Data Fragmentation Multipath Secure Coherent Optical Communication System Based on Electrical Signal Processing

Kunpeng Zhai, Sha Zhu, *Member, IEEE*, Yinfang Chen, Huashun Wen, Ya Jin, Wei Chen, and Ninghua Zhu, *Member, IEEE*

***Abstract*—In this paper, we report a novel optical data fragmentation multipath (ODFM) scheme for coherent optical communication based on electrical signal processing in simulation. Under the control of a pseudo-random sequence (PRBS), we randomly disperse the user data and assign them to paths corresponding to different wavelengths for transmission. To reduce the hardware complexity of the system and the requirements for receiver sensitivity, we adopt binary phase shift keying (BPSK) modulation and homodyne coherent detection in the scheme. To verify the feasibility of the proposed ODFM scheme, we demonstrated an error-free transmission through 40 km fiber with 10 Gbps hopping rate and 10 Gbps data rate by the simulation tools. The proposed scheme can be widely used in the physical layer secure communication of backbone network, large-scale data transmission and physical layer encryption of free space optical (FSO) communication.**

***Index Terms*—Coherent optical secure communication, optical data fragmentation multipath, physical layer security.**

I. Introduction

WITH the continuous improvement of optical communication data bandwidth and rate, personal and commercial information, as well as military confidential data, tend to be transmitted via optical signals [1]–[3]. Due to the advantages of anti-electromagnetic interference and low loss characteristics in long-distance transmission, optical fiber network has become a research hotspot in expanding the capacity and speed of confidential communication [4], [5]. Compared with the conventional intensity-modulation and direct-detection (IM DD) scheme in high-capacity wavelength-division multiplexed (WDM) systems, coherent optical communication has higher sensitivity and can further increase the transmission distance, making it widely used in backbone network communication [6]–[10]. However, the coherent optical communication system also faces the problem of optical network security.

Optical fiber communication networks are now the backbone of many critical communication systems ranging from personal to commercial to military communications [11]. The advantages of optical communications include wider bandwidth and higher security, allowing it to carry most of the information in the world. However, some hackers, thieves and spies have sparked the cyber cold war through cyber and physical layer attacks, in order to obtain military, political and economic information in various ways [12]. Therefore, the optical security communication is very important. In the past few years, optical fiber communication system has been considered relatively safe. Whereas, dismantling and bending the fiber enables a non-intrusive signal extraction without disrupting the service, with the rapid development of optical physical layer eavesdropping technologies, it is easy for eavesdroppers to illegally obtain user's data through fiber bending, splitting, evanescent coupling, scattering, and V-grooves [13], [14], etc. Therefore, it is important to improve the security of optical network in physical layer (PL). The PL security can be regarded as building block of a multi-layer security concept rather than a substitution of state-of-the-art security schemes on the upper layers. The information security of optical fiber communication has attracted lots of attentions. By designing reasonable transmission methods and forms, the difference between legal channels and illegal channels is increased to ensure the reception performance of legitimate users and effectively prevent non-partners from obtaining information. The traditional security research on cryptographic algorithms based on complex mathematical calculations at the application layer. Data fragmentation multipath technology is another PL security method besides optical code division multiple access (OCDMA) technology, optical stealth communication, chaotic optical communication, all-optical encryption technology, quantum communication and so on, which is completely capable of existing Internet system. It has been proved that OCDMA technology uses On-Off Keying (OOK) modulation to obtain

Manuscript received 12 June 2022; revised 17 July 2022; accepted 28 July 2022. Date of publication 2 August 2022; date of current version 9 August 2022. This work was supported in part by the National Key R&D Program of China under Grants 2019YFB2203104 and 2020YFB2205801, in part by the Natural Science Foundation of China under Grants 61805231, 61835010, and 61620106013, in part by the High-End Talent Team Construction Plan of Beijing University of Technology, and in part by the Zhejiang Lab's International Talent Fund for Young Professionals. *(Corresponding authors: Sha Zhu; Ninghua Zhu.)*

Kunpeng Zhai and Ya Jin are with the State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China, and also with University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: kpzhai@semi.ac.cn; jinya@semi.ac.cn).

Sha Zhu is with the College of Microelectronics, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China (e-mail: zhusha@bjut.edu.cn).

Yinfang Chen, Huashun Wen, Wei Chen, and Ninghua Zhu are with the State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China (e-mail: yfchen17@semi.ac.cn; whs@semi.ac.cn; wchen@semi.ac.cn; nhzhu@semi.ac.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3195753

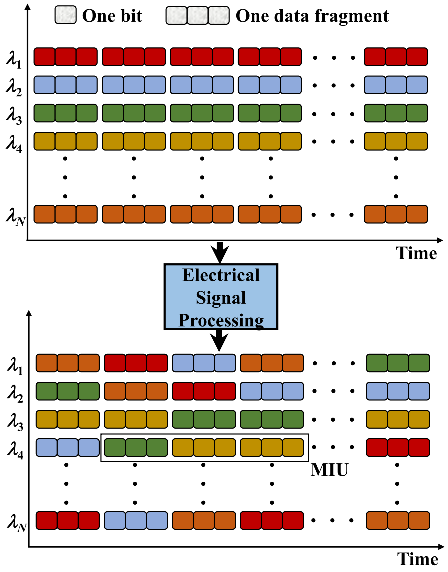

Fig. 1. Scheme of optical data fragmentation multipath secure transmission, MIU: Minimum information units.

information by detecting energy, which has major security vulnerabilities [15]. The optical stealth communication uses noise to hide the signal. However, the optical stealth signal always be recognized as noise and cannot be amplified by relay, its transmission distance is limited [16]. The long-distance chaotic synchronization and compensating the high-order dispersion of chaotic optical communication makes it is hard to apply practically [17], [18]. All-optical encryption technology also has some problems, such as noise accumulation and wrong logic signal in optical network transmission [19]. Quantum optical communication has not realized single photon light source, which limits the transmission distance and is not compatible with WDM system [20]. The development of practical physical layer secure communication technology compatible with the existing optical fiber communication system is a means to solve the current problem of secure transmission.

With the increasing demand for high-capacity communication, coherent optical communication is widely used. However, incompliant power-consuming digital signal processing (DSP) and costly narrow-linewidth lasers are usually required. As a compromise solution, homodyne coherent detection attracts increasing attention due to its ability to reduce the complexity as the power consumption, the local oscillator shares the same kind of laser with the signal at the transmitter side and is delivered remotely to the receiver for coherent detection, permitting a remarkable tolerance to laser linewidth.

The optical data fragmentation multipath (ODFM) secure transmission, i.e., optical frequency-hopping (OFH) technology, can be regarded as a new optical physical layer security technology, as shown in Fig. 1. The core idea is to use a bandwidth far greater than the minimum bandwidth required for information transmission to improve the anti-interference capabilities. The information is fragmented and randomly allocated to different channels for hiding to ensure communication security. The OFH system includes an optical transmitter and an optical receiver. The transmitter can fragment the user information, allocate the carrier channel of the fragmented information according to the pseudo-random binary sequence (PRBS), and the receiver can synchronize, decode and recover the fragmented information. Microwave photonics has the characteristics of high carrier frequency, large bandwidth, low loss, small size, easy reconfiguration and integration. Thus, the use of microwave photonic technology to generate different channels can build a more flexible optical frequency hopping transmission system and provide more possibilities for the secure coherent optical communications in the future backbone network or free space.

It is worth noting that the eavesdropping scenario of optical fiber communication and free space optical (FSO) communication differs in physical layer security. FSO communication needs to consider the effects of link fading, atmospheric turbulence, and the position of eavesdroppers [21], [22]. Its eavesdropping scenarios include the proximity of legitimate receivers and eavesdroppers, antenna deployments, and scattering conditions. In order to better simulate the real scene of FSO communications, consider that its main and wiretap links are different [23]. However, for the physical layer security technology of optical fiber communication, the eavesdropping scenario is more about the interception, bending, and coupling of optical fiber, so as to obtain information.

Based on OFH theory, a dual channel system using field-programmable gate array (FPGA) as data encryption and decryption processing tool is proposed [24], which can realize 1 Gb/s communication. However, this is still the IM-DD system. At the same time, it can only use the private network optical fiber for transmission, the rate can be further improved. 1 Gb/s has been difficult to meet the needs of modern communication. In [25], it has been applied to free space optical communication (FSO) to realize 1.25 Gb/s for 50 m in secure communication. However, in this scheme, coherent optical communication has not been adopted, which will greatly reduce the sensitivity of the receiver in space optical communication and can't realize long-distance transmission. In [26], four LDs are used to realize a 25 Gbps IM-DD system which increases the cost and complex of the system. In [27], by encrypting the transmitted data using an algorithm, and then randomly assigning it to multiple channels corresponding to Internet Protocol (IP), the results show that the maximum throughput can reach 60 Mb/s, which is still difficult to meet the needs of coherent communication.

In this paper, we have proposed and demonstrated a novel ODFM secure transmission scheme that can realize coherent optical communication without DSP in simulation. By making use of optical carrier suppression modulation, a simple and tunable multi-channel structure is realized. A Mach-Zehnder modulator (MZM) is used to realize binary phase shift keying (BPSK) modulation, which can be used in coherent optical secure communication to increase the security. The system uses homodyne coherent detection to reduce the hardware complexity and power consumption, so the scheme requires no extra DSP chip. The transmitter only needs one laser (LD) to realize the coherent ODFM secure scheme, which reduces the complexity of the system and plays an important role in backbone network and free space communication. The proposed secure communication

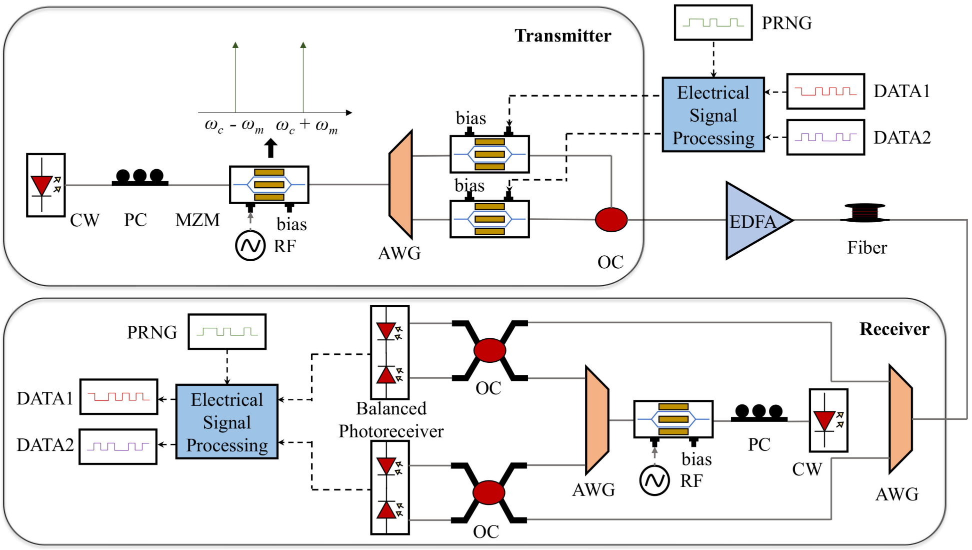

Fig. 2. Schematic diagram of the proposed optical data fragmentation multipath coherent secure transmission system. CW: Continuous waveform laser, PC: Polarization controller, MZM: Mach-Zehnder modulator, AWG: Arrayed waveguide grating, FPGA: Field-programmable gate array, PRNG: Pseudorandom number generator, EDFA: Erbium-doped fiber amplifier, OC: Optical coupler, BPD: balanced photodetector.

system has a high sensitivity for wavelength reconfigurability for secure coherent optical communication. In the simulation, we performed an error-free transmission with a single path optical power of -32 dBm, a frequency hopping of 10 Gbps, and a user data rate of 10 Gbps by VPI Transmission Maker. The security performance of the proposed scheme was also analyzed.

II. Operation Principles

Fig. 2 illustrates the schematic diagram of the proposed ODFM secure transmission scheme. The optical carrier is modulated by an MZM to realize carrier suppression modulation. The generated $\pm 1^{st}$-order optical sideband is used as the two carrier frequencies of the OFH respectively. The BPSK user data modulation signal is loaded to the two cascaded MZMs. Under the control of PRBS, electrical signal processing technology is used to disperse user data into different frequencies. The same PRBS is used at the receiving end to demodulate the frequency hopping signal, and the laser with the same wavelength is used for carrier suppression modulation to obtain the $\pm 1^{st}$-order sideband with the same frequency as the transmitting end as the local oscillator signal for signal demodulation, and homodyne detection is carried out in BPD. In the case of 40 km transmission and 10 Gbps transmission rate, the bit error ratio (BER) curve and eye pattern of the scheme prove that the ODFM coherent secure system is feasible and reconfigurable. Finally, we established the security analysis model of the physical layer system, proposed the probability of eavesdroppers obtaining minimum information units (MIU) in the case of brute force attacking, and proved the security of the system. This puts forward a new idea and a feasible method for the physical layer security system.

A continuous-wave (CW) light beam with the frequency of ω is connected to a polarization controller (PC), and then fed into the MZM with the polarization state of maximum modulation efficiency. A radio frequency (RF) signal is applied to the MZM. By setting the direct current (DC) bias of the MZM at minimum transmission point and considering small signal modulation, the optical signal at the output of the MZM can be given by

$$E_{out}(t) = E_c \cdot \begin{bmatrix} j^{-1} \cdot J_{-1}(\beta) \cdot e^{j\beta\cos(\omega_c - \omega_m)t} \\ +j \cdot J_1(\beta) \cdot e^{j\beta\cos(\omega_c + \omega_m)t} \end{bmatrix} \tag{1}$$

where E_{c} is the amplitude of the optical carrier, ω_{c} is the angular frequency of the optical carrier, ω_{m} is the RF signal angular frequency, $\beta = \pi V_{\mathrm{RF}}/V_{\pi}$ is the modulation indexes of the RF signal, V_{π} is the half-wave voltage of the MZM, J_1 represents the 1^{st}-order Bessel function of the first kind. J_{-1} represents the -1^{st}-order Bessel function of the first kind. It can be found in (1) that a carrier-suppressed double-sideband modulated optical signal, which consists of $\pm$ 1^{st}-order sidebands in the same phase, is generated after the MZM. The two sidebands are transported to the arrayed waveguide grating (AWG) to be separated into $\omega_{\mathrm{c}} - \omega_{\mathrm{m}}$ and $\omega_{\mathrm{c}} + \omega_{\mathrm{m}}$. The separated two optical signals are sent to two MZMs to realized BPSK modulation.

At the same time, the user data is controlled by the FPGA. The proposed ODFM secure transmission scheme is under the control of the frequency hopping sequence (HS) generated by pseudorandom number generator (PRNG), where bit '0' is for data retention status and bit '1' is for data exchange. HS is controlled by FPGA, including synchronization of HS at transmitter and receiver. For third-party eavesdroppers, the random hopping of the upper and lower branches makes it difficult to decipher the contained data. After modulation, the two BPSK signals are coupled by an optical coupler (OC) into the fiber for transmission.

In the receiver part, the optical beams carrying modulation information is first divided into $\omega_{\mathrm{c}} - \omega_{\mathrm{m}}$ and $\omega_{\mathrm{c}} + \omega_{\mathrm{m}}$ frequencies using AWG, and then input into a 50:50 OC to work as modulation signals respectively. A LD with the same frequency in the transmitter is fed into another MZM for carrier suppression modulation. The generated two signals at frequencies of $\omega_{\mathrm{c}} -$

ω_m and $\omega_\mathrm{c} + \omega_\mathrm{m}$ are fed into a 50:50 OC, which can be seen as a 180° hybrid, as the local oscillator signals. Finally, the signals are fed into a balanced photodetector (BPD) for photoelectric conversion. The electrical signal processing module in receiver is driven by the HS generated by PRNG, which is the same as the HS at the transmitting end. In this way, the correct BPSK modulation sequence can be obtained. In the BPD, the PC is used to ensure that the received signal (E_S) and the local oscillation signal (E_LO) are in the same polarization state, and the optical beams entered the BPD can be written as [28]

$$E_1(t) = \frac{1}{\sqrt{2}}(E_S + E_{LO}) \tag{2}$$

$$E_2(t) = \frac{1}{\sqrt{2}}(E_S - E_{LO}) \tag{3}$$

Under the condition that the initial frequency and phase of E_S and E_LO are basically the same, the photocurrent of the BPD can be expressed as [28]

$$\begin{aligned} I(t) &= I_1(t) - I_2(t) \\ &= \frac{R}{2}\left(P_S + P_{LO} + 2\sqrt{P_S P_{LO}}\right) \\ &\quad - \frac{R}{2}\left(P_S + P_{LO} - 2\sqrt{P_S P_{LO}}\right) \\ &= 2R\sqrt{P_S P_{LO}} \end{aligned} \tag{4}$$

where $I_1(t)$ and $I_2(t)$ are the electrical current of the single PD in BPD, P_S and P_LO are the power of the signal, $R = e\eta/\hbar\omega_\mathrm{s}$ is the responsiveness of PD, e is the electron charge, η is the quantum efficiency of PD, $\hbar$ is the reduced Planck constant, ω_s is the optical frequency, which is $\omega_\mathrm{c} - \omega_\mathrm{m}$ and $\omega_\mathrm{c}+\omega_\mathrm{m}$ respectively. Therefore, the original user data is recovered. The scheme has high sensitivity due to BPSK modulation, so it can realize coherent optical communication without DSP.

III. Results and Discussions

In this section, the construction and parameter definition of the simulation system are introduced, and the ODFM secure transmission simulation results are analyzed and discussed.

A. Simulation Setup

A dual-frequency-hopping ODFM coherent secure system was simulated and demonstrated using a single laser. The output frequency of the laser is 193.1 THz, which is compatible with the C-band in existing optical communication. As shown in Fig. 3(a), when the optical carrier is modulated by a 20 GHz microwave signal, a ±1^st-order double-sideband optical signal with a frequency difference of 40 GHz can be obtained. The side mode rejection ratio of sideband to carrier is 25 dB. Fig. 3(b) shows the optical spectrum of the -1^{st}-order sideband after passing through the AWG, and its extinction ratio (ER) is more than 70 dB. Fig. 3(c) indicates the optical spectrum of the $+1^{st}$-order sideband after passing through AWG which has an ER of more than 70 dB. Therefore, the $\pm1^{st}$-order sideband can be used as optical carrier for user information transmission.

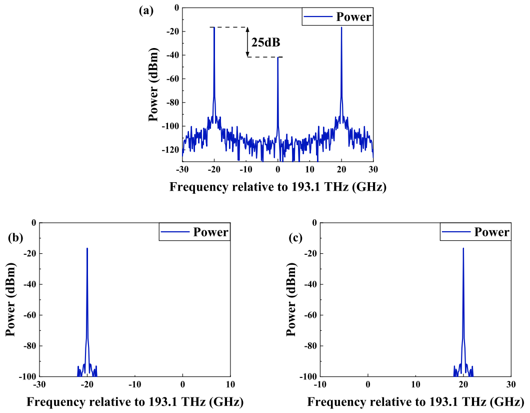

Fig. 3. The optical spectra for (a) Carrier suppression modulation after MZM, (b) -1^{st}-order sideband after AWG, (c) $+1^{st}$-order sideband after AWG.

TABLE I
Simulation Parameter Settings of the System

Specifications		Value	Unit
Laser diode	wavelength	1550	nm
	linewidth	10.0	kHz
	output power	1.0	mW
Modulator	RF V_π	5.0	V
	DC bias V_π	5.0	V
	extinction ratio	35	dB
WDM	center frequency 1	193.11	THz
	center frequency 2	193.09	THz
Photodiode	responsivity	1.0	A/W
	thermal noise	10e-12	A/Hz$^{1/2}$

In the simulation, the half-wave voltage of the MZM is set to 5 V and the modulation rate is adjusted to 10 Gbps. By adjusting the voltage of RF signal to 10 V and DC signal to 5 V, the BPSK modulation can be realized. The more detailed simulation parameter settings are listed in Table I.

The length of the single-mode fiber (SMF) used in the transmission process is 32 km and the dispersion coefficient is 1.6 × 10^{-5} s/m^2. An 8 km dispersion compensation fiber (DCF) with dispersion coefficient of -6.4×10^{-5} s/m^2 is used to ensure the transmission performance. The modulation signal is 10 Gbps Not-Return-to-Zero (NRZ), and a 10 Gbps PRBS is used to control the speed of frequency hopping to realize the ODFM secure scheme. By using electrical signal processing module to control PRBS code, the hop of user data is realized.

Fig. 4 shows the principle and results of FPGA. The PRBS code controlled by electrical signal processing module is used to change the information channel. After the user data DATA1 and DATA2 is scattered at the transmitter, the user data needs to be recovered at the receiver, then the output two channels of data can be PATH1 and PATH2. The specific formula is written as:

$$\begin{aligned} \mathrm{PATH1} &= \mathrm{DATA1} \cdot PRBS + \mathrm{DATA2} \cdot \overline{PRBS} \\ \mathrm{PATH2} &= \mathrm{DATA1} \cdot \overline{PRBS} + \mathrm{DATA2} \cdot PRBS \end{aligned} \tag{5}$$

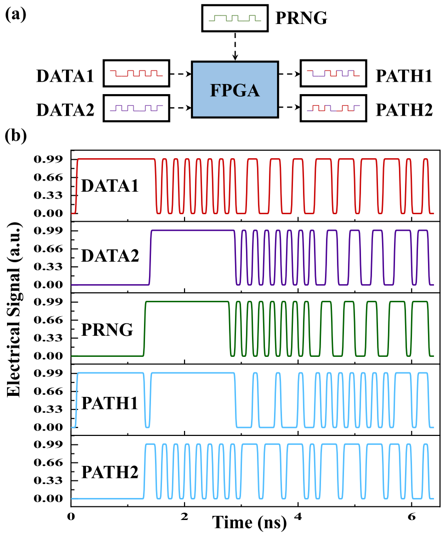

Fig. 4. (a) Schematic diagram of optical frequency hopping with FPGA. (b) The electrical signal of the optical frequency hopping based on PFGA control. DATA1 and DATA2 is the user data, PRBS is the hopping sequence, PATH1 and PATH2 are the two channels of data after optical frequency hopping.

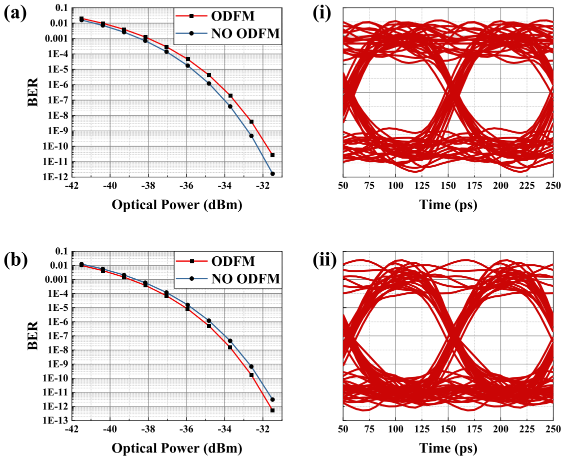

Fig. 5. (a) The BER performance of the received decrypted ODFM signal (red line) and NO ODFM signal (blue line) under different optical power at frequency $\omega_{\rm c} - \omega_{\rm m}$, (i) the eye pattern of received decrypted signal at frequency $\omega_{\rm c} - \omega_{\rm m}$, (b) the BER performance of received decrypted ODFM signal (red line) and NO ODFM signal (blue line) signal under different optical power at frequency $\omega_{\rm c} + \omega_{\rm m}$, (ii) the eye pattern of received decrypted signal at frequency $\omega_{\rm c} + \omega_{\rm m}$.

B. *Eye Patters and BER Performance*

The eye patterns and bit-error-rate (BER) performance are used to represent the performance of the coherent ODFM secure scheme. Fig. 5(a) and (i) show the BER curve and eye patterns of the frequency $\omega_c - \omega_m$, respectively. A high quality of 10 Gbps communication are obtained. From the BER curve, error-free transmission results can be achieved in 40 km SMF and DCF with the optical power below -32 dBm, which means coherent optical frequency hopping system has a high sensitivity. Fig. 5(b) and (ii) show the BER curve and eye patterns of the frequency $\omega_c + \omega_m$, respectively. Fig. 5(a) and (b) in red lines shows the BER performance result of the receiver processed by FPGA. In terms of system stability, the use of ODFM technology has not significantly increased the BER performance while increasing the system security. In terms of security, for eavesdroppers, it is difficult to decipher effective information because of the ODFM technology. By comparing the eye diagram and BER curves, it can be found that the transmission performance of the two channels is the same, indicating that the system has good scalability and can increase the number of channels.

C. *Security Analysis*

The physical layer security evaluation system is constructed to evaluate the security of coherent ODFM secure scheme. The illegal eavesdropper (Eve) who obtains the minimum information units (MIU) of the transmitter (Alice) is considered as successful eavesdropping. In the coherent ODFM secure scheme, Alice and receiver (Bob) do not need physical layer authentication. It is difficult for the eavesdropper to obtain the synchronous key. The Eve can only use exhaustive methods to crack the encrypted information, that is, try all HS combinations to find the real key. For this purpose, suppose that the MIU with the size of M bits, which is composed of $A_1, A_2, \ldots, A_M$. The m bits constitute one data fragment, which is composed of $Z_1, Z_2, \ldots, Z_{\lceil M/m \rceil}$, and Z_1 is known. The possible location of Z_2 needs to be analyzed from two aspects. In terms of space, N is the number of transmission channels corresponding to different frequencies, Z_2 may appear in any of N channels. In terms of time, due to the different dispersion of different frequencies in SMF, after long-time transmission, it is assumed that the transmission rate is R, the delay time is t, and the total number of bits where Z_2 may appear is L, where $L = 2Rt + 1$. For a data fragment, its probability of being cracked is directly proportional to its length m, because the smaller the data fragment, the more channel N occupied by MIU, and the lower the probability of being cracked, then the probability of cracking a data fragment is $P_{\rm F} = [N(2Rt + 1)/m]^{-1}$, then the probability of cracking MIU can be expressed as

$$P_{intercept} = \prod_{i=1}^{\lceil \frac{M}{m} \rceil} P_{F_i} = \left[\frac{N \cdot (2Rt + 1)}{m} \right]^{-\lceil M/m \rceil} \tag{6}$$

where $\lceil M/m \rceil$ is the number of data fragments contained in MIU. The security of our system is realized through three parts: transmitter, fiber link, receiver. In the transmitter, the number of channels N and reducing the length of data fragments m is increased, which makes it difficult for Eve to obtain effective information in transmitter. In the fiber link, due to BPSK modulation, the signal phase changes will lead it hard for the Eve to recover the modulation information directly through a PD. In the receiver, use the same LD as the transmitter to ensure that the LO and carrier signal frequency are the same, and improve the system sensitivity without DSP.

Assuming that the MIU of the coherent ODFM secure scheme is cracked, its probability distribution diagram can be represented as Fig. 6. For an 8-channel scheme, since the transmission rate is $R = 10$ Gbps, $M = 8$ bits, $t = 1$ ns, and the length of fragments is 1 bit, the $P_{\rm intercept}$ is about 9.0949×10^{-21}. If a third party wants to threaten the security of the system

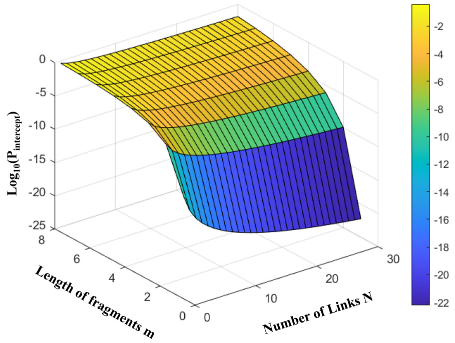

Fig. 6. The total probability of cracking MIU within the space-time domain for different number of channels and size of data slice, m is data fragment length, N is the channel number, the ordinate is the logarithm of probability (assuming $N = 8$, $R = 10$ Gbps, $M = 8$ bits, $t = 1$ ns).

by means of brute force decoding, it will need the help of a supercomputer. Even with Fugaku, the fastest supercomputer with $R_{\max} = 442010.0$ TFlop/s in the world, it is still hard to decode, so the system can be considered safe and reliable.

IV. Conclusion

In conclusion, we have proposed and demonstrated a carrier suppressed modulation-based coherent ODFM secure scheme in simulation. The user data is randomly hopped in two channels by the help of FPGA. The BPSK modulation is used to improve the sensitivity and realize coherent data fragmentation multipath secure transmission, which provides a new approach for the physical layer security of backbone network, and can realize large-scale secure data transmission and physical layer encryption of free space optical communication. Limited by the conditions of the laboratory, we do not have enough signal generators to realize the experimental verification, but this scheme is proved to be feasible in theory and simulation. The simulation results may be slightly different from the actual results, but it provides an idea for the development of physical layer security technology.

Acknowledgment

The authors declare no conflicts of interest.

References

[1] J. Zhang, W. Chen, M. Gao, and G. Shen, "K-means-clustering-based fiber nonlinearity equalization techniques for 64-QAM coherent optical communication system," *Opt. Exp.*, vol. 25, no. 22, pp. 27570–27580, Oct. 2017.

[2] Z. Zhao, J. Liu, Y. Liu, and N. Zhu, "High-speed photodetectors in optical communication system," *J. Semicond.*, vol. 38, no. 12, pp. 5–11, Dec. 2017.

[3] H. Zhu et al., "Complementary coding optical stealth transmission based on amplified spontaneous emission light source," *Opt. Exp.*, vol. 22, no. 23, pp. 28346–28352, Nov. 2014.

[4] P. J. Winzer, D. T. Neilson, and A. R. Chraplyvy, "Fiber-optic transmission and networking: The previous 20 and the next 20 years," *Opt. Exp.*, vol. 26, no. 18, pp. 24190–24239, Sep. 2018.

[5] M. H. Khadr and H. Elgala, "Augmented communications: Spectral efficiency and security enhanced visible light communications by design," *Chin Opt. Lett.*, vol. 18, no. 9, 2020, Art no. 1671.

[6] K. Kikuchi, "Fundamentals of coherent optical fiber communications," *J. Lightw. Technol.*, vol. 34, no. 1, pp. 157–179, Jan. 2016.

[7] M. S. Faruk and S. J. Savory, "Digital signal processing for coherent transceivers employing multilevel formats," *J. Lightw. Technol.*, vol. 35, no. 5, pp. 1125–1141, Mar. 2017.

[8] S. Ishimura and K. Kikuchi, "Multi-dimensional permutation-modulation format for coherent optical communications," *Opt. Exp.*, vol. 23, no. 12, pp. 15587–15597, Jun. 2015.

[9] P. Shi, G. Wu, L. Hu, Q. Li, and J. Chen, "Stable RF transfer over a fiber-optic ring with DSBCS modulation and a DSB RF signal," *Chin. Opt. Lett.*, vol. 18, no. 2, Feb. 2020, Art no. 020603.

[10] Y. Mori, C. Zhang, and K. Kikuchi, "Novel configuration of finite-impulse-response filters tolerant to carrier-phase fluctuations in digital coherent optical receivers for higher-order quadrature amplitude modulation signals," *Opt. Exp.*, vol. 20, no. 24, pp. 26236–26251, Nov. 2012.

[11] Q. Huang, Y. Chen, C. Yang, L. Wang, W. Chen, and N. H. Zhu, "An optical frequency-hopping scheme based on phase modulator-embedded optical loop mirror," *Opt. Commun.*, vol. 452, no. 1, pp. 422–427, Dec. 2019.

[12] S. Aftergood, "Cybersecurity the cold war online," *Nature,* vol. 547, pp. 30–31, Jul. 2017.

[13] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention," in *Proc. IEEE Mil. Commun. Conf.*, Monterey, CA, 2004, pp. 711–716.

[14] R. P. Webb et al., "All-optical header processing in a 42.6 Gb/s optoelectronic firewall," *IEEE J. Sel. Topics Quantum Electron.*, vol. 18, no. 2, pp. 757–764, Mar./Apr. 2012.

[15] D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: A code-switching scheme," *Electron. Lett.*, vol. 41, no. 14, pp. 817–819, Jul. 2005.

[16] B. B. Wu and E. E. Narimanov, "Analysis of stealth communications over a public fiber-optical network," *Opt. Exp.*, vol. 15, no. 2, pp. 289–301, Jan. 2007.

[17] Z. Yang, L. Yi, J. Ke, Q. Zhuge, Y. Yang, and W. Hu, "Chaotic optical communication over 1000 km transmission by coherent detection," *J. Lightw. Technol.*, vol. 38, no. 17, pp. 4648–4655, Sep. 2020.

[18] J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate," *Opt. Exp.*, vol. 43, no. 6, pp. 1323–1326, Mar. 2018.

[19] F. F. Froehlich, C. H. Price, T. M. Turpin, and J. A. Cooke, "All-optical encryption for links at 10 Gbps and above," in *Proc. IEEE Mil. Commun. Conf.*, Atlantic City, NJ, USA, 2005, pp. 2158–2164.

[20] R. Qi et al., "Implementation and security analysis of practical quantum secure direct communication," *Light: Sci. Appl.*, vol. 8, Feb. 2019, Art. no. 22.

[21] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art no. 7901110.

[22] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, Dec. 2020, Art no. 7906617.

[23] Y. Ai, A. Mathur, L. Kong, and M. Cheffena, "Secure outage analysis of FSO communications over arbitrarily correlated Málaga turbulence channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3961–3965, Apr. 2021.

[24] S. L. Wang, W. Chen, N. H. Zhu, J. G. Liu, W. T. Wang, and J. J. Guo, "A novel optical frequency-hopping scheme for secure WDM optical communications," *IEEE Photon. J.*, vol. 7, no. 3, Jun. 2015, Art no. 7201108.

[25] Q. Huang et al., "Secure free-space optical communication system based on data fragmentation multipath transmission technology," *Opt. Exp.*, vol. 26, no. 10, pp. 13536–13542, May 2018.

[26] D. C. Ban, Q. C. Huang, Y. F. Chen, Y. C. Qi, W. Chen, and N. H. Zhu, "A novel optical frequency-hopping scheme based on a flexible structure for secure optical communications," *IEEE Photon. J.*, vol. 11, no. 1, Feb. 2019, Art no. 7901207.

[27] Y. Jin, Y. Qi, Y. Chen, W. Chen, W. Li, and N. Zhu, "Secure fiber-optic communication system based on internet-accessible multipath transmission of ciphertext fragments," *Opt. Exp.*, vol. 29, no. 16, pp. 24919–24927, Aug. 2021.

[28] K. Kikuchi, "Digital coherent optical communication systems: Fundamentals and future prospects," *IEICE Electron. Exp.*, vol. 8, no. 20, pp. 1642–1662, Oct. 2011.