Encryption Technology of Optical Communication Network Based on Artificial Intelligence Technology

Ying Wang[1,*], Xiaojun Zuo[1], Yuling Guo[1], Huiying Liu[1]
and Jianchun Zhou[2]

[1] *State Grid Hebei Electric Power Research Institute, Shijiazhuang, China*
E-mail: dyywangy@163.com; hbszxj01@163.com; guoyuling18@126.com; liuhuiying@126.com; xintong-zhoujc@epri.sgcc.com.cn
[2] *China Electric Power Research Institute Co., Ltd, Beijing, China*
[*] *Corresponding Author*

Received 28 December 2023; Accepted 21 February 2024

Abstract

At present, research on enhancing information transmission security by addressing the two key issues of time delay signal elimination and key space expansion in chaotic secure communication systems has become a hot topic. In order to improve the encryption effect of optical communication network, this paper analyzes the encryption technology of optical communication network with AIT (artificial intelligence technology), designs the encryption scheme of optical communication network with the help of AIT, and takes the digital random sequence as the key. Moreover, this paper uses the digital signal processor to control the arbitrary wave generator to generate multi-ary step square wave, modulate the optical feedback and realize the highly random change of external cavity delay, thus eliminating the long external cavity delay information. This article proposes a chaotic secure communication system using digital sequences as keys and external cavity optical feedback, a device for forming a chaotic source through arbitrary

Journal of Cyber Security and Mobility, Vol. 13_4, 633–656.
doi: 10.13052/jcsm2245-1439.1343

wave phase modulation and single loop feedback, and a chaotic secure communication system with single feedback key phase modulation and injection synchronization. At the same time, this paper proposes a system scheme using single-loop optical feedback phase modulation, the CS(chaotic signal) with complex dynamic behavior is output, and the time-delay signal is effectively eliminated. This paper analyzes the strength and phase information of CS by autocorrelation and mutual information technology, and verifies the effect of optical communication network encryption technology. Through the analysis of experimental results, it can be seen that the optical communication network encryption technology based on AIT proposed in this paper can effectively improve the encryption effect of optical communication network. The algorithm model camera proposed in this article can be used in subsequent practice to improve communication encryption performance

Keywords: Artificial intelligence, optical communication, encryption technology, key.

1 Introduction

Traditional information encryption technology mainly uses mathematical algorithms as encryption schemes, which are mainly divided into symmetric encryption and asymmetric encryption. Meanwhile, both sides of legitimate communication need to use the same algorithm to generate the same key with the seed and realize the key exchange. The sender uses the negotiated key and a specific encryption algorithm (such as AES (Advanced Encryption Standard), SM4 (Symmetric encryption algorithm)) to convert the plaintext information into ciphertext and send it. Then, the receiver restores the received secret text to plaintext information with the same key and encryption algorithm.

The public key used for encryption and the private key used for decryption come from complex mathematical problems such as factorization of large numbers (RSA) and elliptic curve (ECC). This avoids the transmission of keys in the channel and to some extent alleviates the security risks brought by the sending and storage of keys in symmetric encryption. Reducing the efficiency of encryption. But whether it is symmetric encryption or asymmetric encryption, the main source of its security is the complexity of mathematical problems. With the increasing demand for high-speed and high-capacity data encryption by users, it is necessary to generate and send keys with the same length as the information. This not only poses dual challenges to encryption efficiency and current communication networks. Moreover, with the improvement of computing power in electronic computers, the improvement of efficiency in solving mathematical problems through artificial intelligence and deep learning, and the rise of quantum computers, encryption schemes based on mathematical algorithms are constantly being challenged [1].

PL (Physical layer) security is a technology that improves the security of communication systems based on the inherent randomness of communication transmission channels. It emerged as a supplementary technology to the upper level security based on traditional encryption technology, also known as password technology, and is the first line of defense to effectively prevent eavesdroppers from stealing communication information. It can greatly enhance the security performance of the entire system. In the PL security system, the transmitter utilizes the similarities and differences between different receiver channels, using signaling or encoding schemes to ensure reliable reception by the intended receiver, while preventing non intended or unauthorized receivers from deciphering the sent messages. Because uploading optical signals on the VLC(Visible Light Communications) channel does not require fiber optics or any type of waveguide, PL security has become an important means of protecting VLC communication from eavesdropping [2].

In the performance analysis of VLC PL security, reference [3] obtained a lower bound for the secure capacity of single input single output (SISO) channels, analyzed the upper and lower bounds for the secure capacity of key transmission in SISOVLC scenarios, and analyzed the multi input single output (MISO) VLC key transmission strategy. Reference [4] adopts beamforming and interference techniques to improve the confidentiality of MISOVLC systems in the presence of multiple eavesdroppers. Using the theory of random geometry, considering the randomness of the positions of legitimate receivers and eavesdroppers, the confidentiality performance of VLC systems with legitimate receiver and eavesdropper groups was studied, and closed form analytical expressions for SOP and ASC were derived. However, compared to traditional RF communication, the dynamic range of the emission power of the LED at the emission end of VLC is limited, and excessive signal power can lead to shear effects. Therefore, in addition to traditional average power constraints, VLC transmission systems also have certain peak power constraints. Reference [5] points out that when the transmission limit is not the average power but the instantaneous peak power, at most an expression in the form of upper and lower limits can only be obtained. Therefore, it is not difficult to find that the PL security performance analysis of VLC systems is still an unresolved issue. Reference [6] introduces eavesdropping channels and defines confidentiality capacity as the maximum error free rate difference between legitimate users and eavesdroppers. When the signal power received by legitimate users is greater than that received by eavesdroppers, the confidentiality rate of the eavesdropping channel is non-zero. However, due to channel fading, this non zero confidentiality condition may not always be applicable in practical scenarios. In order to cope with unreliable channels, transmitters can use multi antenna beamforming technology. Although the PL security of multi antenna RF systems has been widely studied, these methods cannot be directly applied to VLC systems. Compared with research on RF systems, there is relatively little literature on the PL security of VLC systems. Reference [7] adopted a probability measure of non zero confidentiality capacity and analyzed the different confidentiality capacities between legitimate users and eavesdroppers. Reference [8] found that under amplitude constraints, the confidentiality ability of Gaussian eavesdropping channels can be achieved through discrete input distribution. The lower and upper limits of the confidentiality capacity of Gaussian eavesdropping channels are given, and suboptimal and robust beamforming are designed in terms of confidentiality rate.

In recent years, the PL security encryption of VLC has also received great attention from the research community. Although there are no detailed research results, some literature has proposed preliminary methods for VLC PL encryption. Reference [9] utilized a public key encryption scheme (i.e. RSA algorithm) to encrypt broadcast beam signals, encrypting the entire frame of VLC's IEEE802.15.7 standard at the PL. RSA, based on the principles of digital theory, is considered one of the most secure traditional data protection encryption methods. However, RSA requires an independent key distribution system, which results in extremely high complexity and therefore leads to the proposed model requiring too much power. The designed 8-bit and 16-bit keys are considered too short to truly achieve confidentiality for a true encryption system. Therefore, the proposed solution cannot be implemented in actual VLC systems. Reference [10] designed a security model using zero guided (zero forced) precoding technology, claiming that it can eliminate the reception of eavesdroppers and fully ensure the communication of the target in the presence of eavesdroppers. Add artificial noise to the transmission signal to prevent eavesdroppers from receiving and improve achievable confidentiality. However, adding artificial noise to unauthorized users is not feasible for a true multi user VLC system, as this process may affect other users

Reference [11] used Zero Forcing (ZF) technology in VLC systems to make the useful signal eavesdropped by eavesdroppers zero, and calculated the secure transmission rate. On the basis of ZF precoding, the precoding matrix was further optimized and the fairness problem in multi user state was studied. We optimized the precoding matrix for different fairness performance indicators, obtained the achievable secure transmission rate of the system, and demonstrated that its performance is superior to the ZF precoding method, but the complexity slightly increases. Reference [12] proposes a precoding matrix to achieve secure transmission of user signals. The average secure transmission rate was calculated when the location of the eavesdropper is random and the signal follows a truncated Discrete Generalized Normal (TDGN) distribution. Reference [13] studied the design of secure encoding based on polarity codes, which ensures both PL security and transmission reliability. However, this scheme requires feedback channel gain and complicates the communication process. Reference [14] proposed a VLC beamforming scheme based on reinforcement learning (RL), and proposed dynamically selecting beamforming parameters based on Markov decision processes. In addition, deep reinforcement learning was proposed to improve learning rate and system performance. Unlike beamforming based on the location of the eavesdropper, reference [15] uses statistical data from the eavesdropper to perform beamforming and proposes a scheme to approximate the beamforming method by selecting the LED closest to the user for communication, and derives the interruption probability in both cases. Reference [16] established a scrambling matrix with user location and angle information, which is iteratively uncorrelated with MIMO (Multiple Input Multiple Output) channels. Due to the fact that users are aware of various user information, they are not affected by the scrambling matrix. Eavesdroppers do not know user information, and eavesdroppers cannot eavesdrop on information in a short period of time.

Reference [17] proposes methods such as AP(Accesspoint) collaboration to ensure security. In the case of AP collaboration and AP non collaboration, the closed forms of interruption probability and traversal secure transmission rate were derived. And establish a disk shaped confidential area near the AP, where there are no eavesdroppers, which improves the security performance of users. Reference [18] first established a protected area without eavesdroppers. Furthermore, the closed form expressions for the lower bounds of the average secure transmission rate and the probability of secure interruption were derived when the positions of users and eavesdroppers were uniformly distributed under unknown channel gain. Reference [19] proposes the use of angle diversity transmitters and the establishment of secure regions to improve VLC security. Narrow beam data transmission can effectively avoid message leakage. Moreover, in the confidential area, the optical AP can detect eavesdroppers, improving communication security performance.

This paper analyzes the encryption technology of optical communication network with AIT(artificial intelligence technology), designs the encryption scheme of optical communication network with the help of AIT, and takes the digital random sequence as the key. Moreover, this paper uses the digital signal processor to control the arbitrary wave generator to generate multi-ary step square wave, modulate the optical feedback and realize the highly random change of external cavity delay, thus eliminating the long external cavity delay information

The innovation of this article compared to traditional literature lies in proposing some simpler and more effective solutions. Using a digital random sequence as a key, the arbitrary wave generator is controlled by a digital signal processor to generate a multi band step square wave, which modulates the time of the laser external cavity optical feedback and achieves highly random changes in the external cavity delay, thereby eliminating the long delay information of the external cavity.

This paper analyzes the encryption technology of optical communication network with AIT, and designs the encryption scheme of optical communication network with the help of AIT, so as to find a scheme to improve the security of optical communication network.

2 Encryption of Optical Communication Network

A single loop optical feedback system using quaternary level sequence phase modulation is proposed, which is simple and easy to operate. By adjusting and optimizing laser parameters such as feedback intensity, modulation frequency, and modulation depth, chaotic laser source signals with time delay information suppression can be generated.

2.1 Two-way CSC (Chaotic Secure Communication)

The digital random sequence is used as the key, and the arbitrary wave generator is controlled by the digital signal processor to generate multi-ary step square wave, which modulates the optical feedback in time, and realizes the highly random change of external cavity delay, thus eliminating the long external cavity delay information. Random digital sequences with different

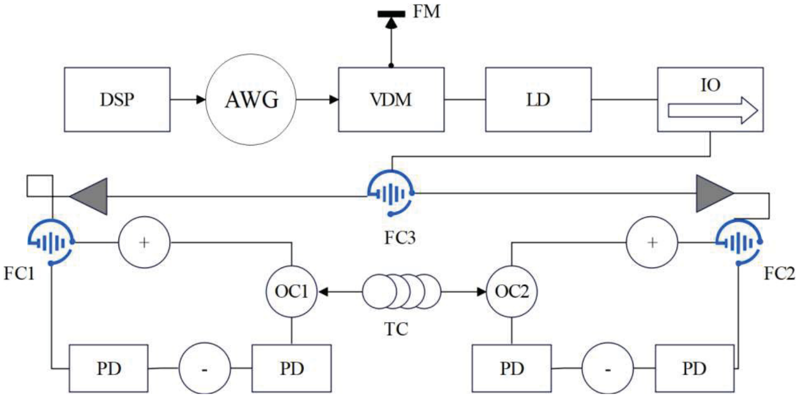


Figure 1 Schematic diagram of digital key and optical feedback bidirectional CSC.

lengths can be generated by computer, and the key space of its communication system is significantly expanded. When the chaotic carrier signal does not have accurate delay information, the attacker cannot reconstruct the symmetrical operation conditions and demodulate the accurate data.

Figure 1 illustrates the process of bidirectional CSC in the form of schematic diagram. The laser outputs high-dimensional CSs. The process of CL (chaotic light) formed by random feedback delay can be described by L-K equation as follows [20]:

$$\frac{dN}{dt} = \frac{I}{eV} - \frac{N}{\tau_n} - G(N,S) \tag{1}$$

$$\frac{dS}{dt} = \frac{\beta\Gamma N}{\tau_n} + \Gamma G(N,S)S - \frac{S}{\tau_P} + 2k_{cf}\sqrt{S(t)S(t-\tau)}\cos(\theta(t)) \tag{2}$$

$$\frac{d\Phi}{dt} = \frac{1}{2}\alpha\left(\Gamma G(N,S)S - \frac{1}{\tau_P}\right) - 2k_{cf}\sqrt{\frac{S(t-\tau)}{S(t)}}\sin(\theta(t)) \tag{3}$$

$$G(N,S) = \frac{g(N-N_0)}{(1+\varepsilon S)} \tag{4}$$

$$\theta(t) = \omega_{th}\tau + \Phi(t) - \Phi(t-\tau) \tag{5}$$

Among them, Equations (1)–(3) are respectively the rate equations of carrier density, photon density and phase. I is the pump current, e is the charge quantity, V is the active region volume of the laser cavity, τ_n is the carrier lifetime, τ_P is the photon lifetime, g is the differential gain coefficient,

N_0 is the transparent carrier density, ε is the saturation coefficient, β is the spontaneous emission factor, Γ is the confinement factor, α is the linewidth enhancement factor, k_{cf} is the feedback rate. Equation (5) represents the relative phase of feedback introduction, ω_{th} is the output angular frequency, τ is the external cavity optical feedback time. In this paper, CL with complex dynamics is output through the random delay feedback of light in the external cavity.

Among many methods for extracting CT(chaotic time) delay signals, autocorrelation and mutual information are the most insensitive and robust technologies to noise signals. By using autocorrelation function and delay mutual information technology to extract the time delay characteristics of CT series, it is proved whether there are obvious time delay peak signals in the two curves, thus confirming whether the CT delay signals are eliminated. The expressions for autocorrelation function (ACF) and delayed mutual information (DMI) are defined as follows:

$$ACF(\Delta t) = \frac{\langle [P(t) - \langle P(t) \rangle][P(t-\Delta t) - P(t)] \rangle}{[\langle P(t) - \langle P(t) \rangle \rangle]^2} \tag{6}$$

$$DMI(\Delta t) = \sum_{P(t)P(t-\Delta t)} \phi(P(t), P(t-\Delta t)) \times \ln \frac{\phi(P(t), P(t-\Delta t))}{\phi(P(t))\phi P(t-\Delta t)} \tag{7}$$

In the above two equations, Δt is the time delay, $P(t) = |E(t)|^2$ is the optical power of CT series, $\langle\ \rangle$ is the average information, $\phi(A, B)$ is the joint distribution probability density, and the corresponding $\phi(A)$ and $\phi(B)$ are the edge distribution probability density respectively. Autocorrelation function is used to delay mutual information is an information measure of the correlation between two event sets. Using these two techniques, the peak signal of feedback delay can be determined, thus proving whether the delay information is eliminated. If delay mutual information curve, it shows that the chaotic feedback time delay signal is effectively eliminated.

2.2 Delay Signal Cancellation

Compared with the photoelectric feedback scheme, the all-optical feedback scheme is simple in structure and easy to integrate into a chaotic laser optical chip. From the point of view of CL source, many schemes for suppressing time-delay signals have been proposed. In the single feedback system, the CT-delay signal can be eliminated by optimizing the feedback intensity

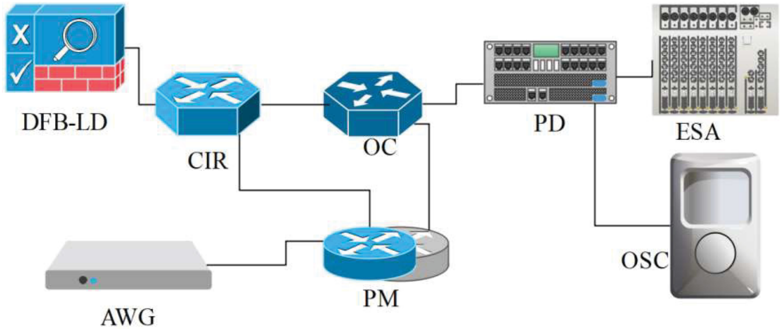


Figure 2 Schematic diagram of CL formed by optical feedback arbitrary wave phase modulation.

and setting the appropriate injection current. Improved feedback schemes, including double feedback, modulated multi-feedback, fiber Bragg grating feedback, chirped fiber Bragg grating feedback, random fiber Bragg grating feedback, scattering feedback and feedback loop with dispersion modulation, are proposed to eliminate CT delay information. For the above scheme, the suppression of time delay signal is confirmed only by analyzing the intensity time series of chaotic laser signal. However, in all-optical feedback system, phase plays an important role in the identification of time-delay signals. In order to overcome this shortcoming, a double-loop fast phase modulation feedback scheme for pseudo-random sequences is proposed, and the CS strength and phase information are analyzed, which proves that CT-delay signals can be effectively eliminated.

Figure 2 illustrates the process of CS formed by optical feedback arbitrary wave phase modulation in a schematic diagram. DFB(Distributed Feedback) laser takes 1550 nm as the central wavelength to output continuous light. When the light enters the optical circulator. Among them, one path is returned to the optical circulator through external optical feedback phase modulation, and then CSs with complex dynamic characteristics are output. The arbitrary wave generator outputs an arbitrary wave signal and acts on the phase modulator to modulate the phase of the FI(feedback light). The other CS enters spectrum analyzer and oscilloscope through photoelectric detector to detect and analyze the CS in real time.

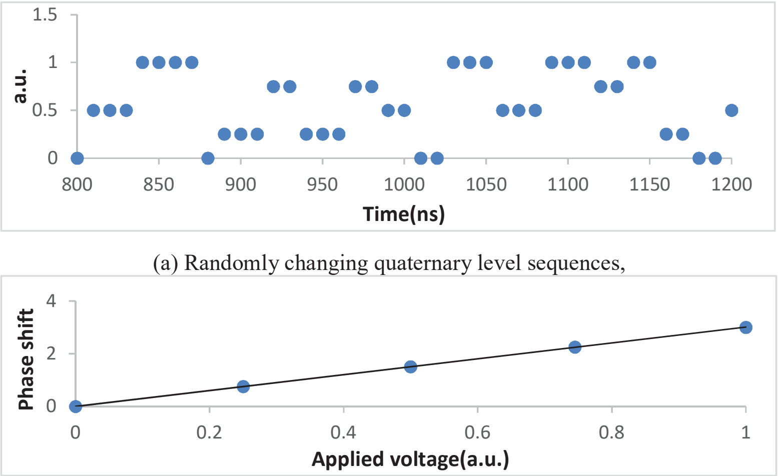
$$\frac{dE(t)}{dt} = \frac{1}{2}(1 + i\alpha)\left[G(t) - \frac{1}{\tau_p}\right] E(t) + kE(t-\tau)\exp(-i\omega\tau + i\phi_m(t)) \tag{8}$$

$$\frac{dN(t)}{dt} = \frac{I}{q} - \frac{1}{\tau_n} N(t) - G(t)|E(t)|^2 \tag{9}$$

$$G(t) = \frac{g[N(t) - N_0]}{1 + \varepsilon |E(t)|^2} \tag{10}$$

Among them, E is the strength of the compound power field, N is the density, g is the micro-company gain coefficient, α is the line width enhanced factor, N_0 is a transparent load density, q is a charge and electricity, and τ_p is the photon life, τ_n is the carrier life, I is a laser pump current, ω is the angle frequency output by the semiconductor laser, k is the feedback strength, ε is the gain saturation coefficient, τ is the feedback delay, and $\phi_m(t)$ is the phase modulation function.

Quaternary level sequence is used as arbitrary wave modulation signal. Figure 3(a) shows a randomly generated quaternary level normalized sequence signal, which conforms to the balanced code characteristics, and each level can be represented by four binary digital codes (0001, 0010, 0011, 0100). Figure 3(b) represents the functional relationship between phase change and modulation voltage, and it can be seen from the diagram that there is a linear relationship between them. When randomly changing quaternary level sequence acts on the phase modulator, it will inevitably cause the corresponding phase change of FI.



(a) Randomly changing quaternary level sequences,

(b) Functional relationship between modulation voltage and phase change

Figure 3 Quaternary modulation voltage and corresponding phase change.

2.3 CSC

In this paper, the key to phase modulate the FI, and the CS with complex dynamic behavior is output. Therefore, the proposed system scheme has enhanced improvement significance.

Chaotic system adopts chaotic injection synchronization, which ensures chaotic comparison synchronization and information demodulation synchronization at the receiving end. The information is modulated in chaotic carrier wave and effectively demodulated and output at the receiving end. By comparing the synchronization of two CSs and the bit error rate of demodulation output information in different channel signal-to-noise ratios, two kinds of information encryption methods, chaotic information modulation and chaotic hiding, are studied.

Figure 4 illustrates the schematic diagram of a CSC device with phase modulation optical feedback of a single loop feedback key. The phase modulated optical feedback is returned to the optical circulator and the optical fiber coupler to output CL, and then the information is loaded into the chaotic carrier wave and reaches the receiving end through the transmission channel. The phase modulation parameters of laser output and feedback are the same as those of transmitter. When CSs pass through optical fiber coupler, one signal is injected into feedback optical signal through variable attenuator, one signal is used as comparison signal, and two CLs pass through photodetector respectively to demodulate and output original information.

The FI output CS using multi-ary phase modulation and the CSC process is described by L-K equation as follows:

$$\begin{aligned}\frac{dE_A(t)}{dt} &= \frac{1}{2}(1+i\alpha)\left[G(t)-\frac{1}{\tau_p}\right]E_A(t)\\ &\quad + kE_A(t-\tau)\exp(-i\omega\tau+i\phi_m(t)) \qquad (11)\end{aligned}$$

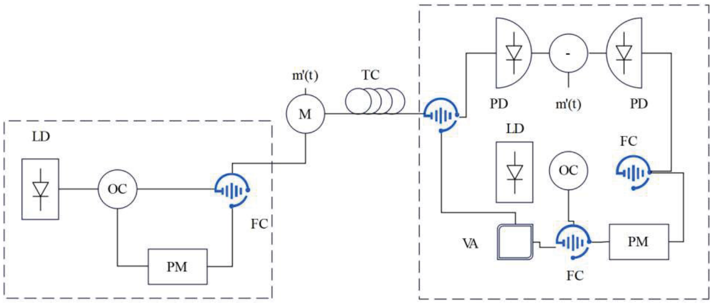


Figure 4 Schematic diagram of CSC device with phase modulation of single feedback key.

$$\frac{dE_B(t)}{dt} = \frac{1}{2}(1+i\alpha)\left[G(t) - \frac{1}{\tau_p}\right]E_B(t) + kE_B(t-\tau)\exp(-i\omega\tau + i\phi_m(t)) + k_{inj}E_A(t-T_c) \times (1 + A \times m(t-T_c))\exp(-i\omega T_c)\exp(i\Delta\omega t_c) \quad (12)$$

$$\frac{dN_{A,B}(t)}{dt} = \frac{I}{q} - \frac{1}{\tau_n}N_{A,B}(t) - G(t)|E_{A,B}(t)|^2 \quad (13)$$

$$G(t) = \frac{g[N_{A,B}(t) - N_0]}{1 + \beta|E_{A,B}(t)|^2} \quad (14)$$

Equations (11) and (12) are respectively the rate of change of complex electric field at both ends of the communication network, and Equation (3) is the rate of change of carriers at both ends. g is the differential gain coefficient, k is the optical feedback coefficient, τ is the feedback delay, $\phi_m(t)$ is the phase modulation function, k_{inj} is the injection coefficient, T_c is the channel transmission time, $m(t)$ is the original information, A is the information modulation coefficient, β is the gain saturation coefficient, ω is the central angular frequency, and $\Delta\omega$ is the difference between the central angular frequencies at both ends.

The synchronization of two CSs at the receiving end can be expressed by the synchronization rate $C(s)$, as shown in the following equation:

$$C(s) = \frac{\langle[P_A(t-\Delta t) - \langle P_A(t-\Delta t)\rangle][P_B(t) - \langle P_B(t)\rangle]\rangle}{\sqrt{\langle[P_A(t-\Delta t) - \langle P_A(t-\Delta t)\rangle]^2\rangle\langle[P_B(t) - \langle P_B(t)\rangle]^2\rangle}} \quad (15)$$

Among them, $P_{A,B}(t)|E_{A,B}(t)|^2$, and $\langle\ \rangle$ represents the average value, andΔt is the channel transmission time.

3 Verification of Intelligent Encryption Model of Optical Communication Network

After that, this paper combines the algorithm in the second part to build the encryption system model. In the design of this paper, the sequence of one-time cipher book used in single encryption is 32 bits. The basic idea of encryption algorithm is that the 32-bit information to be encrypted is processed by scrambling matrix, which scrambles the sorting of digital information, and then carries out bit-by-bit exclusive OR operation with the

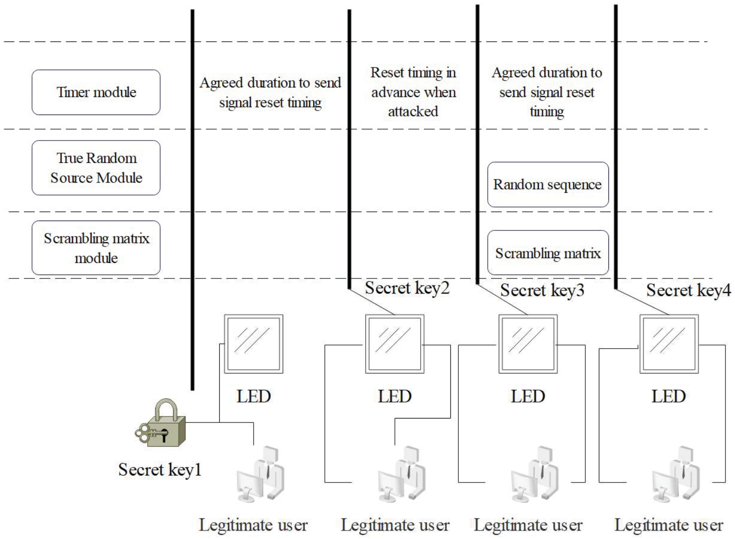


Figure 5 Flow chart of complete secure communication.

sequence of one-time cipher book, loads the information into the random sequence, and then sends the sequence.

The experimental environment for this article is as follows: Network controller: Floodlight-1 0 Switch: Open vSwitch; Experimental environment setting program: Mininet software; Operating system: Win10 and above systems; Security module: The PC comes with a built-in security module

As shown in Figure 5, firstly, the node LED and the legitimate user carry out key agreement in advance in a secure environment, obtain key one containing the first one-time cipher book and the first scrambling matrix, and start the first information transmission based on key one encryption. Then, after a preset period of time, the node LED of the timer module signal and the agreed time signal sent by the true random source module and the scrambling matrix generation module are obtained. The true random source module intercepts the second one-time cipher book from the uninterrupted true random sequence generated by the running true random source in real time, and forms the second key with the second scrambling matrix generated by the scrambling matrix generating module, and transmits the second key to the node LED, thus entering the key updating stage.

In the key updating stage, the node LED continues to send the key updating signal and the key 2 containing the second one-time cipher book

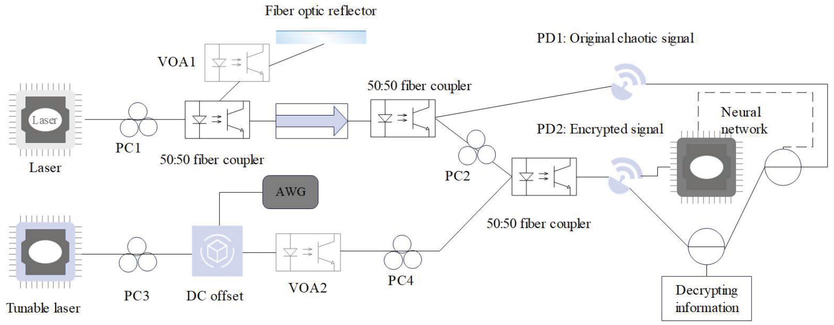
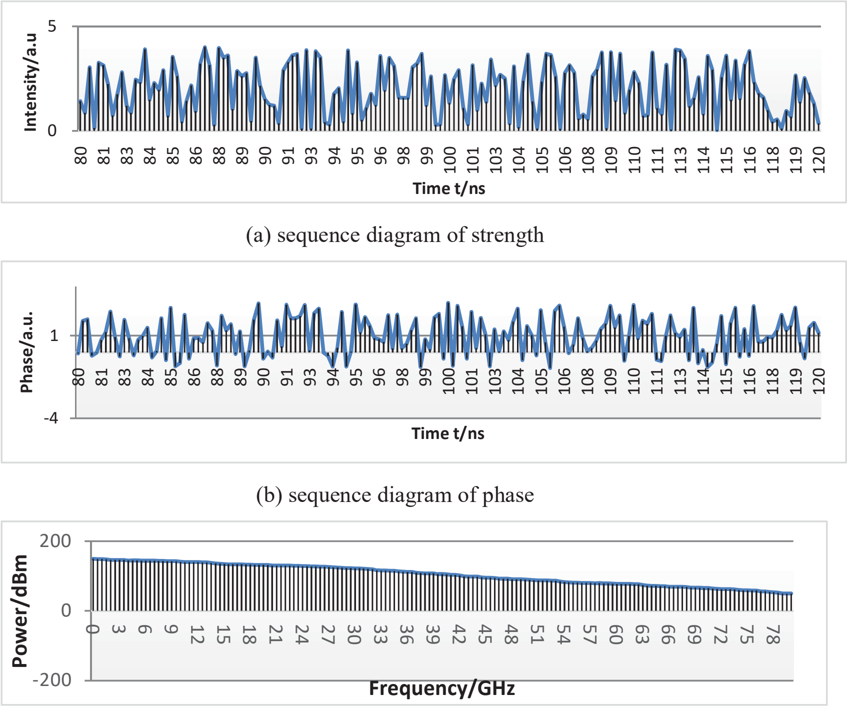


Figure 6 Schematic diagram of experimental device (PC: Polarization Controller; VOA: Variable Optical Attenuator; ISO: Isolator; MZM: Mach-Zehnder Modulator; AWG: Arbitrary Waveform Generator; PD: Photodetector).

and the second scrambling matrix to the legal user in the key 1 encryption mode. After the legal user receives the key 2, the key 2 is sent back to the node LED through the uplink channel for comparison. If there is an error, the node LED will send the key 2 again in the key 1 encryption mode until the node LED confirms that there is no error, and the key updating stage is ended. Due to the characteristics of VLC communication, the uplink communication of legitimate users is almost absolutely secure, which ensures the smooth progress of the key update stage.

Subsequently, the node LED will start the second information transmission encrypted with the key 2. Before the end of the preset time, if the node LED receives the attack warning signal, the node LED will send the agreed time signal to the true random source module and the scrambling matrix generation module and reset the timer module to re-time, thereby obtaining the key 3 containing the third one-time cipher book and the third scrambling matrix, and entering the key updating stage in advance to exchange the key 3.

Figure 6 shows the schematic diagram of the whole experimental principle and system structure. Chaotic carriers are generated using an optical feedback structure of the laser, in which a dimmable optical attenuator (VOA1) is used to adjust the intensity of the FI and a polarization controller (PC1) is used to adjust the polarization state of the FI. The encrypted signal is detected by photodetector (PD2) and used as the input of neural network. Then, the neural network performs training and regression under the supervision of the original CS. The trained neural network is tested by a part of the training data set, and the tested neural network can be used for chaotic synchronization in the actual process. Finally, the information can



(a) sequence diagram of strength

(b) sequence diagram of phase

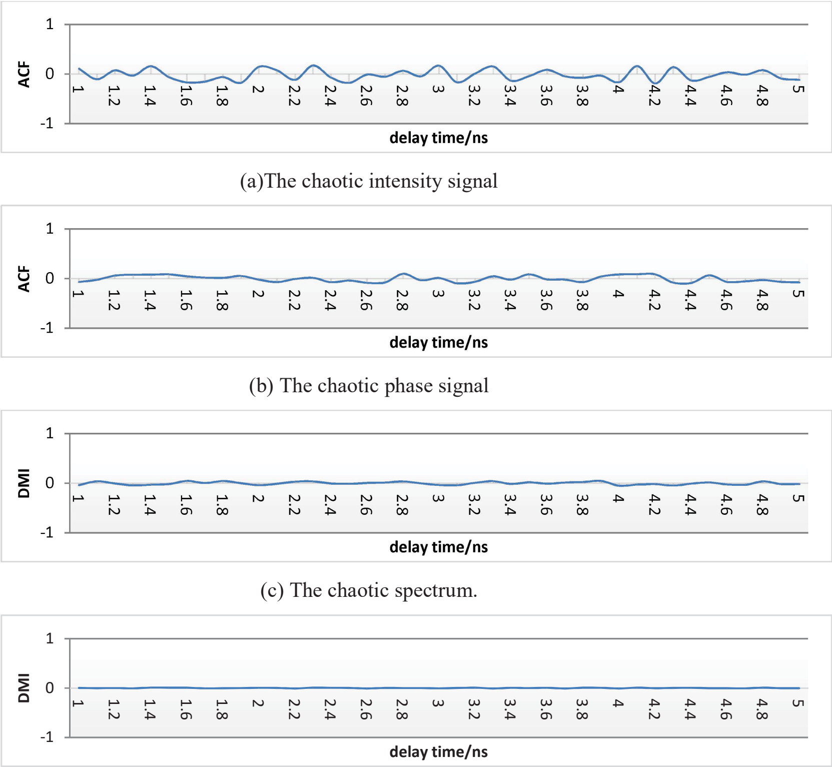
(c) spectrum diagram of CS

Figure 7 Sequence diagram of CS.

be decrypted by subtracting the synchronization signal from the encrypted signal.

Figure 7 shows the analog output CS, Figure 7(a) is the chaotic intensity signal, Figure 7(b) is the chaotic phase signal, and Figure 7(c) is the chaotic spectrum, Figure 7(d) is the Chaotic phase spectrum. From Figures 7(a) and 7(b). Figure 7(c) shows that CSs have wide and flat spectrum. Figure 7 overall shows that the scheme generates the CL signal of complex dynamic and stable output. From Figure 7, it can be seen that there is a certain connection between the output chaotic signal and the system characteristics.

The strength and phase information of CS are analyzed by autocorrelation and mutual information technology, as shown in Figure 8. These images are: (a) The Chaotic intensity signal; (b) The Chaotic phase signal; (c) The Chaotic spectrum; (d) The Chaotic phase spectrum. It can be seen from the figure that the CS has no obvious peak at the feedback delay of 2 ns.



(a)The chaotic intensity signal

(b) The chaotic phase signal

(c) The chaotic spectrum.

(d)The Chaotic phase spectrum

Figure 8 The autocorrelation diagrame.

The reason of using phase modulation scheme to eliminate CT-delay signal is explained as follows: in the single loop feedback structure, a photoelectric phase modulator is added, the phase of FI is randomly modulated, the chaotic dynamic behavior is significantly enhanced, and the high-dimensional CS is output. The intensity and phase information of CSs are extracted by using autocorrelation and mutual information technology. Because the CSs after phase modulation have highly random noise-like characteristics, which shows that the CT-delay signals are randomized.

There are two main ways to load information in chaotic carrier: chaotic information hiding and chaotic information modulation. Figure 9 shows the information synchronization rate variation curves of the two corresponding modulation modes under different signal-to-noise ratios of the transmission channel. It can be seen from the figure that as the signal-to-noise ratio

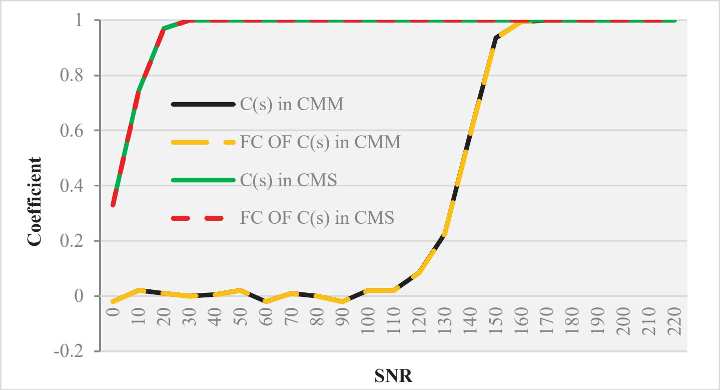


Figure 9 The variation curve of synchronization rate coefficients of chaotic information modulation and chaotic information hiding in different channel signal-to-noise ratio environments.

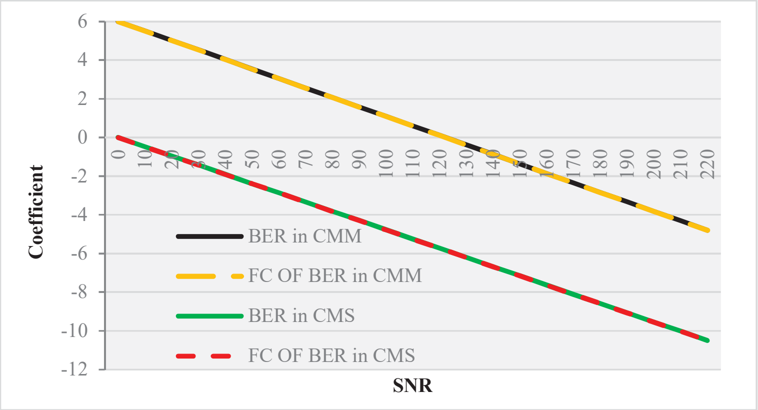


Figure 10 The relationship curve between the error rate of the disciplinary output information and the change of the channel signal-to-noise ratio in the two information loading methods of chaos information modulation and chaos information hiding.

increases, the synchronization of the two modulation methods has gradually increased and both approach 1. However, chaos information is made to a higher signal-to-noise ratio than the hidden method of chaos to synchronize.

Figure 10 shows the influence of chaotic information modulation and chaotic information hiding on bit error rate under different channel signal-to-noise ratios. With the increase of signal-to-noise ratio, the bit error rate of information decreases gradually, and they have the same change trend.

However, it can be seen that the chaotic information hiding method has lower bit error rate than the chaotic information modulation method in the same channel signal-to-noise ratio environment. This phenomenon is mainly because chaotic information modulation has higher transmission security than chaotic information hiding, but it also leads to the increase of bit error rate of demodulation information at the receiving end.

Through the above analysis, we can see that the optical communication network encryption technology based on AIT proposed can effectively improve the encryption effect of optical communication network, and has a certain effect on the popularization and application of optical communication technology.

4 Conclusion

Optical communication technology mainly uses light wave as the basic data transmission medium to complete the communication function of information and data, and achieves the same processing effect as wireless information communication technology. In essence, optical communication technology belongs to the core of electromagnetic wave communication technology, but compared with the traditional light wave propagation, this technology exceeds the conventional use standard of radio waves in operation mode, and the wavelength distance produced by optical communication technology is short, so the information capacity carried in the technology is larger when actually transmitting information.

In order to solve the PL security problem of optical communication network, this paper focuses on the field of PL secure optical communication, focusing on two specific aspects: chaotic optical communication and quantum key distribution, and has carried out a large number of scheme innovations and experimental research for the key technologies needed, and carried out related research based on the hot issues of CSC. Moreover, this paper proposes a secure communication system with random change of digital key laser external cavity FI, a device for output chaotic source with arbitrary wave phase modulation by laser external loop single feedback, and a CSC system with synchronization of key phase modulation single loop FI and injection. Through the analysis of experimental results, we can see that the optical communication network encryption technology based on AIT proposed can effectively improve the encryption effect of optical communication network, and has a certain effect on the popularization and application of optical communication technology.

The chaotic signal source designed in this article is a discrete structure. How to transform the laser feedback system structure into an integrated chaotic source and output a stable chaotic signal is a direction for future research on chaotic secure communication.

References

[1] Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., ... and Martin, V. (2019). The engineering of software-defined quantum key distribution networks. IEEE Communications Magazine, 57(7), 20–26.

[2] Aguado, A., Lopez, V., Martinez-Mateo, J., Peev, M., Lopez, D., and Martin, V. (2018). Virtual network function deployment and service automation to provide end-to-end quantum encryption. Journal of Optical Communications and Networking, 10(4), 421–430.

[3] Bi, M., Fu, X., Zhou, X., Zhang, L., Yang, G., Yang, X., ... and Hu, W. (2017). A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON. IEEE Photonics Journal, 9(1), 1–10.

[4] Cao, Y., Zhao, Y., Yu, X., and Wu, Y. (2017). Resource assignment strategy in optical networks integrated with quantum key distribution. Journal of Optical Communications and Networking, 9(11), 995–1004.

[5] Guan, M., Yang, X., and Hu, W. (2019). Chaotic image encryption algorithm using frequency-domain DNA encoding. IET image processing, 13(9), 1535–1539.

[6] He, R., Zhong, Z., Ai, B., Ding, J., Yang, Y., and Molisch, A. F. (2012). Short-term fading behavior in high-speed railway cutting scenario: Measurements, analysis, and statistical models. IEEE Transactions on Antennas and Propagation, 61(4), 2209–2222.

[7] Huang, Q., Liu, D., Chen, Y., Wang, Y., Tan, J., Chen, W., ... and Zhu, N. (2018). Secure free-space optical communication system based on data fragmentation multipath transmission technology. Optics express, 26(10), 13536–13542.

[8] Jiang, N., Zhao, A., Xue, C., Tang, J., and Qiu, K. (2019). Physical secure optical communication based on private chaotic spectral phase encryption/decryption. Optics letters, 44(7), 1536–1539.

[9] Karinou, F., Brunner, H. H., Fung, C. H. F., Comandar, L. C., Bettelli, S., Hillerkuss, D., ... and Poppe, A. (2018). Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photonics Technology Letters, 30(7), 650–653.

[10] Ke, J., Yi, L., Xia, G., and Hu, W. (2018). Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate. Optics letters, 43(6), 1323–1326.

[11] Liang, X., Zhang, C., Luo, Y., Wang, X., and Qiu, K. (2022). Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion. Journal of Lightwave Technology, 41(6), 1619–1625.

[12] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., . . . and Voznak, M. (2020). Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR), 53(5), 1–41.

[13] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., . . . and Wallden, P. (2020). Advances in quantum cryptography. Advances in optics and photonics, 12(4), 1012–1236.

[14] Sultan, A., Yang, X., Hajomer, A. A., and Hu, W. (2018). Chaotic constellation mapping for physical-layer data encryption in OFDM-PON. IEEE photonics technology letters, 30(4), 339–342.

[15] Wengerowsky, S., Joshi, S. K., Steinlechner, F., Zichi, J. R., Dobrovolskiy, S. M., Van der Molen, R., . . . and Ursin, R. (2019). Entanglement distribution over a 96-km-long submarine optical fiber. Proceedings of the National Academy of Sciences, 116(14), 6684–6688.

[16] Yazdeen, A. A., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Ahmed, O. M., and Zebari, R. R. (2021). FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. Qubahan Academic Journal, 1(2), 8–16.

[17] Zhang, W., Zhang, C., Chen, C., and Qiu, K. (2017). Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement. Journal of Lightwave Technology, 35(9), 1524–1530.

[18] Zhang, Z., Luo, Y., Zhang, C., Liang, X., Cui, M., and Qiu, K. (2022). Constellation shaping chaotic encryption scheme with controllable statistical distribution for OFDM-PON. Journal of lightwave technology, 40(1), 14–23.

[19] Zhao, A., Jiang, N., Liu, S., Zhang, Y., and Qiu, K. (2021). Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling. Journal of Lightwave Technology, 39(8), 2288–2295.

[20] Zhao, J., Liu, B., Mao, Y., Ullah, R., Ren, J., Chen, S., . . . and Shen, J. (2020). High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization. Optics Express, 28(14), 21236–21246.

Biographies

Ying Wang, Senior Engineer of State Grid Hebei Electric Power Research Institute, and Master's degree in Communication and Information System from North China Electric Power University. The current research interests are focused on communication technology, network security, and artificial intelligence.

Xiaojun Zuo holds a Master's degree in Computer Technology from Tianjin University. Current research interests are focused on network security technology, big data technology, and artificial intelligence technology.

Yuling Guo, Senior Engineer of State Grid Hebei Electric Power Research Institute, and Master's degree in Computer Technology from North China Electric Power University. The current research interests are focused on software testing, information security, information operation and maintenance, etc.

Huiying Liu, Senior Engineer of State Grid Hebei Electric Power Research Institute, and Master's degree in Computer Science and Technology from North China Electric Power University. The current research interests are focused on information and communication technology, network security, and artificial intelligence.

Jianchun Zhou, Testing Engineer at China Electric Power Research Institute, Bachelor's degree from Hunan University of Science and Technology. The main research areas are information systems, communication equipment detection, and network security technology.