Vector Perturbation-Based Multi-dimensional Domain Physical Layer Encryption System

YiChao Huang(✉) and KunPeng Zhao

Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China
532241524@qq.com, kp.zhao@outlook.com

Abstract. Different from cryptography encryption, physical-layer encryption(PLE) can provide a higher level of data security by adjusting a structure of signal, and the process of adjustment serves as the key. Based on vector perturbation, a multi-dimensional PLE is proposed in this paper, which is performed to change the structure of signal transmitted in time and frequency domains by introducing a set of phase perturbation sequences as a secret key. This key sequence utilizes a phase-shift property of rotation factor, which never changes the spectral structure of the original signal and prevents SNR loss. Furthermore, an impact of encryption by time and frequency vector perturbation is analyzed on constellation. To ensure the peak to average ratio (PAR) of encrypted waveforms, a circular constellation with a certain width is developed. Verified by simulations, the proposed scheme has no impact on the detection performance of the collaborative receiver.

Keywords: Physical Layer Encryption · Constellation Rotation · Frequency Domain Encryption

1 Introduction

Nowdays, more and more people begin to pay attention to privacy protection, security of data transmission turns to be increasingly important in wireless communication systems. Traditional methods mainly focuses on cryptography encryption [1], but its drawback is obvious that cannot prevent eavesdroppers from demodulation for signal.

As a development of artificial intelligence and supercomputer technology, the risk of data being cracked is increasing. Physical-layer encryption(PLE) can provide a higher level of data security by adjusting a structure of signal, and its operation of adjustment serves as the key [2,3]. Current main works about PLE focus on phase encryption [4], amplitude encryption [5], subcarrier confusion [6].

Ma uses a key composed of a set of time-domain rotation factors. A random phase shift is produced for each modulation symbol under this secret key, and the

J. Wang (Ed.): MobiMedia 2023, LNICST 576, pp. 199–209, 2025.
https://doi.org/10.1007/978-3-031-60347-1_17

encrypted signal constellation is a circle [7]. Following this idea, Mao multiplies each symbol for encryption in the time domain by a random sequence value between 0 and 1. This will produce amplitude-phase changes, which can enhance the security of system but brings BER loss [8]. Zhang proposed an encryption algorithm based on chaotic sequences for OFDM systems [9]. It uses chaotic theory to make a new map of amplitude and phase of QAM symbols. However, the change of amplitude must inevitably bring a loss of signal energy. Similarly, Wen proposed an amplitude-phase encryption algorithm. To obscure the signal's spectrum. The signal is replaced by the signal's second-order intermodulation difference frequency component [10]. So that eavesdroppers are unable to recover the signal spectrum and cannot correctly demodulate the encrypted signal.

Furthermore, some researchers have utilized an uniqueness and reciprocity of wireless channels as a security key of transmission. Some use shared channel state information (CSI) as an initial seed to generate chaotic sequences [11], which rotates constellation of modulation symbols to make it difficult for demodulation by eavesdroppers. Meng proposes a designing of constellation encryption based on chaotic sequences and RSA algorithm [12]. By combining chaotic sequences and RSA, a map of constellation is generated for encryption. Although eavesdroppers cannot obtain the information key correctly, constellation has a regulation of cycle of change, posing a potential risk of decipher. In a study by Amber Sultan's team [13], an encryption algorithm using chaotic sequences as keys was proposed, which performs XOR operations between data symbols and chaotic sequences for encrypting constellation . However, a kind of coding encryption exsits two problem: one is a possibility of loss of SNR, and the other is that a relationship between structure of constellation and PAPR has no explanation.

Therefore, this paper proposes a multi-dimensional domain encryption algorithm based on vector perturbation by introducing a set of phase perturbation sequences as the encryption key, the signal can be encrypted in both the time and frequency domains. This encryption has no change the signal's spectral structure, and utilizes a phase-shift characteristic of rotation factors to avoid a change of noise power.

The major contributions of this study are summarized as follows:

A novel algorithm of time-frequency phase encryption is proposed, which can solve a loss of SNR in comparison of signal amplitude variation in the conventional phase encryption scheme.

An expression of the time-domain encrypted signal is derived. Afterward, an impact of encryption by time and frequency vector perturbation is analyzed in constellation, and a designing of constellation is given in a constraint of a certain circular width.

2 Vector Perturbation Based on the Time-Frequency Domain

In this section, the basic idea and system model of physical layer encryption are first explained. After that, a time-frequency domain encryption system is

proposed. Finally, a specific time-domain expression of the frequency-domain encryption system is derived, and the impact of the frequency-domain encryption system on the time-domain signal is further examined.

Designing of Phase Perturbation in Time Domain. In previous work, many researchers have used constellation rotation to implement phase encryption. The commonly used time-domain phase encryption model is shown below:

$$s_e(n) = s(n) \cdot e^{j\phi_n}, 0 \leq n \leq N-1 \tag{1}$$

where N is the number of sampling points, $e^{j\phi_n}$ is the phase shift factor, the value of ϕ_n is usually restricted to the range $(0, 2\pi)$. $s(n)$ represents the signal before encryption, and $s_e(n)$ denotes after encryption.

The constellation diagram of the QPSK phase-based encryption system is shown in Fig. 3b. The red pentagram indicates the constellation of the encrypted signal, and the circle represents the constellation point of the encrypted signal.

Designing of Phase Perturbation in Frequency Domain. Based on the idea of phase encryption, we propose a frequency domain encryption algorithm. Since the frequency domain only adjusts the phase, it will not change the noise power spectral density in the frequency domain and will not affect the SNR. Finally, the specific time-domain expression of the encrypted signal in the frequency domain is derived. The effect of frequency-domain encryption on the time-domain signal is discussed.

The basic idea of frequency domain encryption is to convert the encrypted signal to the frequency domain and then perform secondary encryption on the frequency domain signal. The encryption method is the same as the time domain encryption method, and the phase encryption factor is introduced directly in the frequency domain:

$$S_e(k) = FFT[s_e(n)] \tag{2}$$

$$S_{ee}(k) = S_e(k) \cdot e^{j\theta_k} \tag{3}$$

where $S_e(k)$ is the spectrum of the time-domain encrypted signal $s_e(n)$, θ_k is the frequency-domain encryption factor having the same structure as the time-domain encryption factor, and $S_{ee}(k)$ is the spectrum of the time-frequency encrypted signal after frequency-domain encryption.

For the frequency-domain phase shift factor $e^{j\theta_k}$ mentioned in this paper. Where θ_k is specified as a periodic segmentation function that fills in random values between equal frequency intervals in one period and then performs M periods extensions to finally obtain a random phase that can cover the full frequency band. It is worth noting that the value of the random phase should be within $(0, 2\pi)$. The diagram of θ_k is shown in Fig. 1. where F_r is the length of a single period, F_s is the sampling frequency of the discrete system, and L is the number of phase shift factors in each period.

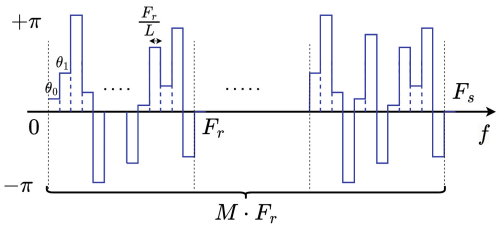


Fig. 1. Schematic diagram of the structure of the frequency-domain encryption sequence period extension sequence.

The specific expression within the first period is given by [14]:

$$P(k) = e^{j\theta_k}, l\frac{F_r}{L} \leq k \leq (l+1)\frac{F_r}{L}, 0 \leq l \leq L-1 \tag{4}$$

The periodicity of θ_k makes $P(k)$ have the same periodicity, i.e., $P(k+mF_r) = P(k), 0 \leq m \leq M-1$. $p(k)$ The expression of the discrete Fourier transform of P(k) is given by:

$$P(k) = \sum_{n_\tau=0}^{N-1} p(n_\tau) e^{-j\frac{2\pi}{N}n_\tau k} \tag{5}$$

where $p(n_\tau)$ is the time-domain discrete value of $P(k)$. The formula for frequency-domain encryption can be expressed in the following format, using Eq. (3) as a starting point:

$$S_{ee}(k) = S_e(k) \cdot P(k) \tag{6}$$

By inverting its discrete Fourier transform, the final encrypted signal $s_{ee}(n)$ can be expressed in the time domain as:

$$\begin{aligned} s_{ee}(n) &= \frac{1}{N}\sum_{k=0}^{N-1} S_e(k)P(k)e^{j\frac{2\pi}{N}nk} \\ &= \frac{1}{N}\sum_{k=0}^{N-1} S_e(k)\sum_{n_\tau=0}^{N-1} p(n_\tau)e^{-j\frac{2\pi}{N}n_\tau k}e^{j\frac{2\pi}{N}n_k} \\ &= \sum_{n_\tau=0}^{N-1} p(n_\tau)\frac{1}{N}\sum_{k=0}^{N-1} S_e(k)e^{j\frac{2\pi}{N}(n-n_\tau)k} \\ &= \sum_{n_\tau=0}^{N-1} p(n_\tau)s(n-n_\tau) \end{aligned} \tag{7}$$

The final encrypted signal is expressed in the time domain by Eq. (7) , where N is the number of IFFT.

When P(k) consists of a sequence of M periods of length L, it can be written in the following form:

$$P(k) = \sum_{m=0}^{M-1} P_0(k) * \delta(k - mL) \tag{8}$$

where $P_0(k)$ is the first period. According to the Fourier transform property, the time domain signal $p(n)$ of $P(k)$ can be written as:

$$\begin{aligned} p(n) &= \sum_{m=0}^{M-1} p_0(n)\delta(n - mL) \\ &= \sum_{m=0}^{M-1} p_0(mL)\delta(n - mL) \end{aligned} \tag{9}$$

where $p_0(n)$ is the first period. The formula of key-loading can be written in the following form:

$$\begin{aligned} s_{ee}(n) &= s_e(n) * p(n) \\ &= \sum_{m=0}^{M-1} p_0(mL)\delta(n - mL) * s_e(n) \\ &= \sum_{m=0}^{M-1} p_0(mL)s_e(n - mL) \end{aligned} \tag{10}$$

Figure 2 shows the encryption process of the encryption system. It can be seen that each symbol is extended periodically. The period is L and the length is M. Interference from other symbols is present at the judgment point. The intensity of the interference is $p_0(mL)$ and the length is M. This interference affects the normal judgment of the code element. But the interference is controllable and receiver can restore the original signal $s_e(n)$ if it knows $p(n)$.

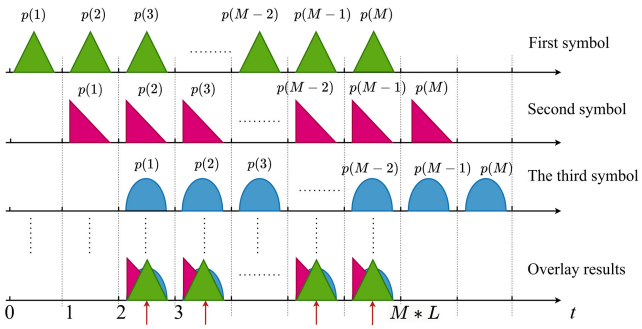


Fig. 2. Explanation of time domain signal expressions.

After the above analysis. It is found that the frequency domain phase perturbation changes the magnitude of the judgment point. Time-domain phase perturbation produces a rotation effect. The combination of the two schemes will make the constellation into a circular shape. Figure 3 shows the process of the constellation change. In Fig. 3c, the constellation becomes a ring. In this paper, the width of ring structure is denoted as Δr, which is the red arrow. It can be found that after the time-frequency double encryption. If eavesdroppers does not have the key, they cannot recognize the modulation method of the transmitter. So better data security can be obtained.

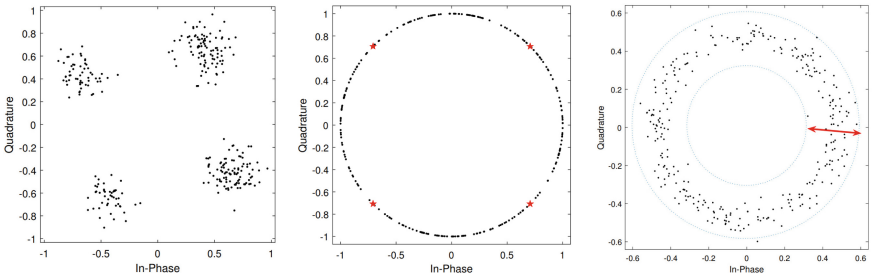


Fig. 3. (a) Constellation of frequency domain phase encryption. (b) Constellation of time domain phase encryption. (c) Constellation after time-frequency encryption.

Designing of Secret Key Under Circular Bandwidth Constraint of the Constellation. In this section, A method for solving Δr is first introduced. Then a secret key design method is proposed. The solution of Δr is as follows: When the signal is encrypted, its amplitude will be randomized. The length and number of periods of the phase shift factor do not change, only the value. and the resulting constellation is recorded. Subtract the minimum value from the maximum value of the radius in the constellation to get Δr. The formula is expressed as follows:

$$\Delta r = max\left\{max(|s_{ee}|) - min(|s_{ee}|)\right\} \tag{11}$$

where s_{ee} is the output signal after encryption. The next section describes how to determine the target encryption sequence.

The search process for the phase factor $e^{j\theta_k}$ is as in Algorithm 1. The expectation value of Δr is first given, and then a set of phase factors is randomly generated and loaded in this encryption system. And the constellation diagram of the judgment points after encryption by this system is found, and the corresponding Δr_i is found according to Eq. (11), and it is judged whether its value satisfies $\Delta r_i \in (a, b)$. If it satisfies, the obtained set of phase factors is the target secret key.

Algorithm 1: Target Key Search Algorithm

Input: The target ring band width $\Delta r \in (a, b)$, $S_e(k)$
Output: phase encryption factors $P(k)$

At the beginning, assume that $\Delta r \notin (a, b)$;
while $\Delta r_i \notin (a, b)$ **do**
  Generate a random set of $P(k)$;
  $S_{ee}(k) = S_e(k) \cdot P(k)$;
  $S_{ee}(n) = FFT[S_{ee}(k)]$;
  $\Delta r_i = max\{max(|s_{ee}|) - min(|s_{ee}|)\}$;
end
return Δr_i;

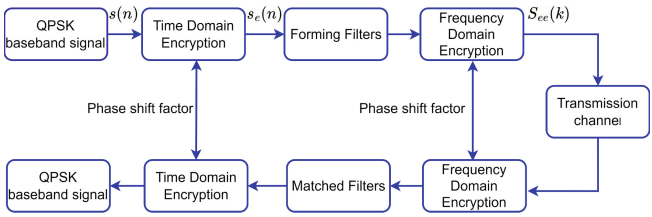


Fig. 4. Block diagram of the QPSK simulation of this encryption scheme.

3 Results and Discussion of the Simulation

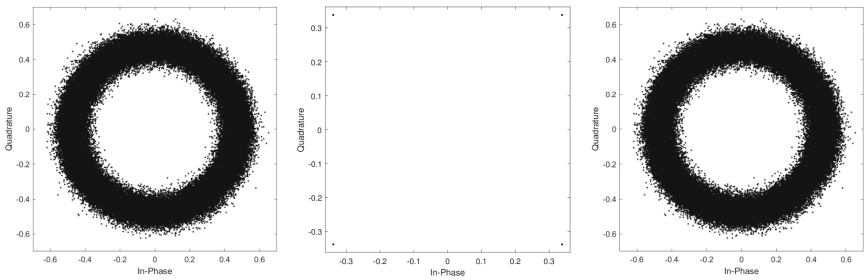
This section analyzes the encryption effect of the time-frequency domain encryption scheme. The encryption effect of the scheme is observed by comparing the changes of constellation diagrams before and after decryption. The encryption performance with different encryption factors is analyzed by comparing the PAPR of encrypted signals with different loop band widths Δr. The SNR losses are analyzed by comparing the BER of collaborators and eavesdroppers at different SNR. The simulation system structure of this encryption system is shown in Fig. 4.

Table 1. System parameter setting.

Simulation parameters	Value
Sampling rate	40 M
Signal Bandwidth	10 M
Modulation	QPSK
Symbols rate	8 M
Forming filter roll-off factor	0.5
Channel model	AWGN
SNR	0–10 dB

Firstly, QPSK baseband signal $s(n)$ is encrypted in the time domain phase to obtain the encrypted signal $s_e(n)$. It passes through a shaping filter and then undergoes frequency-domain phase encryption. Finally, the signal reaches the receiver through a Gaussian white noise channel. When the signal from the transmitter is received by the collaborator, frequency domain phase decryption is performed first. Then the decrypted signal is passed through a matched filter. Time domain decryption is performed immediately to obtain baseband signals. The encryption performance of this algorithm is evaluated by analyzing the BER, constellation, etc. of this simulation system.

In this paper, MATLAB is used as the simulation platform. Table 1 shows the simulation parameters used in the simulation to implement this cryptosystem. In particular, to observe the encryption effect of this scheme more visually. A comparison system has been purposely built. It is called the reference system(RS). RS has the same parameters as this simulation, but without any encryption measures applied.



(a) (b) (c)

Fig. 5. (a) The constellation of encrypted signals. (b) The constellation of the cooperators. (c) The constellation of the eavesdropper.

First, the constellation changes under noiseless conditions were analyzed. Figure 5 shows the constellation diagrams of the transmitter, collaborator, and eavesdropper, respectively. Figure 5a shows the constellations of the encrypted signal. The constellations are successfully scrambled and the signal is well hidden. The constellation is a circle. It is difficult for the eavesdropper to determine which debugging method is used, and it is difficult in demodulation in the first place.

Figure 5b shows the constellation plot after the decryption of the received signal from the collaborator in an ideal noise-free channel. The phase and amplitude of the signal are corrected, the constellation diagram is reconstructed losslessly, and the receiver can perform demodulation and judgment normally. Figure 5c shows the constellation diagram after decryption by the eavesdropper. Since the key is not obtained, the decrypted constellation diagram is still confusing.

Figure 6 shows the simulation plot of the PAPR distribution for different circular bandwidths. It can be seen that different Δr bring different PAPR distributions. The smaller Δr, the smaller PAPR losses of the encryption system. When

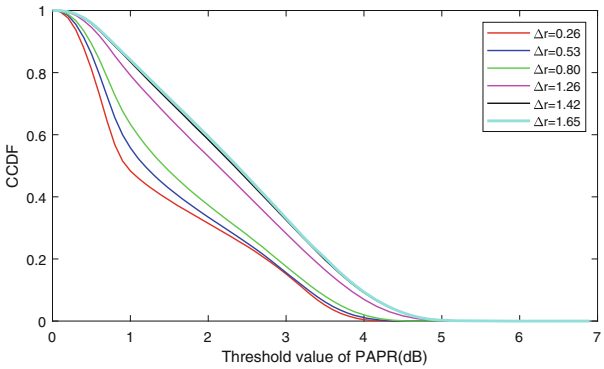


Fig. 6. Simulation curves of PAPR at different circular bandwidths.

the width is 1.65, the maximum PAPR is 5 dB. and when the loop band width is 0.26, the maximum PAPR is 4 dB, which is a 1 dB reduction.

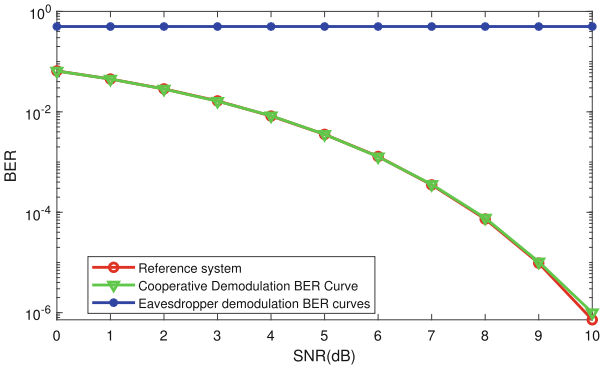


Fig. 7. BER analysis of the cooperator and eavesdropper sides is performed.

Figure 7 is the BER curve of this simulation. The image shows that the collaborator can decrypt correctly. Compared with RS, there is no BER loss at low SNR. The BER loss at high SNR crosses 0.1 dB. However, the BER of the eavesdropper is around 0.5. Therefore, the algorithm proposed in this paper can achieve encrypted communication. Compared with the conventional QPSK system without the introduction of encryption mechanism, this algorithm has no loss of SNR.

4 Conclusion

Based on both perturbation of time and frequency, a key from conversion of waveform is proposed for physical encryption, which can design a ring shape with controllable ring width. By derivation of frequency vector perturbation, it is found that the operation in frequency domain is similar to a long inter-symbol or inter-sampling point interference, and there is an advantage of encryption proposed is no loss of SNR in comparison of existing encryption of frequency perturbation. Besides, a relationship between width of ring and PAPR is analyzed by simulation, which is the higher PAPR as the wider width of the ring.

References

1. Xu, D., Liu, L., Zhang, N., Dong, M., Leung, V.C.M., Ritcey, J.A.: Nested hash access with post quantum encryption for mission-critical IoT communications. IEEE Internet Things J. **10**, 12204 (2023)
2. Li, W., Mclernon, D., Lei, J., Ghogho, M., Zaidi, S.A.R., Hui, H.: Cryptographic primitives and design frameworks of physical layer encryption for wireless communications. IEEE Access **7**, 63660–63673 (2019)
3. Hou, Y., Li, G., Dang, S., Hu, L., Hu, A.: Physical layer encryption scheme based on dynamic constellation rotation. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), pp. 1–5. IEEE (2022)
4. Sultan, A., Yang, X., Hussain, S.B., Hu, W.: Physical-layer data encryption using chaotic constellation rotation in OFDM-PON. In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 446–448 (2018)
5. Zhang, C., Yan, Y., Wu, T., Zhang, X., Wen, G., Qiu, K.: Phase masking and time-frequency chaotic encryption for DFMA-PON. IEEE Photonics J. **10**(4), 1–9 (2018)
6. Naderi, S., da Costa, D.B., Arslan, H.: Joint random subcarrier selection and channel-based artificial signal design aided PLS. IEEE Wirel. Commun. Lett. **9**(7), 976–980 (2020)
7. Ma, R., Dai, L., Wang, Z., Wang, J.: Secure communication in TDS-OFDM system using constellation rotation and noise insertion. IEEE Trans. Consum. Electron. **56**(3), 1328–1332 (2010)
8. Xiang-ning, M., Kai-jia, L., Hao, L.: A physical layer security algorithm based on constellation. In: 2017 IEEE 17th International Conference on Communication Technology (ICCT), pp. 50–53. IEEE (2017)
9. Zhang, X., Zhang, S., Shan, X., Ma, L.: A physical layer encryption scheme based on chaotic maps in OFDM systems. In: 2020 27th International Conference on Telecommunications (ICT), pp. 1–6 (2020)
10. Zhao, W., Li, B., Tang, P., Lu, Z.: A low probability of interception method based on nonlinear transformation of channel transmission characteristic. Adv. Comput. Commun. **3**(1), 1–15 (2022)
11. Xu, Z., Yuan, T., Gong, Y., Lu, W., Hua, J.: Achieving secure communication through random phase rotation technique. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 2073–2078. IEEE (2017)

12. Quan, M., Jin, Q., Ba, B., Zhang, J., Jian, C.: Constellation encryption design based on chaotic sequence and the RSA algorithm. Electronics **11**(20), 3346 (2022)
13. Sultan, A., Yang, X., Hussain, S.B., Hu, W.: Physical-layer data encryption using chaotic constellation rotation in OFDM-PON. In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 446–448. IEEE (2018)
14. Proakis, J.G.: Digital Communications. McGraw-Hill, Higher Education, New York (2008)