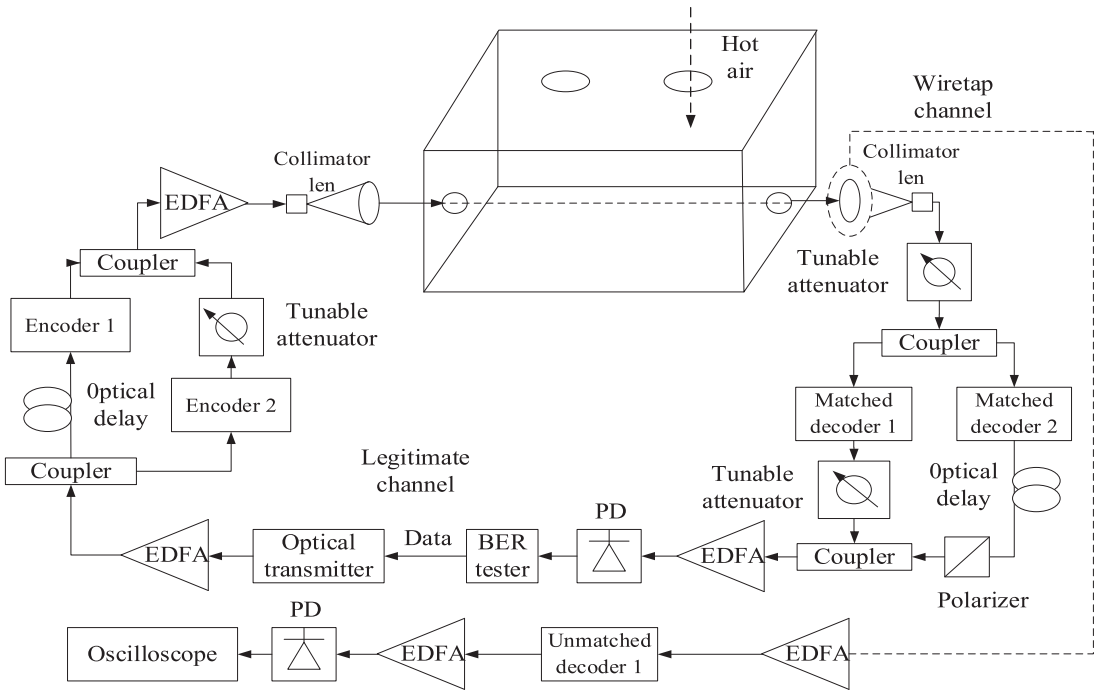
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Design and Investigation of 10 Gb/s FSO Wiretap Channel Using OCDMA Time-Diversity Reception

Volume 12, Number 3, June 2020

Jianhua Ji
Bing Wu
Jianjia Zhang
Ming Xu
Ke Wang



DOI: 10.1109/JPHOT.2020.2985747

Design and Investigation of 10 Gb/s FSO Wiretap Channel Using OCDMA Time-Diversity Reception

Jianhua Ji, Bing Wu, Jianjia Zhang, Ming Xu, and Ke Wang

Shenzhen Key Lab of Communication and Information Processing, College of Electronics and Information, Engineering, Shenzhen University, Shenzhen 518060, China

DOI:10.1109/JPHOT.2020.2985747

Manuscript received January 13, 2020; revised March 2, 2020; accepted April 1, 2020. Date of publication May 10, 2020; date of current version May 26, 2020. This work was supported in part by the National Natural Science Foundation of China (NSFC) (61671306); in part by Fundamental Research Project of Shenzhen (2020N227). Corresponding author: Jianhua Ji (e-mail: jjh@szu.edu.cn).

Abstract: In this paper, 10 Gb/s free space optical (FSO) wiretap channel using optical code division multiple access (OCDMA) time-diversity reception is designed and demonstrated for the first time. Reliability and security are investigated under weak and strong turbulence conditions. Two-dimensional optical encoder and decoder are constructed by wavelength selective switches and optical delay lines, and one-dimensional optical encoder and decoder are constructed by couplers and tunable optical delay lines. Experimental results show that reliability and security can be enhanced simultaneously using OCDMA time-diversity reception. At the received power of 2.58 dBm in strong turbulence, compared to non-diversity system, bit error rate (BER) of legitimate user in OCDMA time-diversity system is reduced from 3.9×10^{-7} to 6.73×10^{-8}. Furthermore, the reliability improvement is more obvious when the correlation between the two signals of OCDMA time-diversity is smaller. The secrecy capacity can be increased from 0.546 bit/symbol to 0.665 bit/symbol in strong turbulence when received power is 2.28 dBm. On the other hand, the secrecy capacity of strong turbulence is about 15% higher than that of weak turbulence.

Index Terms: Atmospheric turbulence, free space optical communication, OPTICAL code division multiple access, security capacity, time-diversity.

1. Introduction

Free space optical (FSO) communications are highly susceptible to atmospheric turbulence, which can cause fluctuations in both the intensity and the phase of the received signal [1], [2]. Diversity is an effective method to overcome the effects of turbulence-induced fading. Diversity techniques used in FSO communications include time-diversity, frequency-diversity and spatial diversity. In [3], a spatial diversity reception with multiple receivers is proposed. It can reduce the influence of atmospheric turbulence effectively. However, the analysis is based on the condition that the receiver aperture diameter is smaller than the correlation length of the intensity fluctuation. It is not suitable for most FSO communication systems, so the results are limited. Although frequency-diversity technology can overcome the shortcomings of spatial diversity [4], it occupies too many bandwidth resources and lacks security. In [5], polarization shift keying system applied with wavelength and time-diversity technique is considered to mitigate the turbulence induced fading. In [6], a 1.25 Gb/s wavelength and time-diversity reception scheme is experimentally demonstrated to enhance the

reliability of optical wireless transmission links corrupted by the atmospheric turbulence effects. The efficiency of several channel coding techniques for different time-diversity orders and turbulence conditions is investigated in [7]. Based on the experimental study of the channel fading effects, turbo product code is proposed to be used as the channel coding scheme, which features good resistance to burst errors and no error floor [8]. However, physical-layer security cannot be improved in these time-diversity schemes. In [9], a 2.5 Gb/s optical wireless transmission system for high energy physics is designed and analyzed. Experiment on all-optical relay-assisted 10 Gb/s FSO link over the atmospheric turbulence channel is investigated in [10].

On the other hand, FSO communications can suffer from optical tapping risks [11]. Since the laser beam experiences divergence due to optical diffractions, one possibility for a successful eavesdropping is to locate eavesdropper (Eve) in the divergence region of the beam. For long distances FSO communication, Eve has a stronger chance for eavesdropping on the FSO link by collecting the power not captured by legitimate peers. The communication between two legitimate peers in the presence of an external Eve is studied from a physical-layer security perspective in the context of FSO communications [12]. Analysis results show that the joint effect of laser-beam divergence and turbulence-induced fading on the received irradiance allows an external Eve close to the legitimate receiver to compromise the communication. Secrecy issues of FSO links realizing information-theoretic security and high transmission rates are discussed in [13]. It is shown that, under reasonable degraded conditions, information theoretically secure communications should be possible in a much wider distance range than the range limit of quantum key distribution. In [14], the closed-form expressions for the average secrecy capacity, the secrecy outage probability and the strictly positive secrecy capacity are derived by considering the specific nature of FSO channels modeled by the general M distribution.

Optical code division multiple access (OCDMA) is considered as a candidate to provide physical-layer security [15], [16]. With the increase of code cardinality, Eve is more difficult to crack codeword, so the physical-layer security will be improved. For optical orthogonal code (OOC), the security improves with the increase of code length. For two-dimensional optical code, the security improves with the number of wavelengths. Confidentiality performance is analyzed in detail for a 2-D incoherent OCDMA system, especially a multi-user two-code-keying wavelength-hopping time-spreading code system [17]. BER performance of atmospheric one-dimensional OCDMA system is evaluated in [18], in presence of MAI, atmospheric turbulence, background light, shot noise and thermal noise. In this study, pulse position modulation and lognormal fading model are adopted. Performances of code acquisition system in atmospheric OCDMA communications using optical orthogonal codes are analyzed in [19], and significant improvement in reducing the acquisition time and required power for synchronization is achieved. In [20], BER performance of one-dimensional OCDMA system is analyzed in different weather conditions (fog, rain, and snow) without considering turbulence as a random process, i.e., without any fading model. BER performances of one-dimensional and two-dimensional FSO/CDMA systems are discussed and compared in [21]. Effect of atmospheric turbulence on the BER performance of FSO/CDMA system employing multi-wavelength pulse position modulation is comprehensively analyzed in [22]. The system's robustness against brute-force attacks is discussed. The physical-layer security of OCDMA-based optical fiber communication system is analyzed in [23], and the authors use security leakage factor to evaluate the physical-layer security level. By establishing the eavesdropping model of the FSO/CDMA wiretap channel, the performance of physical-layer security and reliability are evaluated simultaneously in [24]. OCDMA based hybrid FSO/fiber wiretap channel is proposed in [25], and the physical-layer security is analyzed theoretically, using the conditional secrecy outage probability as the performance metric. However, this paper only analyzes the performance of hybrid FSO/fiber wiretap channel, and does not study how to overcome the effect of atmospheric turbulence. As reported in [26], bit error rate (BER) of a single-user time-diversity FSO/CDMA system is studied by considering random variation of cross-correlation value. Based on the binary asymmetric channel model, the physical-layer security performance of the time-diversity FSO/CDMA is analyzed theoretically in [27].

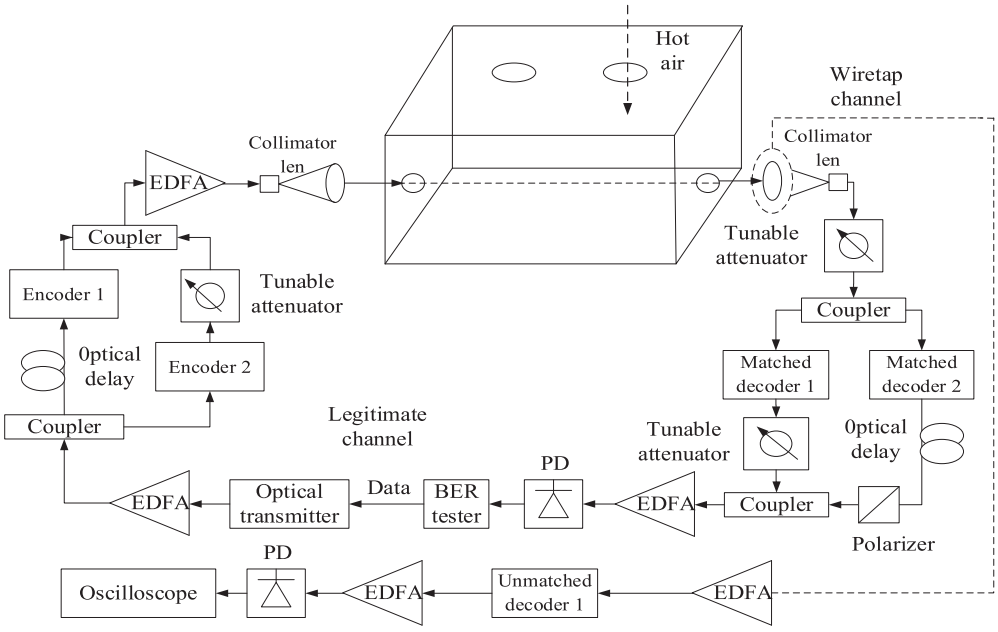


Fig. 1. 10 Gb/s experimental system of FSO wiretap channel using OCDMA time-diversity reception.

However, experimental investigation of FSO wiretap channel using OCDMA time-diversity reception has not been reported yet, to the best of our knowledge. In this paper, for the first time, we design and demonstrate a 10 Gb/s FSO wiretap channel using OCDMA time-diversity reception in weak and strong turbulence conditions. 10 Gb/s one-dimensional optical encoder and two-dimensional encoder are constructed. Experiments show that reliability and security can be enhanced simultaneously. This paper is organized as follows. In Section 2, we will build an experimental system of 10 Gb/s FSO wiretap channel using OCDMA time-diversity reception. In Section 3, BER performances of legitimate user are evaluated. In Section 4, physical-layer security will be analyzed. This paper is concluded in Section 5.

2. System Design and Realization

Fig. 1 shows the 10 Gb/s FSO wiretap channel using OCDMA time-diversity reception, where the legitimate users want to communicate over the FSO transmission link, and the Eve observes their transmission in the divergence region of the beam. 10G BER tester SeBERT-10S sends the signal to the optical transmitter for on-off keying (OOK) modulation. The optical transmitter SPTX15ps-10G outputs optical pulses with a width of 15 ps and a spectrum of 1548.7–1550.1 nm, corresponding to the Wavelength Selective Switch (WSS) wavelength of 53 (1549.72 nm), 54 (1550.12 nm) and 55 (1550.52 nm). The output power is −3.48 dBm. The modulated optical signal is amplified by an erbium doped fiber amplifier (EDFA). Then, the optical signal is split by the coupler. One path is first delayed by an optical fiber, and then encoded by one-dimensional optical encoder 1. Another is encoded by the two-dimensional optical encoder 2. Tunable attenuator is used to make the power of the two optical encoded signals consistent. In order to achieve time-diversity, users need to send the same data signal at different times. At the receiving end, the user needs to ensure that the two receiving signals are combined synchronously. The relative delay of the two coded signals is realized by the optical delay line introduced after the coupler. When the relative delay of two encoded signals is greater than the coherency time of atmospheric turbulence channel, the two signals will be completely uncorrelated at the receiver. Conversely, when the delay is less than the coherency time, the two signals will be partially correlated at the

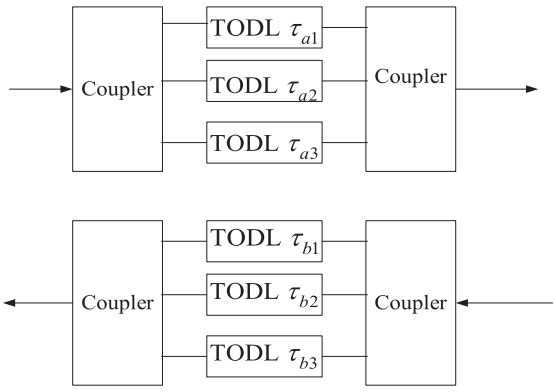


Fig. 2. One-dimensional optical encoder/decoder with couplers and tunable optical delay lines (TODL).

receiver. The two optical encoded signals are amplified by EDFA after they are combined by the coupler. Then, the collimating lens will be used for atmospheric channel transmission. In a real FSO communication system, the attenuation and turbulence will be changed with the distance at the same time. In this experiment, we simulate a FSO channel with fixed turbulence effect, but the attenuation varies with the transmission distance. The transmission distance of FSO is 1.8 m. In order to simulate the atmospheric turbulence effect, a 40 cm $\times$ 40 cm $\times$ 80 cm box is designed. The holes at the left and right ends are used for optical signal transmission. The hairdryer provides hot air. Different temperature and wind speed correspond to different turbulence effects.

At the receiving end, the legitimate user receives the optical signal with a collimating lens. The received optical signal is split by the coupler. A matched optical decoder 1 is used to decode one of the signals in one dimension, and a matched optical decoder 2 is used to decode another signal. Then, the decoded signal is delayed by an optical fiber. By adjusting the optical delay, the two decoded signals are fully aligned. The tunable attenuator is adjusted to ensure the same power of the two optical decoding signals. Once fully aligned, the two codes will interfere with each other. In this experiment, a polarizer is used to stabilize the waveform of combined signal. Then, the two decoded signals are combined by the coupler. After amplified by EDFA, 18.5-ps IR photodetector is used to detect optical signals. Then, BER is analyzed by SeBERT-10S. Waveforms and eye diagrams are tested by 20G Tektronix DPO 72004C digital oscilloscope.

At the same time, due to the expansion of the beam radius, there is an Eve at the receiving end. We assume that part of the power collected by Eve is r_e (extraction ratio), and the power collected by the legitimate user is $1 - r_e$ [10]. According to Kerckhoffs's principle, the Eve knows what types of OCDMA signals are being sent, but does not know the code of the legitimate user. Therefore, Eve can employ unmatched optical decoder. In this experiment, we assume that the legitimate user knows the specific code. For example, the legitimate user can transmit the code information through the quantum key distribution scheme.

In this experiment, we use tunable optical delay lines (TODL) to construct one-dimensional optical encoder and decoder. Hence, we employ OOC $(n, w, \lambda_a, \lambda_c)$, where n is code length, w is code weight, λ_a and λ_c are auto-correlation sidelobe and cross-correlation values respectively. Because the data rate is 10 Gb/s and the pulse width of laser is 15 ps, the code length of OOC is 7. The specific OOC is {0110010} [28]. As shown in Fig. 2, one-dimensional optical encoder and decoder are constructed by couplers and TODL. The TODL model is VDL-002-D-35-33-SS-FC/APC. The maximum delay is 400 ps and the resolution is 0.1 ps. Different ports connect different lengths of TODL to achieve time-domain coding/decoding. The delay of each port of the decoder is complementary to the delay of the corresponding port of the encoder. Because the TODL is tunable, it is reasonably easy for the legitimate user to change the optical code. We have considered the influence of coupler's pigtails. The total delay of each chip is the sum of TODL delay and coupler's pigtails delay. Then, by adjusting TODL, the delay of each chip is guaranteed to be exactly the

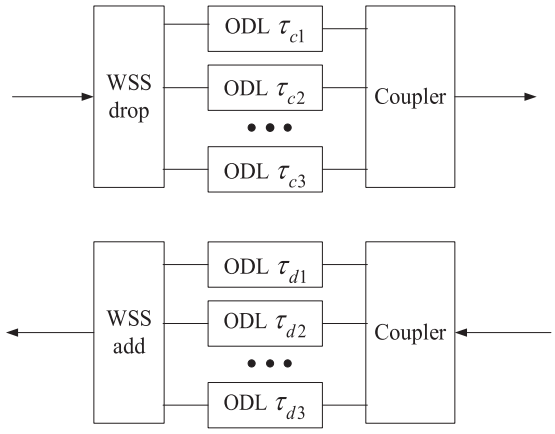


Fig. 3. Two-dimensional optical encoder/decoder with WSS and fiber delay lines (ODL).

same as that of the code. The relative delays of encoder are 14.3 ps, 28.6 ps, 71.4 ps, and the relative delays of decoder are 85.7 ps, 71.4 ps and 28.6 ps, respectively.

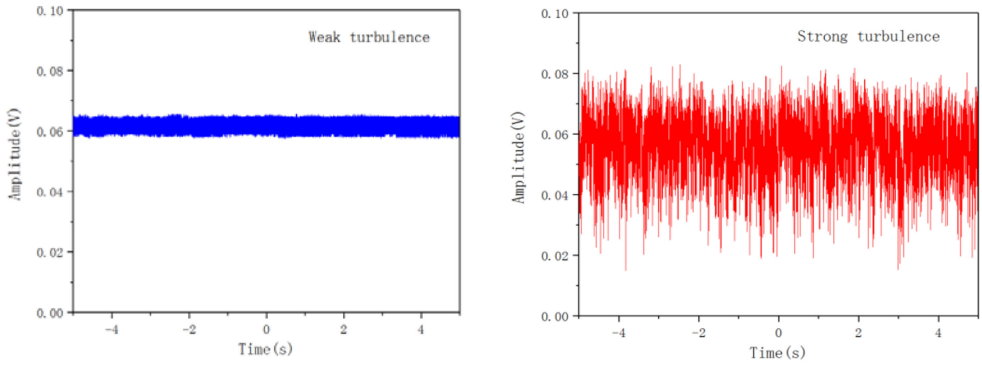
In this experiment, two-dimensional optical encoder and decoder are constructed by WSS. Because the spectral width of laser is about 1.2 nm, the code length is 7 and code weight is 2. Hence, we employ two-dimensional prime hopping code $\{\lambda_{53}0\lambda_{54}0000\}$ [29]. As shown in Fig. 3, the two-dimensional optical encoder consists of WSS drop and optical fiber delay lines (ODL), and the optical decoder consists of WSS add and ODL. Each port of WSS corresponds to different wavelengths for wavelength-domain coding. Different ports connect different lengths of ODLs for time-domain coding. The delay of each port of the decoder is complementary to the delay of the corresponding port of the encoder. Since the delay of each port is different and the wavelength of each port can be selected by computer, it is easy for the legitimate user to change the optical code. Similarly, we have considered the influence of pigtails of WSS and coupler. The relative delays of encoder are 0 ps and 28.6 ps, and the relative delays of decoder are 100 ps and 71.4 ps, respectively.

3. Reliability Analysis

Different turbulence conditions can be simulated by controlling hot wind temperature and wind speed, and different received power p_{rb} (dBm) (corresponding to different distances) can be controlled by tunable attenuator. Fig. 4 shows the received signal waveforms of weak and strong turbulence cases. The x label (s) represents the time, and the y label (V) indicates the signal amplitude. The test time is 10 s and the sampling interval is 0.01 ms. Due to different wind speeds and temperatures of the channel, the waveform jitter of strong turbulence is particularly severe.

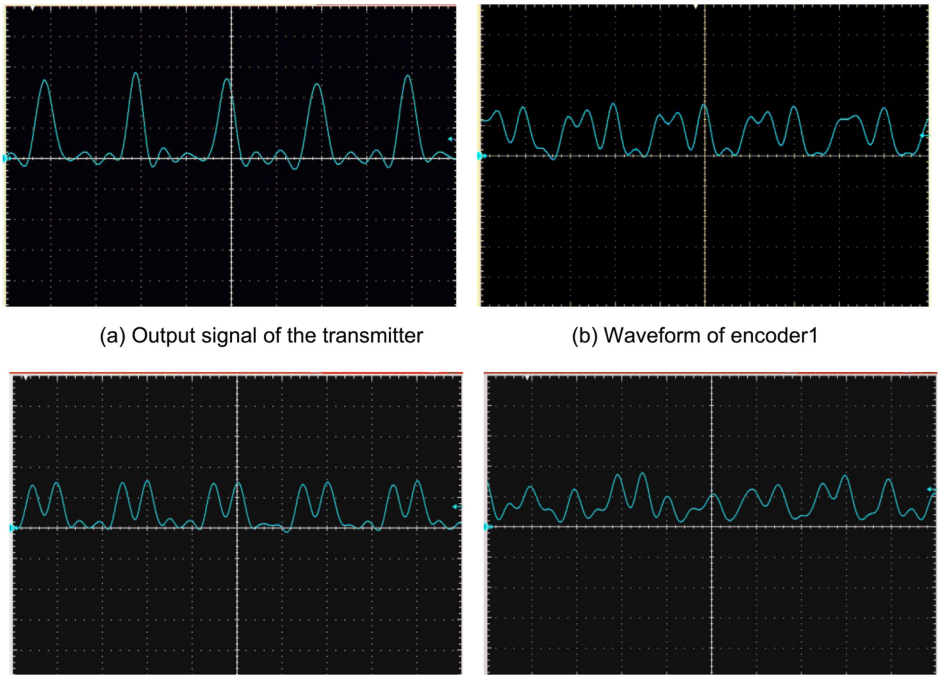
In [6], refractive index structure coefficient is used to represent turbulence strength. We can obtain the refractive index structure coefficient $c_n^2 = \frac{\sigma_1^2}{1.23} k^{\frac{-7}{6}} L^{\frac{-11}{6}}$, where k is wave number, and L is the link distance in meters. σ_1^2 is variance, which can be calculated by $\sigma_1^2 = \langle I_1^2 \rangle / \langle I_1 \rangle^2 - 1$, where I_1 is the received intensity after passing through the turbulent channel [30]. In this experiment, the refractive index structure coefficients are 1.53×10^{-13} and 4.96×10^{-15} in strong turbulence and weak turbulence respectively [21].

Fig. 5 shows the signal waveforms. The x label (100 ps/div) represents the time, and the y label (20 mV/div) indicates the signal amplitude. For the OOK system, when the data bit is “1”, the transmitter sends the optical pulse, while when the data bit is “0”, the transmitter does not send the optical pulse. Fig. 5(a) is the output signal of the transmitter at a data rate of 10 Gb/s. Fig. 5(b) is the encoded waveform of the one-dimensional optical encoder employing optical orthogonal code {0110010}. Fig. 5(c) is the encoded waveform of the two-dimensional optical encoder employing



(a) weak turbulence (b) strong turbulence

Fig. 4. Received signal waveforms of different turbulences.



(a) Output signal of the transmitter (b) Waveform of encoder1

(c) Waveform of encoder2 (d) Combined waveform

Fig. 5. Signal waveforms of one encoder and two encoders.

prime hopping code $\{\lambda_{53}0\lambda_{54}0000\}$. It can be seen from Figs. 5(b) and 5(c) that, for single-user non-diversity system, Eve can recover user data directly through bit energy detection without optical decoder. Fig. 5(d) is the waveform of the signals after the coupler. As can be seen from 5(d), for the combined waveform signal, Eve cannot directly recover the original signal through energy detection, but needs a matched decoder. Therefore, the physical-layer security of OCDMA time-diversity system is improved.

In OCDMA time-diversity reception system, the reliability of the system is affected by the different delay of two coded signals. In order to verify the relationship between the performance improvement of OCDMA time-diversity and the correlation of the two signals, we set up two different delays in this experiment. In case 1, the 20 m fiber delay line with a delay of about 103 ns is used. At this time, the two signals of the system are highly correlated. In case 2, the 25 Km single-mode optical

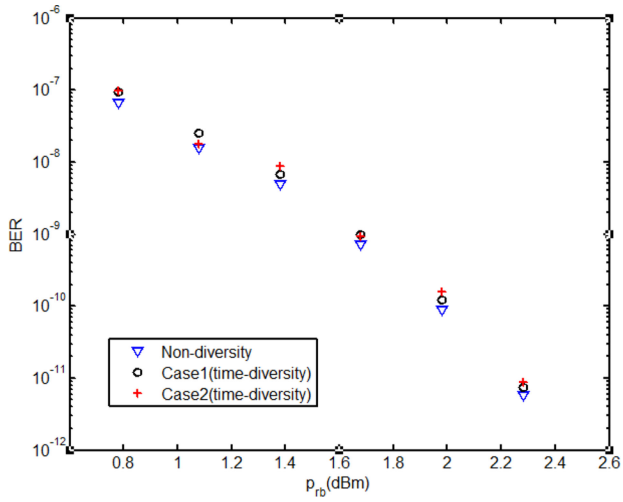
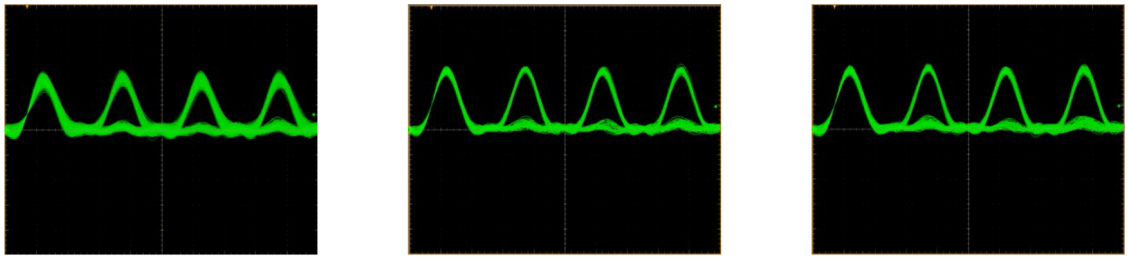


Fig. 6. BER of legitimate user in back-to-back transmission.



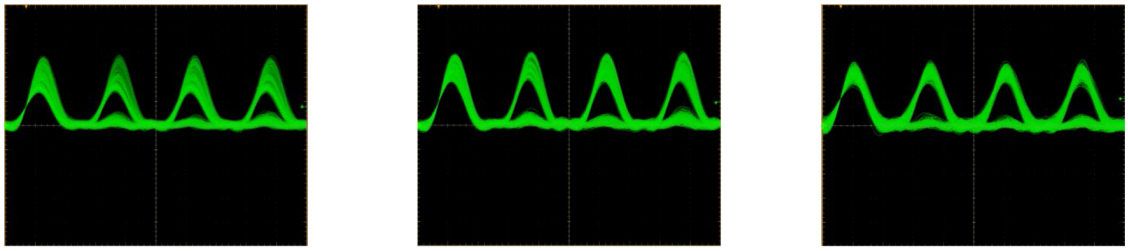
(a) Non-diversity (b) Case1 (c) Case2

Fig. 7. Eye diagrams of legitimate user in weak turbulence.

fiber with a delay of about 0.129 ms is used. In this case, the correlation between the two signals of the system is small. Because different channel characteristics correspond to different coherency time in a real FSO system, the delay setting of diversity signal needs to be changed according to the channel turbulence intensity and transmission distance.

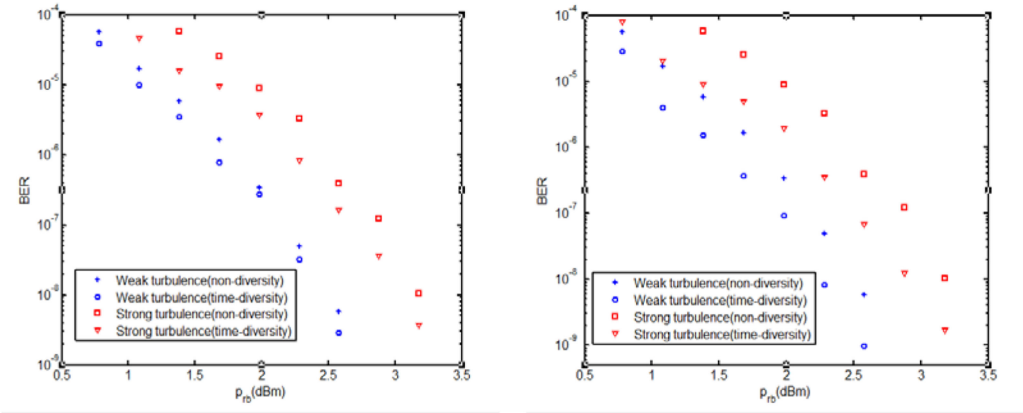
In OCDMA time-diversity reception system, code cross-correlation depends on the relative delay of two optical codes. Incomplete orthogonality of two codes will lead to multiple access interference (MAI). However, in the non-diversity system, users only send one encoded signal (encoder 2), so there is no MAI. In the back-to-back situation, when there is no MAI, the performance of non-diversity system should be exactly the same as that of time-diversity system. When there is MAI, the performance of non-diversity system is better than that of time-diversity system. In the experiment, the relative delay of two encoded signals is adjusted to minimize the code cross-correlation. However, the MAI of the experimental system cannot be eliminated completely. Fig. 6 shows the BER of legitimate user in the back-to-back transmission. For each data test, we tested three sets of data and then averaged the results. It can be seen that the BER of non-diversity system is slightly lower than that of time-diversity system. For example, when the received power is 2.28 dBm, BERs are 5.68×10^{-12}, 7.52×10^{-12}, 8.83×10^{-12} in non-diversity, case1 and case 2, respectively.

Fig. 7 shows the eye diagrams of legitimate user in weak turbulence at received power of 3.18 dBm. Fig. 8 shows the eye diagrams of legitimate user in strong turbulence. The x label (40 ps/div) represents the time, and the y label (50 mV/div) indicates the signal amplitude. It can be seen that OCDMA time-diversity can improve the system reliability, especially in strong turbulence.



(a) Non-diversity (b) Case1 (c) Case2

Fig. 8. Eye diagrams of legitimate user in strong turbulence.



(a)Case1 (b)Case2

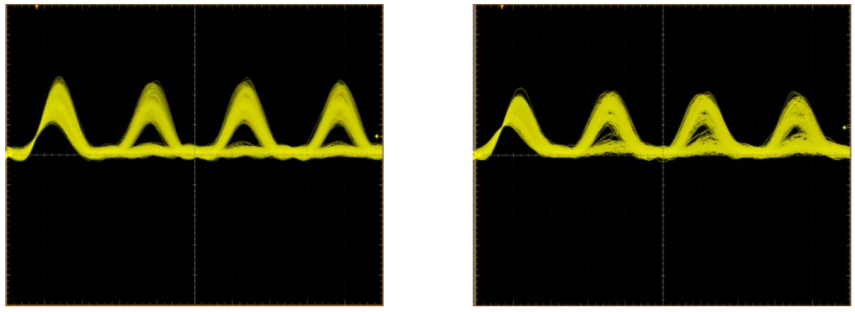
Fig. 9. BER of legitimate user with different delays.

Furthermore, when the two signals of OCDMA time-diversity become less dependent, the reliability improvement is more obvious.

Fig. 9 shows the BER of legitimate users with different delays. Whether in case 1 or case 2, OCDMA time-diversity can reduce the BER of FSO channel in both of weak turbulence and strong turbulence. In strong turbulence, the signal fluctuates greatly. Because OCDMA time-diversity can reduce the impact of atmospheric turbulence, the improvement of system reliability in strong turbulence is greater than that in weak turbulence. Compared with Figs. 9(a) and 9(b), the improvement of case 2 is more obvious. At the received power of 2.58 dBm in weak turbulence, the BERs are 5.81×10^{-9}, 2.86×10^{-9}, 9.85×10^{-10} in non-diversity, case1 and case 2 respectively. In case of strong turbulence, BERs are 3.9×10^{-7}, 1.59×10^{-7}, 6.73×10^{-8} in non-diversity, case 1 and case 2 respectively. This shows that the reliability improvement is more obvious when the correlation between the two signals of time-diversity is smaller. One method to further improve performance is to increase the number of OCDMA diversity.

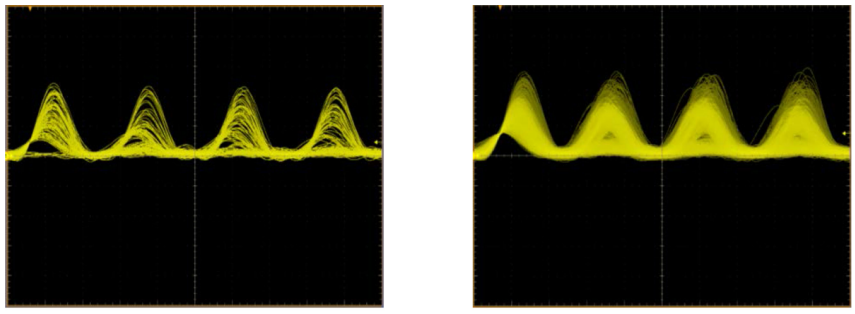
4. Physical-Layer Security

Because the delay of OCDMA time-diversity FSO wiretap channel is variable and the specific code is reconfigurable, Eve cannot accurately obtain the specific delay settings and optical code. Therefore, Eve cannot crack the optical code and must employ unmatched decoder with non-diversity reception. In this experiment, the optical power of Eve is changed by the angle of the receiving collimator lens, which corresponds to different extraction ratio of eavesdropping. Then, Eve can use an EDFA to amplify the optical signal, so that the power received by the Eve is consistent with that of the legitimate user.



(a)Non-diversity (b) Time-diversity, case 2

Fig. 10. Eve's eye diagrams in weak turbulence.



(a) Non-diversity (b) Time-diversity, case 2

Fig. 11. Eve's eye diagrams in strong turbulence.

Fig. 10 plots Eve's eye diagrams in weak turbulence, and Fig. 11 depicts Eve's eye diagrams in strong turbulence. Here, the received power of legitimate user is 3.18 dBm, and the extraction ratio r_e is 1%. As can be seen from Fig. 10 and Fig. 11, compared with non-diversity system, Eve's eye diagrams become worse in OCDMA time-diversity system. This is due to MAI in OCDMA signals with different time-diversity, which will reduce the SNR of Eve.

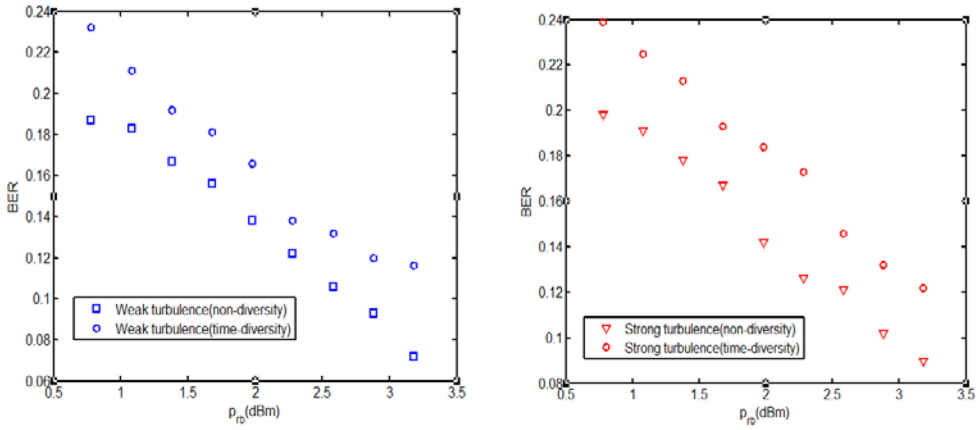
Fig. 12 shows the BER of Eve in FSO wiretap channel (case 2). At the same turbulence and received power, OCDMA time-diversity increases the BER of Eve. This is because Eve does not know the specific delay settings and codes, and can only use non-diversity reception and unmatched decoder, which will reduce the signal noise ratio (SNR) of Eve. Therefore, OCDMA time-diversity can enhance the physical-layer security of FSO wiretap channel.

In [31], the performance of the optimum quantum receiver for on-off keying and optical binary phase shift keying is examined as a pure state (no noise) problem. The classical capacity of the binary symmetric channel for these two modulation schemes is then evaluated for the optimum quantum receiver by making use of the concept of quantum measurement states. Fig. 13 is the binary symmetric channel model for legitimate channel and Eve channel respectively. X is the channel input, Z is the channel output of legitimate user, and Z_e is the channel output of Eve. P_b is the BER of legitimate channel, and P_e is the BER of Eve channel. Channel capacity (bit/symbol) of legitimate channel is

$$C_{XZ} = \max_{p(x)} \{I(X;Z)\} = \max_{p(x)} \{H(X) - H(X/Z)\} \tag{1}$$

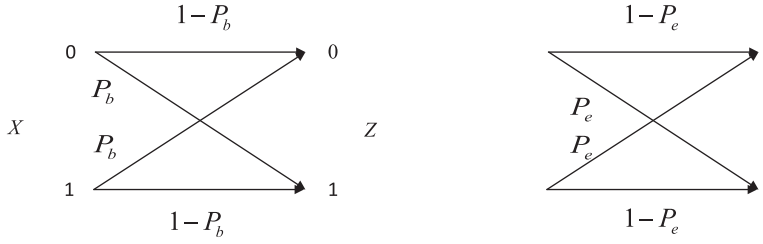
Here, *p(x)* is the input probability at Alice. $I(X;Z)$ is the average mutual information. $H(X)$ is source entropy, and $H(X/Z)$ is conditional entropy. Similarly, channel capacity of Eve is

$$C_{XZe} = \max_{p(x)} \{I(X;Ze)\} = \max_{p(x)} \{H(X) - H(X/Ze)\} \tag{2}$$



(a) Weak turbulence (b) Strong turbulence

Fig. 12. BER of Eve in FSO wiretap channel.



(a) Legitimate channel (b) Eve channel

Fig. 13. Binary symmetric channel model.

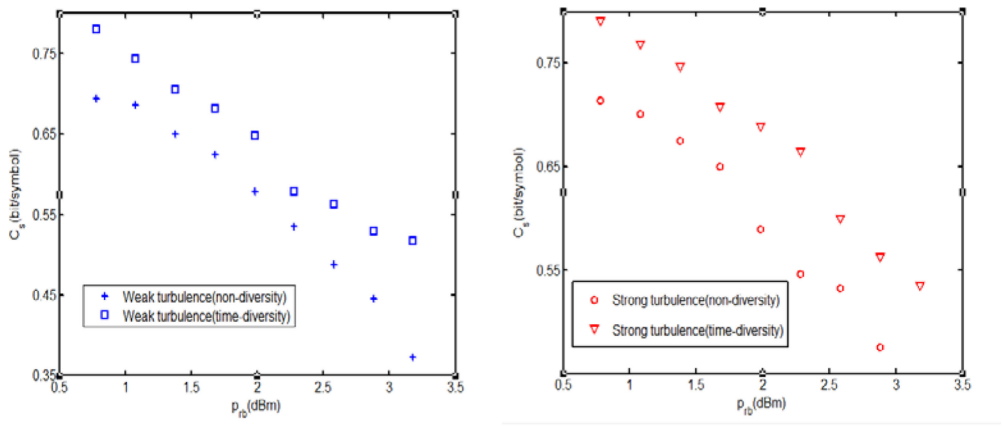
We assume that users will send bit data "0" and "1" equally, hence $H(X) = 1$. Then, channel capacity can be calculated as

$$C_{XZ} = 1 - [-(1-P_b)\log_2(1-P_b) - P_b\log_2 P_b]$$
$$C_{XZe} = 1 - [-(1-P_e)\log_2(1-P_e) - P_e\log_2 P_e] \quad (3)$$

Here, we use the secrecy capacity to evaluate the physical-layer security of FSO wiretap channel using OCDMA time-diversity reception. Secrecy capacity is the maximum transmission rate at which Eve is unable to extract any information. Secrecy capacity is defined as [32]

$$C_S = \begin{cases} C_{XZ} - C_{XZe}, & C_{XZ} > C_{XZe} \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

Fig. 14 is the secrecy capacity in FSO wiretap channel. It can be seen that the secrecy capacity of time-diversity system is larger than that of non-diversity system in both weak and strong turbulence, which indicates that OCDMA time-diversity can improve the physical-layer security of FSO wiretap channel. The reason is that legitimate users can use diversity reception and matched decoder, while Eve can only use non-diversity reception and unmatched decoder. At the received power 2.28 dBm in weak turbulence, secrecy capacities are 0.535 bit/symbol and 0.579 bit/symbol in non-diversity and time-diversity respectively. In case of strong turbulence, secrecy capacities are 0.546 bit/symbol and 0.665 bit/symbol in non-diversity and time-diversity respectively. On the other hand, at the same received power, the secrecy capacity of strong turbulence is about 15% higher than that of weak turbulence. The reason is that, the strong turbulence has less influence on the legitimate



(a) Weak turbulence (b) Strong turbulence

Fig. 14. Secrecy capacity in FSO wiretap channel.

user when the signal power is high. However, duo to non-diversity reception and extraction ratio 1%, the signal power of Eve is very low. Therefore, the strong turbulence has larger effect on the BER performance of Eve than that of weak turbulence.

5. Conclusion

In this paper, for the first time, we design and demonstrate a 10 Gb/s experimental system of FSO wiretap channel using OCDMA time-diversity reception. The BERs of the legitimate user and Eve are measured, and the secrecy capacity of the system is obtained. As a result, OCDMA time-diversity scheme can not only improve the reliability of FSO wiretap channel, but also enhance the physical-layer security.

The reliability improvement is more obvious when the correlation between the two signals of time-diversity is smaller. For example, at the received power of 2.58 dBm in weak turbulence, BERs are 5.81×10^{-9}, 2.86×10^{-9}, 9.85×10^{-10} in non-diversity, 103 ns delay and 0.129 ms delay, respectively. It should be pointed out that in a real FSO system, the delay setting of diversity signal needs to be changed according to the channel turbulence intensity and transmission distance. The secrecy capacities in weak turbulence are 0.535 bit/symbol and 0.579 bit/symbol in non-diversity and time-diversity (case 2) respectively when received power is 2.28 dBm. On the other hand, the secrecy capacity of strong turbulence is higher than that of weak turbulence. For example, at the received power of 2.28 dBm in time-diversity (case 2), secrecy capacities are 0.579 bit/symbol and 0.665 bit/symbol in weak turbulence and strong turbulence respectively.

In future research, we will realize long transmission distance of OCDMA time-diversity FSO wiretap channel. In addition, we will study the performance of multi-user FSO wiretap channel with OCDMA time-diversity reception.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions.

References

[1] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *Commun. Surv. Tut. IEEE*, vol. 16, no. 4, pp. 2231–2258, Oct./Dec. 2014.

[2] X. Zhu and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1293–1300, Nov. 2002.

[3] A. Jurado-Navas *et al.*, "Hybrid optical CDMA-FSO communications network under spatially correlated gamma-gamma scintillation," *Opt. Express*, vol. 24, no. 15, pp. 16799–16814, 2016.
[4] D. Shah, D. Kothari, and A. Ghosh, "Performance of free-space optical link with wavelength diversity over exponentiated Weibull channel," *Opt. Eng.*, vol. 55, no. 11, 2017, Art. no. 116112.
[5] K. A. Balaji and K. Prabu, "Performance evaluation of FSO system using wavelength and time diversity over malaga turbulence channel with pointing errors," *Opt. Commun.*, vol. 410, pp. 643–651, 2018.
[6] C. H. Kwok, R. V Penty, and I. H. White, "Link reliability improvement for optical wireless communication systems with temporal-domain diversity reception," *IEEE Photon. Technol. Lett.*, vol. 20, no. 9, pp. 700–702, May 2008.
[7] F. Xu *et al.*, "Channel coding and time-diversity for optical wireless links. [J]," *Opt. Express*, vol. 17, no. 2, pp. 872–87, 2009.
[8] Y. Han *et al.*, "Theoretical and experimental studies of turbo product code with time diversity in free space optical communication," *Opt. Express*, vol. 18, no. 26, pp. 26978–88, 2010.
[9] W. Ali *et al.*, "Design and assessment of a 2.5-Gb/s optical wireless transmission system for high energy physics," *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no. 7907208.
[10] N. A. M. Nor *et al.*, "Experimental investigation of all-optical relay-assisted 10 Gb/s FSO link over the atmospheric turbulence channel," *J. Lightw. Technol.*, vol. 53, no. 1, pp. 43–53, Jan. 2017.
[11] D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photon. J.*, vol. 8, no. 5, Oct. 2016, Art. no. 7804809.
[12] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, Apr. 2015, Art. no. 7901014.
[13] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," *IEEE Photon. J.*, vol. 7, no. 5, Oct. 2015, Art. no. 7903418.
[14] M. J. Saber, and S. M. S. Sadough, "On secure free-space optical communications over málaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, Apr. 2017.
[15] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," *J. Lightw. Technol.*, vol. 23, no. 4, pp. 1652–1663, Apr. 2005.
[16] T. H. Shake "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.
[17] Z. Wang, J. Chang, and P. R. Prucnal, "Theoretical analysis and experimental investigation on the confidentiality of 2-d incoherent optical CDMA system," *J. Lightw. Technol.*, vol. 28, no. 12, pp. 1761–1769, Jun. 2010.
[18] M. Jazayerifar and J. A. Salehi, "Atmospheric optical CDMA communication systems via optical orthogonal codes," *IEEE Trans. Commun.*, vol. 54, no. 9, pp. 1614–1623, Sep. 2006.
[19] N. R. Mirzaei, L. A. Rusch, and J. A. Salehi, "Two stage code acquisition in wireless optical cdma communications using optical orthogonal codes," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3480–3491, Aug. 2016.
[20] M. J. Islam, "Performance analysis of FSO-CDMA at different atmospheric condition," *Int. J. Adv. Electron. Commun. Syst.*, vol. 2, no. 1, pp. 1–5, May 2012.
[21] A. Yadav, S. Kar, and V. K. Jain, "Performance of 1-D and 2-D OCDMA systems in presence of atmospheric turbulence and various weather conditions," *IET Commun.*, vol. 11, no. 9, pp. 1416–1422, Jun. 2017.
[22] N. T. Dang and A. T. Pham, "Performance improvement of FSO/CDMA systems over dispersive turbulence channel using multi-wavelength PPM signaling," *Opt. Express*, vol. 20, no. 24, pp. 26786–26797, 2012.
[23] J. Ji, G. Zhang, W. Li, L. Sun, K. Wang, and M. Xu, "Performance analysis of physical-layer security in an OCDMA-based wiretap channel," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 813–818, Oct. 2017.
[24] J. Jianhua *et al.*, "Performance analysis of FSO/CDMA system based on binary symmetric wiretap channel," *IET Commun.*, vol. 13, no. 1, pp. 116–123, Jan. 2019.
[25] J. Ji, Q. Huang, X. Chen, and L. Sun, "Performance analysis and experimental investigation of physical-layer security in OCDMA-based hybrid FSO/fiber wiretap channel," *IEEE Photon. J.*, vol. 11, no. 3, Jun. 2019, Art. no. 7903420.
[26] P. Liu *et al.*, "Bit error rate performance analysis of optical CDMA time-diversity links over gamma-gamma atmospheric turbulence channels," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Cancun, Mexico, 2011, pp. 1932–1936.
[27] J. Ji, B. Wu, J. Zhang, M. Xu, and K. Wang. "Enhancement of reliability and security in a time-diversity FSO/CDMA wiretap channel," *OSA Continuum*, vol. 2, no. 5, pp. 1524–1538, 2019.
[28] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.
[29] L. Tancevski, I. Andonovic, M. Tur, and J. Budin, "Massive optical LANs using wavelength hopping/time spreading with increased security," *IEEE Photon. Technol. Lett.*, vol. 8, no. 7, pp. 935–937, Jul. 1996.
[30] M. Abtahi, P. Lemieux, W. Mathlouthi, and L. A. Rusch, "Suppression of turbulence-induced scintillation in free-space optical communication systems using saturated optical amplifiers," *J. Lightw. Technol.*, vol. 24, no. 12, pp. 4966–4973, Dec. 2006.
[31] V. A. Vilnrotter, and C. W. Lau, "Quantum detection and channel capacity for communications applications," *Proc SPIE*, vol. 4635, pp. 103–115, 2002.
[32] M. Bloch, *Physical-Layer Security - From Information Theory to Security Engineering*. Cambridge U.K.: Cambridge Univ. Press, 2011, pp. 49–83.