Research on Physical Layer Encryption Scheme of Tactical Network Based on WFRFT

Research on Physical Layer Encryption Scheme of Tactical Network Based on WFRFT

Jialong Wu*, Qinghua Ren[a] and Ming Li[b]

College of Information and Navigation, Air Force Engineering University, Xi'an Shannxi, China

*Corresponding author e-mail: 813544351@qq.com, [a]18991932692@163.com, [b]1160963264@qq.com

Abstract. In view of the characteristic of all-domain openness of tactical network, a Weighted-type Fractional Fourier Transform-based encryption modulation scheme of physical layer constellation is proposed based on the aliasing characteristic of WFRFT signal constellation diagram. On this basis, the influence of weighted parameters on system safety capacity and reliability is considered, and WFRFT weighted parameters are optimized. The simulation results show that when SNR is 15dB, the BER of the system meets the requirements of secure communication, and the low interception performance of the system will be well realized.

1. Introduction

As a highly integrated large-scale information network system, tactical network includes multiple system network structures, which is a combination of "multi-system integration system" and "multi-network integration network". In order to better adapt to the demands of network-centric operations and joint operations, a large number of wireless Ad Hoc networks are adopted in the tactical information network, which brings about a large area of wireless network access points and network interfaces. However, due to the openness of the tactical network, a large number of wireless interfaces and access points become the most vulnerable part of the whole battlefield network system, vulnerable to electronic and network attacks.

In order to ensure the high-speed and efficient transmission of military communication and the absolute security of communication signals, the traditional information encryption system can no longer adapt to the current battlefield environment. With the strengthening of computer computing power and speed of ascension as well as changing of the enemy attack means, encryption above the link layer become no longer efficient completely, the password system which based on the computational complexity will no longer widely used [1], safe transmission scheme which has low interception rate and high resource utilization has become the urgent needs of the military communication.

As the bottom layer of the protocol stack, the physical layer is responsible for providing modulation signals for transmission to the upper layer of the protocol stack. At present, the physical layer security technology is mainly divided into three categories: channel security encoding, physical layer security transmission and physical layer security key generation. It can make it impossible for unauthorized users to extract effective information from the transmission signals and realize absolute

security on the premise of satisfying the communication needs of legitimate users [2]. Therefore, the physical layer security technology can be used as a supplement to the traditional encryption method, and make use of the characteristics of the channel instead of the complicated mathematical calculation method to ensure the confidentiality of military communication.

Studies have shown that in the fading channel, the improvement of bit error rate and diversity performance can be achieved through constellation rotation [5], and the use of APSK constellation satisfying more gaussian discrete distribution can improve the performance of classified rate [6].

Modulation and demodulation, as an indispensable link in message transmission, is a key point in the realization of physical layer security. In order to ensure that the original transmission performance is not reduced, this paper proposes a wfrft-based constellation modulation encryption scheme based on the random aliasing characteristic of WFRFT on constellation diagram, aiming at achieving low interception and high confidentiality of information on the physical layer, and effectively improving the security of tactical wireless network communication.

2. Analysis of constellation encryption system

2.1. Modulation constellation encryption principle

When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

The modulation signal after constellation mapping can be expressed as:

$$x_i = I_i + jQ_i = Am_i e^{j\theta_i} \tag{1}$$

Among them, x_i is the modulated signal, I_i and Q_i represent the real and imaginary parts of the modulated signal respectively, Am_i and θ_i represents the amplitude and phase of the modulated signal respectively.

Phase encryption schematic diagram is shown in figure 1.

$$x_i = Am_i e^{j\theta_i} \xrightarrow{\text{Phase encryption}} x_i' = Am_i e^{j(\theta_i + \Delta\theta_i)}$$

Figure 1. Phase Encryption process of modulated signal.

Based on the concept of traditional constellation rotation, literature [4] proposed the random phase angle as a key to encrypt the signal constellation. The modulation signal through constellation encryption can be expressed as:

$$x_i^{'} = Am_i e^{j(\theta_i + \Delta\theta_i)} \tag{2}$$

Among them, $x_i^{'}$ is the modulation signal encrypted through the physical layer, $\Delta\theta_i$ is the random phase rotation angle of the modulation signal, which is generated randomly by the physical layer encryption sequence.

Pappu pointed out that when considering encryption algorithm, physical irreversible function is more effective than reversible function [7]. The phase generated by the random phase sequence is irreversible and only the legitimate receiver can obtain the real phase rotation information. The study shows that the error rate of the illegal receiver or eavesdropper is 50%. In the absence of real phase information, the eavesdropper can only hack the transmitted information by increasing the

computation. Even though the emergence of quantum technology has greatly promoted the computing speed, the urgency of battlefield situation is not enough to support the time cost of brute force cracking in military communication. The existence of high error rate can have sufficient influence on the information acquisition ability of eavesdropping parties. As can be seen from figure 2, 3 and 4, when the signal constellation is encrypted with random phases, the signal constellation diagram will be changed into a circle, which is different from the constellation diagram with fixed Angle rotation. The encrypted signal phase can be randomly covered in the unit circle.

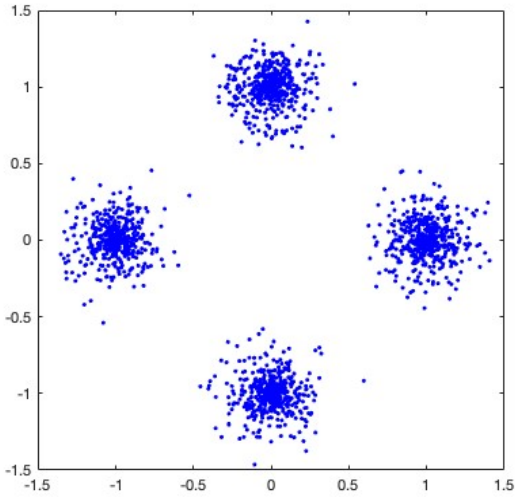

Figure 2. Traditional QPSK modulation mapping.

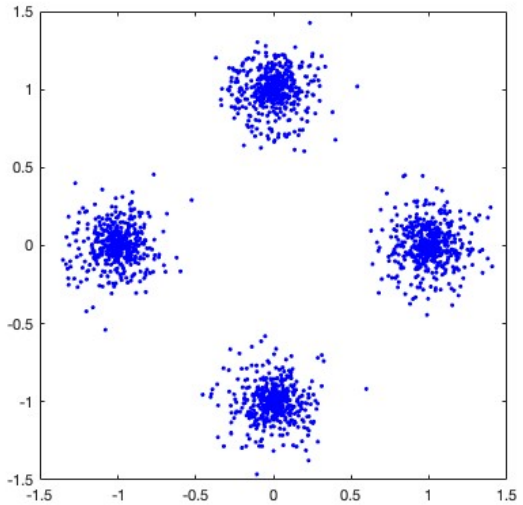

Figure 3. Fixed phase rotation constellation mapping.

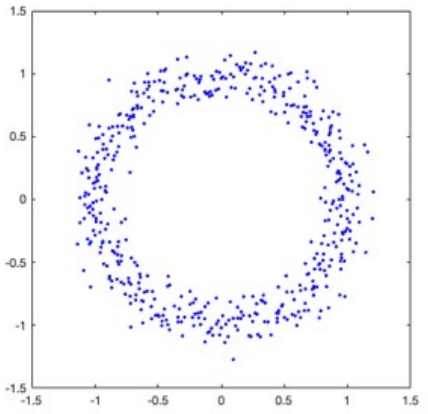

Figure 4. Random phase rotation constellation mapping.

2.2. WFRFT

After Namias, Mcbride, and Kerr obtained the CFRFT with solving Schrödinger, Shih proposed the classic weighted fraction Fourier transform based on the fractional Fourier transform. Its definition can be expressed as:

$$F_{4w}^{\alpha} = w_0(\alpha)g(x) + w_1(\alpha)G(x) + w_2(\alpha)g(-x) + w_3(\alpha)G(-x) \tag{3}$$

Among them, $g(x)$ is the continuous function, $\mathcal{F}$ is the Fourier transform, $g(x)$, $G(x)$, $g(-x)$ and $G(-x)$ are the weighted term, and the correlation between them can be expressed as:

$$\begin{cases} \mathcal{F}^1\left[g(x)\right] = G(x) \\ \mathcal{F}^2\left[g(x)\right] = \mathcal{F}^1\left[G(x)\right] = g(-x) \\ \mathcal{F}^3\left[g(x)\right] = \mathcal{F}^1\left[g(-x)\right] = G(-x) \\ \mathcal{F}^4\left[g(x)\right] = \mathcal{F}^1\left[G(-x)\right] = g(x) \end{cases} \tag{4}$$

The weighting coefficient w_l can be defined as:

$$w_l(\alpha) = \cos\left[\frac{(\alpha-1)\pi}{4}\right]\cos\left[\frac{2(\alpha-1)\pi}{4}\right]\exp\left[\frac{3(\alpha-1)\pi i}{4}\right] \quad (l = 0,1,2,3) \tag{5}$$

In order to make WFRFT applicable to digital communication system, the discrete sequence of WFRFT is directly given through fractionation of DFT operator, which is defined as follows:

$$\mathcal{F}_{4w}^{\alpha,y}\left[X_0\right] = w_0X_0 + w_1X_1 + w_2X_2 + w_3X_3 \tag{6}$$

Among them, $\{X_0, X_1, X_2, X_3\}$ is the 0-3 times DFT of X_0 respectively, and X_0 is the DFT of X_3. When DFT adopts the definition form of energy normalization, the above equation can be rewritten as:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} w_0 & w_1 & w_2 & w_3 \\ w_3 & w_0 & w_1 & w_2 \\ w_2 & w_3 & w_0 & w_1 \\ w_1 & w_2 & w_3 & w_0 \end{bmatrix} \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} w_0X_0 + w_1X_1 + w_2X_2 + w_3X_3 \\ w_3X_0 + w_0X_1 + w_1X_2 + w_2X_3 \\ w_2X_0 + w_3X_1 + w_0X_2 + w_1X_3 \\ w_1X_0 + w_2X_1 + w_3X_2 + w_0X_3 \end{bmatrix} \tag{7}$$

For any N-long plural sequence $X_0 = \{x_0, x_1, \cdots, x_{N-1}\}^T$, the definition of WFRFT for discrete sequence can be written as:

$$\begin{aligned} S_0 &= \mathcal{F}_{4w}^{\alpha,V}\left[X_0\right] \\ &= w_0F^0X_0 + w_1F^1X_0 + w_2F^2X_0 + w_3F^3X_0 \\ &= w_0\mathrm{I}X_0 + w_1FX_0 + w_2\mathrm{II}X_0 + w_3F^HX_0 \\ &= \left(w_0\mathrm{I} + w_1F + w_2\mathrm{II} + w_3F^H\right)X_0 \\ &= F_{4W}\left(\alpha,V\right)X_0 \end{aligned} \tag{8}$$

Among them, $F = \frac{1}{\sqrt{N}}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & Q^{(N-1)(N-1)} \end{bmatrix}$, $Q = e^{\frac{-i2\pi}{N}}$.

That is, the 4-WFRFT of the column vectors X_0 can be obtained by making a matrix of pairings $F_{4W}(\alpha,V)$.

The physical implementation process of WFRFT is shown in figure 5. After information sequence of N-length is transformed into four branches for processing. Among them, the signal data which go through branch w_1 and w_3 has passed through DFT module before weighted processing, so they just correspond to the multi-carrier system structure of OFDM. In the corresponding branch w_0 and w_2, there is no DFT module in the process, and the corresponding is the single-carrier system structure.

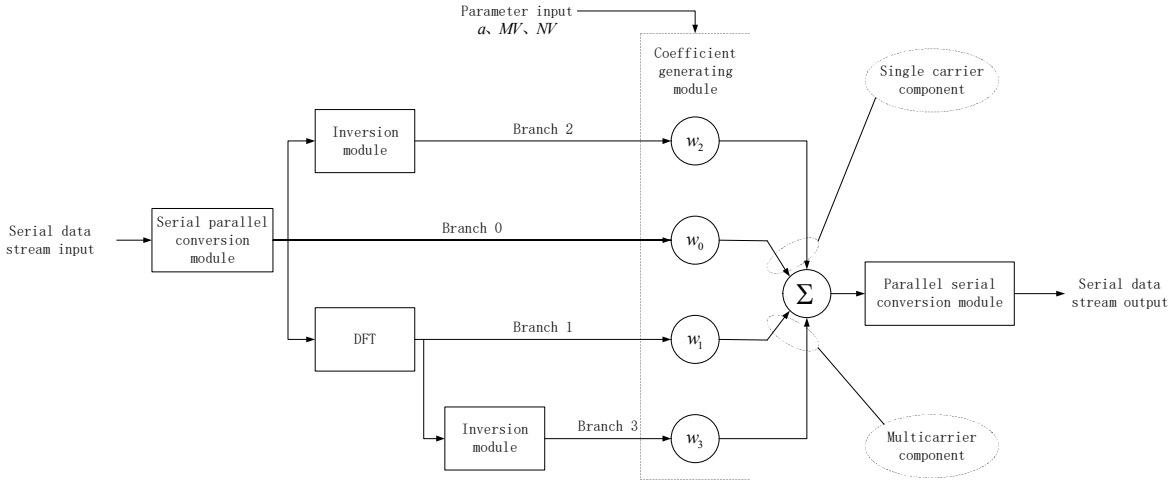

Figure 5. Physical implementation process of WFRFT.

In this paper, a physical layer constellation encryption security system is proposed, as shown in figure 6. In the constellation encryption mixed carrier modulation system, the signal constellation diagram is encrypted through random phase rotation while WFRFT-based mixed carrier modulation is adopted. After the signal passes the baseband modulation, the α order WFRFT modulation of M points sends the signal to the physical layer encryption module for random phase constellation rotation, and sends the signal to the channel. The receiver first uses the phase information generated by the random phase generator to unscramble and rotate the encrypted signal, removes the encrypted information after channel equalization, and sends the signal synchronously to the signal station after the $-\alpha$ order WFRFT demodulation of M point.

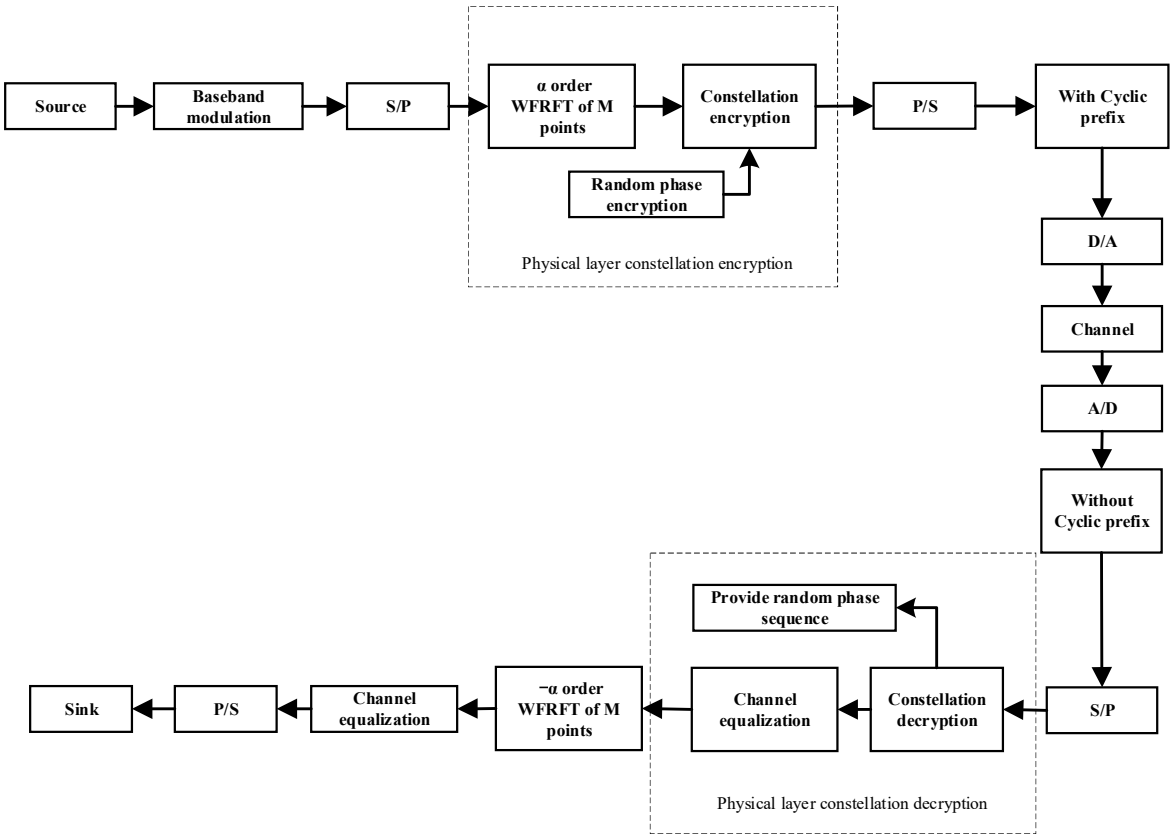

Figure 6. Flow chart of physical layer encryption scheme.

3. Simulation Analysis

As can be seen from figure 7, with the increase of weighted parameters, the safety capacity of the system also increases. The reason is that with the increase of weighted parameters, the chaotic degree of the constellation diagram of WFRFT modulation encryption signal in the system also gradually increases, and the non-cooperative party cannot determine the correct useful information during the demodulation process. However, when the weighted parameter is 1, the modulation mode turns into traditional OFDM modulation, and the current message interception method for OFDM is very mature, so the weighted parameter which close to 1 should not be selected. Through traversing the calendar, 0.91 will be selected as the parameter to analyze the reliability of the system.

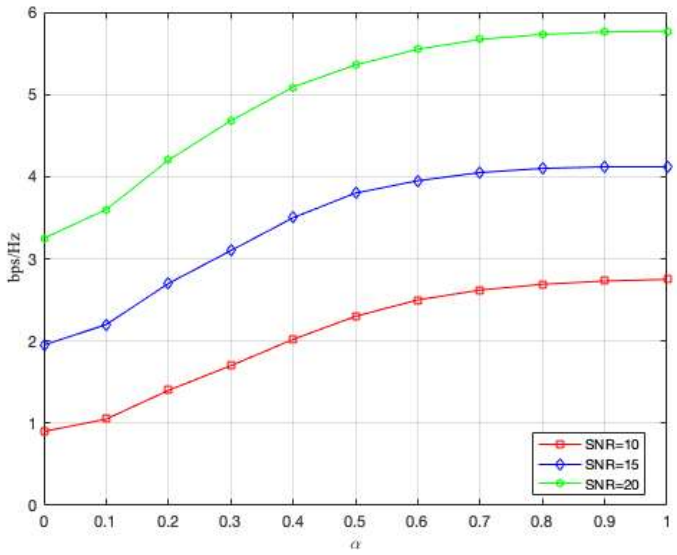

Figure 7. The relationship between weighted parameters and system safety capacity.

It can be seen from figure 8 that when the signal-to-noise ratio is 15dB, the eavesdropper's bit error rate is close to 0.5 on the premise that the eavesdropper cannot know the modulation mode, so it is basically impossible to intercept the transmitted message. In the case that the eavesdropper knows the modulation mode but cannot know the parameters, the bit error rate can be reduced to 10^{-2}; at this time, the error rate of the legitimate recipient is close to 10^{-5}, meeting the communication requirements.

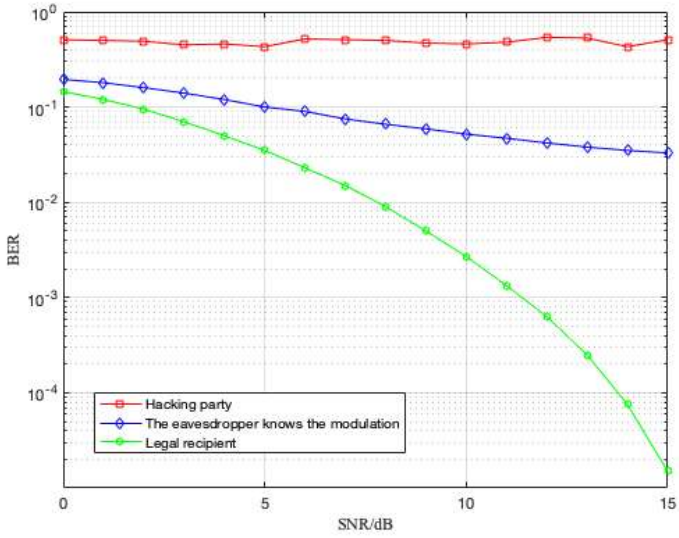

Figure 8. The performance under optimized weighted parameter.

4. Conclusion

This paper proposes a physical layer constellation encryption technology based on WFRFT. By using the constellation aliasing feature of WFRFT, the interception of messages by eavesdropping parties can be further suppressed. Taking the reliability and security capacity of the communication system into comprehensive consideration, the low interception performance of the system can be better realized through the selection of weighted parameters, it will provide the possibility to secure messages on the physical level.

Acknowledgments
This work was financially supported by cooperative fund for state key laboratories (KX162600022).

References
[1] WANG L, GUAN X R, LIN Z, et al. An Overview of Physical Layer Security in Wireless Networks [J]. Journal of Military Communication Technology, 2015, 36 (03): 54-60.
[2] ZHANG Y X, LIU A J, WANG Y G, et al. Physical Layer Security in Satellite Communications [J]. Telecommunication Engineering, 2013, 53 (03): 363-370.
[3] XI C C, GAO Y Y, SHAN N, et al. Intorduction of Signal Constellation Design Approach for Physcial Layer Security [J]. Journal of Chinese Computer Systems, 2018, 39 (12): 2675-2680.
[4] Ma R, Dai L, Wang Z, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion [J]. IEEE Transactions on Consumer Electronics, 2010, 56 (3): 1328-1332.
[5] Han C, Hashimoto T, Suehiro N. Constellation-rotated vetor OFDM and its performance analysis over Rayleigh fading channels [J]. IEEE Transactions on Communications, 2010, 58 (3): 828-838.
[6] Ma R, Wang Z, Yang Z. Improving physical layer security using APSK constellations with finite-alphabet inputs [C]. 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013: 149-152.
[7] Pappu R, Recht B, Taylor J, et al. Physcial one-way functions [J]. Science, 2002, 297 (5589): 2026-2030.
[8] Chaudhary S, Kapoor R, Sharma A. Empirical Evaluation of 4 QAM and 4 PSK in OFDM-based Inter-Satellite Communication System [J]. Journal of Optical Communications, 2017.
[9] Mei L, Sha X, Zhang N. Covert communication based on waveform overlay with Weighted Fractional Fourier Transform signals [C] // IEEE International Conference on Wireless Communications, NETWORKING and Information Security. IEEE, 2010: 472-475.
[10] XU J, GAO B J, LUO Y L, et al. Physical Layer Security Aalgorithm Based on Parallel Random Phase Rotation [J]. Application of Electronic Technique, 2013, 39 (01): 143-146.
[11] ZHOU J, ZHOU Q, WANG X. Physical-Layer Security Transmission in HF Communications [J]. Communications Technology, 2019, 52 (03): 692-695.
[12] Pöpper C, Tippenhauer N O, Danev B, et al. Investigation of signal and message manipulations on the wireless channel [C]. European Conference on Research in Computer Security, Spring-Verlag, 2011: 40-59.