Secrecy Rate Analysis of Satellite Communications With Frequency Domain NOMA

Zhisheng Yin, *Student Member, IEEE*, Min Jia, *Senior Member, IEEE*, Wei Wang, *Student Member, IEEE*, Nan Cheng, *Member, IEEE*, Feng Lyu, *Member, IEEE*, Qing Guo, *Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—Due to the inherent broadcasting nature and broad coverage of satellite, satellite communications are well known to be vulnerable to security threats. Since the distance difference from satellite to terrestrial terminals is negligible, the channels of different users are similar, posing a challenge of achieving secure satellite downlink transmission in the presence of eavesdroppers (Eves). In this paper, we consider satellite communications in areas without terrestrial networks converge, and investigate the physical layer security in the satellite downlink. To achieve a positive secrecy rate, a frequency domain non-orthogonal multiple access (FD-NOMA) scheme and an according multiuser cooperative scheme are proposed. Particularly, by adopting the FD-NOMA, the spectrum efficiency can be improved at the cost of raising inter-user interference (IUI), and the inherent IUI is elegantly leveraged to suppress the signal-to-interference-plus-noise ratio (SINR) of Eves while the intended SINR of legitimate users can be enhanced by the cooperative scheme. The secrecy rate of satellite communications with FD-NOMA is analyzed, and a tight lower bound is derived, which is validated via numerical results. In addition, the secrecy rate is found to be affected by the level of spectral overlapping, and there exists an optimal spectral overlapping factor (SOF) which can maximize the secrecy rate.**

***Index Terms*—Satellite communications, FD-NOMA, physical layer security, cooperation, secrecy rate.**

I. Introduction

CHARACTERIZED by large coverage, seamless connection, and high communication capacity, satellite plays a significant role in future space-air-ground (SAG) integrated networks. It has attracted extensive attention from both the academia and industry, to enable cognitive satellite-terrestrial networks, hybrid integrated satellite-terrestrial networks, satellite-supported Internet of remote things (IoRT) networks, and SAG integrated vehicular networks [1]–[6], etc. Due to the inherent broadcasting nature and broad coverage of satellite, satellite communications are susceptible to many malicious attacks [7]. Particularly, unauthorized users can eavesdrop signals without a hitch if the broadcast information is not encrypted, and the possible locations of eavesdroppers (Eves) can be distributed within a large geographical region [8], [9]. Typical cryptographic solutions are realized at upper layers including encryption algorithms [10], and incorporating security solutions such as the Internet security protocol and the secure socket layer.

Different from the upper layer approaches which are computationally intractable, physical layer security (PLS) can also achieve secure transmission by means of the intrinsic randomness of wireless channels [11], [12], and has been widely applied in terrestrial wireless networks [13]. Particularly, common PLS techniques can be summarized as PLS coding, multi-antenna, and cooperative relaying. Error-control codes such as low-density parity-check (LDPC) and polar codes have shown that a level of information-theoretic secrecy can be achieved and the amount of information leakage can be controlled [14]. More specifically, by adopting LDPC codes, a multi-message authentication scheme is proposed to achieve perfect security with the same key over binary-input wiretap channel [15]. By equipping large antenna arrays, massive multiple-input multiple-output (MIMO) techniques can improve secrecy performance by generating very narrow beams to focus the signal to the desired users to enhance the legitimate channel, or generate artificial noise (AN) to degrade the eavesdropping channel [16]. To enhance the secrecy performance, relay selection schemes are also proposed in cooperative networks [17]–[19]. In power domain non-orthogonal multiple access (NOMA), legitimate users are subjected to co-channel interference due to full bandwidth sharing, where the successive information cancellation (SIC) is adopted to eliminate the co-channel interference. These characteristics in NOMA make it promising to implement PLS, which has attracted extensive attention recently [20], [21]. For instance, without knowing the decoding order, the co-channel interference cannot be canceled by unsuccessful SIC processing at Eves [21], and thus a positive secrecy performance can be achieved.

The aforementioned PLS solutions can be effectively and feasibly implemented in terrestrial networks as shadow and fading in terrestrial channels are complicated and diversified.

Manuscript received April 12, 2019; revised August 5, 2019; accepted September 23, 2019. Date of publication October 1, 2019; date of current version December 17, 2019. This work was supported in part by the National Natural Science Foundation of China under Grants 61671183 and 61771163 and in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The review of this article was coordinated by Prof. X. Wang. *(Corresponding author: Min Jia.)*

Z. Yin, M. Jia, and Q. Guo are with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150008, China (e-mail: zsyin@stu.hit.edu.cn; jiamin@hit.edu.cn; qguo@hit.edu.cn).

W. Wang, F. Lyu, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: wei_wang@nuaa.edu.cn; f2lyu@uwaterloo.ca; sshen@uwaterloo.ca).

N. Cheng is with the State Key Laboratory of ISN, School of Telecommunications Engineering, Xidian University, Xian 710071, China (e-mail: dr.nan.cheng@ieee.org).

Digital Object Identifier 10.1109/TVT.2019.2944875

Besides, the spatial degrees of freedom in terrestrial networks is sufficient to assist in the implementation of PLS. However, in satellite communications, the difference of distances between satellite and terrestrial users is negligible. Thus, the channel quality of satellite to legitimate user (Sat-Leg) links become indistinguishable from that of satellite to Eve (Sat-Eve) links, which poses a challenge to implement PLS in satellite communication systems.

To guarantee the security in satellite communication links, several related works on PLS in satellite-terrestrial communications are conducted. In cognitive satellite terrestrial networks and hybrid satellite-terrestrial systems, the co-channel interference caused by the spectrum sharing between satellite and terrestrial networks is normally treated as a drawback of the system performance [22]. However, the interference is able to improve the secrecy performance for satellite users as long as the channel quality of Sat-Eve and Sat-Leg links are unequally degraded. To enhance the secrecy performance of primary satellite network, the base station (BS) as secondary terrestrial network generates a green interference to interfere Eves without affecting the legitimate users through beamforming techniques [23]. Considering multiple antennas equipped in satellite, a joint beamforming scheme at both the terrestrial BS and satellite is proposed to achieve the secrecy rate for satellite users while satisfying the requirement of quality-of-service (QoS) for terrestrial users [24], [25]. Given the transmission quality and security requirement of the fixed satellite service (FSS), a cooperative beamforming scheme (combining adaptive beamforming at satellite, AN generation, and beamforming at the terrestrial BS) is proposed to suppress the received signal-to-interference-plus-noise-ration (SINR) at Eves and meanwhile to facilitate the FSS terminals [26]. To guarantee the secrecy rate for satellite link at the minimum transmission power, a joint cooperative beamforming and AN scheme is proposed in [27], and a stochastic beamforming framework is presented in [28].

The aforementioned schemes are effective under the satellite and terrestrial coexisting scenario, where the terrestrial BS can generate green interferences to implement PLS for satellite links. However, considering satellite-supported applications in remote areas, the aforementioned schemes become invalid due to the lack of terrestrial networks. Moreover, as satellite beams are not narrow enough to focus only on legitimate users, conventional beamforming approaches lose practical feasibility in satellites. As a result, given the resource constraints in satellite such as antennas and power, it is rather challenging to implement PLS in satellite communications with limited available resource under an isolated scenario.

In this paper, inspired by the concept of power domain NOMA to provide secrecy, we propose a frequency-domain non-orthogonal multiple access (FD-NOMA) scheme for downlink satellite communications to cope with the PLS problem (i.e., eavesdropping). Specifically, as shown in Fig. 1, satellite broadcasts signals through multi-beam where multiple clusters exist in each beam. We consider one passive Eve in a cluster targeting to wiretap an interested user in the cluster. To enhance the channel difference between satellite to legitimate user and Eve, multiuser interference deliberately introduced by FD-NOMA is leveraged as a green interference to degrade the Sat-Eve link. In addition, to obtain a positive secrecy rate, we propose a cooperative scheme to conduct interference cancellation at legitimate users to improve the capacity of main channel. The main contributions of this work are as follows.

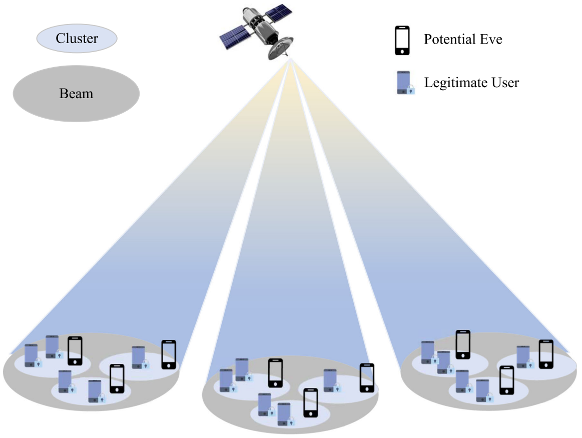

Fig. 1. Multiuser access downlink satellite communications in the presence of a passive Eve.

- To provide high spectral efficiency in satellite communications, we explore the FD-NOMA where excessive spectral overlapping among adjacent users is designed to improve the spectral efficiency. Additionally, the multi-user interference brought by the overlapping is elegantly leveraged to implement PLS.
- To improve the secrecy performance for legitimate users, a multiuser cooperative scheme is proposed to conduct inter-user interference (IUI) cancellation. Under the cooperation, the closed-form expression of the average SINR is derived and verified via numerical results, demonstrating an improvement of legitimate SINR.
- With the knowledge of channel distribution information of all legitimate users as well as the Eve, the performance of secrecy rate is analyzed, and a lower bound of the average secrecy rate is also derived. Based on the theoretical analysis, we reveal a trade-off between the spectral efficiency and secrecy rate in the FD-NOMA system.

The remainder of this paper is organized as follows. We first describe the system model and the principle of FD-NOMA in Section II, and then propose the corresponding multiuser cooperation scheme in Section III. In Section IV, the secrecy performance of FD-NOMA is analyzed and the lower bound of secrecy rate is derived. In Section V, numerical results and discussions are provided. Finally, we conclude this paper and direct our future work in Section VI.

II. System Model

As shown in Fig. 1, we consider multiuser access downlink satellite communications in the presence of a passive Eve. The frequency reuse factor between beams is considered to be large enough, and thus the inter-beam interference can be ignored [29, pp. 406]. The spectral resource is allocated to multiple clusters

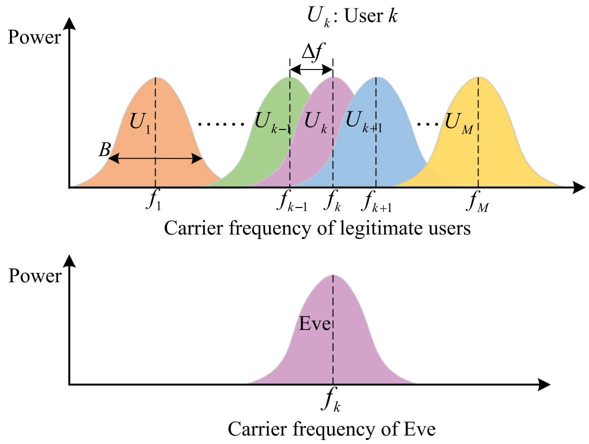

Fig. 2. Illustration of FD-NOMA users in the presence of a passive Eve.

in each beam by frequency division without overlapping. To improve the spectral efficiency of satellite and achieve a secure transmission, we propose a spectrum efficient and secure multiple access scheme named FD-NOMA. Specifically, the downlink spectrum resource is allocated to users through frequency division and users within each cluster share partial spectrum with other users, which is shown in Fig. 2. The downlink resource is divided into multiple time-frequency resource blocks, which are available for multiuser access, and all users in a cluster share the full time blocks. Without loss of generality, equal bandwidth B is allocated to each user and the same level of spectrum overlapping is adopted between adjacent users. We consider M legitimate users in a cluster and the frequency allocation of FD-NOMA is shown in Fig. 2. The satellite allocates a group of carrier frequencies $\{f_k, k = 1, \ldots, M\}$ for a cluster and the frequency spacing between two adjacent users is $|f_k - f_{k-1}| = \Delta f$, with $\Delta f < B$. Note that FD-NOMA reduces to the power domain NOMA if the whole spectrum is shared among all users in a cluster or to the orthogonal multiple access (OMA) if the minimum orthogonal frequency spacing among users is maintained. However, the conventional power-domain NOMA generally achieves capacity improvements relying on the channel difference to carry out optimal power allocation. Particularly, a passive Eve is assumed to wiretap the concerned cluster under the satellite coverage. User k (U_k) is supposed to be the target user of Eve and Eve works in the same frequency band with U_k, i.e., f_k.

We consider M legitimate users in a cluster, and the total transmission power is denoted by $\sum_{k=1}^{M} p_{l,k}$, where $p_{l,k}$ is the power allocated to U_k in the l^{th} time slot. The time domain transmitted signal from satellite with FD-NOMA can be expressed as

$$x(t) = \frac{1}{\sqrt{T}} \sum_{l=-\infty}^{\infty} \sum_{k=0}^{M} \sqrt{p_{l,k}} X_{l,k} e^{j2\pi k(t-lT)\Delta f}, \tag{1}$$

where $\Delta f = \alpha/T$ denotes the frequency interval between adjacent users with T being the duration of a FD-NOMA frame, and the parameter $0 < \alpha < 1$ is defined as the level of spectral overlapping between two adjacent users (termed as spectral overlapping factor (SOF)). In addition, $X_{l,k}$ is the l^{th} normalized symbol transmitted to U_k through the k^{th} subchannel, and $X_{l,k}$ is independent for different l or k.

We adopt the widely used shadowed Rician channel model in this work. The channel state information (CSI) from satellite to U_k is given by $h_{l,k} = \sqrt{\beta_{l,k}} g_{l,k}$ [30], where $\beta_{l,k}$ and $g_{l,k}$ denote the large-scale path loss and the small-scale fading component, respectively, and $g_{l,k} \sim \mathcal{CN}(\mu_k, \delta_k^2)$ denotes the Rician channel state [31]. The Rician factor of the channel is denoted by $K_B^k = \lambda_k/\delta_k^2$, where $\lambda_k = |u_k|^2$ is the noncentrality parameter. The channels from satellite to terrestrial users are assumed to be independent from each other.

Based on FD-NOMA, the received baseband signal at user k in the l^{th} symbol period can be expressed as

$$\begin{aligned} Y_{l,k} &= h_{l,k}\sqrt{p_{l,k}} X_{l,k} + N_{l,k} \\ &\quad + h_{l,k} \frac{1}{M} \sum_{m=0}^{M-1} \sum_{\substack{i=0\\ i\neq k}}^{M-1} \sqrt{p_{l,i}} X_{l,i} e^{j2\pi \frac{(i-k)m}{M}\alpha}, \end{aligned} \tag{2}$$

where $N_{l,k}$ denotes the zero-mean additive white Gaussian noise (AWGN) with variance δ_n^2, and $N_{l,k}$ is independent for different l or k. From (2), we can observe that within the cluster, U_k receives IUI from other users (i.e., $X_{l,i}, i \neq k$) due to the partial bandwidth multiplexing, and the IUI can be obtained as

$$I_{l,k} = h_{l,k} \frac{1}{M} \sum_{m=0}^{M-1} \sum_{\substack{i=0\\ i\neq k}}^{M-1} \sqrt{p_{l,i}} X_{l,i} e^{j2\pi \frac{(i-k)m}{M}\alpha}. \tag{3}$$

The power of $I_{l,k}$ can be calculated as

$$\begin{aligned} |I_{l,k}|^2 &= \left| h_{l,k} \frac{1}{M} \sum_{m=0}^{M-1} \sum_{\substack{i=0\\ i\neq k}}^{M-1} \sqrt{p_{l,i}} X_{l,k} e^{j2\pi \frac{(i-k)m}{M}\alpha} \right|^2 \\ &= |h_{l,k}|^2 \left| \frac{\sqrt{p_{l,i}}}{M} \sum_{i=0, i\neq k}^{M-1} \sum_{m=0}^{M-1} e^{j2\pi \frac{(i-k)m}{M}\alpha} \right|^2 \\ &= p_{l,i} \beta_{l,k} |g_{l,k}|^2 c_{l,k}, \end{aligned} \tag{4}$$

where the correlation coefficient describes correlation between the U_k and other users in the same cluster, which is given by

$$c_{l,k} = \sum_{i=0, i\neq k}^{M-1} \left| \frac{\text{sinc}\left(\alpha\left(i-k\right)\right)}{\text{sinc}\left(\alpha\left(i-k\right)/M\right)} \right|^2. \tag{5}$$

The channel of Sat-Eve link is also modeled as shadowed Rician channel and the distance form Eve to U_k can be ignored as compared to the link of satellite. Similarly, the received signal at Eve from satellite can be expressed as

$$\begin{aligned} Y_{l,e} &= h_{l,e}\sqrt{p_{l,k}} X_{l,k} + N_{l,e} \\ &\quad + h_{l,e} \frac{1}{M} \sum_{m=0}^{M-1} \sum_{\substack{i=0\\ i\neq k}}^{M-1} \sqrt{p_{l,i}} X_{l,k} e^{j2\pi \frac{(i-k)m}{M}\alpha}, \end{aligned} \tag{6}$$

where $h_{l,e} = \zeta_{l,e} g_{l,e}$ denotes the CSI from satellite to Eve with $\zeta_{l,e}$ being the large-scale path loss and $g_{l,e}$ being the small-scale fading with $g_{l,e} \sim \mathcal{CN}(\mu_e, \delta_e^2)$, and $N_{l,e}$ is the zero mean AWGN received at Eve with variance δ_e^2. Obviously, the Eve not only receives what it concerns but also the unexpected information from other users, where the term containing $X_{l,k}$ in (6) is the targeted signal and the unexpected signal competent received by Eve is

$$I_{l,e} = h_{l,e}\frac{1}{M}\sum_{m=0}^{M-1}\sum_{\substack{i=0\\i\neq k}}^{M-1}\sqrt{p_{l,i}}X_{l,i}e^{j2\pi\frac{(i-k)m}{M}\alpha}, \tag{7}$$

and the power of $I_{l,e}$ is given by

$$|I_{l,e}|^2 = p_{l,i}\zeta_{l,e}|g_{l,e}|^2 c_{l,k}. \tag{8}$$

From (2) and (4), we calculate the instantaneous achievable SINR at U_k as follows

$$\begin{aligned}\text{SINR}_{l,k} &= \frac{\left|h_{l,k}\sqrt{p_{l,k}}X_{l,k}\right|^2}{|I_{l,k}+N_{l,k}|^2}\\ &\overset{(a)}{=} \frac{p_{l,k}\beta_{l,k}|g_{l,k}|^2}{p_{l,i}\beta_{l,k}|g_{l,k}|^2 c_{l,k} + p_{l,k}/\rho}\\ &\triangleq \frac{\kappa|g_k|^2}{|g_k|^2+\eta},\end{aligned} \tag{9}$$

where (a) holds since the IUI is independent of AWGN, and $\rho = p_{l,k}/\delta_n^2$ is the input signal-to-noise ratio (SNR) for U_k at the l^{th} time slot, $\eta = \frac{1}{\rho c_{l,k}\beta_{l,k}}$ and $\kappa = \frac{1}{c_{l,k}}$.

Similar to (9), using (6) and (8), the received SINR at Eve is given by

$$\begin{aligned}\text{SINR}_{l,e} &= \frac{\left|h_{l,e}\sqrt{p_{l,k}}X_{l,k}\right|^2}{|I_{l,k}+N_{l,k}|^2}\\ &= \frac{p_{l,k}\zeta_{l,e}|g_{l,e}|^2}{\zeta_{l,e}|g_{l,e}|^2 c_{l,k} + p_{l,k}/\rho}\\ &\triangleq \frac{\kappa|g_{l,e}|^2}{|g_{l,e}|^2+\varepsilon},\end{aligned} \tag{10}$$

where $\varepsilon = \frac{1}{\rho c_{l,k}\zeta_{l,e}}$.

From (9) and (10), the self-induced IUI affects the legitimate user as well as the Eve simultaneously. As shown in (4) and (8), the received IUI at legitimate user and Eve is affected by the channel gain, the power of other legitimate users in FD-NOMA, input SNR, and the SOF. Considering the similar channel gain in satellite communications, the powers in (4) and (8) are almost equal. It indicates that similar SINR is received at the main channel and the eavesdropping channel. To achieve the positive secrecy rate under this scenario, a cooperative scheme is proposed in Section III.

III. Multiuser Cooperation Scheme

Based on FD-NOMA, each user works at different sub-bands and the IUI from other sub-bands in the same cluster degrades the channel quality, due to non-orthogonal frequency division multiple access. To improve the achievable secrecy rate, the IUI at legitimate users should be suppressed properly to improve the capacity of the main channel while that at Eve is expected to degrade the quality of eavesdropping channel.

For the concerned U_k, the green interference needs to be canceled where information from other users in the same cluster is required. Based on (3), the IUI can be canceled by using $X_{l,i}$ $(i \neq k)$. However, for the frequency division, U_k cannot access information from other users directly, and thus the information exchange among legitimate users should be carried out on the ground. Particularly, a secure local area network is assumed to support the information exchange among users,[1] and then a cooperative scheme could be conducted to suppress the IUI among legitimate satellite users. Since we only consider one Eve in a cluster, the IUI at the Eve cannot be canceled.

Without loss of generality, users $(U_m, m \neq k)$ decode and forward (DF) their information to U_k, then U_k can execute IUI cancellation with information from DF links. Although the cooperation with DF and multiuser detection in power domain NOMA has been investigated to mitigate interference in [33] and [34], it is worth pointing out that cooperation based on SIC is unsuitable for FD-NOMA. Moreover, the DF links in our work are implemented in an assumed secure local area network on the ground, which can realized by encryption algorithms [10].

We propose a cooperative scheme to cancel IUI between legitimate users shown in Fig. 3, where $\hat{S}_n (n \neq k)$ is the data decoded and forwarded by U_n. For the l^{th} time slot, the IUI of U_k after cancellation can be obtained as

$$I'_{l,k} = \frac{1}{M}h_{l,k}\sum_{m=0}^{M-1}\sum_{\substack{i=0\\i\neq k}}^{M-1}\sqrt{p_{l,i}}\left(X_{l,i}-\hat{S}_{l,i}\right)e^{j2\pi\frac{(i-k)m}{M}\alpha}, \tag{11}$$

where $\hat{S}_{l,i}$ is the estimated sample at U_i in the l^{th} symbol period and $I'_{l,k}$ denotes the residual interference at U_k. To obtain $\hat{S}_{l,i}, i = 1,\ldots,M$, we assume that each user knows its CSI, which can be estimated before data transmission. For the ease of theoretical analysis, we assume the perfect CSI for each legitimate user and Eve [35].

Based on (11), the received signal at U_k with cooperation can be written as

$$Z_{l,k} = h_{l,k}\sqrt{p_{l,k}}X_{l,k} + I'_{l,k} + N_{l,k}. \tag{12}$$

By substituting (11) into (12), $Z_{l,k}$ can be further simplified as

$$\begin{aligned}Z_{l,k} &= h_{l,k}\sqrt{p_{l,k}}X_{l,k} + N_{l,k}\\ &\quad + \frac{h_{l,k}}{M}\sum_{m=0}^{M-1}\sum_{\substack{i=0\\i\neq k}}^{M-1}\sqrt{p_{l,i}}\left(X_{l,i}-\hat{S}_{l,i}\right)e^{j2\pi\frac{(i-k)m}{M}\alpha}\\ &= h_{l,k}\sqrt{p_{l,k}}\hat{S}_{l,k} + \frac{h_{l,k}}{M}\sum_{m=0}^{M-1}\sum_{i=0}^{M-1}\sqrt{p_{l,i}}X_{l,i}e^{j2\pi\frac{(i-k)m}{M}\alpha}\end{aligned}$$

[1] We focus on the secure transmission from satellite to legitimate users in this work, and the cooperation can be realized through a secure communication network on the ground for the legitimate satellite users [32].

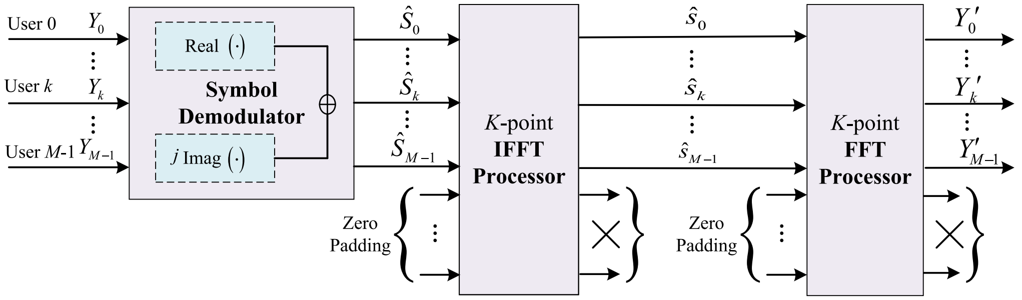

Fig. 3. Multiuser cooperation scheme with information exchange.

$$\begin{aligned} &- \frac{h_{l,k}}{M}\sum_{m=0}^{M-1}\sum_{i=0}^{M-1}\sqrt{p_{l,i}}\hat{S}_{l,i}e^{j2\pi\frac{(i-k)m}{M}\alpha} + N_{l,k} \\ &= h_{l,k}\sqrt{p_{l,k}}\hat{S}_{l,k} + Y_{l,k} - h_{l,k}Y'_{l,k} + N_{l,k}, \end{aligned} \tag{13}$$

where $Y'_{l,k}$ denotes the symbol estimation and it is required to eliminate the IUI. To obtain $Y'_{l,k}$, an inverse fast Fourier transformation (IFFT) and fast Fourier transformation (FFT) architecture can be utilized, as shown in Fig. 3.

By changing α/M to $1/K$ and keeping $\alpha = M/K, (K \geq M)$, $Y'_{l,k}$ in (13) can be reshaped as the form of IFFT/FFT implementation, i.e.,

$$\begin{aligned} Y'_{l,k} &= \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=0}^{M-1}\sqrt{p_{l,i}}\hat{S}_{l,i}e^{j2\pi\frac{(i-k)m}{M}\alpha} \\ &= \frac{1}{\sqrt{M}}\sum_{m=0}^{K-1}\left(\frac{1}{\sqrt{M}}\sum_{i=0}^{K-1}\sqrt{p_{l,i}}\hat{S}_{l,i}e^{j2\pi\frac{im}{K}}\right)e^{-j2\pi\frac{km}{K}}, \end{aligned} \tag{14}$$

where $\hat{S}_{l,i} = 0$ when $M \leq i \leq K-1$, corresponding to a zero padding operation.

Based on (14), we propose the approach of implementing multiuser cooperation scheme by the IFFT/FFT architecture. Firstly, a corresponding symbol demodulator is adopted to obtain symbol estimation at each user's side. The symbol estimations from other users $\{\hat{S}_{l,0}, \ldots, \hat{S}_{l,k-1}, \hat{S}_{l,k+1}, \ldots, \hat{S}_{l,M-1}\}$ are shared with the U_k through a secure link, which are then transformed into $\hat{\mathbf{s}} = [\hat{s}_0, \ldots, \hat{s}_{M-1}]^T$ through K points IFFT after $(K-M)$ zeros padding. Thus, we can obtain

$$\hat{\mathbf{s}} = \boldsymbol{\Omega}\mathbf{F}^{-1}\begin{bmatrix}\mathbf{W}_p\hat{\mathbf{S}} \\ \mathbf{0}_{(K-M)\times 1}\end{bmatrix}, \tag{15}$$

where $\boldsymbol{\Omega} = [\begin{smallmatrix}\mathbf{I}_M & \\ & \mathbf{0}_{(K-M)\times(K-M)}\end{smallmatrix}]$ denotes a truncating operation, $\mathbf{F}^{-1}$ is the normalized IFFT matrix with K dimensions, $\mathbf{W}_p = diag(\sqrt{p_{l,0}}, \ldots, \sqrt{p_{l,k}}, \ldots, \sqrt{p_{l,M-1}})$ denotes power allocation for legitimate users, and the k^{th} estimated sample in (15) is written by

$$\hat{s}_{l,k} = \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}\sqrt{p_{l,m}}\hat{S}_{l,m}e^{j2\pi\frac{mk}{M}\alpha}, 0 \leq k \leq M-1. \tag{16}$$

Then, $\hat{\mathbf{s}}$ is sent to K points FFT processor after a zeros padding and the output of FFT can be expressed as

$$\mathbf{Y}' = \boldsymbol{\Omega}\mathbf{F}\begin{bmatrix}\hat{\mathbf{s}} \\ \mathbf{0}_{(K-M)\times 1}\end{bmatrix}, \tag{17}$$

where $\mathbf{F}$ denotes the normalized FFT matrix with K dimensions and the k^{th} output element of the FFT is given by

$$\begin{aligned} Y'_{l,k} &= \frac{1}{\sqrt{M}}\sum_{m=0}^{K-1}\hat{s}_{l,m}e^{-j2\pi\frac{km}{K}} \\ &= \sqrt{p_{l,k}}\hat{S}_k + \frac{1}{M}\sum_{m=0}^{M-1}\sum_{\substack{i=0\\ i\neq k}}^{M-1}\sqrt{p_{l,i}}\hat{S}_{l,i}e^{j2\pi\frac{(i-k)m}{M}\alpha}, \end{aligned} \tag{18}$$

which is equal to (14). Thus, the expected signal expressed in (13) can be obtained by our proposed cooperative scheme. Based on (12), the SINR received at U_k after IUI cancellation in the cooperative mode is given by

$$\mathrm{SINR}_{l,k}^{co} = \frac{p_{l,k}\beta_{l,k}|g_{l,k}|^2}{\left|I'_{l,k}\right|^2 + p_{l,k}/\rho}, \tag{19}$$

where the residual interference power can be calculated by using (11), i.e.,

$$\left|I'_{l,k}\right|^2 = \beta_{l,k}|g_{l,k}|^2\sum_{i=0, i\neq k}^{M-1}p_{l,i}\Delta_i\left|\frac{\mathrm{sinc}\left(\alpha\left(i-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(i-k\right)/M\right)}\right|^2, \tag{20}$$

where $\Delta_i = |X_{l,k} - \hat{S}_{l,k}|^2$ is a constant and which is explained in Theorem 1.

Theorem 1: For quadrature phase shift keying (QPSK) modulation case, we define the hypotheses $\mathcal{H}_0$: correct demodulation, $\mathcal{H}_1$: only the real or imaginary part is detected correctly, and $\mathcal{H}_2$: both the real and imaginary parts occur error, then the value of Δ_i is given by

$$\Delta_i = \begin{cases} 0, & \mathcal{H}_0, \\ 2, & \mathcal{H}_1, \\ 4, & \mathcal{H}_2, \end{cases} \tag{21}$$

and the corresponding probability is $P_{\mathcal{H}_0} = (1-P_b)^2$, $P_{\mathcal{H}_1} = 2(1-P_b)P_b$, and $P_{\mathcal{H}_2} = {P_b}^2$, where P_b is the error probability of detection from $Y_{l,k}$ to $\hat{S}_{l,k}$.

Proof: Please see Appendix A. ■

Finally, (19) can be simplified as

$$\mathrm{SINR}_{l,k}^{co} = \frac{p_{l,k}\beta_{l,k}|g_{l,k}|^2}{\beta_{l,k}|g_{l,k}|^2\xi_k + p_{l,k}/\rho} = \frac{\omega|g_{l,k}|^2}{|g_{l,k}|^2 + \upsilon}, \tag{22}$$

where $\omega = 1/\xi_k$, $\upsilon = \frac{1}{\rho\beta_{l,k}\xi_k}$, and

$$\xi_k = \sum_{i=0, i\neq k}^{M-1} \Delta_i \left|\frac{\mathrm{sinc}\left(\alpha\left(i-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(i-k\right)/M\right)}\right|^2. \tag{23}$$

To simplify (23), we define Λ_0 as the set of index of symbols which is consistent with $\mathcal{H}_0$ (i.e., $\{i \in \Lambda_0 | \Delta_i = 0\}$). Accordingly, Λ_1 and Λ_2 are defined for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, (i.e., $\{i \in \Lambda_1 | \Delta_i = 2\}$ and $\{i \in \Lambda_2 | \Delta_i = 4\}$). Thus, we have $|\Lambda_0| + |\Lambda_1| + |\Lambda_2| = M - 1$ and ξ_k can be rewritten as

$$\begin{aligned}\xi_k &= \sum_{i=0, i\neq k}^{M-1} \Delta_i \left|\frac{\mathrm{sinc}\left(\alpha\left(i-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(i-k\right)/M\right)}\right|^2 \\ &= 2\sum_{i\in\Lambda_1} \left|\frac{\mathrm{sinc}\left(\alpha\left(i-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(i-k\right)/M\right)}\right|^2 \\ &\quad + 4\sum_{m\in\Lambda_2} \left|\frac{\mathrm{sinc}\left(\alpha\left(m-k\right)\right)}{\mathrm{sinc}\left(\alpha\left(m-k\right)/M\right)}\right|^2. \end{aligned} \tag{24}$$

Based on Theorem 1, we further investigate the impact of the error performance on the achievable SINR in the following Corollary 1.

Corollary 1: Given a SOF and input SNR, the achievable SINR of FD-NOMA with the cooperation scheme increases as the estimation accuracy of $\hat{\mathbf{S}}_l$ increases.

Proof: Based on Theorem 1, the average value of Δ_i can be given by

$$\Delta_i = 2P_{H_1} + 4P_{H_2} = 4P_b. \tag{25}$$

From (25), it indicates that the value of Δ_i monotonically increases with P_b. Thus, the residual interference power reduces with P_b based on (20) and (23). As a result, the SINR in (22) increases with P_b. The proof of this Corollary is completed. ■

IV. Achievable Secrecy Rate Analysis

In this section, we first analyze the characteristics of achievable SINR for the legitimate user and Eve, and a lower bound of the average secrecy rate of FD-NOMA is then derived.

Given bandwidth B and SOF α, the channel capacity of U_k is calculated as

$$C_k = \frac{B}{\alpha}\log_2\left[1 + \frac{p_{l,k}}{\left(N_0/2\right)B + p_I}\right] \text{ bit/s}, \tag{26}$$

where N_0 is the noise power spectral density and p_I is the power of interference. Thus, the normalized achievable rates for the legitimate user and Eve can be written respectively as

$$R_b = \frac{1}{\alpha}\log_2\left(1 + \mathrm{SIN}R_{l,k}^{co}\right), \tag{27}$$

and

$$R_e = \frac{1}{\alpha}\log_2\left(1 + \mathrm{SINR}_{l,e}\right). \tag{28}$$

The instantaneous secrecy rate at U_k is defined as [36]

$$R_s = [R_b - R_e]^+, \tag{29}$$

where $[x]^+ = \max(x, 0)$. The average secrecy rate at U_k is given by [37]

$$\begin{aligned}\bar{R}_s &= E\left\{\left[\frac{1}{\alpha}\log_2\left(1 + \mathrm{SINR}_{l,k}^{co}\right) - \frac{1}{\alpha}\log_2\left(1 + \mathrm{SINR}_{l,e}\right)\right]^+\right\} \\ &\geq E\left[\frac{1}{\alpha}\log_2\left(1 + \mathrm{SINR}_{l,k}^{co}\right)\right] - E\left[\frac{1}{\alpha}\log_2\left(1 + \mathrm{SINR}_{l,e}\right)\right] \\ &\triangleq \bar{R}_b - \bar{R}_e, \end{aligned} \tag{30}$$

where $\bar{R}_b$ and $\bar{R}_e$ denote the average achievable rates of the legitimate user and Eve, respectively. To analyze the secrecy performance, the statistical properties of SINRs in (30) are investigated as follows.

From (5), $c_{l,k}$ is a constant when $p_{l,i}$, α and M are given. Since $g_{l,k} \sim \mathcal{CN}(\mu_k, \delta_k^2)$, thus $|g_{l,k}|^2$ follows a non-central chi-square distribution with two degrees of freedom. Then, the cumulative distribution function (CDF) of $|g_{l,k}|^2$ can be expressed as

$$F_{|g_{l,k}|^2}(x) = 1 - Q_1\left(\sqrt{\frac{2\lambda_k}{\delta_k^2}}, \sqrt{\frac{2x}{\delta_k^2}}\right), x \geq 0, \tag{31}$$

where $Q_1(x, y)$ denotes Marcum-Q-function of order one, which is given by [38]

$$Q_1(x, y) = e^{-\frac{x^2}{2}} \sum_{k=0}^{\infty} \frac{x^{2k}}{2^k k!} \frac{\Gamma\left(k+1, \frac{y^2}{2}\right)}{\Gamma\left(k+1\right)}, \tag{32}$$

where $\Gamma(x, y)$ denotes the upper incomplete gamma function and $\Gamma(x)$ denotes the Euler gamma function. The probability density function (PDF) of $|g_{l,k}|^2$ can be given by

$$f_{|g_{l,k}|^2}(x) = \begin{cases} \frac{e^{-\frac{x+\lambda_k}{\delta_k^2}}}{\delta_k^2} I_0\left(\frac{2\sqrt{\lambda_k x}}{\delta_k^2}\right), & x \geq 0, \\ 0, & \text{otherwise}, \end{cases} \tag{33}$$

where the zeroth order modified Bessel function of the first kind $I_0(x)$ can be represented by the infinite series as

$$I_0(x) = \sum_{k=0}^{\infty} \frac{\left(\frac{x}{2}\right)^{2k}}{\left(k!\right)^2}. \tag{34}$$

To derive the CDF and PDF of the achievable SINR in (22), the following Lemma is given.

Lemma 1: The CDF of $\mathrm{SINR}_{l,k}^{co}$ is given by

$$F_{\mathrm{SINR}_{l,k}^{co}}\left(\gamma\right) = 1 - Q_1\left(\sqrt{\frac{2\lambda_k}{\delta_k^2}}, \sqrt{\frac{2\upsilon\gamma}{\left(\omega-\gamma\right)\delta_k^2}}\right), 0 \leq \gamma \leq \omega, \tag{35}$$

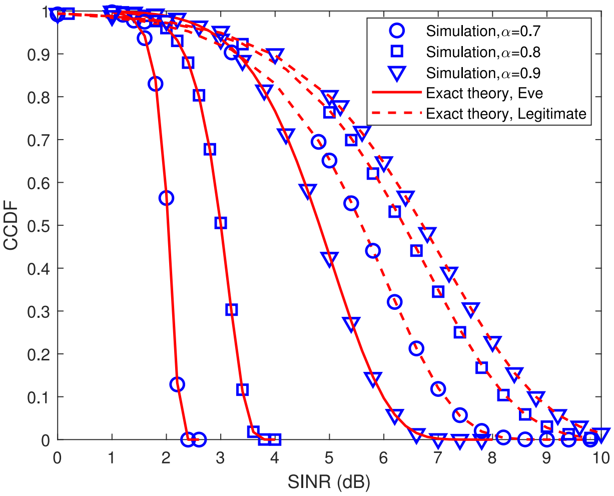

Fig. 4. CCDF of the received SINR for FD-NOMA in downlink satellite.

and the PDF of $\mathrm{SINR}_{l,k}^{co}$ can be derived as

$$f_{\mathrm{SINR}_{l,k}^{co}}(\gamma) = \frac{\upsilon\omega}{(\omega-\gamma)^2\delta_k^2} e^{-\frac{1}{\delta_k^2}\left(\frac{\upsilon\gamma}{\omega-\gamma}+\lambda_k\right)} I_0\left(\frac{2}{\delta_k^2}\sqrt{\lambda_k\frac{\upsilon\gamma}{\omega-\gamma}}\right). \tag{36}$$

Proof: Please refer to Appendix B. ■

By using the result in Lemma 1, the complementary cumulative distribution function (CCDF) for $\mathrm{SINR}_{l,k}^{co}$ can be obtained by $\overline{F}_{\mathrm{SINR}_{l,k}^{co}} = 1 - F_{\mathrm{SINR}_{l,k}^{co}}$, which is verified by numerical results demonstrated in Fig. 4. It can be seen that the numerical results show perfect agreements with our analytical expressions for various SOFs, i.e., $\alpha = 0.7$, 0.8, and 0.9, where the input SNR $= 10\log_{10}(\rho) = 10$ dB.

Based on (22) and using the results in Lemma 1, the average SINR at U_k with multiuser cooperation can be given by the following Theorem.

Theorem 2: For $0 \leq \gamma < \kappa$, the following expression is valid,

$$\begin{aligned}&\bar{\gamma}_{co}\\&= \omega e^{\frac{\upsilon-\lambda_k}{\delta_k^2}} \sum_{n=0}^{\infty} \frac{(K_B^k)^2}{(n!)^2}\left(\frac{\upsilon}{\delta_k^2}\right)^{n+1}\Gamma(n+2)\,\Gamma\left(-n-1,\frac{\upsilon}{\delta_k^2}\right).\end{aligned} \tag{37}$$

Proof: Please see Appendix C. ■

Note that the channel of Eve has the same distribution with U_k, the statistical characteristics of $\mathrm{SINR}_{l,e}$ can be similarly obtained. By using the result in Lemma 1, the PDF of $\mathrm{SINR}_{l,e}$ can be obtained as

$$\begin{aligned}&f_{\mathrm{SINR}_{l,e}}(\gamma_e)\\&= \frac{\varepsilon\kappa}{(\kappa-\gamma_e)^2\delta_e^2} e^{-\frac{1}{\delta_e^2}\left(\frac{\eta\gamma_e}{\kappa-\gamma_e}+\lambda_e\right)} I_0\left(\frac{2}{\delta_e^2}\sqrt{\lambda_e\frac{\varepsilon\gamma_e}{\kappa-\gamma_e}}\right),\end{aligned} \tag{38}$$

where $\lambda_e = |u_e|^2$ and $0 \leq \gamma_e < \kappa$. Moreover, using the result in Theorem 2, the average SINR received at Eve is given by

$$\begin{aligned}&\bar{\gamma}_e\\&= \kappa e^{\frac{\varepsilon-\lambda_e}{\delta_e^2}} \sum_{n=0}^{\infty} \frac{(K_B^e)^n}{(n!)^2}\left(\frac{\varepsilon}{\delta_e^2}\right)^{n+1}\Gamma(n+2)\,\Gamma\left(-n-1,\frac{\varepsilon}{\delta_e^2}\right),\end{aligned} \tag{39}$$

where $K_B^e = \lambda_e/\delta_e^2$ is the Rician factor of the Eve's channel, and $\lambda_e = |u_e|^2$ is the noncentrality parameter.

Further, using the PDFs in (36) and (38) we derive the lower bound of average secrecy rate for FD-NOMA with cooperative scheme as follows.

Theorem 3: For $0 \leq \gamma < \kappa$, the lower bound of average secrecy rate is given by

$$\begin{aligned}\bar{R}_s \geq\ & \frac{e^{-K_B^k}}{\alpha\ln 2}\sum_{n=0}^{\infty}\frac{\left(K_B^k\right)^n}{(n!)^2}\left(\Phi\left(\frac{\omega+1}{\upsilon}\right)-\Phi\left(\frac{1}{\upsilon}\right)\right)\\&-\frac{e^{-K_B^e}}{\alpha\ln 2}\sum_{n=0}^{\infty}\frac{\left(K_B^e\right)^n}{(n!)^2}\left(\Phi\left(\frac{\kappa+1}{\varepsilon}\right)-\Phi\left(\frac{1}{\varepsilon}\right)\right),\end{aligned} \tag{40}$$

where $\Phi(\cdot)$ is given by

$$\begin{aligned}\Phi(\theta) =& \sum_{u=0}^{n-1}\frac{n!}{(n-u)!}\left[\frac{(-1)^{n-u-1}}{\theta^{n-u}}e^{\frac{1}{\theta}}\mathrm{Ei}\left(-\frac{1}{\theta}\right)\right.\\&\left.+\sum_{q=1}^{n-u}(q-1)!\left(-\frac{1}{\theta}\right)^{n-u-q}\right]n!e^{\frac{1}{\theta}}\mathrm{Ei}\left(\frac{1}{\theta}\right).\end{aligned} \tag{41}$$

Note that $\mathrm{Ei}(x) = -\int_{-x}^{\infty} e^{-t}t^{-1}dt$ is the exponential integral function.

Proof: Please refer to Appendix D. ■

Based on (10), we can obtain that $\lim_{\rho\to\infty}\mathrm{SINR}_{l,e} = \kappa$ in high SNR region and κ is a constant when α and M are fixed. It means that the eavesdropping channel is interference limited in high SNR region. According to (30), the average secrecy rate can be approximated as

$$\begin{aligned}\bar{R}_s &\approx \frac{1}{\alpha}E\left[\log_2\left(1+\mathrm{SINR}_{l,k}^{co}\right)\right] - \frac{1}{\alpha}\log_2(1+\kappa)\\&= \bar{R}_b - \frac{1}{\alpha}\log_2(1+\kappa),\end{aligned} \tag{42}$$

where the average secrecy rate is determined by $\bar{R}_b$ in high input SNR region. Based on Corollary 1, $\xi_{l,k}$ in (22) decreases as the input SNR ρ, and then $\mathrm{SINR}_{l,k}^{co}$ is monotonously increasing with ρ. Thus, the average secrecy rate increases as the input SNR.

Since we concentrate on the satellite communications scenario and the channel of Sat-Eve is similar to that of Sat-Leg, the same Ricean factor of them can be assumed, i.e., $K_B^k = K_B^e$. Thus, we can see that the secrecy rate with FD-NOMA is mainly affected by the SOF and the parameters ω, υ, κ and ε refers to the input SNR and SOF. Based on the above analysis, FD-NOMA is proved to be a self-interference scheme and is able to degrade the legitimate and Eve links unevenly. With the multiuser cooperation, legitimate users can improve the achievable SINR. Specially, the self-interference can be canceled more effectively with high SOFs or high input SNR. In contrast, higher SOF imposes more eavesdropping risk. We can conclude that, in FD-NOMA,

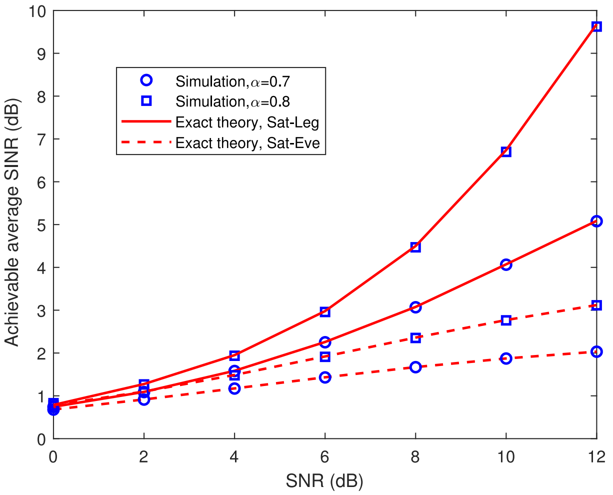

Fig. 5. Achievable average SINR of FD-NOMA.

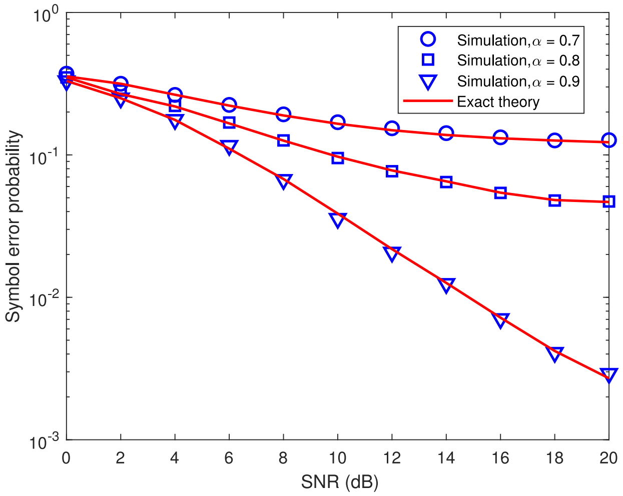

Fig. 6. Symbol error probability of estimation of $\hat{\mathbf{S}}$.

there is a trade-off between secrecy rate improvement and the level of non-orthogonal spectral overlapping among users.

V. Numerical Results and Discussions

In this section, to verify the secrecy performance of satellite communication with FD-NOMA, relevant numerical results and discussions are carried out. The impact of input SNR and SOF on the achievable secrecy rate are also investigated. Specifically, the number of users in a cluster is assumed to be $M = 128$, the channel Rician factor in dB is set to $10\log_{10}(K_B) = 10$ dB (including both legitimate users and Eve), and the product of the transmission power and its corresponding large scale loss is normalized. In addition, the same large-scale path loss is assumed for both legitimate users and Eve to demonstrate a worst-case scenario in satellite downlink communications.

Based on the proposed cooperation scheme and analytical results in (37) and (39), the achievable average SINR of FD-NOMA is presented in Fig. 5. Based on (10) and (22), the SINR of legitimate user and Eve both monotonically increases as the input SNR ρ, which is also verified by simulations. From this figure, it can be seen that the SINR can be improved significantly with cooperative scheme in the Sat-Leg link, resulting from effective interference cancellation through cooperative information exchange. Furthermore, the gain of SINR between Sat-Leg and Sat-Eve increases as the input SNR increases. This is because a better detection performance can reduce the power of residual interference, which is in consistent with Corollary 1. As shown in Fig. 6, the detection performance improves as the input SNR increases. Due to the error function in (44) is monotonically decreasing as the received SINR, thus the symbol error probability decreases as the input SNR. From Figs. 5 and 6, we can see that our derived analytical expressions match well with the simulation results. Moreover, it indicates that the higher SOF or higher input SNR can benefit the cooperation among legitimate users.

With employing FD-NOMA, the achievable secrecy rate of legitimate user is investigated versus the input SNR with different SOFs, which are shown in Fig. 7 (low SNR region) and Fig. 8 (high SNR region). The lower bound is drawn by using (40) in Fig. 7 and the curve of approximate theory is based on (42). From these two figures, we have the following informative observations: 1) FD-NOMA with cooperative scheme achieves positive secrecy rates at different SOFs, which indicates that the achievable SINR improves with user cooperation, whereas the received SINR of Eve is suppressed through the interference introduced by FD-NOMA; 2) the achievable secrecy rate improves as the input SNR increases. Since the error performance gets better as the input SNR increases, less residual interference remains and thus higher achievable SINR gain is achieved at Sat-Leg link. In addition, according to our analysis based on (42), the Sate-Eve link is interference limited while Sate-Leg link is noise limited with cooperation. Thus the secrecy rate is mainly affected by the input SNR; 3) in particular, two curves referring to SOFs $\alpha = 0.7$ and 0.8 cross at about SNR = 8 dB in Fig. 7, and a cross by $\alpha = 0.8$ and 0.9 at about SNR = 23 dB in Fig. 8. It is because more interference is produced by FD-NOMA as SOF decreases which damages the Sat-Eve link more, meanwhile the lower SOF leads to a worse error performance, indicating that

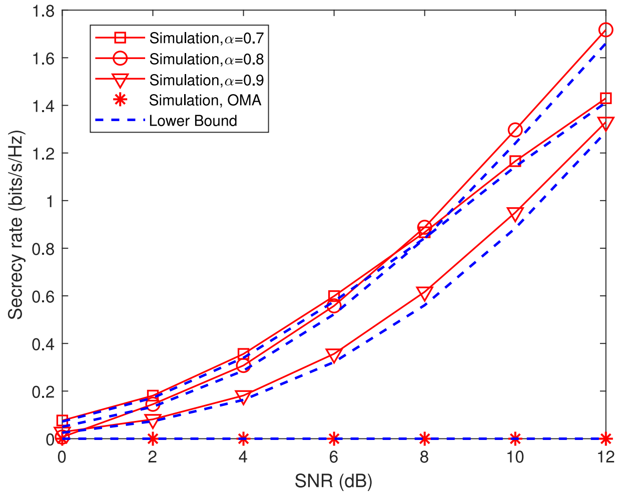

Fig. 7. Secrecy rate with multiuser cooperation versus the input SNR.

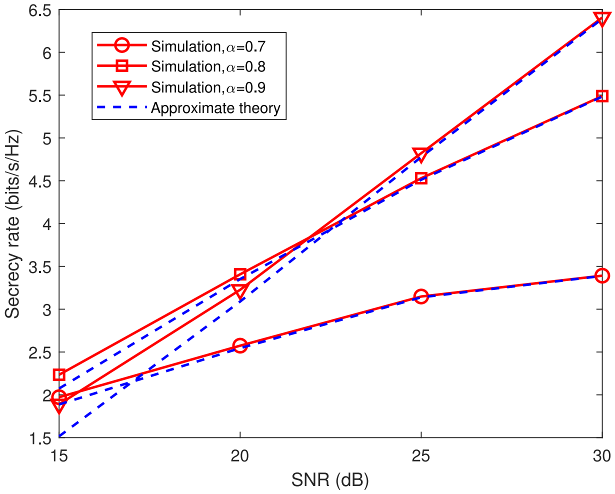

Fig. 8. Secrecy rate with multiuser cooperation versus the input SNR.

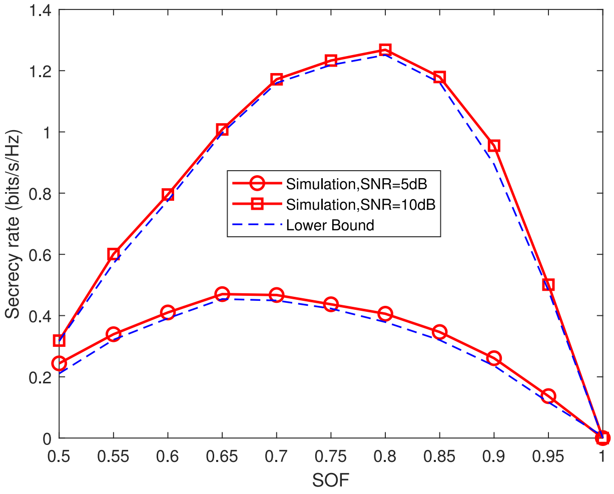

Fig. 9. Secrecy rate with multiuser cooperation versus SOF.

there is a trade-off between the spectral overlapping level and the achievable secrecy rate; 4) traditional OMA scheme (OFDMA) in similar channel quality case cannot provide secrecy. As we know that resource blocks are allocated orthogonally in OMA systems, there is no green interference can be utilized to degrade the Sat-Eve link.

In Fig. 9, the impact of SOF (ranging from 0.5 to 1) on the achievable secrecy rate is then investigated, where two cases with the input SNR $\rho = 5$ dB and $\rho = 10$ dB are displayed. As shown in Fig. 9, given an input SNR, the achievable secrecy rate will not always increase as α decreases, and there exists an optimal SOF to achieve maximum secrecy rate. Based on (42), the SOF affects secrecy rate at two aspects, i.e., the received SINR and spectral efficiency. On one hand, the received SINR decreases as α decreases since more interference is received with more spectral overlapping. On the other hand, spectral efficiency improves as α decreases in a specific region, which promotes the secrecy rate. Thus, there is a trade-off between spectral efficiency and secrecy rate in the FD-NOMA system.

VI. Conclusion and Future Work

In this paper, we have proposed a spectrum efficient and secure transmission scheme for satellite communication system, in which legitimate users access the satellite downlink network with FD-NOMA. As partial spectral resource is reused among users, FD-NOMA can improve the spectral efficiency at the cost of self-induced interference. To aim at the PLS issue, we have leveraged the interference to degrade the Sat-Eve link and meanwhile proposed a cooperative scheme to conduct interference cancellation to enhance the Sat-Leg link. The achievable secrecy rate has been analyzed, and the lower bound has also been derived. Our analysis results have shown that without the assistance of terrestrial networks or cooperative relay nodes, FD-NOMA is a promising approach to achieve secure transmission in satellite communications. To make the analysis tractable, in this study, only a single Eve is considered within a cluster. For the future work, we will investigate the multiple Eves case by considering their collusion.

Appendix A
Proof of Theorem 1

From (20), we can calculate the value of $|X_{l,k} - \hat{S}_{l,k}|^2$ as

$$\begin{aligned}\Delta_i &= \left|\mathrm{Re}\left(X_{l,k} - \hat{S}_{l,k}\right)\right|^2 + \left|\mathrm{Im}\left(X_{l,k} - \hat{S}_{l,k}\right)\right|^2\\ &= \left|\mathrm{Re}\left(X_{l,k}\right) - \mathrm{Re}\left(\hat{S}_{l,k}\right)\right|^2 + \left|\mathrm{Im}\left(X_{l,k}\right) - \mathrm{Im}\left(\hat{S}_{l,k}\right)\right|^2.\end{aligned} \tag{43}$$

Then, we can obtain the values in (21). For a given input SNR ρ, the follow real/imaginary symbol error probability of detection from $Y_{l,k}$ to $\hat{S}_{l,k}$ is obtained,

$$\begin{aligned}P_b &= \mathbb{P}\left(\mathrm{Re}\left(X_{l,k}\right) \neq \mathrm{Re}\left(\hat{S}_{l,k}\right)\right)\\ &= \mathbb{P}\left(\mathrm{Im}\left(X_{l,k}\right) \neq \mathrm{Im}\left(\hat{S}_{l,k}\right)\right)\\ &= \int_0^\infty Q\left(\sqrt{2\gamma}\right) f_{\mathrm{SINR}_{l,k}}(\gamma)\, d\gamma,\end{aligned} \tag{44}$$

where $Q(x)$ is the Gaussian Q function. Then the symbol error probability is given by [39]

$$P_s = \int_0^\infty Q\left(\sqrt{\gamma}\right)\left(2 - Q\left(\sqrt{\gamma}\right)\right) f_{\mathrm{SINR}_{l,k}}(\gamma)\, d\gamma. \tag{45}$$

For the convenience of calculation, we let A denote the case $\mathrm{Re}(X_{l,k}) \neq \mathrm{Re}(X_{l,k})$ and B denote the case $\mathrm{Im}(X_{l,k}) \neq \mathrm{Im}(X_{l,k})$. For the case of $\mathcal{H}_0$, the probability is calculated as

$$P_{\mathcal{H}_0} = \mathbb{P}(A, B) = \mathbb{P}(A)\mathbb{P}(B) = (1 - P_b)^2, \tag{46}$$

and the probability for cases $\mathcal{H}_1$ and $\mathcal{H}_2$ are respectively given by

$$\begin{aligned}P_{\mathcal{H}_1} &= \mathbb{P}\left(A, \overline{B}\right) + \mathbb{P}\left(B, \overline{A}\right)\\ &= \mathbb{P}\left(A|\overline{B}\right)\mathbb{P}\left(\overline{B}\right) + \mathbb{P}\left(B|\overline{A}\right)\mathbb{P}\left(\overline{A}\right)\\ &= 2(1 - P_b)^2,\end{aligned} \tag{47}$$

and

$$P_{\mathcal{H}_2} = \mathbb{P}\left(\overline{A}, \overline{B}\right) = \mathbb{P}\left(\overline{A}\right)\mathbb{P}\left(\overline{B}\right) = P_b^2. \tag{48}$$

Then, the proof of Theorem 2 is completed. ■

Appendix B
Proof of Lemma 1

Based on (22), $\mathrm{SINR}_{l,k} = \frac{\omega |g_k|^2}{|g_k|^2 + \upsilon} < \omega$. We calculate the CDF as

$$\begin{aligned}\mathbb{P}\left(\mathrm{SINR}_{l,k} < \gamma\right) &= \mathbb{P}\left(\frac{\omega |g_k|^2}{|g_k|^2 + \upsilon} < \gamma\right)\\ &= \mathbb{P}\left(|g_{l,k}|^2 < \frac{\upsilon\gamma}{\omega - \gamma}\right),\end{aligned} \tag{49}$$

Using (31), (49) can be simplified as

$$\begin{aligned}F_{\mathrm{SINR}_{l,k}}(\gamma) &= F_{|g_{l,k}|^2}\left(\frac{\upsilon\gamma}{\omega-\gamma}\right)\\ &= \mathbb{P}\left(|g_{l,k}|^2 < \frac{\upsilon\gamma}{\omega-\gamma}\right)\\ &= 1 - Q_1\left(\sqrt{\frac{2\lambda_k}{\delta_k^2}}, \sqrt{\frac{2\upsilon\gamma}{(\omega-\gamma)\,\delta_k^2}}\right).\end{aligned} \tag{50}$$

The PDF of $\mathrm{SINR}_{l,k}$ can be obtained by deriving (50)

$$\begin{aligned}f_{\mathrm{SINR}_{l,k}}(\gamma) &= f_{|g_{l,k}|^2}\left(\frac{\upsilon\gamma}{\omega-\gamma}\right) d\left(\frac{\upsilon\gamma}{\omega-\gamma}\right)/d\gamma\\ &= \frac{\upsilon\omega}{(\omega-\gamma)^2\delta_k^2} e^{-\frac{1}{\delta_k^2}\left(\frac{\upsilon\gamma}{\omega-\gamma}+\lambda_k\right)} I_0\left(\frac{2}{\delta_k^2}\sqrt{\lambda_k\frac{\upsilon\gamma}{\omega-\gamma}}\right).\end{aligned} \tag{51}$$

Therefore, Lemma 1 is proved. ■

Appendix C
Proof of Theorem 2

Using the PDF of $\mathrm{SINR}_{l,k}$ in (51), the average $\mathrm{SINR}_{l,k}$ can be given by

$$\begin{aligned}\bar{\gamma} &= \int_0^\infty \gamma f_{\mathrm{SINR}_{l,k}}(\gamma) d\gamma\\ &= \int_0^\kappa \gamma \frac{\eta\kappa}{(\kappa-\gamma)^2\delta_k^2} e^{-\frac{1}{\delta_k^2}\left(\frac{\eta\gamma}{\kappa-\gamma}+\lambda_k\right)} I_0\left(\frac{2}{\delta_k^2}\sqrt{\lambda_k\frac{\eta\gamma}{\kappa-\gamma}}\right) d\gamma\\ &\overset{(b)}{=} \int_0^\kappa \gamma \frac{\eta\kappa}{(\kappa-\gamma)^2\delta_k^2} e^{-\frac{1}{\delta_k^2}\left(\frac{\eta\gamma}{\kappa-\gamma}+\lambda_k\right)} \sum_{n=0}^\infty \frac{\left(K_B^k\right)^n\left(\frac{\eta\gamma}{(\kappa-\gamma)\delta_k^2}\right)^n}{(n!)^2} d\gamma\\ &\overset{(c)}{=} \kappa e^{-K_B^k}\int_0^\infty \frac{y\delta_k^2}{\left(y\delta_k^2+\eta\right)} e^{-y}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n y^n}{(n!)^2} dy\\ &= \kappa e^{-K_B^k}\int_0^\infty \sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\frac{e^{-y}y^{n+1}\delta_k^2}{\left(y\delta_k^2+\eta\right)} dy\\ &= \kappa e^{-K_B^k}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\int_0^\infty \frac{e^{-y}y^{n+1}}{\left(y+\eta/\delta_k^2\right)} dy,\end{aligned} \tag{52}$$

where (b) simplifies $I_0(\frac{2}{\delta_k^2}\sqrt{\lambda_k\frac{\eta\gamma}{\kappa-\gamma}})$ using (34) and (c) replaces $\frac{\eta\gamma}{(\kappa-\gamma)\delta_k^2}$ by y. Using the result given in [40, (EH II 137(3)), pp. 350], (52) can be further simplified, as shown in (37). Hence, the proof of Theorem 2 is completed. ■

Appendix D
Proof of Theorem 3

Using (30), we first calculate the average achievable rate of Sat-Leg user

$$\begin{aligned}\bar{R}_b &= E\left[\frac{1}{\alpha}\log_2\left(1+\mathrm{SINR}_{l,k}^{co}\right)\right]\\ &= \frac{1}{\alpha}\int_0^\infty \log_2\left(1+\gamma\right) f_{\mathrm{SINR}_{l,k}^{co}(\gamma)} d\gamma.\end{aligned} \tag{53}$$

Substituting (22) and (36) into (53) and replacing $\frac{\upsilon\gamma}{\omega-\gamma}$ by x, (53) can be simplified as

$$\begin{aligned}\bar{R}_b &= \frac{e^{-K_B^k}}{\alpha}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\int_0^\infty \log_2\left(1+\frac{\omega x}{\upsilon+x}\right)e^{-x}x^n dx\\ &= \frac{e^{-K_B^k}}{\alpha\ln 2}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\int_0^\infty \ln\left(1+\frac{(\omega+1)}{\upsilon}x\right)e^{-x}x^n dx\\ &\quad - \frac{e^{-K_B^k}}{\alpha\ln 2}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\int_0^\infty \ln\left(1+\frac{x}{\upsilon}\right)e^{-x}x^n dx.\end{aligned} \tag{54}$$

Using the result in [40, (5.12), pp. 604], (54) can be simplified as

$$\bar{R}_b = \frac{e^{-K_B^k}}{\alpha\ln 2}\sum_{n=0}^\infty \frac{\left(K_B^k\right)^n}{(n!)^2}\left(\Phi\left(\frac{\omega+1}{\upsilon}\right) - \Phi\left(\frac{1}{\upsilon}\right)\right). \tag{55}$$

Similarly, using (10) and (38), the average achievable rate of the Sat-Eve is given by

$$\begin{aligned}\bar{R}_e &= E\left[\frac{1}{\alpha}\log_2\left(1+\mathrm{SINR}_{l,e}\right)\right]\\ &= \frac{e^{-K_B^e}}{\alpha\ln 2}\sum_{n=0}^\infty \frac{\left(K_B^e\right)^n}{(n!)^2}\left(\Phi\left(\frac{\kappa+1}{\varepsilon}\right) - \Phi\left(\frac{1}{\varepsilon}\right)\right).\end{aligned} \tag{56}$$

We then have (40) by substituting (55) and (56) into (30) and thus Theorem 3 is proved. ■

References

[1] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 4, pp. 2714–2741, May 2018.

[2] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, Jul. 2017.

[3] M. Jia, X. Gu, Q. Guo, W. Xiang, and N. Zhang, "Broadband hybrid satellite-terrestrial communication systems based on cognitive radio toward 5G," *IEEE Wireless Commun.*, vol. 23, no. 6, pp. 96–106, Dec. 2016.

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

[5] N. Cheng *et al.*, "Space/Aerial-assisted computing offloading for IoT applications: A Learning-based approach," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1117–1129, May 2019.

[6] F. Lyu *et al.*, "Characterizing urban vehicle-to-vehicle communications for reliable safety applications," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2019.2920813.

[7] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[8] 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.

[9] W. Xu, S. Li, C. Lee, Z. Feng, and J. Lin, "Optimal secure multicast with simultaneous wireless information and power transfer in presence of multiparty eavesdropper collusion," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9123–9137, Nov. 2016.

[10] K. Yang, Z. Liu, X. Jia, and X. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," *IEEE Trans. Multimedia*, vol. 18, no. 5, pp. 940–950, May 2016.

[11] Y. Liu, H. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels—An approach based on ordered Eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Sec.*, vol. 12, no. 3, pp. 617–630, Mar. 2017.

[12] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6437–6449, Dec. 2018.

[13] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[14] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[15] D. Chen *et al.*, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.

[16] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Artificial-noise-aided optimal beamforming in layered physical layer security," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 72–75, Jan. 2019.

[17] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.

[18] W. Wang, K. C. Teh, and K. H. Li, "Generalized relay selection for improved security in cooperative DF relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28–31, Feb. 2016.

[19] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1670–1683, Jun. 2019.

[20] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[21] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[22] 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.

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

[24] M. Lin, Z. Lin, W. Zhu, and J. 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.

[25] Z. Lin, M. Lin, J. Wang, Y. Huang, and W. 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.

[26] 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.

[27] 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.

[28] B. Li, Z. Fei, Z. Chu, F. Zhou, 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.

[29] L. J. Ippolito and L. J. Ippolito Jr., *Satellite Communications Systems Engineering: Atmospheric Effects, Satellite Link Design and System Performance*, 2nd ed. Hoboken, NJ, USA: Wiley, 2017.

[30] A. G. Kanatas and A. D. Panagopoulos, *Radio Wave Propagation and Channel Modeling for Earth–Space Systems*. Boca Raton, FL, USA: CRC Press, 2016.

[31] Y. Zhao, H. Gao, N. C. Beaulieu, Z. Chen, and H. Ji, "Echo state network for fast channel prediction in Ricean fading scenarios," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 672–675, Mar. 2017.

[32] H. Wang and X. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[33] R. Zeng and C. Tepedelenlioglu, "Multiple device-to-device users overlaying cellular networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2017, pp. 1–6.

[34] L. Liu, Y. Chi, C. Yuen, Y. L. Guan, and Y. Li, "Capacity-achieving MIMO-NOMA: Iterative lmmse detection," *IEEE Trans. Signal Process.*, vol. 67, no. 7, pp. 1758–1773, Apr. 2019.

[35] G. C. Alexandropoulos and K. P. Peppas, "Secrecy outage analysis over correlated composite Nakagami-m/Gamma fading channels," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 77–80, Jan. 2018.

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

[37] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[38] F. J. Lopez-Martinez and J. M. Romero-Jerez, "Asymptotically exact approximations for the symmetric difference of generalized Marcum Q-functions," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2154–2159, May 2015.

[39] P. Singh, R. Budhiraja, and K. Vasudevan, "SER analysis of MMSE combining for MIMO FBMC-OQAM systems with imperfect CSI," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 226–229, Feb. 2019.

[40] D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed. New York, NY, USA: Academic, 2015.

Zhisheng Yin (S'17) received the B.E. degree from the Wuhan Institute of Technology, the B.B.A. degree from the Zhongnan University of Economics and Law, Wuhan, China, in 2012, and the M.Sc. degree in information and communication engineering from the Civil Aviation University of China, Tianjin, China, in 2016. He is currently working toward the Ph.D. degree with the Communication Research Center, School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China. From September 2018 to September 2019, he visited in BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His current research interests include space-air-ground integrated communications, aviation mobile communications, and physical layer security.

Min Jia (M'13–SM'17) received the Ph.D. degree from Sung Kyung Kwan University, Seoul, South Korea, and the Harbin Institute of Technology, Harbin, China, in 2010. She is currently an Associate Professor and a Ph.D. Supervisor with the Communication Research Center, School of Electronics and Information Engineering, Harbin Institute of Technology. Her current research interests include cognitive radio, digital signal processing, machine learning, and broadband satellite communications.

Wei Wang (S'14) received the B.Eng. degree in information countermeasure technology and the M.Eng. degree in signal and information processing from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2018. He was as a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, from September 2018 to September 2019. His research interests include wireless communications, space-air-ground integrated networks, wireless security, and physical layer security. He was the recipient of the IEEE Student Travel Grants for IEEE ICC'17, and the Chinese government award for outstanding self-financed students abroad in 2019.

Nan Cheng (S'12–M'16) received the B.E. and M.S. degrees from Tongji University, Shanghai, China, in 2009 and 2012, respectively, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2016. He is currently a Professor with the School of Telecommunication Engineering, Xidian University, Shaanxi, China. He was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, from 2017 to 2018. His current research focuses on space-air-ground integrated system, big data in vehicular networks, and self-driving system. His research interests also include performance analysis, MAC, opportunistic communication, and application of AI for vehicular networks and also interested in space-air-ground integrated networks.

Feng Lyu (S'16–M'18) received the B.S. degree in software engineering from Central South University, Changsha, China, in 2013, and the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, in 2018. Since September 2018, he has been working as a Postdoctoral Fellow with BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research interests include vehicular ad hoc networks, space-air-ground integrated network, cloud/edge computing, and big data driven application design. He is a member of the IEEE Computer and IEEE Communication Society.

Qing Guo (M'11) received the M.Eng. and Ph.D. degrees in information and communication engineering from the Harbin Institute of Technology, Harbin, China, in 1990 and 1998, respectively. He is currently a Professor and the Dean with the School of Electronics and Information Engineering, Harbin Institute of Technology. His research interests include satellite communications, deep space communications, wireless transmission, and broadband multimedia communication techniques.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990. He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on resource management, wireless network security, social networks, smart grids, and vehicular ad hoc and sensor networks. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. Dr. Shen was the recipient of the R.A. Fessenden Award in 2019 from IEEE, Canada, the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, the Joseph LoCicero Award in 2015 and the Education Award in 2017 from the IEEE Communications Society. He was also the recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award five times from the University of Waterloo and the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada. He was as the Technical Program Committee Chair/Co-Chair for the IEEE Globecom'16, the IEEE Infocom'14, the IEEE VTC'10 Fall, the IEEE Globecom'07, the Symposia Chair for the IEEE ICC'10, the Tutorial Chair for the IEEE VTC'11 Spring, the Chair for the IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He is an Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL and the Vice President on Publications of the IEEE Communications Society.