sensors

MDPI

Article

Spatial Modulation and MP-WFRFT-Aided Multi-Beam Wireless Communication Scheme Based On Random Frequency Diverse Array

Jianbang Gao [1,*], Bin Qiu [2] and Jing Zhou [1]

[1] School of Electronic Engineering, Xi'an Shiyou University, Xi'an 710000, China; jzhou@xsyu.edu.cn
[2] School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China; qiubin@mail.nwpu.edu.cn
* Correspondence: 2017100143@mail.nwpu.edu.cn

Received: 22 July 2020; Accepted: 12 September 2020; Published: 16 September 2020

Abstract: A security-enhanced, spectral-efficient, and power-efficient multi-beam wireless communication scheme based on random frequency diverse array (RFDA) is proposed in this paper. (AN)-aided directional modulation (DM) schemes. Furthermore, with the aid of spatial modulation (SM) technology and cooperative legitimate users (LUs), we can transmit more information bits by the use of LU number informations than the single modulation symbols. Unlike conventional zero-forcing (ZF) beamforming for multi-beam DM, we design a FDA beamforming vector for each LU based on the minimum transmit power method. Numerical simulations show that (1) the proposed scheme is power-efficient compared to the conventional schemes, (2) the proposed scheme can transmit more information bits than the conventional schemes, and (3) the proposed scheme can ensure communication security when eavesdroppers (Eves) are proximal to LUs or even in same locations.

Keywords: physical layer security; spatial modulation; MP-WFRFT; cooperative LUs; power efficient

1. Introduction

Wireless communication has attracted increasing attention in recent years. However, wireless communication occurs in an open environment and broadcasts information to all users in free space [1,2]. Therefore, wireless communication security has become a serious problem in both civil and military fields. Traditionally, upper-layer encryptions technology has been widely used in wired communication. However, encryption systems are inherited from the traditional computer network and ignores the special physical layer characteristics of wireless communication system, such as the openness wireless channel, time-varying network topology, and resource limitation of mobile terminal [3,4]. As a result, physical layer (PHY) security was introduced to achieve the confidentiality of messages at the PHY [5]. PHY security enables wireless communications to exploit the properties of physical layer to scramble information content that could be potentially intercepted by eavesdroppers, while simultaneously delivering it to its desired receivers. DM, as a keyless physical-layer security transmitting technique with great potentials, has attracted a great deal of attention over the past decade. It uses antenna arrays to transmit a signal only along the desired directions while distorting signal constellations in all other directions [6,7].

Traditionally, DM technology has been mainly implemented based on phased arrays (PA) in the past decade [8–11]. However, the previous communication schemes based on PA can no longer guarantee secure transmission when eavesdroppers locate in the desired direction of LU due to the transmit beampattern being only angle-focusing. Accordingly, it is necessary to investigate other schemes that can prevent eavesdroppers in the desired direction from intercepting messages. Therefore,

we depart from PA and apply a frequency diverse array (FDA) into DM implementations because of its extra range dimension dependence, rather than being dependent on only the angle used [12–17].

FDA delivers a new opportunity for secure wireless communications. However, the beampattern of FDA is still angle-range coupling, which means that confidential messages are accessible to illegitimate receivers that are located at some angle-range pair curves. Several works have focused on frequency offsets to address the coupling problem of FDA [18]. To this end, in [19,20], the authors proposed a logarithmic frequency increments scheme. Furthermore, with random frequency increments between each element, the author of [21] proposed a new FDA structure, named random FDA, to indicate targets' direction and range without coupling. Besides the radio frequency fronted technology, adding AN at the baseband is another effective technology used to deteriorate the received messages of Eves that has been employed in DM systems [22,23]. An FDA DM scheme with AN [24,25] has been proposed to further improve secrecy performance, and a robust synthesis scheme with AN was proposed in [26] for a single user scenario.

In summary, the current studies cannot deal with the PHY security problem of multiple receivers obtaining different messages simultaneously, which needs to be addressed in practical applications. The traditional DM schemes with AN need to allocate power to the AN, which will lower the power efficiency of total transmitting power. Furthermore, in practical cases, the Eves would be located as close to LU as possible (even in the same locations as the LUs) to eavesdrop on the confidential signal, and the previous studies have shown that it is difficult to ensure the security of the independent confidential message in this case. In addition, the received power at each LU is not accurately controlled according to the prescribed power.

In order to address the limitations of the previous works and further enhance the PHY security, we proposed a spatial modulation (SM) and multiple parameter weighted-type fractional Fourier transform (WFRFT)-aided scheme based on a random frequency diverse array (RFDA).

WFRFT, as a new transformation domain signal processing method based on Fourier transform [27], is gradually being applied to the wireless communication systems. WFRFT is actually the process of rotating the signal in the time-frequency plane to realize the time-frequency redistribution of signal power, and only when the users rotate the signal in same angle, but the opposite direction can the signal power be concentrated. Therefore, due to its power redistribution on the time-frequency plane, WFRFT technology can be regarded as a cryptographic method to further improve secrecy performance [28–31]. Furthermore, in [32], a synthesis scheme combining WFRFT and FDA DM was investigated to achieve power efficiency multi-beam secure communication. The contributions to physical layer security were promising. Apart from the above-mentioned WFRFT schemes based on a single parameter, the multiparameter WFRFT synthesis approaches have also been investigated intensively [33,34]. The MP-WFRFT system has a good parameter resistance, allowing it to detect in the condition of the eavesdroppers with a known signal transformation mode; in particular, this method can be combined with the existing DM technology, which can further improve the capacity for anti-interception and anti-detection based on the original system confidentiality.

SM, as an emerging information modulation technology, has gradually been introduced into wireless communication in recent years due to its high data rate and spectral efficiency. The basic idea of SM is to use the transmit antenna number as an additional information bearing unit to transmit more information bits than the single modulation symbols. However, in this paper, unlike previous works which applied SM to the multiple-input multiple-output (MIMO) system [35–38], the authors use SM technology based on FDA with cooperative LUs in order to avoid high interchannel interference at receivers and complicated estimate algorithms (e.g., maximum likelihood [35] and MRRC [38]) are required.

On the basis of the previous work, we propose a spectrally efficient and power-efficient multi-beam security communication scheme with the joint use of multiple techniques including MP-WFRFT, SM, and FDA–DM. Our main contributions can be summarized as follows.

(1) The proposed scheme combining MP-WFRFT realizes the embedding process of "AN" from the modulation level of digital baseband signal. Therefore, the proposed scheme based on MP-WFREFT avoids the power resource waste compared with traditional AN added scheme.

(2) In this paper, we apply SM technology into the FDA system with cooperative LUs, which can transmit additional information bits by using LUs number information compared to single modulation symbols to improve the capacity of communication system. Furthermore, the proposed scheme can ensure communication security when Eves are proximal to LUs or even in same locations.

(3) Unlike conventional beamforming method for multi-beam DM, we design the FDA beamforming matrix based on the minimum transmission messages power rule, which also can accurately control the received power of LUs.

The rest of this paper is organized as follows. Section 2 provides a review of DM PHY, MP-WFRFT and SM. Then, in Section 3, we propose the SM- and MP-WFRFT-aided scheme based on FDA. The performance is deduced in Section 4 and is numerically evaluated in Section 5. Finally, Section 6 draws conclusions.

2. Related Works

2.1. DM PHY

DM is a secure transmission technology without encryption for physical layer security. It uses antenna arrays to transmit confidential message only along desired directions while distorting signal constellations in all other directions. DM has received great attention in recent years, and it can be classified as PA-DM and FDA-DM. In this paper, we mainly research wireless communication scheme based on DM physical layer security technology.

PA-DM have been employed in many applications; however, these works based on PA-DM schemes can only achieve angle-dependent wireless physical layer security transmission [8–10]; Random subcarrier selection (RSCS) based on orthogonal frequency division multiplexing (OFDM) [11] only focuses on the single LU. Unless otherwise stated, other schemes are based on FDA-DM. The AN-aided DM schemes [14,22–26] can achieve the multi-beam secure transmission, regardless of the power efficiency. Moreover, those methods cannot achieve the neighbor security because of constraint on beamwidth. Furthermore, in [32], a synthesis scheme combined WFRFT and FDA DM was investigated to achieve power efficiency and the neighbor security. The contributions to physical layer security are solid. However, WFRFT DM schemes cannot guarantee the security of confidential messages when the WFRFT parameters are leaked to Eves.

On the basis of the previous work, we propose a synthesis multi-beam security communication scheme with the joint use of multiple techniques including MP-WFRFT, SM, and FDA-DM. Moreover, there are four potential practical applications for the proposed schemes in free space.

The first is the secure transmissions of satellite communications (SatCom) from ground station to satellites or from one satellite to others. The second is the secure transmissions of unmanned aerial vehicles (UAV) from the ground controller to UAVs or from one UAV to others. The third is the secure 5G millimeter wave (mmWave) communication. We can ignore the very few multi-path components in mmWave transmission, and the far-field and LoS assumptions can hold simultaneously due to the tiny array size, usually in magnitude of millimeters. The fourth is application in the Internet of Things (IoT). IoT is an indispensable part of our lives. Traditional security mainly relies on key encryption mechanism, but for the IoT with large number of nodes and heterogeneous networks, it is difficult to extract, distribute, and manage the keys. This has led us to develop new security solutions for IoT applications. Our proposed synthesis scheme based on FDA-DM can achieve security of IoT in physical layer, and it can solve the problem of spectrum scarcity in the IoT due to the SM technology.

2.2. MP-WFRFT

MP-WFRFT, known as a variation of the Fourier transform, is essentially the weighted sum of four basis functions. MP-WFRFT can be regarded as the process of rotating the signal in the time–frequency plane to realize the time–frequency redistribution of signal power. Only when the users rotate the signal in the same angle but the opposite direction can the signal power be concentrated. The representation of the 4-WFRFT of discrete sequences was proposed in [27] and has been widely employed in communication systems. Therefore, the classical 4-MP-WFRFT approach is adopted in this paper. For an arbitrary complex sequence $\mathbf{x} = [x_1, x_2, \cdots, x_Q]^{\mathrm{T}}$, the corresponding MP-WFRFT can be defined as

$$\mathfrak{F}_{\alpha}^{(\mathbf{m},\mathbf{c})}(\mathbf{x}) = \omega_0\mathbf{x}+\omega_1\mathcal{F}(\mathbf{x})+\omega_2\mathcal{F}^2(\mathbf{x})+\omega_3\mathcal{F}^3(\mathbf{x}), \tag{1}$$

where $\mathfrak{F}$ denotes the transform operator of MP-WFRFT; $\mathcal{F}$, $\mathcal{F}^2$, and $\mathcal{F}^3$ denote 1–3 times discrete Fourier transform (DFT) of sequence $\mathbf{x}$, respectively; α is the MP-WFRFT modulation order; $\mathbf{m} = [m_0, m_1, m_2, m_3]^{\mathrm{T}}$ and $\mathbf{c} = [c_0, c_1, c_2, c_3]^{\mathrm{T}}$ are integer vectors; and the weighting coefficient $\omega_l (l = 0, 1, 2, 3)$ is defined as

$$\omega_l = \frac{1}{4}\sum_{k=0}^{3}\exp\{\frac{2\pi j}{4}[\alpha(4m_k+1)(4c_k+k) - lk]\}, \tag{2}$$

Based on the principles of transform operator $\mathcal{F}$, $\mathcal{F}^2(\mathbf{x}) = \mathbf{P}\mathbf{x}$, $\mathcal{F}^3(\mathbf{x}) = \mathbf{P}\mathcal{F}(\mathbf{x})$, where $\mathbf{P}$ is the $Q \times Q$ reverse matrix. Therefore, (2) can be expressed as

$$\mathfrak{F}_{\alpha}^{(\mathbf{m},\mathbf{c})}(\mathbf{x}) = \omega_0\mathbf{x}+\omega_1\mathcal{F}(\mathbf{x})+\omega_2\mathbf{P}\mathbf{x}+\omega_3\mathbf{P}\mathcal{F}(\mathbf{x}), \tag{3}$$

Furthermore, MP-WFRFT satisfies additive property, which can be expressed as

$$\mathfrak{F}_{\alpha+\beta}^{(\mathbf{m},\mathbf{c})}(\mathbf{x}) = \mathfrak{F}_{\alpha}^{(\mathbf{m},\mathbf{c})}[\mathfrak{F}_{\beta}^{(\mathbf{m},\mathbf{c})}(\mathbf{x})], \tag{4}$$

where $\alpha, \beta \in \mathbb{R}$ are real numbers.

The implementation of the MP-WFRFT operation is demonstrated in Figure 1. It is obvious that the MP-WFRFT can be quickly realized by means of an inversion module and DFT module. Furthermore, from (4), the original sequence for 4-MP-WFRFT can be easily recovered only under the premise that the WFRFT parameter α is substituted with $-\alpha$, i.e., $\mathbf{x} = \mathfrak{F}_{-\alpha}^{(\mathbf{m},\mathbf{c})}[\mathfrak{F}_{\alpha}^{(\mathbf{m},\mathbf{c})}(\mathbf{x})]$. Therefore, the MP-WFRFT technique provides encryption security with parameters $(\alpha, \mathbf{m}, \mathbf{c})$. LUs can decode confidential messages by using perfect MP-WFRFT parameters, and Eves only receive a distorted signal that is equivalent to noise.

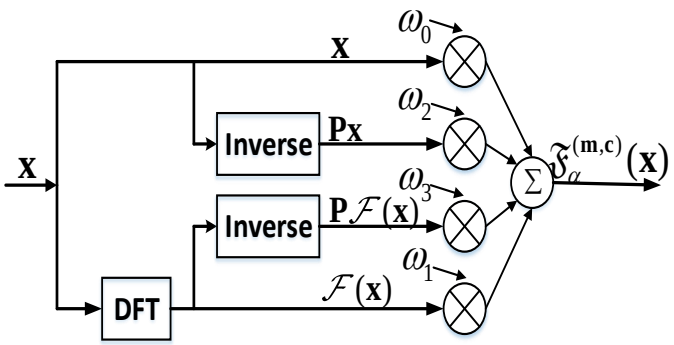


Figure 1. The implementation of the MP-WFRFT.

2.3. SM Based On FDA

SM, as an emerging information modulation technique, has gradually been used in wireless communication in recent years. The basic idea of SM is to exploit spatial location information to transmit messages. Traditional SM is to map block of upcoming information based on transmit antenna number carrying unit and constellation diagram carrying unit (e.g., M-PSK). However, in this paper, we research wireless communication based on FDA with cooperative LUs. Therefore, unlike the traditional SM technique, we apply SM into FDA by directly using LUs number information as a carrying unit to transmit more information bits. At the receiving end, one or some LUs will be active and receive messages. The other LUs are inactive and receive zero power. In our scheme, only if we correctly estimate the LUs number informations and the received symbols will the block of information bits retrieved by the cooperative LUs. We achieve security communication in the case Eves are proximal to LUs or even in same locations.

In general, our proposed scheme maps the block of information bits, which is determined by the number of LUs and digital modulation. The size of each block for a system that use M-PSK or M-QAM constellation diagram and K LUs can be calculated as

$$B = \log_2(K) + Q\log_2(M), \tag{5}$$

where the first term $\log_2(K)$ is the number of information bits carried by LUs number. Q is the number of active LUs, and the second term $Q\log_2(M)$ is the number of information bits carried by symbols of constellation diagram, which are received by Q active LUs, respectively. For example, we set the BPSK constellation diagram ($M = 2$), the number of LUs is $K = 4$, and the number of active is $Q = 3$, which maps five message bits as a block to be transmitted at one time, as shown in Table 1.

Table 1. SM map.

Bits Block	LUs Numbers	$\mathbf{u}(t)$	Bits Block	LUs Numbers	$\mathbf{u}(t)$
00000	1,2,3	$[-1,-1,-1,0]$	10000	1,3,4	$[-1,0,-1,-1]$
00001	1,2,3	$[-1,-1,+1,0]$	10001	1,3,4	$[-1,0,+1,-1]$
00010	1,2,3	$[-1,+1,-1,0]$	10010	1,3,4	$[-1,0,-1,+1]$
00011	1,2,3	$[+1,-1,-1,0]$	10011	1,3,4	$[+1,0,-1,-1]$
00100	1,2,3	$[-1,+1,+1,0]$	10100	1,3,4	$[-1,0,+1,+1]$
00101	1,2,3	$[+1,-1,+1,0]$	10101	1,3,4	$[+1,0,+1,-1]$
00110	1,2,3	$[+1,+1,-1,0]$	10110	1,3,4	$[+1,0,-1,+1]$
00111	1,2,3	$[+1,+1,+1,0]$	10111	1,3,4	$[+1,0,+1,+1]$
01000	1,2,4	$[-1,-1,0,-1]$	11000	2,3,4	$[0,-1,-1,-1]$
01001	1,2,4	$[-1,-1,0,+1]$	11001	2,3,4	$[0,-1,-1,+1]$
01010	1,2,4	$[-1,+1,0,-1]$	11010	2,3,4	$[0,-1,+1,-1]$
01011	1,2,4	$[+1,-1,0,-1]$	11011	2,3,4	$[0,+1,-1,-1]$
01100	1,2,4	$[-1,+1,0,+1]$	11100	2,3,4	$[0,-1,+1,+1]$
01101	1,2,4	$[+1,-1,0,+1]$	11101	2,3,4	$[0,+1,-1,+1]$
01110	1,2,4	$[+1,+1,0,-1]$	11110	2,3,4	$[0,+1,+1,-1]$
01111	1,2,4	$[+1,+1,0,+1]$	11111	2,3,4	$[0,+1,+1,+1]$

3. SM and MP-WFRFT Aided Scheme Based On FDA

3.1. The Architecture of System with Cooperative LUs

The traditional PA-DM schemes and even the AN-aided PA-DM synthesis schemes cannot achieve range dependence, and so these schemes cannot prevent eavesdroppers from intercepting messages and recognize private users in same direction. Therefore, we depart from PA and apply FDA into our DM implementations because of its extra range dimension dependence rather than simply angle dependence. In this paper, the line-of-sight (LoS) channel, far-field communication, and Gaussian wiretap channel are considered. As shown in Figure 2, the system consists of a legitimate transmit

station, K LUs whose information can be shared with each other, and J passive Eves whose locations are unavailable to transmitter station.

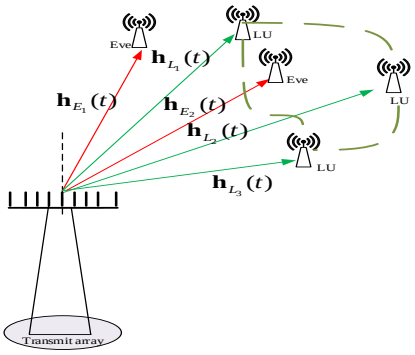


Figure 2. System model.

A uniform N elements linear array with a spacing d is utilized for the transmitter. The transmitting frequency at the $n-th$ (n = 1, 2, ..., N) antenna is designed as $f_n = f_c + \Delta f_n$, where f_c is the carrier wave frequency and Δf_n is the frequency increment. Here, we propose RFDA whose beam pattern is angle-range independent without coupling. Therefore, Δf_n can be replaced as $\Delta f_n = \lambda_n \Delta f$, where Δf refers to a fixed frequency increment, and λ_n represents a random variable.

For an arbitrary receiver at (r, θ), the normalized steering vector is denoted by

$$\mathbf{h}(\theta, r, t, \mathbf{f}) = \frac{\rho(r)}{\sqrt{N}} \left[e^{-j2\pi f_1 \left(t - \frac{r}{c}\right)}, e^{-j2\pi f_2 \left(t - \frac{r - d\sin\theta}{c}\right)}, \ldots, e^{-j2\pi f_N \left(t - \frac{r-(N-1)d\sin\theta}{c}\right)} \right]^T \tag{6}$$

where c denotes light speed, $\rho(r)$ refers to the path loss factor due to the free space propagation.

The location of LU K is (r_{l_k}, θ_{l_k}), and for simplicity $\mathbf{h}(t)_{L_k} \triangleq \mathbf{h}_{L_k}(r, \theta, t, \mathbf{f})$ is the normalized steering vector of LU K. Furthermore, we use the steering matrix $\mathbf{H}_L(t)$ to denote steering vectors of all LUs, i.e.,

$$\mathbf{H}_L(t) \triangleq [\mathbf{h}_{L_1}(t), \mathbf{h}_{L_2}(t), \cdots, \mathbf{h}_{L_k}(t), \cdots, \mathbf{h}_{L_K}(t)], \tag{7}$$

where $\mathbf{h}_{L_k}(t)$ is the instantaneous normalized steering vector of k-th LU at (r_{L_k}, θ_{L_k}).

3.2. The Radiating Signal Processed by SM and MP-WFRFT

The architecture of transmit station is shown in Figure 3. In this paper, we innovatively apply two key modulation techniques into FDA-DM. Before transmitting the confidential signal to LUs, we first use the SM module for the confidential signal stream $x(t)$ and $x(t)$ is normalized, i.e., $\mathbb{E}[|x(t)|^2] = 1$. Then, we divide the confidential information bit stream into blocks. As mentioned in previous section, each block contains $\log_2(KM^Q)$ bits. The SM is operated to the confidential information block, which yields the transmitting symbol vector

$$\mathbf{u}(t) = \mathcal{U}[x(t)] = [u_1(t), u_2(t), \ldots, u_K(t)]^T, \tag{8}$$

where $u_k(t)$ is the transmitting symbol for the k-th LU, and $\mathcal{U}[\cdot]$ is the SM mapping.

Second, the transmitting symbol vector $\mathbf{u}(t)$ is performed by MP-WFRFT with parameters $[\alpha_s, \mathbf{m}_s, \mathbf{c}_s]^T$, which can be expressed as

$$\mathbf{v} = \mathfrak{F}_{\alpha_s}^{(\mathbf{m}_s, \mathbf{c}_s)}(\mathbf{u}) = w_0\mathbf{u} + w_1\mathcal{F}(\mathbf{u}) + w_2\mathbf{P}\mathbf{u} + w_3\mathbf{P}\mathcal{F}(\mathbf{u}), \tag{9}$$

The vector $\mathbf{u}(t)$ is rotated in the time-frequency plane to realize the time-frequency redistribution of signal power. Therefore, only when the users rotates the signal in same angle but the opposite direction can the signal power be concentrated.

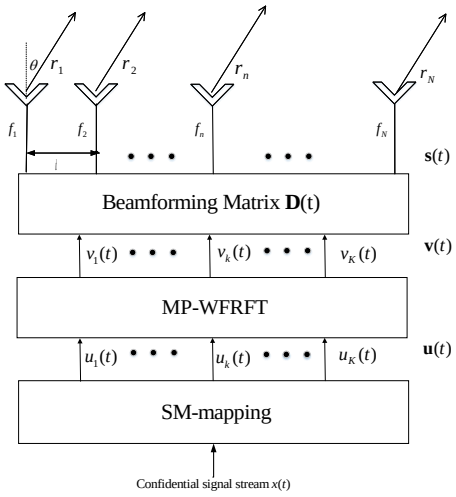


Figure 3. The architecture of the transmit station.

Before radiating, we design the beamforming matrix $\mathbf{D}$ to further process the symbol vector $\mathbf{v}$ to match all transmit antennas. The beamforming matrix $\mathbf{D}$ is given by

$$\mathbf{D} = [\mathbf{d}_1(t,\mathbf{f}), \mathbf{d}_2(t,\mathbf{f}), \ldots, \mathbf{d}_K(t,\mathbf{f})], \tag{10}$$

where $\mathbf{d}_k(t,\mathbf{f}) = [d_{k,1}(t,\mathbf{f}), d_{k,2}(t,\mathbf{f}), \ldots, d_{k,N}(t,\mathbf{f})]^T$, for $k = 1,2\ldots,K$, is the beamforming vector to process symbol $v_k(t)$ that is transmitted to k-th LU.

In order to obtain the beamforming matrix $\mathbf{D}$, the locations of LUs are assumed to be previously known by transmit station, i.e., the steering matrix $\mathbf{H}_L(t)$ is known in advance. Next, we design the beamforming matrix $\mathbf{D}$ based on the rules that (1) the intended LU effectively receives the corresponding confidential messages, while the undesired LUs cannot obtain the messages, and (2) the transmit power is minimum, while satisfying communication performance requirements of each LU. Therefore, the beamforming matrix $\mathbf{D}$ is designed by

$$\mathbf{H}_L^H(t)\mathbf{D} = \mathbf{A}\mathbf{I}_\mathbf{K}, \tag{11}$$

where $\mathbf{A} = \mathrm{diag}[\boldsymbol{\zeta}]$, in which $\boldsymbol{\zeta} \triangleq [\sqrt{\zeta_1}, \sqrt{\zeta_2}, \ldots, \sqrt{\zeta_k}, \ldots, \sqrt{\zeta_K}]$, and ζ_k is the minimum desired power, for $k = 1,2,\cdots,K$.

According to the pseudo-inverse concept, we obtain $\mathbf{D}$ as

$$\mathbf{D} = \mathbf{H}_L(t)(\mathbf{A}^{-1})^H[\mathbf{A}^{-1}\mathbf{H}_L^H(t)\mathbf{H}_L(t)(\mathbf{A}^{-1})^H]^{-1}, \tag{12}$$

After processed by the beamforming matrix, the radiating signal for the N antennas is given by

$$\mathbf{s} = \mathbf{D}\mathbf{v} = \mathbf{D}\mathfrak{F}_{\mathbf{a_s}}^{(\mathbf{m_s},\mathbf{c_s})}[\mathcal{U}(\mathbf{x})], \tag{13}$$

3.3. The Received Signal of LUs and Eves

The receiving structure with cooperative LUs is shown in Figure 4. Because of cooperative LUs, we combine all LUs received signals together as an LUs received vector, i.e., $\mathbf{y}_L(t) = [y_{L_1}(t), y_{L_2}(t), \ldots, y_{L_K}(t)]^T$. In this paper, assuming that (1) the synchronization of time and frequency

is perfect in the ideal scenario, and (2) the MP-WFRFT parameters are securely shared between the transmit station and LUs. As shown in Figure 4, the received symbol is first operated by inverse MP-WFRFT with $(\alpha_l, \mathbf{m}_l, \mathbf{c}_l)$, which yields

$$\mathbf{y}_L(t) = \mathfrak{F}_{\alpha_l}^{(\mathbf{m}_l,\mathbf{c}_l)}(\mathbf{y}_L^{'}(t)) = \mathfrak{F}_{\alpha_l}^{(\mathbf{m}_l,\mathbf{c}_l)}(\mathbf{H}_L^H(t)\mathbf{s}(t)) + \mathfrak{F}_{\alpha_l}^{(\mathbf{m}_l,\mathbf{c}_l)}(\mathbf{n}_L(t)) \tag{14}$$

where the shared parameters $(\alpha_l, \mathbf{m}_l, \mathbf{c}_l) = (-\alpha_s, \mathbf{m}_s, \mathbf{c}_s)$. Based on (9), (11), and (13), (14) can be further simplified as

$$\begin{aligned}\mathbf{y}_L(t) &= \mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{A}\mathbf{v}(t)) + \mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{n}_L(t)) = \mathbf{A}\mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}\mathfrak{F}_{\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{u}(t)) + \mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{n}_s)}(\mathbf{n}_L(t)) \\ &= \mathbf{A}\mathbf{u}(t) + \mathbf{n}_L^{'}(t)\end{aligned} \tag{15}$$

where $\mathbf{n}_L(t) = [n_{L_1}(t), n_{L_2}(t), \ldots, n_{L_k}(t), \ldots, n_{L_K}(t)]^T$ is the AWGN vector with each element having zero mean and variance $\sigma_{L_k}^2$, i.e., $\mathbf{n}_L(t) \sim \mathcal{CN}(\mathbf{0}_{K\times 1}, \sigma_L^2\mathbf{I}_K)$. $\mathbf{n}_L^{'}(t) = [n_{L_1}^{'}(t), n_{L_2}^{'}(t), \ldots, n_{L_k}^{'}(t), \ldots, n_{L_K}^{'}(t)]^T$ is the AWGN vector after MP-WFRFT, which remains the same distribution characteristics, i.e., $\mathbf{n}_L^{'}(t) \sim \mathcal{CN}(\mathbf{0}_{K\times 1}, \sigma_L^2\mathbf{I}_K)$. Thereinto, the received symbol of k-th LU is given by

$$\begin{aligned}y_{L_k}(t) &= \mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{h}_{L_k}^H(t)\mathbf{s}(t)) + n_{L_k}^{'}(t) = \mathbf{h}_{L_k}^H(t)\mathbf{d}_k(t)u_k(t) + \mathbf{h}_{L_k}^H(t)\sum_{i=1,i\neq k}^{K}\mathbf{d}_i(t)u_i + n_{L_k}^{'}(t) \\ &= \sqrt{\zeta_k}u_k(t) + n_{L_k}^{'}(t)\end{aligned} \tag{16}$$

From (15) and (16), it can be seen that each LU can effectively receive the corresponding transmitting symbol under the control of desired received power, and the transmitting symbol vector $\mathbf{u}(t)$ is recovered via inverse MP-WFRFT with cooperative LUs. Then, after the correct reception and inverse MP-WFRFT of all LUs, the confidential signal stream x(t) is obtained by demapping the transmitting symbol vector $\mathbf{u}(t)$.

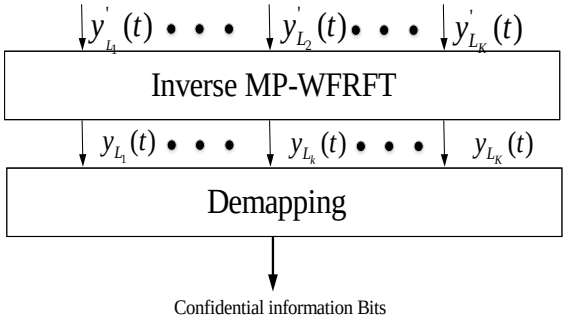


Figure 4. The receiving structure with cooperative legitimate users (LUs).

Next, we assume there are J passive Eves located in different positions intercepting the confidential information. We define (r_{e_j}, θ_{e_j}) as the coordinates of Eve j and use the steering matrix $\mathbf{H}_E(t)$ to denote steering vectors of all Eves, i.e.,

$$\mathbf{H}_E(t) \triangleq [\mathbf{h}_{E_1}(t), \mathbf{h}_{E_2}(t), \cdots, \mathbf{h}_{E_j}(t), \cdots, \mathbf{h}_{E_J}(t)], \tag{17}$$

where $\mathbf{h}_{E_j}(t)$ is the instantaneous normalized steering vector of j-th Eve. Furthermore, we consider a worse case in which Eves in different positions can cooperate with each other. Similarly, the received message of Eves is given by

$$\mathbf{y}_E(t) = \mathbf{H}_E^H(t)\mathbf{D}(t)\mathbf{v}(t) + \mathbf{n}_E(t) = \underbrace{\mathbf{H}_E^H(t)\mathbf{D}(t)w_0\mathbf{u}(t)}_{\text{Scrambled signal}} + \underbrace{\mathbf{H}_E^H(t)\mathbf{D}(t)\mathbf{b}}_{\text{Equivalant AN}} + \underbrace{\mathbf{n}_E(t)}_{\text{AWAG}} \tag{18}$$

where $\mathbf{b} = w_1\mathcal{F}(\mathbf{u}) + w_2\mathbf{P}\mathbf{u} + w_3\mathbf{P}\mathcal{F}(\mathbf{u}) = [b_1(t), b_2(t), \ldots, b_K(t)]^T$, and $\mathbf{n}_E(t)$ is the AWGN vector with each element having zero mean and variance $\sigma_{E_j}^2$, i.e., $\mathbf{n}_E(t) \sim \mathcal{CN}(\mathbf{0}_{J\times 1}, \sigma_E^2\mathbf{I}_J)$. Specifically, the received signal of j-th Eve intercepting k-th LU's information is given by

$$\begin{aligned} y_{E_{j,k}} &= \mathbf{h}_{E_k}^H(t)\mathbf{d}_k(t)\mathbf{v}(t) + n_{E_k}(t) \\ &= \underbrace{\mathbf{h}_{E_k}^H(t)\mathbf{d}_k(t)w_0u_k(t)}_{\text{Scrambled signal}} + \underbrace{\mathbf{h}_{E_k}^H(t)\sum_{i=1,i\neq k}^{K}\mathbf{d}_i(t)w_0u_i}_{\text{Interference from others}} + \underbrace{\mathbf{h}_{E_k}^H(t)\sum_{i=1}^{K}\mathbf{d}_i(t)b_i}_{\text{Equivalant AN}} + \underbrace{n_{E_k}(t)}_{\text{AWAG}} \end{aligned}$$

according to the first part of (18), the amplitude and phase of the received symbol is distorted by MP-WFRFT operations w_0 and the item $\mathbf{H}_E^H(t)\mathbf{D}(t) \notin \mathbb{R}$. The second part of (18) mainly shows interference from other messages, and the third part is the equivalent AN as the process of rotating the signal in the time-frequency plane due to MP-WFRFT. The last part is AWGN. Our proposed scheme does not add noise into the baseband signal, but the application of MP-WFRFT in our proposed method also can achieve an equivalent noise effect on Eves, which means it uses less power compared to conventional AN-DM schemes.

On the other hand, MP-WFRFT technology is dependent on the assumption that the MP-WFRFT parameters are unknown for Eves. Once the MP-WFRFT parameters are leaked to Eves, Eves will demodulate their received signals via inverse MP-WFRFT operation. However, in this paper, we use another SM technique based on FDA with cooperative LUs. After the use of the SM and MP-WFRFT aided multi-beam FDA scheme, it is hard for Eves to wiretap the confidential messages. The Eves can correctly recover the confidential messages, only when estimates of LUs number information, the MP-WFRFT parameters and the corresponding symbols are all correct. Furthermore, even if one or some (but not all) of the Eves' locations are same as one or some LUs' locations and MP-WFRFT parameters are leaked to all Eves, our proposed scheme can also ensure the security wireless communication due to the use of SM technique with cooperative LUs. Therefore, our proposed method is able to degrade Eves' reception and improve transmission security. Furthermore, our proposed method can achieve power efficient due to MP-WFRFT technology and information bits efficient by use of LUs number information as another information carrying unit in addition to constellation diagram.

4. Performance Analysis

With the basic knowledge of the SM and MP-WFRFT aided RFDA-DM scheme, we next analyze the secrecy performance of the system through the symbol error rate (SER) and bit error rate (BER), which are important metrics to measure the performance of wireless communication systems. Moreover, we analyze the anti-interception performance and provide comparisons with different DM schemes.

4.1. Symbol Error Rate

The confidential messages can be recovered only when estimates of MP-WFRFT parameters, the number information of LUs, and the corresponding modulation symbols are all correct. Here, we consider that the MP-WFRFT parameters are securely shared between transmitter station and LUs. Therefore, in order to calculate the overall SER P_s, we should consider the probability of error P_a for the estimates of number information and the SER P_m of corresponding modulation symbols. The overall SER P_s can be calculated as

$$P_s = 1 - (1 - P_a)(1 - P_m). \tag{19}$$

First, the P_m of corresponding modulation symbols is calculated. Only BPSK modulation, i.e., $M = 2$, is considered throughout this paper. Moreover, the number of active LU is $Q = 2$. The theoretical SER P_m over AWGN channel can be obtained by

$$P_m = 1 - (1 - Q(\sqrt{r_k}))^2 = 2Q(\sqrt{r_k}) - Q^2(\sqrt{r_k}), \tag{20}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{x^2}{2})dx$ is the complementary error function. r_k is the signal to interference-plus-noise ratio (SINR). According to Equation (16), we can calculate the r_k of LU k as

$$r_k = \frac{\zeta_k}{\sigma_L^2}. \tag{21}$$

According to the Equations (10), (11), and (12), the total transmit power P_s can be calculated as

$$P_s = \sum_{i=1}^{K} \|\mathbf{d}_k(t, \mathbf{f})\|_2^2. \tag{22}$$

By contrast, with the conventional AN-DM shceme, we need allocate power to AN to suppress the signal received by Eve. Therefore, the transmit power of confidential message can be expressed as $P_m = \beta^2 P_s$, and the SINR r_k of LU k can be obtained by

$$r_k^{AN} = \frac{\beta^2 \zeta_k}{\sigma_L^2} = \beta^2 r_k. \tag{23}$$

where β is the power splitting coefficient for confidential messages.

According to the Equation (19), we can calculate the r_k of j-th Eve intercepting k-th LU's information as

$$r_k = \frac{\left|\mathbf{h}_{E_j}^H(t)\mathbf{d}_k(t)\right|^2}{\sum\limits_{i=1, i\neq k}^{K} \left|\mathbf{h}_{E_j}^H(t)\mathbf{d}_i(t)w_0\right|^2 + \sum\limits_{i=1}^{K} \left|\mathbf{h}_{E_j}^H(t)\mathbf{d}_i(t)b_i\right|^2 + \sigma_E^2}.$$

Next, the probability error P_a at LUs and Eves is calculated, respectively. Here, we consider the probability error P_a for the LUs. In this paper, we assume that the LUs know the SM mapping in advance and that Eves cannot wiretap any SM information. Meanwhile, each independent LU effectively receives the confidential signal, which is verified in the next subsection. Therefore, we consider a reasonable approximation $P_a \approx 0$ at LUs. Then, we calculate P_a at Eves. Due to the arbitrary locations, Eves cannot wiretap any number information. Therefore, P_a at Eves can be obtained by

$$P_a = 1 - \frac{1}{2^K - 1}. \tag{24}$$

4.2. Anti-Interception Performance

In this subsection, the anti-interception performance of the proposed MP-WFRFT- and SM-aided DM scheme is investigated. We assume the LUs know the SM mapping in advance and Eves cannot wiretap any number information. However, before performing the proposed scheme, we also need to exchange the MP-WFRFT parameters between the transmitter station and the LUs through a secure channel. In a practical application scenario, the Eve may know the MP-WFRFT modulation and intercept them with imperfect parameters. Therefore, it is necessary to analyze the effect of the leakage

of MP-WFRFT parameters on the secrecy performance of our proposed scheme. Here, the actual MP-WFRFT parameters can be expressed as

$$\begin{bmatrix} \hat{\alpha} \\ \hat{\mathbf{m}} \\ \hat{\mathbf{c}} \end{bmatrix} = \begin{bmatrix} -\alpha_s \\ \mathbf{m}_s \\ \mathbf{c}_s \end{bmatrix} + \begin{bmatrix} \Delta\alpha \\ \Delta\mathbf{m} \\ \Delta\mathbf{c} \end{bmatrix} \tag{25}$$

where $\Delta\alpha, \Delta\mathbf{m} = [\Delta m_1, \Delta m_2, \Delta m_3, \Delta m_4]^T$, and $\Delta\mathbf{c} = [\Delta c_1, \Delta c_2, \Delta c_3, \Delta c_4]^T$ are the mismatched errors. The detailed simulations and analysis are given in Section 5 for investigating the impact of these nine MP-WFRFT mismatched parameters on secrecy performance.

4.3. Discussion

In this section, we present a comparison with some previous works in Table 2, which fully compares different schemes from different aspects of power efficient (PE), neighbor security (the location of Eve is close to or the same as that of LU, NS), control of received power (CR), range-angle security (RA), and spectral efficiency (SE).

From Table 2, we generalize the advantages of our proposed scheme as follows.

Table 2. Comparisons for different schemes.

ITEM	PA-DM	AN-DM	WFRFT-DM	PROPOSED-DM
PE	NO	NO	YES	YES
NS	NO	NO	YES	YES
CR	NO	NO	NO	YES
RA	NO	YES	YES	YES
SE	LOW	LOW	LOW	HIGH

(1) Compared with PA-based DM schemes, the proposed scheme can achieve the range-angle security due to the FDA characteristics.

(2) The high overall spectral efficiency. The idea of SM is to map a block of information bits to symbols that are chosen from the constellation diagram and numbers information of LUs that are chosen from the sets of LUs. The numbers information of multiple LUs can be directly used as additional sources to transmit information simultaneously.

(3) Compared with AN-aided DM schemes, our proposed scheme is power efficient due to MP-WFRFT technique which realizes the embedding process of "AN" from the modulation level of digital baseband signal.

(4) Our proposed scheme can guarantee security of confidential message in some challenging application scenarios. Based on conventional DM schemes, as long as an Eve is close enough to the LU, the confidential messages can be intercepted by the Eve due to constraint on beamwidth. To illustrate the advantage of the proposed schemes, we consider the worst case where Eves know the MP-WFRFT operation with perfect parameters, and these Eves with same number of LUs can cooperate with each other. Therefore, the received symbol vectors of Eves are first operated by the inverse MP-WFRFT with the shared parameters $(\alpha_e, \mathbf{m}_e, \mathbf{c}_e)$, which yields

$$\begin{aligned} \mathbf{y}_E(t) &= \mathfrak{F}_{\alpha_e}^{(\mathbf{m}_e,\mathbf{c}_e)}(\mathbf{H}_E^H(t)\mathbf{D}\mathbf{v}(t)) + \mathfrak{F}_{\alpha_e}^{(\mathbf{m}_e,\mathbf{c}_e)}(\mathbf{n}_E(t)) \\ &= \mathbf{H}_E^H(t)\mathbf{D}\mathfrak{F}_{\alpha_e}^{(\mathbf{m}_e,\mathbf{c}_e)}\mathfrak{F}_{\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{u}(t)) + \mathfrak{F}_{\alpha_e}^{(\mathbf{m}_e,\mathbf{c}_e)}(\mathbf{n}_E(t)) \end{aligned} \tag{26}$$

Here, we assume Eves know the MP-WFRFT operation with perfect parameters, which means

$$(\alpha_e, \mathbf{m}_e, \mathbf{c}_e) = (-\alpha_s, \mathbf{m}_s, \mathbf{c}_s), \tag{27}$$

Then the (35) can be further written as

$$\mathbf{y}_E(t) = \mathbf{H}_E^H(t)\mathbf{D}\mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}\mathfrak{F}_{\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{u}(t)) + \mathfrak{F}_{-\alpha_s}^{(\mathbf{m}_s,\mathbf{c}_s)}(\mathbf{n}_E(t)) = \mathbf{H}_E^H(t)\mathbf{D}\mathbf{u}(t) + \mathbf{n}_E^{'}(t) \tag{28}$$

Specifically, the received signal of *jth* Eve intercepting *kth* LU's information can be obtained by

$$y_{E_j}(t) = \mathbf{h}_{E_k}^H(t)\mathbf{D}u_k(t) + n_{E_j}^{'}(t) = \underbrace{\mathbf{h}_{E_k}^H(t)\mathbf{d}_k u_k(t)}_{\text{Scrambled signal}} + \underbrace{\mathbf{h}_{E_k}^H(t)\sum_{i=1,i\neq k}^{K}\mathbf{d}_i u_i(t)}_{\text{Interference from others}} + \underbrace{n_{E_j}^{'}(t)}_{\text{AWAG}} \tag{29}$$

From (38), in the worst case, we can see that WFRFT operation cannot achieve encryption security. When the Eve's location is the same as the LUs—i.e., $\mathbf{h}_{E_j}(t) = \mathbf{h}_{L_k}(t)$, $\mathbf{h}_{E_k}^H(t)\mathbf{d}_k = 1$, $\mathbf{h}_{E_k}^H(t)\mathbf{d}_i = 0 (i \neq k)$—the AN–DM scheme and WFRFT-aided DM scheme both fail. However, based on our proposed scheme, it is also difficult for Eves to wiretap confidential messages, as estimates of the index information of LUs also need to be correct. Moreover, even if one or some (but not all) of the Eves' locations are same as one or some LUs' locations, the confidential messages are still difficult to retrieve for Eves. Therefore, our proposed method achieves better anti-interception performance and thus improves transmission security.

5. Numerical Results and Analysis

In this section, we provide several numerical experiments to evaluate the performance of the proposed SM and MP-WFRFT aided RFDA-DM scheme and compare its performance with conventional DM schemes. If not otherwise stated, our main parameters in the numerical experiments are given as Table 3.

Table 3. Simulation parameters.

Parameter	Value
Carrier frequency f_c	1 GHz
Number of FDA elements N	32
Inter-element spacing d	$c/2f_c$
Number of LUs K	4
Number of Eves J	4
Receive noise power,$10\log(\sigma^2)$	-100 dBm
Location of LU1,(r_{l_1}, θ_{l_1})	$(1500$ m, $30^\circ)$
Location of LU2, (r_{l_2}, θ_{l_2})	$(2000$ m, $-50^\circ)$
Location of LU3, (r_{l_3}, θ_{l_3})	$(2500$ m, $50^\circ)$
Location of LU4, (r_{l_4}, θ_{l_4})	$(3000$ m, $-30^\circ)$
MP-WFRFT parameters $(\alpha, \mathbf{m}, \mathbf{c})$	$(0.5, [1,2,3,4], [5,6,7,8])$

5.1. Proposed Scheme Focusing Performance Analysis

As discussed in Section 3, the focusing of FDA-DM depends on range-angle dimensions, whereas the focusing of PA-DM only depends on angle. Therefore, our proposed scheme is based on FDA, and in order to improve the focusing performance, we propose random frequency offset and design the beamforming matrix $\mathbf{D}(\mathbf{t})$. Here, we give the spatial power distribution of confidential messages and the SINR spatial distribution to evaluate the focusing performance.

The first experiment measures the energy distribution of confidential messages without the aid of SM and MP-WFRFT modulation. In this experiment, the minimum required receiving power of all LUs are set as $\sqrt{\varsigma_1}=\sqrt{\varsigma_2}=\sqrt{\varsigma_3}=\sqrt{\varsigma_4}=-90$ dBm. In Figure 5, it can be seen that the received confidential energy of LUs is almost equal to -90 dBm. Moreover, in the other region, the energy of confidential decreases as the distance increases. That means our proposed scheme can achieve confidential message energy focusing and accurate control the received power of each LU only based on RFDA.

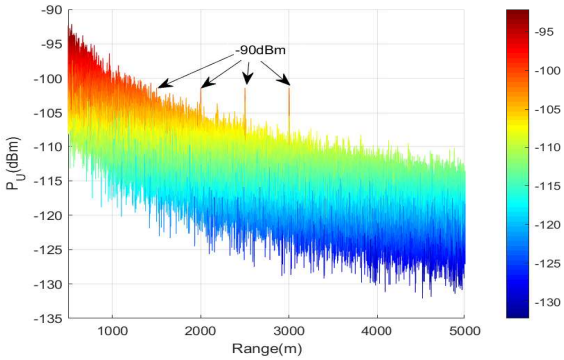
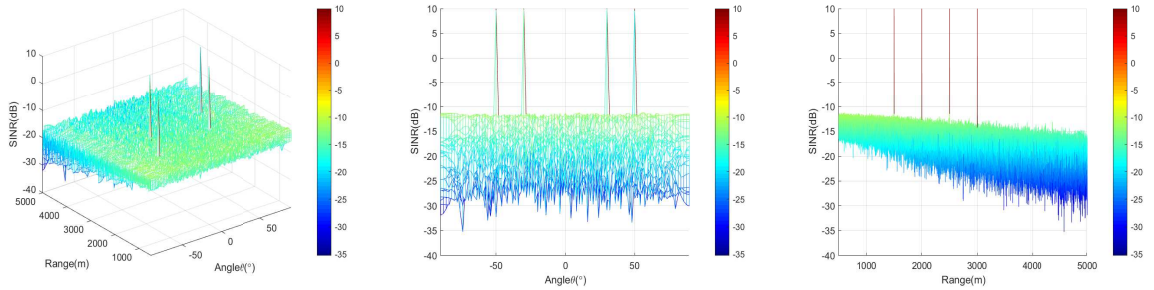


Figure 5. The spatial power distribution of confidential messages in range dimension.

In the second experiment, we simulate and analyze SINR distribution in free space. Here, we consider the case with independent LUs. The proposed approach combined with MP-WFRFT modulation to realize secure wireless communication. MP-WFRFT realizes the embedding process of "AN" from the modulation level of digital baseband signal. From Figure 6, it is obvious that there are four sharp peaks corresponding to each LU due to FDA with the design of beamforming matrix $\mathbf{D}(t)$ and the perfect inverse MP-WFRFT operation on received symbol vectors. Otherwise, the SINR of users in other regions is low, due to the weak received signal that is rotated by MP-WFRFT. In general, we achieve satisfactory focusing performance of wireless communication system.



(**a**) (**b**) (**c**)

Figure 6. The signal to interference-plus-noise ratio (SINR) spatial distribution versus (**a**) angle-range, (**b**) angle dimension, and (**c**) range dimension.

5.2. Secrecy Performance Analysis

In the next experiments, we analyze the secrecy performance of our proposed scheme and compare it with the conventional AN-DM schemes. In a practical case, the Eves would be located as close to LU as possible (even in the same locations as LUs) to eavesdrop messages. We consider that there are four Eves whose locations are closed to LUs, even same as the LUs, and they cooperate with each other. The locations of Eves are set as $(r_{e_1}, \theta_{e_1}) = (1600 \text{ m}, 30^\circ)$ close to LU 1, $(r_{e_2}, \theta_{le_2}) = (2000 \text{ m}, -50^\circ)$ same to LU 2, and $(r_{e_3}, \theta_{e_3}) = (2500 \text{ m}, 55^\circ)$ close to LU 3, $(r_{e_4}, \theta_{e_4}) = (3050 \text{ m}, -35^\circ)$ close to LU 4. In order to show the effective reception of independent LU and verify the superiority of the SM with cooperative LUs, we first analyze BER performance of each LU (without cooperation) under different scenarios, and then simulate the SER performance of cooperative LUs.

Figure 7 illustrates the BER performance of LU and Eve versus the desired received power to noise ratio under different scenarios, where the baseband modulation modes of each LU is BPSK. From Figure 7a, we can observe that (1) our optimal method ensures the effective reception of LU 1; (2) the desired received power to noise ratio requested for the proposed scheme is less than the AN-DM schemes (approximately 1 dB when BER $\approx 10^{-2}$); (3) the BERs at Eve 1 are almost equal to

10^{-5} in Figure 7a, which means that an Eve close to a LU is difficult to receive meaningful message in proposed scheme and AN-DM schemes, respectively. LU 3 and LU 4 have a similar BER performance to LU 1. From Figure 7b, we can see that (1) LU 2 also has satisfactory BER performance; (2) even when the Eve's location is the same as the location of LU 2, the Eve still cannot intercept the message transmitted to LU 2 with the proposed scheme, whereas the Eve successfully wiretaps the confidential message with AN-DM schemes; (3) in a worst case where MP-WFRFT parameters are perfectly leaked to Eves, our proposed scheme also cannot ensure secure transmission between transmitter station and LU 2.

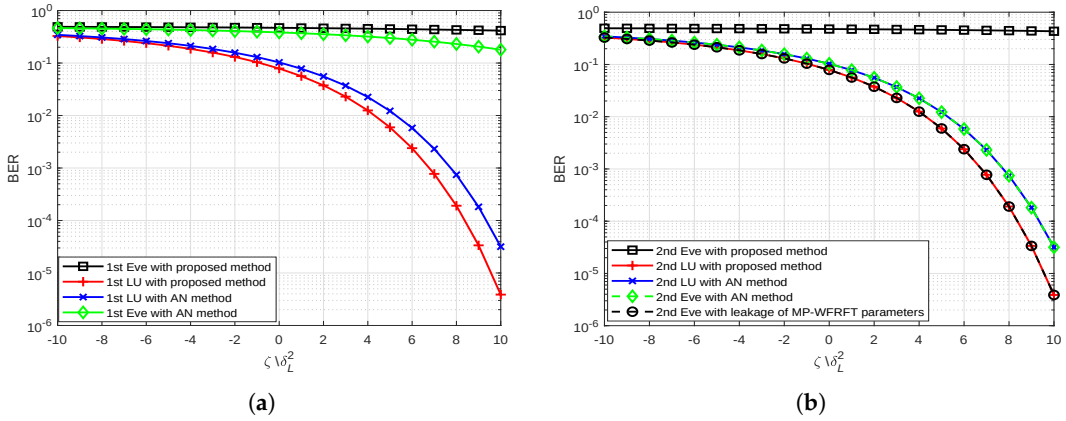


Figure 7. The bit error rate (BER) performance with independent LU versus the desired received power to noise ratio: (**a**) LU 1 and (**b**) LU 2.

Next, Figure 8 shows the SER performance of cooperative LUs versus the desired received power to noise ratio, where the number of active LU is $L = 2$. From Figure 8, we can observe that (1) the SER of Eves is low with all of desired received power to noise ratio, which shows that Eves cannot retrieve the confidential messages without/with the leakage of WFRFT parameters based on the proposed scheme. When MP-WFRFT parameters are leaked to Eves, the SER of Eves is only little better than the case without leakage; (2) the desired received power to noise ratio is less than the AN-DM schemes.

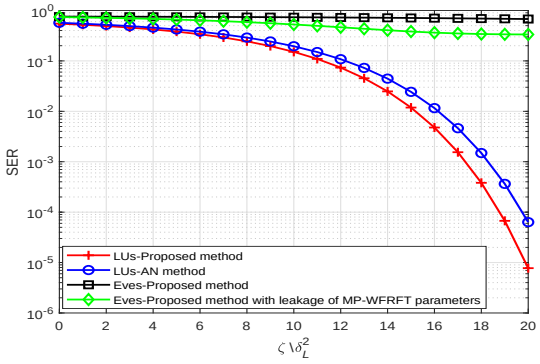


Figure 8. The SER performance of cooperative LUs versus the desired received power to noise ratio.

In general, the proposed scheme can ensure the valid reception for each LU. Moreover, with the SM and MP-WFRFT technology based on cooperative LUs, the eavesdropping capability of Eves is degraded, and thus we can ensure wireless communication security even in the worst case, in which one or some (but not all) independent messages and MP-WFRFT parameters are leaked to Eves. Furthermore, the WFRFT technique overcomes the low-power-efficiency drawback of the conventional

AN-DM schemes, and the SM technology improves the capacity of communication system due to the use of indices information.

5.3. Anti-Interception Performance Analysis

The anti-interception performance of our proposed scheme is depicted in Figures 9 and 10, respectively. It is easy to see that the SER performance of the proposed scheme degrades a great deal along with some mismatched parameters. When the mismatch parameter $\Delta\alpha$ is small, the secrecy performance is almost unaffected, but the secrecy performance of the system declines rapidly with the increase of the $\Delta\alpha$. When the mismatch parameter $\Delta\alpha$ widens to 0.5 , the SER drops to about 0.5, which means that users cannot obtain any meaningful information. From Figure 10, we can conclude that m_k $(k = 1, 2, 3, 4)$ have a similar but richer variation trend. Parameter n_k $(k = 1, 2, 3, 4)$ have similar performance to m_2. Beside correctly estimating the LUs indices information, the eavesdroppers also need to meet the premise that nine parameters are completely consistent. Therefore, our proposed scheme has very good anti-interception performance even under the condition that the Eves know the signal transformation mode (SM modulation and WFRFT modulation).

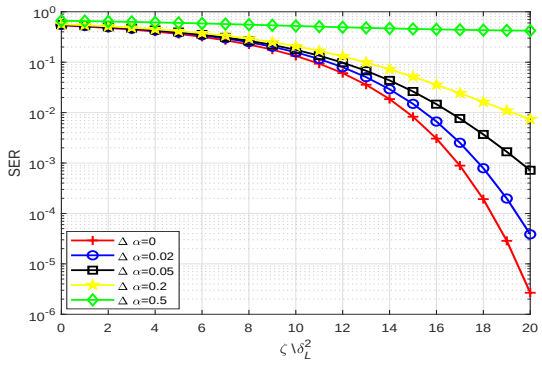
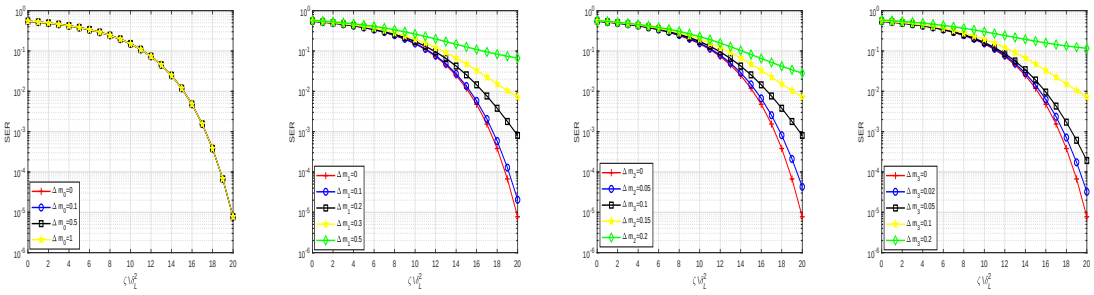


Figure 9. The anti-performance for proposed scheme on parameter α, where $(\mathbf{m}, \mathbf{c}) = ([0, 0, 0, 0], [0, 0, 0, 0])$.



(a) **(b)** **(c)** **(d)**

Figure 10. The anti-performance for proposed scheme on parameter $\mathbf{m}$ **(a)** $(\alpha, \mathbf{m}, \mathbf{c}) = (0.5, [m_0, 0, 0, 0], [0, 0, 0, 0])$, **(b)** $(\alpha, \mathbf{m}, \mathbf{c}) = (0.5, [0, m_1, 0, 0], [0, 0, 0, 0])$, **(c)** $(\alpha, \mathbf{m}, \mathbf{c}) = (0.5, [0, 0, m_2, 0], [0, 0, 0, 0])$, **(d)** $(\alpha, \mathbf{m}, \mathbf{c}) = (0.5, [0, 0, 0, m_3], [0, 0, 0, 0])$.

6. Conclusions

In this paper, a security-enhanced and efficient multi-beam wireless communication scheme with cooperative LUs was proposed. In the proposed scheme, multiple important tools were utilized, including MP-WFRFT technology, SM modulation, and RFDA with the design of the beamforming matrix. With the help of MP-WFRFT, the scheme was found to be more power-efficient than conventional AN-DM schemes. Due to the SM technology, the proposed scheme was shown to have the ability to transmit information bits by the use of LUs number information apart from the modulation

symbols. Finally, SINR distribution, BER performance and SER performance were simulated and analyzed, which verify the advantages of the proposed scheme.

Author Contributions: Investigation, J.G.; methodology, J.G. and B.Q.; simulation and analysis, J.G. and J.Z.; writing and editing, J.G. and J.W.; review, J.Z. and J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key Laboratory Foundation of Education Bureau of Shaanxi Province (Grant no. 14JS075), the National Natural Science Foundation of China (Grant no. 51874238) and the Innovation Foundation for Doctor Dissertation of Northwestern Polytechnical University (Grant no. CX202038).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, B.; Fei, Z.; Zhou, C.; Zhang, Y. Physical Layer Security in Space Information Networks: A Survey. *IEEE Internet Things J.* **2019**, *10*, 142–149. [CrossRef]
2. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2015**, *104*, 1727–1765. [CrossRef]
3. Stallings, W. Cryptography and network security (2nd ed.): Principles and practice. *Int. J. Eng. Comput. Sci.* **2012**, *1*, 121–136.
4. Laurent, M. *An Introduction to Cryptography*; CRC Press, Inc.: Boca Raton, FL, USA, 2000.
5. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 1550–1573. [CrossRef]
6. Kalantari, A.; Soltanalian, M. Directional Modulation via Symbol-Level Precoding: A Way to Enhance Security. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1478–1493. [CrossRef]
7. Xiong, J.; Nusenu, S.Y.; Wang, W.Q. Directional Modulation Using Frequency Diverse Array For Secure Communications. *Wirel. Pers. Commun.* **2017**, *95*, 2679–2689. [CrossRef]
8. Shu, F.; Qin, Y.; Chen, R.; Xu, L.; Shen, T.; Wan, S.; Jin, S.; Wang, J.; You, X. Directional Modulation: A Secure Solution to 5G and Beyond Mobile Networks. *arXiv* **2018**, arXiv:1803.09938.
9. Hafez, M.; Yusuf, M.; Khattab, T.; Elfouly, T.; Arslan, H. Secure Spatial Multiple Access Using Directional Modulation. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 563–573. [CrossRef]
10. Daly, M.P.; Bernhard, J.T. Directional Modulation Technique for Phased Arrays. *IEEE Trans. Antennas Propag.* **2009**, *57*, 2640–2663. [CrossRef]
11. Shu, F.; Wu, X.; Hu, J.; Li, J.; Chen, R.; Wang, J. Secure and Precise Wireless Transmission for Random-Subcarrier-Selection-Based Directional Modulation Transmit Antenna Array. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 890–904. [CrossRef]
12. Li, J.; Xu, L.; Lu, P.; Liu, T.; Zhuang, Z.; Hu, J.; Shu, F.; Wang, J. Performance analysis of directional modulation with finite-quantized RF phase shifters in analog beamforming structure. *IEEE Access* **2019**, *7*, 97457–97465. [CrossRef]
13. Shen, T.; Zhang, S.; Chen, R.; Wang, J.; Hu, J.; Shu, F.; Wang, J. Two practical random-subcarrier-selection methods for secure precise wireless transmissions. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9018–9028. [CrossRef]
14. Qiu, B.; Tao, M.; Wang, L.; Xie, J.; Wang, Y. Multi-beam directional modulation synthesis scheme based on frequency diverse array. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2593–2606. [CrossRef]
15. Nusenu, S.Y.; Basit, A. Frequency diverse array antennas: From their origin to their application in wireless communication systems. *J. Comput. Netw. Commun.* **2018**, *18*, 1–12. [CrossRef]
16. Mai, C.; Lu, S.; Sun, J.; Wang, G. Beampattern Optimization for Frequency Diverse Array with Sparse Frequency Waveforms. *IEEE Access* **2017**, *18*, 1. [CrossRef]
17. Lin, J.; Li, Q.; Yang, J.; Shao, H.; Wang, W.Q. Physical-Layer Security for Proximal Legitimate User and Eavesdropper: A Frequency Diverse Array Beamforming Approach. *IEEE Access* **2018**, *13*, 671–684. [CrossRef]
18. Gao, K.; Wang, W.Q.; Cai, J.; Xiong, J. Decoupled frequency diverse array range–angle-dependent beampattern synthesis using non-linearly increasing frequency offsets. *IET Microw. Antennas Propag.* **2016**, *10*, 880–884. [CrossRef]

19. Khan, W.; Qureshi, I.M.; Saeed, S. Frequency diverse array radar with logarithmically increasing frequency offset. *IEEE Antennas Wirel. Propag. Lett.* **2014**, *14*, 499–502. [CrossRef]
20. Mahmood, M.; Mir, H. Frequency diverse array beamforming using nonuniform logarithmic frequency increments. *IEEE Antennas Wirel. Propag. Lett.* **2014**, *17*, 1817–1821. [CrossRef]
21. Liu, Y.; Ruan, H.; Wang, L.; Nehorai, A. The random frequency diverse array: A new antenna structure for uncoupled direction-range indication in active sensing. *IEEE J. Sel. Top. Signal Process.* **2016**, *11*, 295–308. [CrossRef]
22. Hu, J.; Yan, S.; Shu, F.; Wang, J.; Li, J.; Zhang, Y. Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays. *IEEE Access* **2017**, *5*, 1658–1667. [CrossRef]
23. Shu, F.; Xu, L.; Wang, J.; Zhu, W.; Xiaobo, Z. Artificial-noise-aided secure multicast precoding for directional modulation systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6658–6662. [CrossRef]
24. Xie, T.; Zhu, J.; Li, Y. Artificial-noise-aided zero-forcing synthesis approach for secure multi-beam directional modulation. *IEEE Commun. Lett.* **2017**, *22*, 276–279. [CrossRef]
25. Qiu, B.; Xie, J.; Wang, L.; Wang, Y. Artificial-Noise-Aided Secure Transmission for Proximal Legitimate User and Eavesdropper Based on Frequency Diverse Arrays. *IEEE Access* **2018**, *6*, 52531–52543. [CrossRef]
26. Zhou, F.; Li, Z.; Cheng, J.; Li, Q.; Si, J. Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2450–2464. [CrossRef]
27. Mei, L.; Sha, X.; Ran, Q.; Zhang, N. Research on the application of 4-weighted fractional Fourier transform in communication system. *Sci. China Inf. Sci.* **2010**, *6*, 1251–1260. [CrossRef]
28. Fang, X.; Sha, X.; Mei, L. Guaranteeing wireless communication secrecy via a WFRFT-based cooperative system. *China Commun.* **2015**, *12*, 76–82. [CrossRef]
29. Luo, Z.; Wang, H.; Zhou, K.; Lv, W. Combined Constellation Rotation with Weighted FRFT for Secure Transmission in Polarization Modulation Based Dual-polarized Satellite Communications. *IEEE Access* **2017**, *5*, 27061–27073. [CrossRef]
30. Xiaojie, F.; Xuejun, S.; Yong, L. Secret Communication Using Parallel Combinatory Spreading WFRFT. *IEEE Commun. Lett.* **2015**, *19*, 62–65. [CrossRef]
31. Fang, X.; Zhang, N.; Sha, X.; Chen, D.; Wu, X.; Shen, X. Physical layer security: A WFRFT-basec cooperation approach. In Proceedings of the IEEE International Conference on Communications, Paris, France, 21–25 May 2017; pp. 1–6.
32. Cheng, Q.; Fusco, V.; Zhu, J.; Wang, S.; Wang, F. WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5211–5226. [CrossRef]
33. Liang, Y.; Da, X.; Xu, R.; Ni, L.; Zhai, D.; Pan, Y. Research on Constellation-Splitting Criterion in Multiple Parameters WFRFT Modulations. *IEEE Access* **2018**, *6*, 34354–34364. [CrossRef]
34. Cheng, Q.; Zhu, J.; Luo, J. Secure Spatial Modulation Based on Dynamic Multi-Parameter WFRFT. *Trans. Commun.* **2018**, *11*, 2304–2312. [CrossRef]
35. Jeganathan, J.; Ghrayeb, A.; Szczecinski, L. Spatial modulation: Optimal detection and performance analysis. *IEEE Commun. Lett.* **2012**, *11*, 166–168. [CrossRef]
36. Lee, J.; Lee, J.Y.; Lee, Y.H. Spatial Multiplexing of OFDM Signals With QPSK Modulation Over ESPAR. *IEEE Trans. Veh. Technol.* **2017**, *66*, 4914–4923. [CrossRef]
37. Basar, E.; Wen, M.; Mesleh, R.; Di Renzo, M.; Xiao, Y.; Haas, H. Index Modulation Techniques for Next-Generation Wireless Networks. *IEEE Access* **2017**, *3*, 16693–16746. [CrossRef]
38. Legnain, R.M.; Hafez, R.H.; Legnain, A.M. Improved Spatial Modulation for High Spectral Efficiency. *Int. J. Distrib. Parallel Syst.* **2012**, *3*, 693–746. [CrossRef]