IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 28, 2018, accepted October 1, 2018, date of publication October 22, 2018, date of current version November 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2876878

Power and Time Slot Allocation Method for Secured Satellite Transmission Based on Weighted Fractional Data Carrying Artificial Noise

RUIYANG XU, XINYU DA, HANG HU, YUAN LIANG, AND LEI NI
Department of Communication System, Information and Navigation College, Air Force Engineering University, Xi'an 710077, China
Corresponding author: Ruiyang Xu (lixueyuanxuruiyang@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61571460 and Grant 61271250, in part by the Natural Science Foundation of Shaanxi Province of China under Grant 2018JQ6042, in part by the Post-Doctoral Innovative Talent Fund of China under Grant BX201700108, and in part by the China Postdoctoral Science Foundation on the 63th Grant Program.

ABSTRACT In this paper, a power and time slot allocation method is proposed for the weighted fractional data carrying artificial noise (DCAN) to secure satellite transmission. We first introduce a data carrying artificial noise based on weighted fractional Fourier transform (WFRFT) to achieve physical layer security in satellite transmission which outperforms the traditional artificial noise method when the channel state information (CSI) is not precise at the transmitter. Then, we formulate an optimization problem to optimize the power allocation among the main signal and the weighted fractional DCANs in three steps by adopting the fractional programming, the alternative research, and difference of convex functions (DC) programming, respectively. We further divide the transmission time into different time slots and assign them to the main signals by solving a maximum weighted sum problem to ensure the transmission security with limited transmission power. Simulation results show that the proposed power and time allocation method outperforms the DCAN based on WFRFT with average power allocation when the number of the transmitted signals increases. Meanwhile, the proposed power allocation method is superior to the method based on perfect CSI or the assumption of massive transmission antennas, which may be not possible at the satellite.

INDEX TERMS FH-MWFRFT, artificial noise, physical layer security, satellite communication, power allocation.

I. INTRODUCTION

The development of 5G communication technology has a tendency to integrate the traditional satellite communication system and the terrestrial 5G mobile communication system to a network, so as to meet the increasing consumer date access demands. Such network has many superiority in terms of large coverage area, flexible control of congestion and good resilience [1]. The reasonable deployment of relay nodes can extend the cover range of the signals to the wilderness, ocean or remote mountain areas where terrestrial infrastructures may not be set easily [2]–[4]. Satellite always act as a signal relay in satellite communication and two mainly used relaying methods at present are the amplified-and-forward (AF) [5] and decoded-and-forward (DF) [6]. We adopt DF relay method in this paper in order to process the signals at the satellite to achieve secured transmission.

Due to the open access character of satellite down-link channel, security has always been a critical problem in satellite communication. Started by Wyner [7], a new developed security method named physical layer security draws a great many of attentions. Many physical layer security technologies have been studied such as precoding [8], [9], beamforming [10], [11] and artificial noise [12], [13]. Among all these physical layer security technologies, artificial noise (AN) is the one that being studied most due to its good performance and compatibility. A strategy was proposed in [14] to encode message in the strongest eigen-subchannels and generate AN in the remaining spaces to apply AN in the condition that the number of antennas at the transmitter is not greater than the one at the eavesdropper. Reference [15] extended this strategy to Rician channels using the complex non-central Wishart distribution and computed a closed form expression for

secrecy capacity of such system using majorization theory. Reference [16] investigated AN injection along the temporal and spatial dimensions of a legitimate system to secure its transmissions from potential eavesdropping by considering a multiple-input multiple-output (MIMO) orthogonal frequency-division multiplexing (OFDM) system in the presence of a multiple-antenna passive eavesdropper. The AF matrixes and AN covariances were optimized simultaneously for secrecy rate maximization in [17] to maintain robustness against imperfect channel state information (CSI) of Eves in the presence of multiple multi-antenna eavesdroppers. The cryptographic methods and AN were combined to further enhance secrecy, where the symbols encrypted at the transmitter acted as noise for any potential eavesdroppers [18]. The bounds of secrecy rate in a data carrying artificial noise scheme was derived with and without a Gaussian channel estimation error [18]. The accuracy of CSI and the limitation of power are two critical issues when adopt AN to satellite communication. The inaccurate CSI shall result to a leakage of AN to the main channel and influence the intended receiver. Moreover, adding AN to the transmitted signals requires additional power, which is a precious resource at the satellite. Although some works have made researches on implementing AN when the CSI is imperfect (e.g. [17] and [18]), the solutions often involves optimization procedures which requires plenty of computing resources and time. Meanwhile, the power allocation between the main signal and the artificial noise is also a critical influence factor of the AN method. Reasonable power allocation would result to a better performance while an improper power allocation would worsen the quality of transmission. A secrecy rate maximization algorithm and its simplification, together with power allocation method was studied when considering precoder and AN design for multi-antenna wiretap channels under the finite alphabet input assumption [19]. A power allocation strategy of maximizing secrecy rate was proposed in [20] for secured directional modulation networks by the method of lagrange multiplier. However, these two methods are all based on full CSI of the legitimate channel and may be less robust. Reference [21] developed a lower bound on the ergodic secrecy rate of the artificial noise scheme based on the assumption that the number transmission antennas was very large and derived the optimal power allocation from the lower bound. Reference [22] examined the impact of transmitter-side correlation on the artificial-noise-aided secure transmission and designed a correlation-based power allocation for AN, of which the optimality in terms of achieving the minimum secrecy outage probability was analytically proved in the large system regime with the number of transmit antennas approaching infinity. Nevertheless, the method in [21] and [22] are all based on a background of massive antenna, which is not available at the satellite.

Taking the issues above into account, we adopt a new developed technology named frequency hopping-improved multi-term weighted fractional fourier transform (FH-MWFRFT) to deal with the two main problems that mentioned above when applying AN to satellite communication. WFRFT is a time-frequency analysis tool developed from fourier transform with a basic form of 4-WFRFT and can be extended to Multiple term WFRFT (MWFRFT) and Multiple parameter WFRFT (MP-WFRFT). It was first applied to communication in [23]. The physical layer security of wireless communication was enhanced when WFRFT was applied directly [24] or combined with artificial noise technology and Transform Domain Communication System [25]. Nevertheless, the application of traditional 4-WFRFT is affected due to the simplicity of its parameter. FH-MWFRFT is a combination of MWFRFT and frequency hopping, which is designed to solve this drawback. Via adopting frequency hopping to the kernel part of MWFRFT, the pattern of the traditional 4-WFRFT coefficients and matrix become more random, which can not be deciphered even by the eavesdropper with the transform order. Furthermore, the original property of WFRFT matrix is still kept after the improvement.

In this paper, we first utilize the enhanced secrecy ability of FH-MWFRFT and the orthogonality of the columns and rows of the FH-MWFRFT matrix to achieve physical layer security. Different signals are processed by different columns of the FH-MWFRFT matrix and act as data-carrying ANs to each other. In order to guarantee the secrecy performance, an additional AN is also processed by a column of FH-MWFRFT matrix and sent with the signals. In this condition, the estimation error of the CSI shall not result to leakage of AN to the main channel, which outperforms the traditional AN method under the circumstance of imperfect CSI. Then we find an optimized power and time allocation by fractional programming and difference of convex functions (DC) programming to deal with the secrecy capacity decreasing problem when the number of transmitted signals increases. According to the simulation results, the weighted fractional data-carrying artificial noise (WFDCAN) we proposed here could achieve better performance when the CSI is imperfect. Moreover, the optimized power and time slot allocation method could result to a maximum total secrecy capacity of all the transmitted signals.

The reminder of this paper is organised as follow: In section II, we introduce the system model of this paper in detail. Then the FH-MWFRFT and the WFDCAN are proposed in section III. Furthermore, we propose the power and time slot allocation method in section IV. The simulation results and relative analyses are given in section V. Finally, we draw conclusion in section VI.

Notations: The following notation is used through the paper. Bold-face lowercase type denotes vectors and the uppercase type denotes matrixes. Scalars are denoted by lowercase. $(\cdot)^H$, $\|\cdot\|$ and $|\cdot|$ denote conjugate transpose, the Forbenius norm (Euclidean norm for a vector) and the matrix determinant, respectively. $[a]^+$ represents $\max\{0, a\}$ and $\langle\cdot,\cdot\rangle$ represents the inner product of two vectors. The notations are shown clearly in the Table 1:

TABLE 1. Notations.

Notations	Representations
$\mathbf{a}$	Vectors
$\mathbf{A}$	Matrixes
a	Scalars
$(\cdot)^H$	Conjugate transpose
$\|\|\cdot\|\|$	Forbenius norm (Euclidean norm for a vector)
$\|\cdot\|$	Matrix determinant
$[a]^+$	$\max\{0, a\}$
$\langle\cdot,\cdot\rangle$	Inner product of two vectors

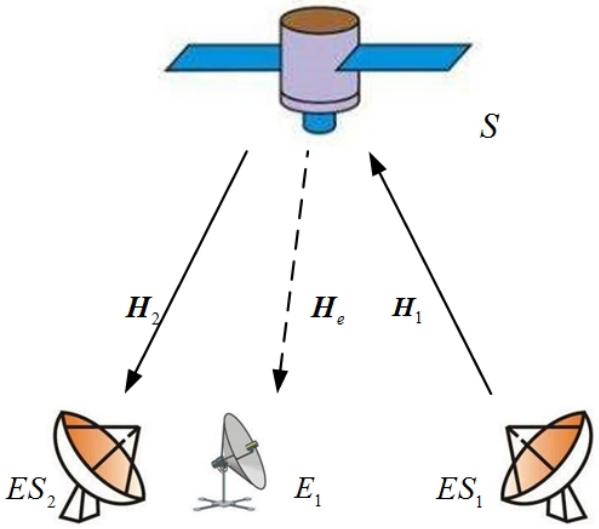

FIGURE 1. Decode-and-forward satellite communication system.

II. SYSTEM MODEL

We consider a satellite communication system based on DF protocol, where a source earth station with N_1 antennas transmits signals to a destination earth station with N_2 antennas, via a N_s antenna based regenerative satellite. An eavesdropper equips N_e antennas at the destination can also receive the signals transmitted by the satellite. The system is showed in Fig. 1. The messages are first transmit from the source earth station to the satellite, then the signals are decoded at the satellite to acquire the original messages. The messages are transmitted to the destination earth station after processed by the satellite. Denoting that $\mathbf{H}_1 \in \mathcal{C}^{N_s \times N_1}$ represents the channel gain matrix between the source earth station and the satellite and $\mathbf{x}$ represents the transmitted signal, the signal received at the satellite is given as:

$$\mathbf{y}_s = \sqrt{P_1}\mathbf{H}_1\mathbf{x} + \mathbf{n}_1 \tag{1}$$

where P_1 is the transmission power at the source earth station and $\mathbf{n}_1$ is the additive gaussian white noise (AWGN) in the source earth station-satellite channel. $\mathbf{n}_1$ obeys the distribution of $\mathcal{CN}(\mathbf{0}, \sigma_1^2\mathbf{I})$.

The received signal is decoded by the satellite and further processed for transmission. Artificial noise is also added here to maintain communication security. Denoting that $\mathbf{H}_2 \in \mathcal{C}^{N_2 \times N_s}$ represents the channel gain matrix between the satellite and the destination earth station and $\mathbf{H}_e \in \mathcal{C}^{N_e \times N_s}$ represents the channel gain matrix between the satellite and the eavesdropper. The signal received at the destination station and the eavesdropper are given as:

$$\mathbf{y}_d = \mathbf{H}_2(\sqrt{\eta P_s}\mathbf{x} + \sqrt{(1-\eta)P_s}\boldsymbol{\nu}\mathbf{n}_a) + \mathbf{n}_2 \tag{2}$$

$$\mathbf{y}_e = \mathbf{H}_e(\sqrt{\eta P_s}\mathbf{x} + \sqrt{(1-\eta)P_s}\boldsymbol{\nu}\mathbf{n}_a) + \mathbf{n}_e \tag{3}$$

where P_s is the transmission power at the satellite, $\boldsymbol{\nu}$ is the signal processing vector and $\mathbf{n}_2$ and $\mathbf{n}_e$ are the AWGN in the corresponding channel respectively. $\mathbf{n}_2 \sim \mathcal{CN}(\mathbf{0}, \sigma_2^2\mathbf{I})$ and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_e^2\mathbf{I})$. $\mathbf{n}_a$ is the artificial noise which obeys the distribution of $\mathcal{CN}(\mathbf{0}, \sigma_a^2\mathbf{I})$. $\eta \in [0, 1]$ is the allocation ratio of the transmission power.

It is always assumed that the AN is added in the null space of the main channel, e.g. the signal processing matrix need to have the property of $\mathbf{H}_2\boldsymbol{\nu} = 0$. According to (2) and (3), the signal interference to noise ratio (SINR) at the destination and eavesdropper are given as:

$$\gamma_d = \frac{\eta P_s|\mathbf{H_2}\mathbf{x}\mathbf{x}^H\mathbf{H_2}^H|}{(1-\eta)P_s\sigma_a^2|\mathbf{H_2}\boldsymbol{\nu}\mathbf{x}\mathbf{x}^H\boldsymbol{\nu}^H\mathbf{H_2}^H| + \sigma_2^2} \tag{4}$$

$$\gamma_e = \frac{\eta P_s|\mathbf{H_e}\mathbf{x}\mathbf{x}^H\mathbf{H_e}^H|}{(1-\eta)P_s\sigma_a^2|\mathbf{H_e}\boldsymbol{\nu}\mathbf{x}\mathbf{x}^H\boldsymbol{\nu}^H\mathbf{H_e}^H| + \sigma_e^2} \tag{5}$$

Thus the secrecy capacity of the DF satellite communication system is given as:

$$\begin{aligned} C_s &= [C_d - C_e]^+ \\ &= [\log_2(1+\gamma_d) - \log_2(1+\gamma_e)]^+ \end{aligned} \tag{6}$$

The aim of this model is to find a maximum secrecy capacity under some constrains such as the transmission power. Assuming the maximum transmission power is P_s, the optimization problem is given as:

$$\begin{aligned} &\max_{\mathbf{W},\eta} \ C_s \\ &s.t. \ \ 0 \leqslant P_s \leqslant p_s \\ &\qquad \mathbf{H}_2\boldsymbol{\nu} = 0 \\ &\qquad \|\boldsymbol{\nu}\| = 1 \end{aligned} \tag{7}$$

III. WEIGHTED FRACTIONAL ARTIFICIAL NOISE BASED TRANSMISSION SCHEME

In this section, we propose the transmission scheme based on the weighted fractional artificial noise. The frequency hopping based weighted fractional fourier transform and relative properties are introduced first, followed by the data carrying AN based on FH-MWFRFT.

A. FREQUENCY HOPPING BASED WEIGHTED FRACTIONAL FOURIER TRANSFORM

One of the critical problems when implementing artificial noise is that the noise should be added in the null space of the main channel, as it is expressed by the second condition in (7). It means that the added AN should be orthogonal with the main channel after being processed. Otherwise there shall be a leakage of the noise and bring interference to the

useful signal. Besides, the effect of artificial noise is decided by its power, which is confined due to the limitation of the transmission power available at the satellite. We introduce the FH-MWFRFT to deal with this problem. FH-MWFRFT is developed from WFRFT, which is defined as the weighted sum of different order fourier transforms of a signal [26]. The basic form of WFRFT is the 4-WFRFT and the expression of 4-WFRFT is given as:

$$\mathcal{F}[\mathbf{x}] = (\omega_0^\alpha \mathbf{I} + \omega_1^\alpha \mathbf{F} + \omega_2^\alpha \mathbf{PI} + \omega_3^\alpha \mathbf{PF})\mathbf{x} \tag{8}$$

where $\mathbf{x}$ is the original signal with length n, $\mathbf{I}$ is a $n \times n$ identity matrix, $\omega_l^\alpha (l = 0, 1, 2, 3)$ are the weight factors denoted as:

$$\omega_l^\alpha = \frac{1}{4}\sum_{k=0}^{3} \exp\Big[\frac{-j2\pi(\alpha - l)k}{4}\Big] \tag{9}$$

$\mathbf{F}$ is the unitary discrete fourier transform matrix. $\mathbf{F}^2 = \mathbf{F} \cdot \mathbf{F}$ and $\mathbf{F}^3 = \mathbf{F} \cdot \mathbf{F} \cdot \mathbf{F}$ are the second and third order of DFT operation respectively. The result of $\mathbf{F}^4$ is an identity matrix, which makes the period of $\mathbf{F}$ four.

According to the property of the WFRFT matrix, the columns and rows of the transform and inverse transform matrix with corresponding order are processed of orthogonality. We aim to utilize this to solve the problems mentioned above.

Theorem 1: The multiplication results of the columns of an α order 4-WFRFT matrix and the corresponding rows of an $-\alpha$ order 4-WFRFT matrix are one and the results of non-corresponding columns and rows are zero.

Proof: Denoting $\mathbf{W}^\alpha$ as the matrix of an α order 4-WFRFT, we can derive from (8) that:

$$\begin{aligned}\mathbf{W}^{-\alpha}\mathbf{W}^{\alpha} = &\sum_{l_1+l_2=0\ or 4} \omega_{l_1}^{-\alpha}\omega_{l_2}^{\alpha}\mathbf{I} + \sum_{l_1+l_2=1\ or 5} \omega_{l_1}^{-\alpha}\omega_{l_2}^{\alpha}\mathbf{F} \\ &+ \sum_{l_1+l_2=2\ or 6} \omega_{l_1}^{-\alpha}\omega_{l_2}^{\alpha}\mathbf{F}^2 + \sum_{l_1+l_2=3} \omega_{l_1}^{-\alpha}\omega_{l_2}^{\alpha}\mathbf{F}^3\end{aligned} \tag{10}$$

According to (9), the multiplication of the coefficients is given as:

$$\begin{aligned}\omega_{l_1}^{\alpha}\omega_{l_2}^{-\alpha} &= \frac{1}{16}\sum_{k_1=0}^{3}\sum_{k_2=0}^{3} \exp(\frac{-j2\pi k_1(\alpha - l_1)}{4}) \\ &\quad \times \exp(\frac{-j2\pi k_2(-\alpha - l_2)}{4}) \\ &= \frac{1}{16}\sum_{k_1=0}^{3}\sum_{k_2=0}^{3} \exp(\frac{-j2\pi\alpha(k_1 - k_2)}{4}) \\ &\quad \times (\frac{j2\pi(k_1 l_1 + k_2 l_2)}{4}) \\ &= \frac{1}{4}\sum_{k_1=k_2=0}^{3} \exp(\frac{j2\pi(k_1 l_1 + k_2 l_2)}{4} \\ &= \begin{cases} 1 & \mathrm{l_1 + l_2 = 0\ or\ 4} \\ 0 & \mathrm{others} \end{cases} \quad l_1, l_2 = 0 \sim 3\end{aligned} \tag{11}$$

During the derivation of (11), we applied the property below:

$$\sum_{k_1=0}^{3}\sum_{k_2=0}^{3} \exp(\frac{-j2\pi(\alpha(k_1 - k_2))}{4}) = \begin{cases} 1 & \mathrm{k_1 = k_2} \\ 0 & \mathrm{k_1 \neq k_2} \end{cases} \tag{12}$$

With the result of (11), we can conclude that the consequence of (10) is an identity matrix, e.g.

$$\mathbf{W}^{-\alpha}\mathbf{W}^{\alpha} = \mathbf{I} \tag{13}$$

Therefore the multiplication results of corresponding columns and rows of the α order 4-WFRFT matrix and the $-\alpha$ order 4-WFRFT matrix are one and results of the non-corresponding columns and rows are zero. Theorem 1 is proved. □

Nevertheless, the main drawback of 4-WFRFT is the simplicity of its parameter. Once the transform method and order are known by the eavesdropper, the signal is not safe anymore. Thus we apply the MWFRFT [27] instead of the original 4-WFRFT and adopt frequency hopping to enhance its performance. The frequency hopping sequence is applied to disrupted the original order of the columns of the discrete fourier matrix (DFT) in MWFRFT. The elements in the DFT matrix of different order after frequency hopping are given as:

$$F_{n,k} = \exp(\frac{-j2\pi n \bmod(k + d, N)}{N})n, \quad k = 0 \sim N - 1 \ d \in \mathbb{N} \tag{14}$$

$$F_{n,k}^2 = \begin{cases} \exp(\frac{-j2\pi nd}{N}) & \mathrm{n + k + d = 0\ or\ N} \\ 0 & \mathrm{others} \end{cases} n, \quad k = 0 \sim N - 1 \tag{15}$$

$$F_{n,k}^3 = \exp(\frac{-j2\pi(-nk - kd - d^2)}{N}) \quad n, \quad k = 0 \sim N - 1 \tag{16}$$

$$F_{n,k}^4 = \begin{cases} \exp(\frac{-j2\pi(-d^2)}{N}) & \mathrm{n = k} \\ 0 & \mathrm{others} \end{cases} n, \quad k = 0 \sim N - 1 \tag{17}$$

where d is the corresponding decimal number of the frequency hopping sequence.

We can deduce from (17) that the period of the DFT matrix after frequency hopping is no longer four. Thus the coefficients shall be different respectively, which is given as:

$$\omega_{l(FH)}^{\alpha} = \frac{1}{n(d)}\sum_{k=0}^{n(d)-1} \exp\Big[\frac{-j2\pi(\frac{n(d)k_m}{M} - l)k}{n(d)}\Big] \quad k_m = 0 \sim M - 1, \quad l = 0 \sim n(d) - 1 \tag{18}$$

where $n(d)$ is the new period of the FH-DFT matrix related to d, M is the number of the terms of MWFRFT. Thus the expression of FH-MWFRFT can be given as:

$$\mathcal{F}[\mathbf{x}] = \sum_{k_m=0}^{M-1} B_{M,k_m}(\alpha)\mathbf{W}_{FH4}^{\frac{n(d)k_m}{M}}\mathbf{x}, \quad M \geqslant 3 \tag{19}$$

where $B_{M,k_m}(\alpha)$ and $\mathbf{W}_{FH4}$ are the MWFRFT coefficient and the FH-WFRFT matrix, whose expressions are given as:

$$B_{M,k_m}(\alpha) = \frac{1}{M}\sum_{m=0}^{M-1}\exp(\frac{-2j\pi m(\alpha-k_m)}{M}) \tag{20}$$

$$\mathbf{W}_{FH4}^{\frac{n(d)k_m}{M}} = \sum_{l=0}^{n(d)-1}\omega_{l(FH)}^{\frac{n(d)k_m}{M}}\mathbf{F}^l \tag{21}$$

Theorem 2: The columns and rows of the FH-MWFRFT matrix with corresponding orders also process of orthogonality.

Proof: The form of $\mathbf{W}_{FH4}^{\frac{n(d)k_m}{M}}$ is similar with the 4-WFRFT matrix, therefore it complies with theorem 1. Besides, the expression of coefficient $B_{M,k_m}(\alpha)$ is also similar with the expression of ω_l^α in 4-WFRFT, which means the result of (11) can also be used to (20), thus the multiplication of two FH-MWFRFT matrix with corresponding orders is also an identity matrix. Consequently, the columns and rows of the FH-MWFRFT matrix with corresponding transform orders are processed of orthogonality. □

We apply the orthogonality among the columns and rows of the FH-MWFRFT matrix to achieve the second condition in (7). Meanwhile, since there exists many pairs of columns and rows, multiple signals can be transmitted simultaneously to enhance the security and make use of the transmission power efficiently.

B. WEIGHTED FRACTIONAL ARTIFICIAL NOISE

To utilize the orthogonality of the FH-MWFRFT matrix, we adopt the columns of the matrix as signal processing vector. Then the received signals at the destination and the eavesdropper are given as:

$$\begin{aligned}\mathbf{y}_{di} &= \mathbf{H}_2(\sqrt{\eta_i P_{si}}\mathbf{w}_{FHM_i}^\alpha\mathbf{x}_i \\ &\quad+\sum_{l=1,l\neq i}^{N}\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{w}_{FHM_l}^\alpha\mathbf{x}_l \\ &\quad+\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{w}_{FHM_{N+1}}^\alpha\mathbf{n}_a)+\mathbf{n}_2 \end{aligned}\tag{22}$$

$$\begin{aligned}\mathbf{y}_{ei} &= \mathbf{H}_e(\sqrt{\eta_i P_{si}}\mathbf{w}_{FHM_i}^\alpha\mathbf{x}_i \\ &\quad+\sum_{l=1,l\neq i}^{N}\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{w}_{FHM_l}^\alpha\mathbf{x}_l \\ &\quad+\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{w}_{FHM_{N+1}}^\alpha\mathbf{n}_a)+\mathbf{n}_e \end{aligned}\tag{23}$$

where $\mathbf{w}_{FHM_i}$ is the *ith* column of the FH-MWFRFT matrix and η_i is the power allocation ratio of the *ith* signal. P_{si} is the transmission power for the *ith* signal. N is the total transmitted number of the signals. Prior to the transmission, we apply the OSTBC to the signals after FH-MWFRFT processing to prevent the orthogonality from being affected by the channel. Related procedures are ignored here for clarity. The destination earth station adopts the rows of the FH-MWFRFT matrix to offset the interference brought by the other signals and the added artificial noise. The signals after interference offsetting are given as:

$$\mathbf{y}_{di} = \mathbf{H}_2\sqrt{\eta_i P_{si}}\mathbf{x}_i + \mathbf{v}_{FHM_i}^{-\alpha}\mathbf{n}_2 \tag{24}$$

$$\begin{aligned}\mathbf{y}_{ei} &= \mathbf{H}_e(\sqrt{\eta_i P_{si}}\mathbf{v}_e\mathbf{w}_{FHM_i}^\alpha\mathbf{x}_i \\ &\quad+\sum_{l=1,l\neq i}^{N}\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{v}_e\mathbf{w}_{FHM_l}^\alpha\mathbf{x}_l \\ &\quad+\sqrt{\frac{(1-\eta_i)P_{si}}{N}}\mathbf{v}_e\mathbf{w}_{FHM_{N+1}}^\alpha\mathbf{n}_a)+\mathbf{n}_e \end{aligned}\tag{25}$$

Since there is a weighted term of $\mathbf{F}^0 = \mathbf{I}$ in every FH-MWFRFT matrix, the corresponding part of the signal is the only information of the original message that may possible be acquired by the eavesdropper. According to (24) and (25), the SINR of the *ith* signal at the destination and eavesdropper are given as:

$$\gamma_{di} = \frac{\eta_i P_{si} D_i}{\sigma_2^2} \tag{26}$$

$$\gamma_{ei} = \frac{\eta_i P_{si} K_0}{\eta_i P_{si} K_m + \frac{(1-\eta_i)P_{si}}{N}((N-1)E_l + E_{AN}) + \sigma_e^2} \tag{27}$$

where

$$D_i = |\mathbf{H}_2\mathbf{x_i}\mathbf{x_i}^H\mathbf{H}_2^H| \tag{28}$$

$$K_0 = |\mathbf{H}_e B_{M,k_0}\mathbf{x_i}\mathbf{x_i}^H B_{M,k_0}^H\mathbf{H}_e^H| \tag{29}$$

$$K_m = |\mathbf{H}_e B_{M,k_{m\neq 0}}\mathbf{x_i}\mathbf{x_i}^H B_{M,k_{m\neq 0}}^H\mathbf{H}_e^H| \tag{30}$$

$$E_l = \sum_{l=1,l\neq i}^{N}|\mathbf{H}_e\mathbf{w}_l\mathbf{x}_l\mathbf{x}_l^H\mathbf{w}_l^H\mathbf{H}_e^H| \tag{31}$$

$$E_{AN} = |\mathbf{H}_e\mathbf{w}_{N+1}\mathbf{n}_a\mathbf{n}_a^H\mathbf{w}_{N+1}^H\mathbf{H}_e^H| \tag{32}$$

in these equations above, $\mathbf{w}_i = \mathbf{v}_e\mathbf{w}_{FHM_i}^\alpha$.

We can infer from (26) and (27) that the adoption of weighted fractional artificial noise deteriorate the SINR at the eavesdropper. The signals and artificial noise processed by the FH-MWFRFT vectors act as interferences to the eavesdropper. The destination receiver with the corresponding vectors could receive all the signals and eliminate the artificial noise while the eavesdropper would be affected by the processed signals. Even the transform order is known, the eavesdropper also can not acquire the right vector due to the pseudorandom sequence and the parameter M. Meanwhile, the second condition in (7) is met by applying the orthogonality between the corresponding vectors instead of the orthogonality between the channel gain matrix and the signal processing vector. The norm of $\mathbf{w}_{FHM_i}^\alpha$ is always one, which meets the third condition in (7). The optimization problem is simplified as:

$$\begin{aligned}\max\ & C_{si} \\ s.t.\ & 0 \leqslant P_{si} \leqslant p_s \\ & 0 \leqslant \eta_i \leqslant 1\end{aligned}\tag{33}$$

Nevertheless, the limited transmission power at the satellite still need to be allocated to all the signals and the artificial noise. To maximize the secrecy capacity of each transmission, we need to search for the best power allocation scheme.

IV. POWER AND TIME SLOT ALLOCATION SCHEME

In this section, we propose the power and time slot allocation scheme based on the fractional programming and DC programming. Specially, we first convert the primal problem (33) into the parametric program problem (40) by using fractional programming to transform the original objective function into a parameterized polynomial subtractive form. Then, a fractional programming algorithm is used to iteratively solve the parametric program problem by alternately solving two DC secondary problems with the form of (46) at each iteration which are based on the DC programming. Furthermore, in the inner of DC programming, two sequential convex subproblems (50) and (51) are solved finally. Moreover, the power allocation scheme would allocate the main part of the transmitted power to the signal being transmitted at present, thus we consequently propose a time slot allocation scheme which divide the transmission time into different time slots and allocate them to different signals and aim to achieve a maximum total secrecy capacity.

A. TRANSFORMATION OF THE OBJECTIVE FUNCTION

According to (6), the objective function of (33) can be expressed as:

$$C_{si} = log_2(\frac{1+\gamma_{di}}{1+\gamma_{ei}}) \tag{34}$$

After some mathematic and by adopting (26) and (27), (34) can be extended as:

$$\begin{aligned} C_{si} &= log_2(\frac{1+\frac{\eta_i P_{si} D_i}{\sigma_2^2}}{1+\frac{\eta_i P_{si} K_0}{\eta_i P_{si} K_m + Q_i + \sigma_e^2}}) \\ &= log_2(\frac{(\sigma_2^2+\eta_i P_{si} D_i)(\eta_i P_{si} K_m + Q_i + \sigma_e^2)}{\sigma_2^2(\eta_i P_{si}(K_0+K_m)+Q_i+\sigma_e^2)}) \end{aligned} \tag{35}$$

where $Q_i = \frac{(1-\eta_i)P_{si}}{N}((N-1)E_l + E_{AN})$.

Since the logarithmic function is a monotonically increasing function, maximize (30) would be equal to maximize:

$$\frac{(\sigma_2^2+\eta_i P_{si} D_i)(\eta_i P_{si} K_m + Q_i + \sigma_e^2)}{\sigma_2^2(\eta_i P_{si}(K_0+K_m)+Q_i+\sigma_e^2)} \tag{36}$$

under the limitation of $L = \{0 \leqslant P_{si} \leqslant P_{si}, 0 \leqslant \eta_i \leqslant 1, i = 1, 2, ..., N\}$.

The form of (36) can be classed into the nonlinear fractional programming which has been studied in [28] and [29]. Denoting φ_i^*, P_{si}^* and η_i^* to be the maximum value of (36) for the *ith* signal, the corresponding transmission power and the power allocation ratio respectively, the objective function is associated with a parametric program problem and can be stated as follows based on the fractional programming:

$$\varphi_i^* = \frac{Y(P_{si}^*, \eta_i^*)}{Z(P_{si}^*, \eta_i^*)} = \max_{(P_{si}^*, \eta_i^*) \in L} \frac{Y(P_{si}, \eta_i)}{Z(P_{si}, \eta_i)} \tag{37}$$

where $Y(P_{si}, \eta_i) = (\sigma_2^2 + \eta_i P_{si} D_i)(\eta_i P_{si} K_m + Q_i + \sigma_e^2)$ and $Z(P_{si}, \eta_i) = \sigma_2^2(\eta_i P_{si}(K_0 + K_m) + Q_i + \sigma_e^2)$. Thus the original objective function is transformed to a parametric program with parameter φ_i, which is defined as:

$$\max_{(P_{si}, \eta_i) \in L} \{Y(P_{si}, \eta_i) - \varphi_i Z(P_{si}, \eta_i)\} \tag{38}$$

As a result, the optimization problem is reformulated to find φ^*, P_{si}^* and η_i^* by solving (38) to satisfy L. By the method in [29] with a initial value $\varphi_i^{(0)}$, (38) can be solved by iteratively by solving

$$\max_{(P_{si}, \eta_i) \in L} \{Y(P_{si}, \eta_i) - \varphi_i^{(j)} Z(P_{si}, \eta_i)\} \tag{39}$$

with a given $\varphi_i^{(j)}$ at each iteration, where j is the iteration index. (39) can be equally expressed as:

$$\min_{(P_{si}, \eta_i) \in L} \{\varphi_i^{(j)} Z(P_{si}, \eta_i) - Y(P_{si}, \eta_i)\} \tag{40}$$

By solving (40) iteratively, we shall acquire the optimal values φ^*, P_{si}^* and η_i^*. To make it available in practice, we define a terminated condition of the iterative process as:

$$|\varphi_i^{(j)} Z(P_{si}, \eta_i) - Y(P_{si}, \eta_i)| \leq \epsilon \tag{41}$$

with a small convergence tolerance $\epsilon > 0$. The algorithm of fractional programming is clarified in Algorithm 1, where J_ϵ is the maximum allowed number of iterations considering the computational time.

Algorithm 1 Fractional Programming Algorithm

Input: $\mathbf{H}_2, \mathbf{H}_e, \mathbf{x_i}, B_{M,k_0}, B_{M,k_m \neq 0}, \mathbf{w}_i$
Output: $\varphi^*, P_{si}^*, \eta_i^*$
1:Choose a initial value $\varphi_i^{(0)}$ and set $j = 0$;
2:**repeat**;
3:For the given $\varphi_i^{(j)}$, find the optimal $P_{si}(\varphi_i^{(j)})$ and $\eta_i(\varphi_i^{(j)})$ by solving (40)(Alternate search);
4:Update $\varphi_i^{(j)}$ to $\varphi_i^{(j+1)}$;
5:j=j+1;
6:**until** the inequality (41) or $j > J_\epsilon$ is satisfied;
7:**return** $\varphi_i^* = \varphi_i^{(j)}$, $P_{si}^* = P_{si}^{(j-1)}$ and $\eta_i^* = \eta_i^{(j-1)}$

Remark 1: Explicitly, the primal problem (36) is relevant to (38), and then solved iteratively by solving a series of parameterized secondary problem (40) with each given $\varphi_i^{(j)}$. The parameter φ_i act as a compensation to the difference between $Z(P_{si}, \eta_i)$ and $Y(P_{si}, \eta_i)$. The greater difference would result to a larger φ_i to reach the minimum point. The iterative process generates a strictly increasing sequence $\{\varphi_i^{(j)}\}$ which superlinearly converges to φ_i^* with an initial value of $\varphi_i^{(0)} < \varphi_i^*$. The convergence of the fractional programming has been detailed in [29] and [30]. Moreover, some physical intuition of the parametric programming (38) can be interpreted by referring to [31].

B. ALTERNATE SEARCH FOR THE TRANSMISSION POWER AND THE POWER ALLOCATION RATIO

We now have transformed the objective function to a series of parameterized secondary problems. However, these parameterized problems are still unsolvable with two variables P_{si} and η_i. Therefore, an approach termed as alternate search is proposed based on the convexity and affinity of Y and Z [32].

According to the definition of Y, it is a quadratic function of P_{si} or η_i when the other variable is fixed. Thus Y is a convex function related to P_{si} or η_i respectively. Z is a affine function due to its definition. Thus, for given P_{si} or η_i, (40) is a DC function with respect to η_i or P_{si}. By exploiting the DC structure, the alternate search strategy can be adopted to solve (40) iteratively. The key idea of the alternate search is that only one of P_{si} or η_i is optimized in every step while the other is fixed. In another word, we could find the solution of (40) by solving a two-level optimization problem that is given as:

$$\min_{P_{si}\in L}\min_{\eta_i\in L}\{\varphi_i^{(j)}Z(P_{si},\eta_i)-Y(P_{si},\eta_i)\} \tag{42}$$

In (42), the lower level subproblem is to decide the maximum power that is needed to make a high secrecy capacity transmission:

$$\min_{P_{si}\in L}\{\varphi_i^{(j)}Z(P_{si},\eta_i^{(j)})-Y(P_{si},\eta_i^{(j)})\} \tag{43}$$

and the higher level subproblem is to decide the power allocation with the obtained transmission power:

$$\min_{\eta_i\in L}\{\varphi_i^{(j)}Z(P_{si}^{(j)},\eta_i)-Y(P_{si}^{(j)},\eta_i)\} \tag{44}$$

Algorithm 2 Fractional Programming Algorithm

Input: $\varphi_i^{(j)}, P_{si}^{(j)}, \eta_i^{(j)}$
Output: $P_{si}^{(j+1)}, \eta_i^{(j+1)}$
1:For a fixed $\eta_i^{(j)}$, find the optimal solution $P_{si}^{(j+1)}$ of (43) (DC programming);
2:For a fixed $P_{si}^{(j)}$, find the optimal solution $\eta_i^{(j+1)}$ of (44) (DC programming);
3:**return** $P_{si}^{(j+1)}, \eta_i^{(j+1)}$

We may obtain a local optimal solution of (40) by solving (43) and (44). The alternate search algorithm is summarized in Algorithm 2. Since (43) and (44) are all special cases of (40), we could draw the conclusion that when η_i is given, (43) and (40) are equivalent. Also, when P_{si} is given, (44) and (40) are equivalent. Therefore, the optimal solution of (43) and (40) are equal with given η_i. Similarly, the optimal solution of (44) and (40) are equal with given P_{si}. Denoting that $U(P_{si},\eta_i)=\varphi_i^{(j)}Z(P_{si},\eta_i)-Y(P_{si},\eta_i)$, we hence can conclude that:

$$U(P_{si}^{(j+1)},\eta_i^{(j+1)})\leqslant U(P_{si}^{(j)},\eta_i^{(j)}) \tag{45}$$

which signifies the sequence $\{U(P_{si}^{(j)},\eta_i^{(j)})\}$ is monotonically decreasing. Thus the algorithm is convergent.

C. THE SOLUTION BASED ON DC PROGRAMMING

According to the analyses above, (43) and (44) are two DC problems with the fixed $\eta_i^{(j)}$ and $P_{si}^{(j)}$. These DC subproblems can be solved by DC programming which was studied in [33].

A standard DC problem is modeled as the difference of two convex functions expressed as $\min_X\{f(X)=f_1(X)-f_2(X)\}$ with also a convex feasible domain of X. It can be worked out iteratively by solving a sequential convex problem [28]

$$\min_X\{f_1(X)-f_2(X^{(j)})-\langle\nabla f_2(X^{(j)}),X-X^{(j)}\rangle\} \tag{46}$$

at each iteration, where $X^{(j)}$ is the optimal solution of the $j-1$ iteration and $\nabla f_2(X^{(j)})$ is the gradient of $f_2(X)$ evaluated at $X^{(j)}$.

Remark 2: Actually, the DC problem is solved by dealing with the different parts of it. At the jth iteration, $f_2(X)$ is replaced with its global underestimator $f_2(X)=f_2(X^{(j)})+\langle\nabla f_2(X^{(j)}),X-X^{(j)}\rangle$ [34], which is similar to [35]. When given a starting point, a solution sequence of $\{X^{(j)}\}$ of the DC problem (46) can be acquired by solving it iteratively.

Since $f_2(X)$ is a convex function, we could infer that:

$$f_2(X^{(j+1)})\geqslant f_2(X^{(j)})+\langle\nabla f_2(X^{(j)}),X-X^{(j)}\rangle \tag{47}$$

As $X^{(j+1)}$ is the optimal solution and $X^{(j)}$ is only a feasible solution, it can be deduced that:

$$f_1(X^{(j+1)})-f_2(X^{(j)})-\langle\nabla f_2(X^{(j)}),X-X^{(j)}\rangle \leqslant f_1(X^{(j)})-f_2(X^{(j)}) \tag{48}$$

By combining (47) and (48), we conclude that:

$$f_1(X^{(j+1)})-f_2(X^{(j+1)})\leqslant f_1(X^{(j)})-f_2(X^{(j)}) \tag{49}$$

Thus we prove here that the solution $X^{(j+1)}$ is better than the solution $X^{(j)}$, which means the sequence $\{f(X^{(j)})\}$ is convergent.

In the light of the foregoing analyses, the problems (43) and (44) can be solved by solving the following problems below respectively.

$$\min_{P_{si}\in L}\{\varphi_i^{(j)}Z(P_{si},\eta_i^{(j)})-Y(P_{si}^{(j)},\eta_i^{(j)}) -\langle\nabla Y(\bar{P}_{si}^{(j)},\eta_i^{(j)}),P_{si}-P_{si}^{(j)}\rangle\} \tag{50}$$

$$\min_{\eta_i\in L}\{\varphi_i^{(j)}Z(P_{si}^{(j)},\eta_i)-Y(P_{si}^{(j)},\eta_i^{(j)}) -\langle\nabla Y(P_{si}^{(j)},\bar{\eta}_i^{(j)}),\eta_i-\eta_i^{(j)}\rangle\} \tag{51}$$

$\nabla Y(\bar{P}_{si}^{(j)},\eta_i^{(j)})$ and $\nabla Y(P_{si}^{(j)},\bar{\eta}_i^{(j)})$ are the gradient of Y with respect to $P_{si}^{(j)}$ and $\eta_i^{(j)}$ whose expressions are given below. According to the analyses above, (50) and (51) are all convex and could be solved by convex programming. Thus by applying DC programming, we transform problem (43) and (44) to problem (50) and (51) and utilizing the CVX toolbox to acquire the best solutions for the

Algorithm 3 DC Programming Algorithm

Input: $\eta_i^{(j)}$(or $P_{si}^{(j)}$)
Output: $P_{si}^{(j+1)}$(or $\eta_i^{(j+1)}$)
1:Input a initial value $\eta_i^{(j)}$(or $P_{si}^{(j)}$);
2:For $P_{si}^{(j)}$(or $\eta_i^{(j)}$), solve (50) (or (51)) to obtain $P_{si}^{(j+1)}$ (or $\eta_i^{(j+1)}$) by the CVX toolbox
3:**return** $P_{si}^{(j+1)}$(or $\eta_i^{(j+1)}$)

optimization problem. The DC programming is expounded in Algorithm 3:

$$\frac{\partial Y}{\partial P_{si}} = \eta_i^{(j)} D_i(\eta_i^{(j)} P_{si}^{(j)} K_m + Q_i + \sigma_e^2) + (1+\eta_i^{(j)} P_{si}^{(j)} D_i)(\eta_i^{(j)} K_m + \frac{1-\eta_i^{(j)}}{N}((N-1)E_l + E_{AN})) \tag{52}$$

$$\frac{\partial Y}{\partial \eta_i} = P_{si}^{(j)} D_i(\eta_i^{(j)} P_{si}^{(j)} K_m + Q_i + \sigma_e^2) + (1+\eta_i^{(j)} P_{si}^{(j)} D_i)(P_{si}^{(j)} K_m + \frac{P_{si}^{(j)}}{N}((N-1)E_l + E_{AN})) \tag{53}$$

Depending on the adoption of these mathematical methods in the subsections hereinbefore, the non convex optimization problem (33) becomes solvable. The proposed scheme is a chain structure with these methods. By applying the related mathematical methods, the original problem is transformed to some simple subproblems which can be solved via the CVX toolbox.

From the convergence analysis of the algorithms above, we have proved that each subproblem has convergence tolerance with finite iterations. In practice, we could preset the maximum allowed number of iterations for each subproblem to make a balance between the computational time and accuracy.

D. TIME SLOT ALLOCATION BASED ON TOTAL SECRECY CAPACITY MAXIMIZATION

The power allocation method proposed above would result to an optimal secrecy capacity of one transmitted signal while other signals shall act as artificial noises. Nevertheless, to ensure that all the signals can be transmitted under a secured condition, we still need to divide the transmission time T into some slots with different length and assign them to those signals. Denoting the ratio of the transmission time allocated to the *ith* signal is β_i, and assuming the secrecy capacity of the *ith* signal has already be acquired via the method above, then the time slot allocation problem is given as:

$$\begin{aligned} \max \quad & \sum_{i=1}^{N} \beta_i C_{si} \\ s.t. \quad & \frac{\iota_i}{\sum_{i=1}^{N} \iota_i} \leqslant \beta_i \leqslant 1 \\ & \sum_{i=1}^{N} \beta_i = 1 \end{aligned} \tag{54}$$

TABLE 2. LMS channel parameters [36].

Shadowing	b	m	Ω
Frequent heavy shadowing (FHS)	0.063	0.739	8.97×10^{-4}
Average shadowing (AS)	0.126	10.1	0.835
Infrequent light shadowing (ILS)	0.158	19.4	1.29

where ι_i is the length of the *ith* signal. The objective function of problem (54) is an affine function and the feasible domain is convex, thus this optimal problem can be solved via using the CVX toolbox.

Remark 3: The optimal solution of (54) will always reach a maximum value, in another word, problem (54) is convergent. Because of the constraint conditions, the optimal value of the objective function will always have an upper bound. Assuming the maximum achievable secrecy capacity among all the signals is C_{sm} and all the signals have achieved this maximum secrecy capacity during transmission, according to the second constraint condition, the total secrecy capacity during one transmission can be given as $C_{stotal} = \sum_{i=1}^{N} \beta_i C_{sm} = C_{sm}$. Since not all the signal can achieve the maximum secrecy capacity C_{sm}, we have $C_{si} \leqslant C_{sm}$. Hence there exists an upper bound for the optimal problem (54).

V. SIMULATION RESULTS AND DISCUSSIONS

To verify the performance of the proposed scheme, we present some simulations under different situations. The destination receiver and the eavesdropper are assumed to be equipped with single antenna. We assume the channel to be shadow-rician channel, which is a new channel model for satellite communication [11]. The parameter of the shadow-rician channel are given in table 1 according to [36]. The variances of the AWGN in both the destination channel and the eavesdropper channel are set to one, e.g. $\sigma_2^2 = \sigma_e^2 = 1$.

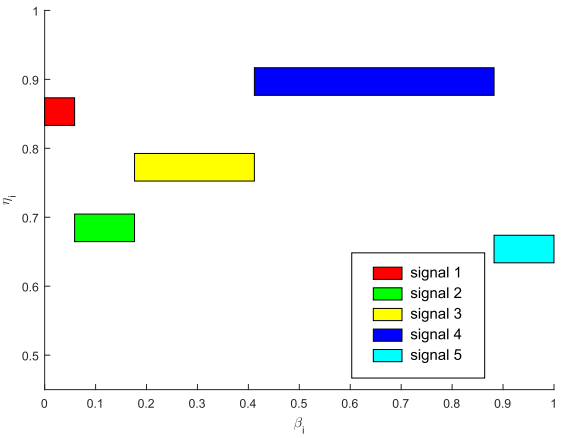

FIGURE 2. The power and time slot allocation factor of different signals when $\alpha = 0.2$ and transmission power $p_s = 40dBm$.

We first demonstrate the power and time slot allocation factors with different FH-MWFRFT order. The results are given with the order of $\alpha = 0.2$, $\alpha = 0.5$ and $\alpha = 0.8$ in Fig. 2–Fig. 4. The number of transmitted signals is 5 and

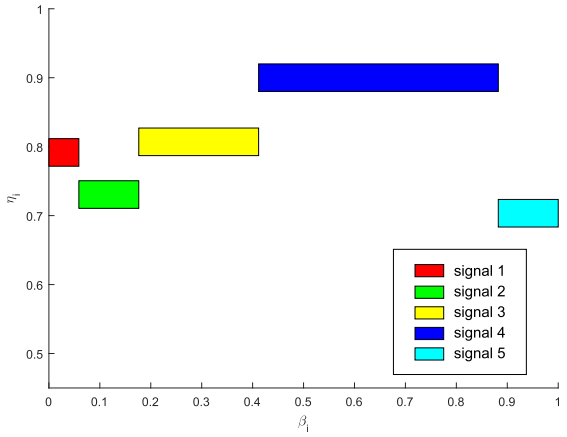

FIGURE 3. The power and time slot allocation factor of different signals when $\alpha = 0.5$ and transmission power $p_s = 40dBm$.

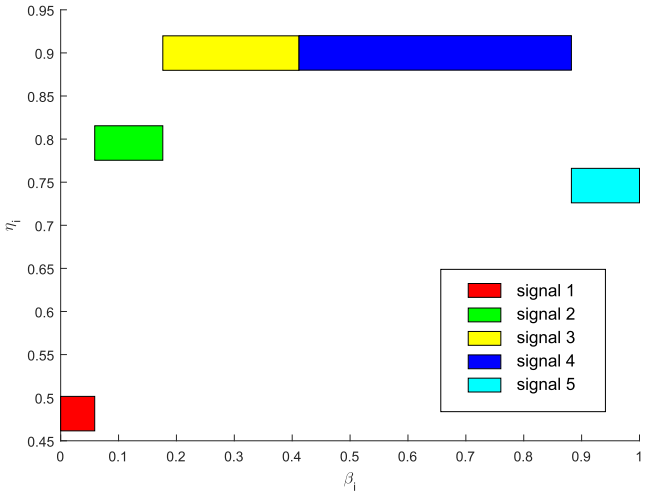

FIGURE 4. The power and time slot allocation factor of different signals when $\alpha = 0.8$ and transmission power $p_s = 40dBm$.

the length of these signals is set as 16, 32, 64, 128 and 32 respectively. The transmission power is set as $40dBm$. The number of antennas at the satellite, destination receiver and eavesdropper are set as $N_s = 2, N_2 = N_e = 1$. The fading of both the main channel and eavesdropper channel are set as average shadowing fading channel. According to these figures, the power and time slot allocation factors are affected by both the transform order and the signal length. When the transform order α is small (Fig. 2), the signal with the length of 16 requires less power for the weighted fractional artificial noise than those with the length of 32, 64. Due to the reason that when the transform order is small, the information of the signal acquired by the eavesdropper is closer to the original signal, thus the shorter signal like signal 1 would be less possible to be detected by the eavesdropper, which means it requires less power for the WFDCAN than the longer signals such as signal 2, 3 and 5. There is a little distinction between the power allocation factors for signal 2 and signal 5. That is caused by the accumulated error during solving the optimization problem. With the increasing of transform order (Fig. 3–Fig. 4), the fourier part of the information acquired by the eavesdropper is raising, hence the power allocated to the main signal is relatively going up for the signal with the length of 32 and 64. Meanwhile, the signal with the length of 128 always keeps a high ratio of power that allocated to the main signal because of the good performance of the WFDCAN when transmitting long signals. The time slot allocation is mainly affected by the proportions of the length of the signal to that of all the transmitted signals.

Then we make a comparison of the secrecy capacity between the WFDCAN with the proposed allocation method and the WFDCAN without allocation method. The number of signals and antennas and the channel condition is identical to that above. The transform order is set as $\alpha = 0.5$. We compare the secrecy capacity of these two situations with the transmission power of $20dBm$, $40dBm$ and $60dBm$ and the results are given in Fig. 5. The figure demonstrates that after power and time slot allocation, the secrecy capacity would keep almost constant when the number of transmitted signals increasing. Meanwhile, the secrecy capacity of the WFDCAN without allocation method decreases with the raising of the number of the transmitted signals. This result proves that the proposed allocation scheme has solved the problem brought by the power decreasing when the number of transmitted signals raise by allocating time slot to each signal and allocating as much power as possible to the main signal during the transmission.

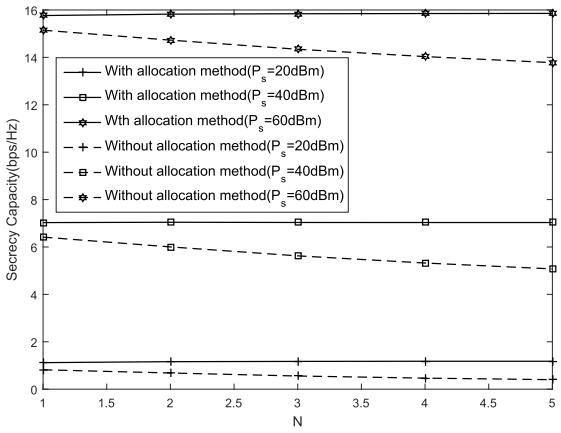

FIGURE 5. The comparison of the secrecy capacity between the WFDCAN with allocation method and the WFDCAN without allocation method with the increasing of the number of transmitted signals.

We also make a comparison among the proposed scheme, the traditional artificial noise with power allocation method proposed in [37] and method proposed in [21]. The number of antennas at the satellite is two and the transform order is 0.5. The CSI of the main channel is assumed to be imperfect. The estimation of the CSI is affected by a error with a complex gaussian distribution whose variance is set as $\tilde{\sigma}^2 = 1$. The simulation results are presented in Fig. 6. We can infer from the results that the proposed scheme can still maintain a

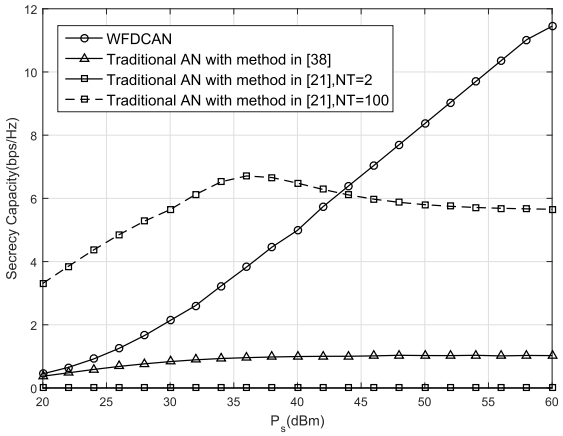

FIGURE 6. The comparison of the secrecy capacity among the proposed scheme, the traditional artificial noise with power allocation method proposed in [37] and method proposed in [21].

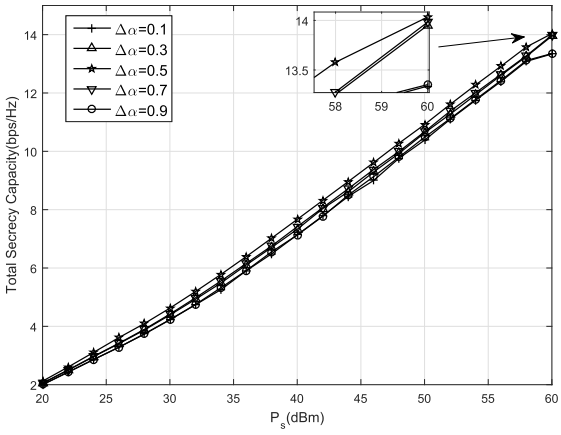

FIGURE 7. The comparison of the secrecy capacity when the difference of the transform order is 0.1, 0.3, 0.5, 0.7,0.9.

good secrecy capacity performance. Because the elimination of the artificial noise is not depended on the orthogonality between the beamforming vector and the channel gain matrix, but depended on the orthogonality between the weighted fractional fourier transform vectors generated at the satellite and the receiver. Nevertheless, the traditional artificial noise with the power allocation method proposed in [37] is affected by the estimation error of the CSI. The secrecy capacity achieved by this method would quickly reach an upper bound that is not very large with the imperfect CSI. The secrecy performance of the method proposed in [21] is also influenced by the number of antennas. When $N_s = 100$, the method proposed in [21] could benefit from the number of antennas and achieve a relatively good secrecy performance. However with the increasing of transmission power, the secrecy brought by this method would reach an upper bound. On the other hand, when the quantity of transmission antennas is small, the secrecy of the transmission can not be guaranteed.

Finally, we make a simulation with the assumption that the eavesdropper has managed to acquired some information of the transform order and have the knowledge of the multi-term WFRFT to demonstrate the secrecy performance of the FH-MWFRFT. We assume that the eavesdropper generates the MWFRFT vector with a difference in transform order as $\Delta\alpha = 0.1$, $\Delta\alpha = 0.3$, $\Delta\alpha = 0.5$, $\Delta\alpha = 0.7$ $\Delta\alpha = 0.9$. The simulation result is shown in Fig. 7. We could find from this figure that the difference between the correct order and the order at the eavesdropper would have some influences to the secrecy capacity. When the difference is 0.5, the secrecy capacity is relatively the largest, followed by the value with the difference of 0.3 and 0.7 and the one with the difference of 0.1 and 0.9. The results are caused by the periodicity of the FH-MWFRFT matrix in regard to the α. However, the influence is small, which demonstrates the superiority of the FH-MWFRFT in secrecy when the transform order has been acquired by the eavesdropper.

VI. CONCLUSION

In our work, we propose a physical layer security method of data-carrying artificial noise for satellite DF down-link transmission based on the weighted fractional fourier transform. The frequency hopping is adopted to the WFRFT to overcome its drawback of may be cracked easily when the information of transform order is known by the eavesdropper. By applying the orthogonality of the rows of the FH-MWFRFT matrix, we could transmit multiple signals together and make one of them the main signal and others the artificial noises, so as to deteriorate the SINR at the eavesdropper and secure the transmission. To deal with the problem that the secrecy capacity will decrease when the number of the transmitted signals increase with a equally allocated power. We propose a power and time slot allocation method based on the fractional programming and DC programming. These two optimization methods are embedded together to transform the original non-convex objective function to a solvable one. We present simulations and make several comparisons to demonstrate the superiority of the method in many aspects: 1)the proposed allocation method can adjust the power and time slot allocation when the parameter of the transmission is changing to maintain a good secrecy performance, 2)the allocation method overcome the drawback of the WFDCAN with equal power allocation and keep the secrecy capacity steady, 3)the proposed WFDCAN method performs well when the CSI of the main channel is imperfect and when the number of antennas at the satellite is small compared with the traditional artificial noise with the method in [21] and [37], 4)the proposed secrecy transmission scheme can keep the signals secured when the eavesdropper has the information of the transform order. The power and time slot allocation method and the WFDCAN transmission scheme proposed in this paper could be applied to many future practical scenarios such as satellite communications and the 5G communication to make the private messages safer.

REFERENCES

[1] J. Liu, Y. Shi, L. Zhao, Y. Cao, W. Sun, and N. Kato, "Joint placement of controllers and gateways in SDN-enabled 5G-satellite integrated network," *IEEE J. Sel. Area Commun.*, vol. 36, no. 2, pp. 221–232, Feb. 2018.

[2] *technical Specification Group Radio Access Network; Study on New Radio Access Technology: Radio Access Architecture and Interfaces*, document, 3GPP, Mar. 2017.

[3] *Backhaul for Rural and Remote Small Cells, 2014–2019*, document, Small Cell Forum, Mar. 2015.

[4] Y. Kawamoto, H. Nishiyama, N. Kato, and N. Kadowaki, "A traffic distribution technique to minimize packet delivery delay in multilayered satellite networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3315–3324, Sep. 2013.

[5] M. K. Arti, "A novel beamforming and combining scheme for two-way AF satellite systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1248–1256, Feb. 2017.

[6] M. R. Bhatnagar, "Performance evaluation of decode-and-forward satellite relaying," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4827–4833, Oct. 2015.

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

[8] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[9] F. Wu, C. Dong, L.-L. Yang, and W. Wang, "Secure wireless transmission based on precoding-aided spatial modulation," in *Proc. IEEE Global Commun. Conf.*, Dec. 2015, pp. 1–6.

[10] J. Tang *et al.*, "Associating MIMO beamforming with security codes to achieve unconditional communication security," *IET Commun.*, vol. 10, no. 12, pp. 1522–1531, Aug. 2016.

[11] K. An *et al.* "Secure transmission in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 3025–3037, Nov. 2016.

[12] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[13] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[14] Y. Liu, H.-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 Security*, vol. 12, no. 3, pp. 617–630, Mar. 2017.

[15] M. Ahmed and L. Bai, "Secrecy capacity of artificial noise aided secure communication in MIMO Rician channels," *IEEE Access*, vol. 6, pp. 7921–7929, 2018.

[16] A. El Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[17] Q. Li, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[18] A. D. Harper and X. Ma, "MIMO wireless secure communication using data-carrying artificial noise," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8051–8062, Dec. 2016.

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

[20] S. Wan *et al.*, "Power allocation strategy of maximizing secrecy rate for secure directional modulation networks," *IEEE Access*, to be published.

[21] S. Yun, S. Im, I.-M. Kim, and J. Ha, "On the secrecy rate and optimal power allocation for artificial noise assisted MIMOME channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3098–3113, Apr. 2018.

[22] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[23] L. Mei, "Weighted fractional Fourier transform and its application in communication systems," M.S. thesis, Harbin Inst. Technol., Harbin, China, 2010.

[24] X. Fang, X. Wu, N. Zhang, X. Sha, and X. Shen, "Safeguarding physical layer security using weighted fractional Fourier transform," in *Proc. Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[25] S. Wang, X. Da, Z. Chu, and L. Zhu, "Secure transmission for TDCS using 4-WFRFT and noise insertion," *J. Sichuan Univ.*, vol. 48, no. 3, pp. 142–147, 2016.

[26] L. Mei, Q. Zhang, X. Sha, and N. Zhang, "WFRFT precoding for narrowband interference suppression in DFT-based block transmission systems," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 1916–1919, Oct. 2013.

[27] L. Yong, "WFRFT and partial FFT-based transmisson methods under rapidly time-varying channels," M.S. thesis, Harbin Inst. Technol., Harbin, China, 2014.

[28] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[29] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

[30] S. Schaible, "Fractional programming. II, on Dinkelbach's algorithm," *Manage. Sci.*, vol. 22, no. 8, pp. 868–873, Apr. 1976.

[31] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in multi-cell OFDMA systems with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3618–3631, Oct. 2012.

[32] J. Gorski, F. Pfeuffer, and K. Klamroth, "Biconvex sets and optimization with biconvex functions: A survey and extensions," *Math. Methods Oper. Res.*, vol. 66, no. 3, pp. 373–407, Dec. 2007.

[33] P. D. Tao and H. A. L. Thi, *Recent Advances in DC Programming and DCA*. Berlin, Germany: Springer, 2014.

[34] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[35] Y. Cheng and M. Pesavento, "Joint optimization of source power allocation and distributed relay beamforming in multiuser peer-to-peer relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 2962–2973, Jun. 2012.

[36] A. Abdi, W. C. Lau, M.-S. Alouini, and M. Kaveh, "A new simple model for land mobile satellite channels: First- and second-order statistics," *IEEE Trans. Wireless Commun*, vol. 2, no. 3, pp. 519–528, May 2003.

[37] X.-Z. Xie, J.-J. Chen, and Y.-X. Fu, "Robust precoding and energy-efficient timeslot allocation for full-duplex SWIPT system," *Acta Electron. Sinica*, vol. 46, no. 5, pp. 1213–1221, 2018.

RUIYANG XU received the B.Sc. degree in automatic control engineering and the M.A.Sc. degree in information and communication engineering from Air Force Engineering University, Xi'an, China, in 2013 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the Institute of Information and Navigation. His research interests include satellite communications, covert communications, optimization, and intelligent algorithm.

XINYU DA received the B.Sc. degree from Xidian University in 1983, the M.A.Sc. degree in communication and electronic system from the Air and Missile Defense College in 1988, and the Ph.D. degree from the School of Marine Science and Technology, NPU, in 2007. He is currently the Professor with the Information and Navigation College, Air Force Engineering University. His research interests include Satellite communications, communication theory, signal processing, transform domain communication system, and cognitive radio.

HANG HU received the B.S. degree in telecommunications engineering from Xidian University, Xi'an, China, in 2010, and the M.S. and Ph.D. degrees in information and communications engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012 and 2016, respectively. He is currently a Lecturer with the Information and Navigation College, Air Force Engineering University, Xi'an, China. His current research interests include cognitive radio technology, cooperative communications, and green communications. He received the Grant of Postdoctoral Innovative Talent Program, China, in 2017.

YUAN LIANG received the B.Sc. degree in information and navigation engineering and the M.A.Sc. degree in information and communication engineering from Air Force Engineering University, Xi'an, China, in 2012 and 2015, respectively, where he is currently pursuing the Ph.D. with the Institute of Information and Navigation. His research interests include intelligent signal processing, wireless communications, secure communications, optimization, and intelligent algorithm.

LEI NI received the B.S. degree from Air and Missile Defense College in 2014 and the M.S. degree from Air Force Engineering University in 2016, where he is currently pursuing the Ph.D. degree with the Graduate School. His current research interests include energy harvesting, cognitive radio networks, physical layer security, and wireless power transfer.