rho_0 \mathbf{a}_d(\theta_0, \varphi_0) + \sqrt{1 - \rho_0^2} \sum_{l=1}^{L} \sqrt{g(\theta_l, \varphi_l)}\rho_l \mathbf{a}_d(\theta_l, \varphi_l) \otimes \mathbf{a}_e(\theta_l, \varphi_l). \tag{2}
\]

where \(L\) is the number of NLoS paths, \(\rho_0\) and \(\rho_l\) represent the path losses associated with the LoS path and the \(l\)-th NLoS path, respectively. The parameters \(\theta_1\) and \(\phi_i \) 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, \(g(\theta, \varphi)\) is the directivity pattern of the antenna elements, while \(\mathbf{a}_d(\theta, \varphi)\) and \(\mathbf{a}_e(\theta, \varphi)\) represent the azimuth and elevation steering vectors, which are expressed as

\[
\mathbf{a}_d(\theta, \varphi) = \begin{bmatrix} e^{-j\beta((N_1-1)/2)d_1 \sin \theta \cos \varphi} & \ldots & \ldots & e^{-j\beta(N_1-1)/2)\sin \theta \cos \varphi} \end{bmatrix}^T,
\]

\[
\mathbf{a}_e(\theta, \varphi) = \begin{bmatrix} e^{-j\beta((N_2-1)/2)\sin \theta \cos \varphi} \ldots \ldots \ldots \ldots \ldots \ldots e^{-j\beta((N_2-1)/2)\sin \theta \cos \varphi} \end{bmatrix}^T.
\]

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 multiscat signal transmitted from the satellite to the ES, which is mapped with BF weight vector \(\mathbf{v} \in \mathbb{C}^{N_1 \times 1}\) 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 \(\mathbf{w}_c \in \mathbb{C}^{N_1 \times 1}\) and \(\mathbf{w}_m \in \mathbb{C}^{N_1 \times 1}\) 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

\[
y_s = \mathbf{g}^H \mathbf{v} x + \mathbf{h}_c^H \mathbf{w}_c s_c + \sum_{m=1}^{M} \mathbf{h}_c^H \mathbf{w}_m s_{p,m} + n_s,
\]

\[
y_{s,k} = \mathbf{g}_{c,k}^H \mathbf{v} x + \mathbf{h}_{c,k}^H \mathbf{w}_c s_c + \sum_{m=1}^{M} \mathbf{h}_{c,k}^H \mathbf{w}_m s_{p,m} + n_{e,k},
\]

\[
y_{c,m} = \mathbf{h}_{c,m}^H \mathbf{w}_c s_c + \sum_{m=1}^{M} \mathbf{h}_{c,m}^H \mathbf{w}_m s_{p,m} + \mathbf{g}_{c,m}^H \mathbf{v} x + n_{c,m}.
\]

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

$$ R_s = \log_2(1 + \frac{|h^H \text{v}|^2}{|h^H w_c|^2 + \sum_{m=1}^{M} |h^H w_m|^2 + \sigma_s^2}), $$

$$ R_{s,k} = \log_2(1 + \frac{|h_{e,k}^H \text{v}|^2}{|h_{e,k}^H w_c|^2 + \sum_{m=1}^{M} |h_{e,k}^H w_m|^2 + \sigma_{e,k}^2}), $$

$$ R_{c,m} = \log_2(1 + \frac{|h_{c,m}^H w_c|^2}{|h_{c,m}^H w_m|^2 + \sigma_{c,m}^2}), $$

$$ R_{p,m} = \log_2(1 + \frac{|h_{p,m}^H w_m|^2}{\sum_{m=1}^{M} |h_{p,m}^H w|^2 + \sigma_{p,m}^2}). $$

(5)

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

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

$$ \begin{align*}
\max_{v,w,c,w_m} & \quad R_s - \max_{e_{g,k},e_{h,k}} R_{s,k} \\
\text{s.t.} & \quad R_s - R_{s,k} \geq \Gamma_s, \forall k \\
& \quad R_{c,m} \geq \Gamma_c, \forall m, \\
& \quad R_{p,m} \geq \Gamma_p, \forall m, \\
& \quad ||v||^2 \leq P_s, \quad ||w_c||^2 + \sum_{m=1}^{M} ||w_m||^2 \leq P_b,
\end{align*} $$

(6)

where $\mu_1$ and $\mu_2$ are the power amplifier inefficiencies of the satellite and that of the BS, $P_c$, $P_a$ and $P_b$ denote the constant circuit power consumption, power budget of the satellite and of the BS, respectively. In addition, $\Gamma_s$ represents the secrecy rate threshold of the ES, while $\Gamma_c$ and $\Gamma_p$ 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 sub-optimal 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 $H_t = h_t h_t^H$ and $G_{\ell} = g_{\ell} g_{\ell}^H$ denote the terrestrial and satellite channel matrices, respectively, where $\ell$ stands for the index identifying the particular link under consideration. To evaluate the channel uncertainty error of the wiretap channel matrices, we can rewrite $|g_{c,e,k}^H v|_F$ as

$$ |g_{c,e,k}^H v|_F = \sqrt{h^H (\bar{g}_{e,k} + e_{g,k} + e_{g,k}^H \bar{g}_{e,k} + e_{g,k}) v} = \sqrt{h^H (\bar{g}_{e,k} + \Delta g_{e,k}) v} $$

(7)

where $\Delta g_{e,k} = e_{g,k}$. It can be verified that the error matrix $\Delta g_{e,k}$ is also norm-bounded as follows

$$ \|\Delta g_{e,k}\| \leq \|e_{g,k}\| + \|e_{g,k}^H\| + \|e_{g,k}^H\|^2 \delta.$$  

(8)

Noting that the above inequalities are also applicable to $h_{e,k}$, we assume that $H_{e,k} = \bar{H}_{e,k} + \Delta h_{e,k}$ and $\|\Delta h_{e,k}\| \leq \varepsilon_{h,k}$. By defining $V = v^H$, $W_c = w_c w_c^H$ and $W_m = w_m w_m^H$, we can obtain upper and lower bounds as follows

$$ \begin{align*}
\max_{e_{g,k}} & \quad \text{Tr}(G_{e,k} V) = \text{Tr}( (\bar{G}_{e,k} + \varepsilon_{g,k} I_N) V), \\
\min_{e_{g,k}} & \quad \text{Tr}(G_{e,k} V) = \text{Tr}( (\bar{G}_{e,k} - \varepsilon_{g,k} I_N) V).
\end{align*} $$

(9a-9b)

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

$$ AB \geq \frac{a}{a-1} \text{Tr}(G_{e,k} V), $$

(10)

where $a = 2I_s$ and

$$ A = \text{Tr}(G V) + (1-a)(\text{Tr}(H_s(W_c + \sum_{m=1}^{M} W_m)) + \sigma_s^2), $$

$$ B = \text{Tr}(H_{e,k}(W_c + \sum_{m=1}^{M} W_m)) + \sigma_{e,k}^2 + \frac{a}{a-1} \text{Tr}(G_{e,k} V). $$

(11)

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

$$ \text{Tr}(G_{e,k} V) = |\text{Tr}(G_{e,k} V)|^2, $$

(12)

where $G_{e,k} = g_{e,k} g_{e,k}^H$. Thus, we can further rewrite (9) in the form of a second order cone (SOC), that is,

$$ \left|2 \sqrt{\frac{a}{a-1} \text{Tr}(G_{e,k} V)} \right|_2 \leq B + A $$

(13)

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

$$ \left|2 \sqrt{\frac{a}{a-1} \text{Tr}( (g_{e,k} + \delta g I_N) V)} \right|_2 \leq B_2 + A $$

(14)

where $B_1$ and $B_2$ are found by replacing $G_{e,k}$ 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

$$ \begin{align*}
\max_{v,w,c,w_m,\Phi} & \quad t \\
\text{s.t.} & \quad x - y - z \geq \xi, \\
& \quad \mu_1 \text{Tr}(V) + \mu_2 (\text{Tr}(W_c) + \sum_{m=1}^{M} W_m) + P_c \leq \zeta.
\end{align*} $$

(15a-15c)
Tr(GV) + Tr(Hs(Wc + \sum_{m=1}^{M} W_m)) + \sigma_s^2 \geq e^x (15d)

Tr(Hs(Wc + \sum_{m=1}^{M} W_m)) + \sigma_s^2 \leq e^y, \quad (15e)

Tr(\tilde{H}_{e,k} + \varepsilon_{h,k} I_{N_k})(W_c + \sum_{m=1}^{M} W_m) + \sigma_{e,k}^2 \leq e^{\theta_k}, \quad \forall k, \quad (15f)

Tr(\tilde{G}_{e,k} - \varepsilon_{q,k} I_{N_k})V + Tr(\tilde{H}_{e,k} - \varepsilon_{h,k} I_{N_k}) (W_c + \sum_{m=1}^{M} W_m) + \sigma_{e,k}^2 \geq e^{y_k}, \quad \forall k, \quad (15g)

Tr(H_{c,m} W_m) - 2^{r-1} \left( \sum_{i \neq m} M \right) Tr(H_{c,m} W_i)
+ Tr(G_{c,m} V) + \sigma_{c,m}^2 \geq 0, \quad \forall m, \quad (15i)

Tr(V) \leq P_s, \quad Tr(W_c) + \sum_{m=1}^{M} W_m \leq P_b, \quad (15j)

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

\text{rank}(V) = \text{rank}(W_c) = \text{rank}(W_m) = 1, \quad \forall m, \quad (15l)

\text{rank}(V) = \text{rank}(W_m) = 1, \quad \forall m, \quad (15m)

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

\[
\begin{align*}
x - y - z & \geq \tau^2, \\
\tau^2/\varsigma & \geq t
\end{align*}
\]

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

\[
\begin{align*}
\frac{x - y - z + 1}{2} & \geq \left\| \frac{x - y - z - 1}{2}, \tau \right\|_2, \\
2\left( \frac{\tau^{(n)}}{\varsigma^{(n)}} \right)^2 \tau - \left( \frac{\tau^{(n)}}{\varsigma^{(n)}} \right)^2 \varsigma & \geq t
\end{align*}
\]

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

\[
\begin{align*}
\text{Tr}(\tilde{H}_{e,k} + \varepsilon_{h,k} I_{N_k})(W_c + \sum_{m=1}^{M} W_m)) + \sigma_{e,k}^2 \leq e^{y_k(q_k - q_k^{(n)} + 1)},
\end{align*}
\]

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

\[
\begin{align*}
V &= v^{(n)} H + v^{(n)} H - v^{(n)} v^{(n)} H, \\
W_c &= w_c^{(n)} H + w_c^{(n)} H - w_c^{(n)} w_c^{(n)} H, \\
W_m &= w_m^{(n)} H + w_m^{(n)} H - w_m^{(n)} w_m^{(n)} H.
\end{align*}
\]

Thus, the original problem (6) is converted to

\[
\begin{align*}
\max_{v,w_c,w_m,\Phi} \quad & t \\
\text{s.t.} & \quad (14), (15c), (15d), (15g) - (15k), (17), (18).
\end{align*}
\]

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, \( f_c = 18 \text{ GHz} \); signal bandwidth, \( B = 500 \text{ KHz} \); number of
the effect of channel uncertainty, we define the error ratio as
private sub-signals, $\Gamma$ generated toward the ES. The mainlobe of beamformer $\omega$ interferes at $-\omega$ lobes point to the uncertainty region of the Eves creating $m$ nulls.

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 $w_c$ and $w_m$ for $m = 2$. It can be observed that the mainlobe of $w_c$ 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 $w_2$ points to the 2nd CU while the interference to the other CUs and ES is well restrained. In addition, $w_2$ also generates $-10$ dB interference towards Eves. Defining the achievable secrecy rate as $R_{sec} = R_s - \max R_{k,s}$, 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 $25$ dBm 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 $\eta$. Also, the SEE performance of both the proposed and SRM schemes increases as $P_b$ 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 $P_b = 29$ 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