In this paper, a transmission scheme based on polarization filtering and weighted fractional Fourier transform (PF-WFRFT) is proposed to enhance the transmission security in wireless communications. Indeed, the distribution of the transmit signals processed by WFRFT can be close to Gaussian, which can significantly improve the low detection probability. However, through scanning the WFRFT order with small step size, an eavesdropper can restore a regular constellation and crack the information. To overcome the problem, in the PF-WFRFT scheme, two polarized signals with mutually orthogonal polarization state are utilized to convey the information, which are processed by WFRFT separately and added up linearly before being transmitted by dual-polarized antennas. In this manner, even by scanning the WFRFT order, recovered signals are composite ones, which make the WFRFT order and the signals’ PSs difficult to crack, thus improving the security. In addition, the polarization-dependent loss (PDL) effect on the proposed scheme is discussed and a preprocessing matrix based on the channel information is constructed to eliminate this effect. Finally, numerical results are given to demonstrate the security performance of the proposed scheme in wireless communications.

1. Introduction

Nowadays, wireless communication is integrated into all aspects of our lives and is becoming increasingly important. With the development of fifth-generation communication, the communication frequency becomes higher and higher and in which condition, it is not enough to rely on multi-antenna technology alone to improve spectrum efficiency [1]. It is better to consider the usage of dual-polarized antennas, which has the potential to double the spectrum efficiency through providing two independent channels in the same frequency, called orthogonal polarization multiplexing (OPM) [2]. In addition, the mutual information between orthogonal polarization antennas can also be utilized for information transmission, like polarization state modulation (PM) [3] and polarization filtering (PF). For PM, the amplitude ratio and phase difference between orthogonal polarization components of the polarized signal were used to convey the information, which was called polarization state (PS). And it can be combined with amplitude-phase modulation (AM) techniques. Thus, the transmission efficiency can be improved [4]. Moreover, with PM, the energy efficiency can also be improved [5, 6]. For PF, PSs acted as the attribute of signal and were used for signal separation, such as in [7], the information was conveyed by two polarized signals, which were added up before transmission. Then, at the receiver side, based on PF, two polarized signals are completely separated for demodulation, thus improving the transmission efficiency. Therefore, dual-polarized wireless communication is of great significance to improve the throughput of existing wireless communication systems.

Notably, in wireless communication systems, the radio frequency is shared and the propagation medium is naturally open, which makes it difficult to guarantee the security of information transmission. Currently, transmission security mainly depends on cryptographic techniques applied at higher layers, which is mainly relied on the computational unbreakable mathematical manipulations. However, they were increasingly threatened due to the rapid development of computer technology [8, 9].
Fortunately, new researches point out that physical layer encryption techniques can guarantee transmission security even if the eavesdropper has unlimited computational capabilities [10], which aims to distort the modulation constellations and improve the secrecy capacity. For example, in [11], the signals are firstly transformed by the discrete Fourier transform (DFT) function and then encrypted by a diagonal encryption matrix. In this manner, the constellation is distorted and the secrecy rate is enhanced. In [12, 13], the phase of the transmit signal was randomized by a pseudorandom sequence, which led to the constellation rotation and thus, the signals were harder to be demodulated by the eavesdropper. Moreover, in [13], signals were randomized by a pseudorandom sequence and processed by WFRFT, which further distorted the constellations and enhanced the protection for the pseudorandom sequence and the WFRFT orders. In [6, 14], information was conveyed by two polarized signals and signals’ PSs were randomly chosen based on the designed rule. For the legitimate user, with the shared rule, two polarized signals could be completely separated from received signals based on polarization filtering. For eavesdroppers, two polarized signals were difficult to separate. Thus, transmission security was enhanced.

Although the above methods can achieve good security performance, there are still some points that should be taken into consideration. For example, in [13], the symbol error rate of AM signals could not achieve the theoretical value under the Gaussian channel due to polarization mismatch. In [6, 14], the transmit signal was easily detected by eavesdroppers, which increased the risk of eavesdropping. Therefore, security performance could be further improved.

In this paper, to further improve the security performance of information transmission, a transmission scheme based on polarization filtering and weighted fractional Fourier transform (PF-WFRFT) is proposed, where the information is divided into two parts and then modulated into two sets of symbols with the same number by modulation techniques, like Phase Shift Keying (PSK), Pulse Amplitude Modulation (PAM), and Quadrature Amplitude Modulation (QAM). Subsequently, two sets of symbols multiply by two orthogonal PSs, respectively. After that, the corresponding terms are added up linearly to form a set of composite signals. Then, two components of the composite signals are processed by WFRFT with different orders and transmitted by dual-polarized antennas, respectively. In the proposed scheme, the distribution of the signals is adjusted to Gaussian by WFRFT, which improves the low detection probability performance [13, 15]. In addition, the WFRFT order is chosen from a designed set based on the rule that is shared between the transmitter and the legitimate receiver. In this way, when the WFRFT order is scanned by eavesdroppers, the recovered signals are composite signals; it is difficult to determine the WFRFT order. Moreover, with a time-varying WFRFT order, transmit signals are well protected.

In addition, the impairment from the nonideal channel will change the PSs of the polarized signals, which would lead to the bit error rate performance degradation [16]. This is called polarization dependent loss effect (PDL). To solve this problem, a preprocessing matrix based on the channel state information is constructed to process the received signals at the receiver side. Finally, the security performance of the proposed scheme is evaluated in terms of bit error rate (BER) by numerical simulations.

Notations: The superscript T and H are used to denote the transpose and the Hermitian transpose of a vector or matrix. Vectors and matrices are represented by bold lowercase or uppercase. E[.] denotes the expectation operator, and | · | denotes the modulus value.

2. Weighted Fractional Fourier Transformation

In this section, we give definition and properties of WFRFT [4, 15]. At first, we provide a definition of WFRFT.

Definition 1. The $a$-order WFRFT of signal $s$ is defined as follows:

$$\mathcal{F}^a(s) = \Psi^a_X[s] = \sum_{l=0}^{M-1} w_\alpha(a) F^{|d/M|}_K s,$$

where $s$ can be any complex signal vector with arbitrary length. $M \geq 4$ is a natural number, which denotes the number of the basic operators involved in the transformation. $F_K$ denotes the unitary Fourier matrix with elements satisfying

$$F_K(g_1, g_2) = \frac{1}{\sqrt{K}} e^{-j \pi (g_1^{-1} g_2^{-1})^2 K},$$

where $g_1, g_2 \in \{1, 2, \ldots, K\}$ and $F_K(g, l)$ is the specific element that is located at the $g_1$-th row and $g_2$-th column in the Fourier matrix.

In our paper, we just consider the WFRFT with 4 basic operators; then the $a$-order WFRFT transformation matrix can be written as follows:

$$W^a_i = w_0(a) I_K + w_1(a) P_K + w_2(a) P_K + w_3(a) P_K^{-1},$$

where $I_K$ denotes the $K \times K$ identity matrix and $P_K$ denotes the shift matrix, which can be represented as follows:

$$P_K = \begin{bmatrix}
1 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & 1 \\
0 & 0 & \cdots & 0 & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 1 & 0 & \cdots \\
0 & 1 & 0 & \cdots & 0
\end{bmatrix}_{K \times K}.$$ (4)

The weighting coefficients $\{w_\alpha(a)\}_{l=0}^3$ can be calculated by the following:

$$w_\alpha(a) = \frac{1}{M} \frac{1 - \exp[-2\pi j (a - l)]}{1 - \exp[-2\pi j (a - l)/M]} \quad l = 1, 2, 3, 4.$$ (5)
Since $\alpha$ is a real number and $\omega_j(\alpha) = \omega_j(\alpha + 4)$, thus, $\alpha \in [0, 4]$ or $\alpha \in [-2, 2]$. The $\alpha$-order WFRFT with $M = 4$ basic operations signal is denoted by $\Psi^\alpha_M(s)$. Then, the following axioms can be obtained [13]:

I. Interchange axiom:
\[ \Psi^\alpha_M[\Psi^{\alpha - \beta}_M(s)] = \Psi^{\alpha - \beta}_M[\Psi^\alpha_M(s)] = s. \]  

II. Boundary axiom:
\[ \Psi^0_M[s] = s, \]
\[ \Psi^1_M[s] = DFT(s). \]

where $DFT(\cdot)$ denotes the discrete Fourier transform.

III. Additive axiom:
\[ \Psi^{\alpha + \beta}_M[s] = \Psi^\alpha_M[\Psi^\beta_M[s]] = \Psi^\beta_M[\Psi^\alpha_M[s]]. \]

Base on equations (1) and (3), it is found that signal $s$ is transformed in mixed signals consisting of time-domain signal $(w_0(\alpha)I_0)S$ and $w_3(\alpha)P_F S$ and frequency-domain signal $(w_1(\alpha)F_E S$ and $w_3(\alpha)P_F E S$. In this manner, by adjusting the order, the weight of the four components of changes leads to the changes in signal distribution. Therefore, a suitable order can bring the transformed signal distribution closer to the Gaussian noise.

3. System Model

The classical eavesdropping model is studied in this paper, which consists of three participants, a transmitter Alice, a legitimate receiver Bob, and an eavesdropper Eve as shown in Figure 1. All of them are equipped with a dual-polarized antenna. If signals are broadcast from Alice without any protection, the same information can be recovered by both Bob and Eve. Thus the information eavesdrops. To prevent eavesdropping, the PF-WFRFT scheme is designed to enhance the transmission security in this paper, which is described in detail in the next sections.

4. Signal Model and Problem Description

The transmit polarized signal can be represented as follows [13]:
\[ s = \begin{bmatrix} s_H \\ s_V \end{bmatrix} = \begin{bmatrix} \cos \gamma \\ \sin \gamma e^{i\eta} \end{bmatrix}_{PS} \begin{bmatrix} A \cos(\omega_j t + \phi) \end{bmatrix}_{AM signal}. \]

It is found that $P = \begin{bmatrix} \cos \gamma \\ \sin \gamma e^{i\eta} \end{bmatrix}$ is the PS of the polarized signal and $Ae^{i(\omega_j t + \phi)}$ denotes the amplitude-phase modulation (AM) signal, where $A$ and $\phi$ denote the amplitude and phase, respectively. $\gamma \in [0, \pi/2]$ is the polarized angle, which reflects the amplitude relationship between two orthogonal dual-polarized components. $\eta \in [0, 2\pi]$ denotes the difference of them in phase; $\omega_j$ denotes the carrier frequency.

As described in [6, 13] that in order to demodulate the signal, the blind demodulation method can be utilized, where three steps should be followed:

1. At first, the PS $P$ of the polarized signal should be recovered by
\[ \gamma_R = \arctan\left(\frac{\text{abs}(s_V)}{\text{abs}(s_H)}\right), \]
\[ \eta_R = \Xi(s_V) - \Xi(s_H), \]
where $\Xi$ is the phase acquisition function.

2. Based on the demodulated PS, polarization matching is conducted to the received signal to obtain the AM signal as follows:
\[ \begin{bmatrix} \cos \gamma \\ \sin \gamma e^{i\eta} \end{bmatrix}^H S = \begin{bmatrix} \cos \gamma_R \\ \sin \gamma_R e^{i\eta_R} \end{bmatrix}^H \begin{bmatrix} \cos \gamma \\ \sin \gamma e^{i\eta} \end{bmatrix} Ae^{i(\omega_j t + \phi)} \]
\[ \approx Ae^{i(\omega_j t + \phi)}. \]

3. Finally, according to the Maximum likelihood estimation criterion, the information carried by the AM signal can be recovered.

If the polarized signals are broadcast without any protection, Eve can recover the same information from the received signals as Bob. Thus, information leakage occurs. To prevent eavesdropping, in the next parts, we mainly introduce the proposed PF-WFRFT scheme.

5. Principle of the PF-WFRFT Scheme

5.1. Signal Modulation. In the PF-WFRFT scheme, the signal processing produced at the transmitter side is shown in Figure 2. At first, the information sequence $I_0$ is divided into $I_1$ and $I_1$ by the Data Rate Allocation Unit (DRAU). Secondly, both of them are modulated by traditional modulation techniques (TM1 and TM2), which yields $K$ symbols:
where $\mathbf{A}_k^x (\mathbf{A}_k^y)$ and $\varphi_k^x (\varphi_k^y)$ denote the $k$th amplitude and phase, respectively, and $P$ is the power. Thirdly, two paths of signals are, respectively, multiplied by two orthogonal PSs:

$$
\mathbf{P}_x = \begin{bmatrix}
\cos \gamma_x \\
\sin \gamma_x e^{i\eta_x}
\end{bmatrix}, \\
\mathbf{P}_l = \begin{bmatrix}
\cos \gamma_l \\
\sin \gamma_l e^{i\eta_l}
\end{bmatrix},$$

where $\gamma_k$ and $\eta_k$ are polarization parameters.

Then, they are divided into several groups and corresponding symbols of two paths of polarized signals are added up. After that, for each group, two components of the mixed signals are separately processed by WFRFT with randomly selected orders. Finally, composite signals are, respectively, transmitted out by horizontal polarization antenna ($H$) and vertical polarization ($R$) antenna.

Then, at the receiver side, the received signals can be written as follows:

$$
\mathbf{y}_c = \mathbf{H} \begin{bmatrix}
\mathbf{y}_x^c \\
\mathbf{y}_l^c
\end{bmatrix} = \mathbf{H} \begin{bmatrix}
\psi_4^x (\mathbf{P}_x \mathbf{x}_c + \mathbf{P}_l \mathbf{l}_c, \text{1: :}) \\
\psi_4^y (\mathbf{P}_x \mathbf{x}_c + \mathbf{P}_l \mathbf{l}_c, \text{2: :})
\end{bmatrix} + \mathbf{n}_c,
$$

where $\mathbf{H}$ denotes the channel coefficient matrix; $\mathbf{c}_c = vu + \mathbf{1}$: ($v + 1)u$ and $v = 0, 1, \ldots, K/u$. As we know, for WFRFT, the longer the matrix length, the higher the computational complexity. Thus, we divide $K$ symbols into $K/u$ groups to simplify the calculation, where $u$ denotes the number of symbols in one group. $\mathbf{n}_c = \begin{bmatrix} n_{c1}^I \\ n_{c1}^Q \end{bmatrix}$ is the noise vector with the probability density function (PDF) as $CN(0, \sigma_v^2 \mathbf{I}_{2n_c})$. In this way, it is found that the received signals are a mixture of two polarized signals. Even by scanning the WFRFT order, the eavesdropper cannot recover a regular constellation with the three steps mentioned in Section 4. In addition, in the PF-WFRFT scheme, the WFRFT order is randomly selected from a designed set, which is shared between the transmitter and the legitimate receiver. In this manner, both the WFRFT order and the PSs of the polarized signals are hard to crack. Therefore, the security performance for information transmission is enhanced.

5.2. Signal Demodulation. At first, the ideal channel condition is taken into consideration, where $\mathbf{H}$ is a unit matrix. For the $c_c$-th group signals, we assume two PSs $\mathbf{P}_x, \mathbf{P}_l$ and the WFRFT orders are $\alpha$ and $\beta$. For the legitimate user Bob, to demodulate the signal, two components of $\mathbf{y}_c$, should be firstly processed by WFRFT with orders $-\alpha$ and $-\beta$, and we obtain the following:

$$
\hat{\mathbf{y}}_c = \mathbf{P}_x \mathbf{x}_c + \mathbf{P}_l \mathbf{l}_c + \begin{bmatrix}
\psi_{-\alpha}^x (n_{c1}^I) \\
\psi_{-\beta}^y (n_{c2}^I)
\end{bmatrix},
$$

It is obvious that $\hat{\mathbf{y}}_c$ is the sum of $\mathbf{P}_x \mathbf{x}_c$ and $\mathbf{P}_l \mathbf{l}_c$, which makes it hard to demodulate the transmit signal directly. Thus, it is necessary to separate them for separately demodulating. According to the oblique projection technique in [5], based on $\mathbf{P}_x$ and $\mathbf{P}_l$, two filtering matrices can be constructed to complete the signal separation, which can be calculated as follows:

$$
\mathbf{Q}_{\mathbf{P}_x|\mathbf{P}_x} = \mathbf{P}_x (\mathbf{P}_x^H \mathbf{P}_x)^{-1} (\mathbf{P}_x)^H \mathbf{P}_x^H, \\
\mathbf{Q}_{\mathbf{P}_l|\mathbf{P}_x} = \mathbf{P}_l (\mathbf{P}_l^H \mathbf{P}_x)^{-1} (\mathbf{P}_l)^H \mathbf{P}_x^H,
$$

where $\mathbf{P}_x^H$ and $\mathbf{P}_x^H$ are orthogonal matrix and can be written as follows:

$$
\mathbf{P}_x^H = \mathbf{I}_2 - \mathbf{P}_x (\mathbf{P}_x^H \mathbf{P}_x)^{-1} (\mathbf{P}_x)^H, \\
\mathbf{P}_l^H = \mathbf{I}_2 - \mathbf{P}_l (\mathbf{P}_l^H \mathbf{P}_x)^{-1} (\mathbf{P}_l)^H.
$$

Then, it obtains that

\[ \]
environment is a complex electromagnetic environment, mission information can be recovered.

According to [6], it is known that the noise power can be written as follows:

$$\tilde{\sigma}^2 = \text{trace}\left(\mathbf{Q}_{P|P'}\mathbf{Q}_{P'|P}H^{-2}\right) = \frac{\sigma^2}{\sin^2 \xi}$$  \hspace{1cm} (19)

where trace(·) represents the trace of a matrix, ξ denotes the principal angle between subspace $\mathbf{Q}_{P|P'}$ and $\mathbf{Q}_{P'|P}$. As two PSs are assumed to be orthogonal to each other, it is obtained that $\xi = (\pi/2)$ and $\tilde{\sigma}^2 = \sigma^2$, the noise power is not amplified. Thus, two signals are completely separated. Finally, by using the maximum likelihood estimation algorithm, the transmission information can be recovered.

5.3. Polarization-Dependent Loss Effect and Signal Demodulation. As we know, the wireless communication environment is a complex electromagnetic environment, where the channel matrix $\mathbf{H}$ is not always an ideal one. Thus, $\mathbf{H}$ can be further written as follows [7]:

$$\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} = \mathbf{U} \Sigma \mathbf{V} = \mathbf{U} \begin{bmatrix} \sqrt{\lambda_1} & 0 \\ 0 & \sqrt{\lambda_2} \end{bmatrix} \mathbf{V},$$  \hspace{1cm} (20)

where $\sqrt{\lambda_i}, i = 1, 2$ denote eigenvalues. $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices. Then, equation (14) can be rewritten as follows:

$$\mathbf{y}_c = \begin{bmatrix} h_{11}\mathbf{y}_L^c + h_{12}\mathbf{y}_R^c \\ h_{21}\mathbf{y}_L^c + h_{22}\mathbf{y}_R^c \end{bmatrix} + \mathbf{n}_c.$$  \hspace{1cm} (21)

After processed by WFRFT, equation (15) is rewritten as follows:

$$\tilde{\mathbf{y}}_c = \begin{bmatrix} h_{11}\mathbf{y}_L^c + h_{12}\mathbf{y}_R^c \end{bmatrix} + \begin{bmatrix} \psi_4^\alpha (n_L^c) \\ \psi_4^\beta (n_R^c) \end{bmatrix}$$  \hspace{1cm} (22)

$$= \mathbf{y}_c + \mathbf{J} + \begin{bmatrix} \psi_4^\alpha (n_L^c) \\ \psi_4^\beta (n_R^c) \end{bmatrix},$$

where $\mathbf{J}$ denotes the interference brought by the nonideal channel, which can be written as follows:

$$\mathbf{J} = \begin{bmatrix} (h_{11} - 1)\mathbf{y}_L^c + h_{12}\psi_4^\alpha (\mathbf{y}_R^c) \\ (h_{22} - 1)\mathbf{y}_L^c + h_{21}\psi_4^\beta (\mathbf{y}_R^c) \end{bmatrix}.$$  \hspace{1cm} (23)

Then, equation (18) is written as follows:

$$\mathbf{Q}_{P|P'}\tilde{\mathbf{y}}_c = \mathbf{x}_c + \mathbf{Q}_{P|P'} \mathbf{J} + \mathbf{Q}_{P'|P} \mathbf{J} + \mathbf{Q}_{P|P'} \mathbf{J}$$  \hspace{1cm} (24)

According to equations (22) and (24), it is found that the nonideal channel would cause interference, which would lead to the BER performance degradation. Therefore, it is better to eliminate this effect before signal demodulation.

In this paper, to overcome the problem, we assume the CSI can be correctly estimated at the receiver side and based on the estimated CSI, a preprocessing matrix is constructed and used to process the received signals before performing WFRFT [17]. The preprocessing matrix can be denoted as follows:

$$\mathbf{W} = \mathbf{H}^{-1} = \frac{\mathbf{H}^+}{\text{det}(\mathbf{H})},$$  \hspace{1cm} (25)

Then, equation (21) is written as follows:

$$\tilde{\mathbf{n}}_c = \mathbf{W} \mathbf{y}_c = \mathbf{W}_c \begin{bmatrix} \mathbf{y}_L^c \\ \mathbf{y}_R^c \end{bmatrix} + \mathbf{W} \begin{bmatrix} \mathbf{n}_L^c \\ \mathbf{n}_R^c \end{bmatrix} = \begin{bmatrix} \mathbf{y}_L^c \\ \mathbf{y}_R^c \end{bmatrix} + \begin{bmatrix} \mathbf{n}_L^c \\ \mathbf{n}_R^c \end{bmatrix}.$$  \hspace{1cm} (26)

The noise power is not changed since WFRFT is a kind of unitary transformation. After being processed with $\mathbf{W}$, the power spectrum density of the noise is changed into the following:

$$\tilde{n}_L^c \sim \sqrt{\frac{|h_{22}|^2 + |h_{12}|^2}{\text{det}(\mathbf{H})^2} \sigma^2}.$$  \hspace{1cm} (27)

As described in [13], the noise power is a little amplitude. In this way, the impairment caused by the nonideal channel is eliminated.

Above all, the signal demodulation diagram for Bob is shown in Figure 3. After sampling and filtering, the received signals firstly multiply with the estimated channel state information (CSI) matrix to eliminate the PDL effect. After that, WFRFT with orders $-\alpha$ and $-\beta$ are performed. Then, based on the PSs, two polarization filtering matrices are constructed and separately multiply by $\mathbf{W}_c$. Finally, through the AM demodulation unit, two AM signals can be demodulated separately.

6. Security Performance Evaluation

In this section, we assume the signals have been detected by Eve and the security performance of the PF-WFRFT scheme is evaluated under an ideal channel condition, which is mainly because Bob and Eve could eliminate the PDL effect based on the channel estimation. For Eve, in order to recover the information, the WFRFT order should be scanned firstly. Then, the received signals can be written as follows:
The signal-to-interference-plus-noise ratio (SINR) for Bob is as follows:

\[
\text{SINR}_B = \frac{E_b}{\frac{1}{2} \left| \sum_{l \neq 1} h_{kl}^r \right|^2 + \sigma^2}
\]

where \(E_b\) is the energy per bit, \(h_{kl}^r\) is the channel gain between Alice and Bob, and \(\sigma^2\) is the noise power.

The capacity of the channel for Alice is given by

\[
C_A = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_A \right)
\]

The capacity of the channel for Bob is given by

\[
C_B = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_B \right)
\]

The capacity of the channel for Eve is given by

\[
C_E = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_E \right)
\]

where \(\text{SINR}_E\) is the signal-to-interference-plus-noise ratio for Eve.

The capacity of the channel for the receiver is given by

\[
C_{RE} = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_{RE} \right)
\]

where \(\text{SINR}_{RE}\) is the signal-to-interference-plus-noise ratio for the receiver.

The capacity of the channel for the transmitter is given by

\[
C_{TX} = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_{TX} \right)
\]

where \(\text{SINR}_{TX}\) is the signal-to-interference-plus-noise ratio for the transmitter.

The capacity of the channel for the channel is given by

\[
C_{CH} = \frac{1}{2} \log_2 \left( 1 + \text{SINR}_{CH} \right)
\]

where \(\text{SINR}_{CH}\) is the signal-to-interference-plus-noise ratio for the channel.
In this part, 16 quadrature amplitude modulation (16QAM) is utilized to modulated both \( I_x \) and \( I_y \). And we take one group of the transmit signals to calculate and observe their Kurtosis. Figure 4 gives the Kurtosis of both the real and imaginary parts of the mixed signals before and after being processed by WFRFT versus \( \alpha \). We take the \( H \) component of them for an example (as the result is almost the same for the \( V \) component). It is found that the Kurtosis of the real component almost equal to that of the imaginary component. In addition, after being processed by WFRFT, the Kurtosis of the mix signals are closer to 0, especially when \( \alpha \in [0.6 \, 1.4] \cup [2.6 \, 3.4] \). In this condition, the distribution of the transmit signal is similar to Gaussian, which is hard to detect.

In addition, in the PF-WFRFT scheme, the WFRFT order is randomly chosen from the design set shared between Alice and Bob, whose elements can be chosen from \([0.6 \, 1.4] \cup [2.6 \, 3.4]\). In this manner, the transmit signals are difficult to detect and the WFRFT orders are safer.

In this simulation, the bit error rate (BER) performance of the PF-WFRFT scheme is evaluated. Indeed, we assume \( \alpha = 0.7, \beta = 2.7 \) and an ideal Gaussian channel condition. Thus there is no PDL effect as Eve can not obtain the information about the WFRFT order and PSs of transmitting signals. We set \( \alpha_E = 0.75, \beta_E = 2.64 \) for Eve and after WFRFT scanning, the blind demodulation method is used to demodulate the signal.

First of all, a random bit sequence \( I_O \) is generated and divided into two parts \( I_x \) and \( I_y \), which are modulated with modulation techniques and two modulated signals are marked with 1 and 2.

We firstly utilize 4th-order Pulse Amplitude Modulation (PAM) to modulate both two-bit sequences and the bit error rate (BER) performance of Bob and Eve versus SNR are given in Figure 5. Then, 4PAM is replaced by 8PAM and BER curves are also plotted in Figure 5. It is found that both 4PAM and 8PAM BER curves of Bob are approaching the theoretical value under the Gaussian channel. However, for Eve, both 4PAM and 8PAM BER curves are almost equal to 0.5, even when SNR equals 15 dB. In this condition, the eavesdropper Eve can not recover the original information \( I_O \).

In addition, we replace PAM with PSK and QAM, respectively. Then, the same operations are performed and the BER curves are given in Figures 6 and 7. In all these conditions, the similar results can be obtained that the BER curves of both two AM signals at Bob are almost the same as the theoretical values while Eve exhibits high BERs. Therefore, based on the PF-WFRFT scheme, Eve can hardly extract any useful information. Thus the transmission security is enhanced.

In this simulation, we assume a non-ideal channel condition to observe the BER performance of Bob since Eve can not achieve a good BER performance even in an ideal channel condition. The channel matrix can be represented as follows:

\[
H = \sqrt{\frac{K}{K+1}} \mathcal{H} + \sqrt{\frac{1}{K+1}} \mathcal{H},
\]

Figure 4: Comparison of Kurtosis of WFRFT signals and normal signals.

Figure 5: BER performance of PAM.
\[
\begin{align*}
\mathcal{H} &= \sqrt{\frac{K}{K+1}} \begin{bmatrix} \sqrt{1-Y} & \sqrt{Y} \\ \sqrt{Y} & \sqrt{1-Y} \end{bmatrix}, \\
\mathcal{H} &= \mathbf{R}_t^{1/2} \times \mathbf{R}_r^{1/2}, \\
\mathbf{R}_t &= \begin{bmatrix} 1 & 2\rho_t \sqrt{\epsilon(1-\epsilon)} \\ 2\rho_t \sqrt{\epsilon(1-\epsilon)} & 1 \end{bmatrix}, \\
\mathbf{R}_r &= \begin{bmatrix} 1 & 2\rho_r \sqrt{\epsilon(1-\epsilon)} \\ 2\rho_r \sqrt{\epsilon(1-\epsilon)} & 1 \end{bmatrix},
\end{align*}
\]

where \( Y \) is the parameter that measures the cross-polarization discrimination (XPD) of the dual-polarized antenna at the receiver side (XPD); \( X \) is a \( 2 \times 2 \) matrix whose elements are a random number with the probability density function (PDF) as \( \mathcal{CN}(0, \sigma^2 \mathbf{I}_{2 \times 2}) \); \( \rho_t \) and \( \rho_r \) are polarization correlation coefficients at the Alice and Bob side, respectively.

In our simulation, it is set that \( \rho_r = 0.2, \rho_t = 0.1, Y = 0.0307, \) and \( \epsilon = 0.1481, K = 10 \). The BER versus SNR curves is plotted in Figure 8, where 4QAM and 16QAM are used to modulate two-bit sequences, respectively. It is found that under a nonideal channel, there is a performance loss for both 4QAM and 16QAM signals. However, with the preprocessing matrix, the BER performance is better than direction demodulation (DD). Therefore, before signal demodulation, it is necessary to relieve the PDL effect.

In this simulation, the secrecy rate performance of the PF-WFRFT scheme is evaluated. We assume an ideal channel condition and \( \alpha = \beta = 0.7, \alpha_E = \beta_E = [0.8 \ 1.2 \ 1.5] \). Thus, the WFRFT order deviations are \( \Delta \alpha = \Delta \beta = [0.1 \ 0.5 \ 0.8] \). QPSK is utilized to modulate two-bit sequences \( I_x \) and \( I_y \). Figure 9 gives the secrecy rate curves with different order deviations versus SNR. It is found that the average secrecy rate increases along with the SNR and a bigger WFRFT order deviation bring better performance. In addition, even a small order deviation, say 0.1 and \( \text{SNR} = 0 \text{ dB} \), we can still choose a positive symbol rate to ensure transmission security.
Simulation results also prove the correctness of the theory and the effectiveness of the PF-WFRFT scheme.

8. Conclusion

This paper proposed a novel scheme to enhance the physical layer security for wireless communications, whereby polarization filtering and WFRFT are used to improve the security level. In the proposed scheme, there is no power waste to design artificial noise and all power is used for signal transmission, which is energy-efficient. In addition, the WFRFT orders are randomly selected, which make the PSs of polarized signals are hard to crack. Moreover, the PF-WFRFT scheme can be used directly in existing wireless communication systems, which is practical and easy to implement. For the next work, the PDL effect elimination method would be further studied and Code Division Multiple Access Technology would be considered for improving the transmission efficiency.

Data Availability

All the data used in this research article are generated by Matlab.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the Complex Electronic System Simulation Laboratory Fund Project.

References

[1] H. Wang, P. Zhang, J. Li, and X. You, “Radio propagation and wireless coverage of LSAA-based 5G millimeter-wave mobile communication systems,” *China Communications*, vol. 16, pp. 1–18, 2019.
[2] K. P. Liolis, J. Gomez-Vilardebo, E. Casini, and A. I. Perez-Neira, “Statistical modeling of dual-polarized MIMO land mobile satellite channels,” *IEEE Transactions on Communications*, vol. 58, no. 11, pp. 3077–3083, 2010.
[3] F. Liu, X. Wang, R. Li, and B. Wang, “Multilevel continuous polarization modulation with high spectral efficiency in the depolarization channels,” *IEEE Access*, vol. 6, pp. 33002–33014, 2018.
[4] X. Fang, N. Zhang, X. Sha, D. Chen, X. Wu, and X. S. Shen, “Physical layer security: a WFRFT-basec cooperation approach,” in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, May 2017.

[5] B. Cao, Q. Y. Zhang, D. Liang, S. M. Wen, L. Jin, and Y. Q. Zhang, “Blind adaptive polarization filtering based on oblique projection,” in *Proceedings of the 2010 IEEE International Conference on Communications (ICC)*, pp. 1–5, Cape Town, South Africa, June 2010.

[6] Z. Luo, H. Wang, and K. Zhou, “Polarization filtering based physical-layer secure transmission scheme for dual-polarized satellite communication,” *IEEE Access*, vol. 5, pp. 24706–24715, 2017.

[7] Z. Luo, H. Wang, and K. Zhou, “A novel transmission scheme for polarization dependent loss elimination in dual-polarized satellite systems,” *IEEE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 101, no. 5, pp. 872–877, 2018.

[8] C. Sahin, B. Katz, and K. R. Dandekar, “Secure and robust symmetric key generation using physical layer techniques under various wireless environments,” in *Proceedings of the 2016 IEEE Radio and Wireless Symposium (RWS)*, pp. 211–214, Austin, TX, USA, January 2016.

[9] S. Spinsante, F. Chiaruluce, and E. Gambi, “Evaluation of AES-based authentication and encryption schemes for telecommand and telemetry in satellite applications,” in *Proceedings of the SpaceOps 2006 Conference*, p. 5558, Marshall, France, June 2006.

[10] E. Jorswieck, S. Tomasin, and A. Sezgin, “Broadcasting into the uncertainty: authentication and confidentiality by physical-layer processing,” *Proceedings of the IEEE*, vol. 10310, pp. 1702–1724, June 2015.

[11] S. Bi, X. Yuan, and Y. J. A. Zhang, “DFT-based physical layer encryption for achieving perfect secrecy,” in *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, June 2003.

[12] R. Ma, L. Dai, Z. Wang, and J. Wang, “Secure communication in TDS-OFDM system using constellation rotation and noise insertion,” *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1328–1332, 2010.

[13] Z. Luo, H. Wang, K. Zhou, and W. Lx, “Combined constellation rotation with weighted FRFT for secure transmission in polarization modulation based dual-polarized satellite communications,” *IEEE Access*, vol. 5, pp. 27061–27073, 2017.

[14] X. Zhang, B. Zhang, and D. Guo, “Physical layer secure transmission based on fast dual polarization hopping in fixed satellite communication,” *IEEE Access*, vol. 5, pp. 11782–11790, 2017.

[15] L. Mei, X. Sha, Q. Ran, and N. Zhang, “Research on the application of 4-weighted fractional Fourier transform in communication system,” *Science China Information Sciences*, vol. 53, no. 6, pp. 1251–1260, 2010.

[16] D. Wei, M. Zhang, W. Fan, and W. Huang, “A spectrum efficient polarized PSK/QAM scheme in the wireless channel with polarization dependent loss effect,” in *Proceedings of the 22nd International Conference on Telecommunications (ICT)*, pp. 249–255, Sydney, Australia, April 2015.

[17] P. Henarejos and A. Perez-Neira, “Dual polarized modulation and reception for next generation mobile satellite communications,” *IEEE Transactions on Communications*, vol. 63, pp. 3803–3812, 2015.