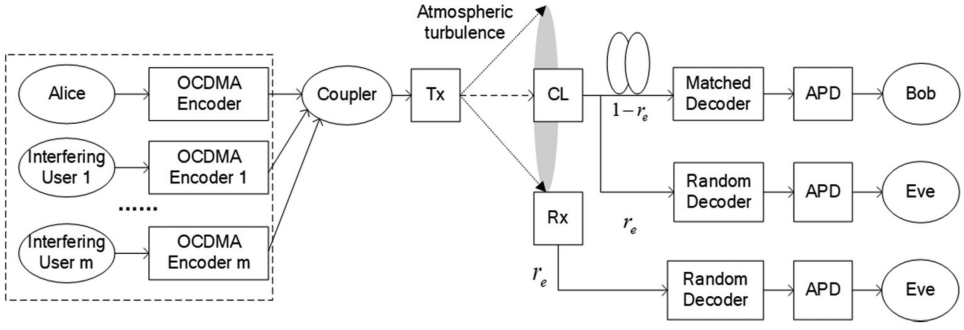
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Performance Analysis and Experimental Investigation of Physical-Layer Security in OCDMA-Based Hybrid FSO/Fiber Wiretap Channel

Volume 11, Number 3, June 2019

Jianhua Ji
Qian Huang
Xuemei Chen
Lu Sun



DOI: 10.1109/JPHOT.2019.2912965
1943-0655 © 2019 IEEE

IEEE photonics SOCIETY

IEEE

Performance Analysis and Experimental Investigation of Physical-Layer Security in OCDMA-Based Hybrid FSO/Fiber Wiretap Channel

Jianhua Ji, Qian Huang, Xuemei Chen, and Lu Sun

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

DOI:10.1109/JPHOT.2019.2912965

Manuscript received March 26, 2019; revised April 16, 2019; accepted April 19, 2019. Date of publication April 23, 2019; date of current version May 13, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61671306 and in part by JCYJ 20160328145357990.
Corresponding author: Jianhua Ji (e-mail: jjh@szu.edu.cn).

Abstract: In this paper, optical code division multiple access (OCDMA) based hybrid free-space optical (FSO)/fiber wiretap channel is proposed, and the physical-layer security is analyzed theoretically, using the conditional secrecy outage probability as the performance metric. Taking into account the background noise, multiple-access interference, shot noise, and thermal noise, the closed expression of the conditional secrecy outage probability is obtained. Under the condition that the eavesdropper intercepts information on the fiber link and the minimum conditional secrecy outage probability is zero, the safe transmission distance and interception distance of the system are defined and studied. Furthermore, a 10-Gb/s experimental system of OCDMA-based hybrid FSO/fiber wiretap channel is built for the first time. The bit error rates of the legitimate user and eavesdropper are measured as well as the interception distance of the system.

Index Terms: Free-space optical communications, optical code division multiple access, physical-layer security, secrecy outage probability.

1. Introduction

Over the past few years, free-space optical (FSO) communications have attracted considerable attention due to the flexibility, cost-effectiveness and high-capacity. They have been considered as an attractive alternative to provide high-speed communication services where fiber infrastructure deployment is impractical or deficient [1]. Moreover, the future optical networks will be hybrid, composed of different fiber and FSO links, in order to support a wide range of services over different network types at a high speed [2]. Therefore, hybrid FSO/fiber networks have been proposed and widely studied recently.

In hybrid FSO/fiber networks, optical beams transmitted through the FSO link can be directly coupled into the fiber core for seamless connection, results in no need to convert the optical signal from electrical to optical formats or vice versa for transmitting or receiving through the atmospheric medium [3]. Hence, hybrid FSO/fiber networks have the advantages of high speed, low cost and simple deployment. They can be employed for metro network extension, last mile access, or as an extension of Radio over Fiber into atmospheric links. Besides, the hybrid networks can also

be used to extend broadband connectivity to under-served areas [4]. A flexible two-way phase modulation-based FSO convergence system was proposed in [5], and it's excellent for integrating the fiber backbone and last-mile applications. Yu and Liaw demonstrated a bidirectional cross-bridge communications system, the FSO link is established across a bridge to provide emergency communications backup to the fiber link [6]. A high-speed and long-reach optical wireless communication system was proposed in [7]. A couple of doublet lenses is deployed to emanate laser beam from the ferrule of single-mode fiber (SMF) (transmitting side) into the free space and to guide laser beam from the free space into the ferrule of SMF (receiving side), significantly extending the free space transmission distance to 180m. A bidirectional FSO system integrated with fiber access network was proposed and investigate experimentally for wireless traffics. In the system, 10 Gbit/s FSO signals propagate through free space and 25 km SMF transmission link, achieving 1000m free space transmission length based on the obtained power sensitivity of each FSO signal [8]. It is also possible to support wireless transmission between remote optical wireless units [9]. Besides, there are other researches of hybrid FSO/fiber networks, which show that the reliability is guaranteed [10]–[13].

However, there are some security risks in hybrid FSO/fiber networks. FSO communications suffer from eavesdropping because of the openness of wireless channels. The FSO communication between two legitimate peers in the presence of an external eavesdropper was studied in [14], where the eavesdropper uses a sensing device to collect a fraction of the power radiated by legitimate user. In addition, the eavesdroppers can get access to a small number of optical signals by bending the optical fiber, which is not easy to be detected by legitimate users [15]. Therefore, it is necessary to study the security of hybrid FSO/fiber networks.

Encryption on the data layer, such as key sharing and key agreement, can provide positive impacts on the security [16], but it cannot guarantee absolute security. Quantum communication technology can provide absolute security, but only for low rate transmission [17]. As a supplement to the traditional encryption technology, physical-layer security was pioneered by Wyner [18]. It now receives more and more attention for it can provide a method to ensure reliable and secure communication. Optical code division multiple access (OCDMA) is considered as a good candidate to provide physical-layer security [19]. In the case of brute-force search, the physical-layer security of OCDMA was measured by code cardinality [20]. And code reconfiguration can increase the difficulty of interception, thus providing significant advantages in security [21]. The physical-layer security of OCDMA-based optical fiber communication system was analyzed in [22], and the author used security leakage factor to evaluate the physical-layer security level. According to the above analysis, OCDMA technology is useful to prevent eavesdropping and improve the physical-layer security.

Although there have been some researches on the application of OCDMA technology in hybrid FSO/fiber networks, the researches on the security are not included. In [23], experimental performance of OCDMA transmission over free space and optical fiber without optical and electrical conversion was reported for the first time. The signals have been successfully demonstrated over free space and 20 km optical fiber transmission link in experiment. A hybrid fiber-optic/FSO CDMA network connecting to fiber-optic CDMA sub-networks was studied in [24], this paper focused on the performance analysis of acquisition system in atmospheric OCDMA communications.

In this paper, OCDMA-based hybrid FSO/fiber wiretap channel is proposed, and the physical-layer security is analyzed by using the conditional secrecy outage probability as the performance metric. The eavesdropper can intercept information on the FSO link or fiber link. Considering the background noise, multiple-access interference (MAI), shot noise and thermal noise, the closed expression of the conditional secrecy outage probability is obtained. And the effects of secrecy rate, transmission distance, eavesdropping ratio and the number of interfering users are analyzed. Assuming the eavesdropper intercepts information on the fiber link and the minimum conditional secrecy outage probability is zero, the safe transmission distance and interception distance of the system are defined and studied. Furthermore, we build a 10 Gb/s experimental system of OCDMA-based hybrid FSO/fiber wiretap channel for the first time. The bit error rates (BERs) of the legitimate user and eavesdropper are measured and the interception distance of the system is obtained.

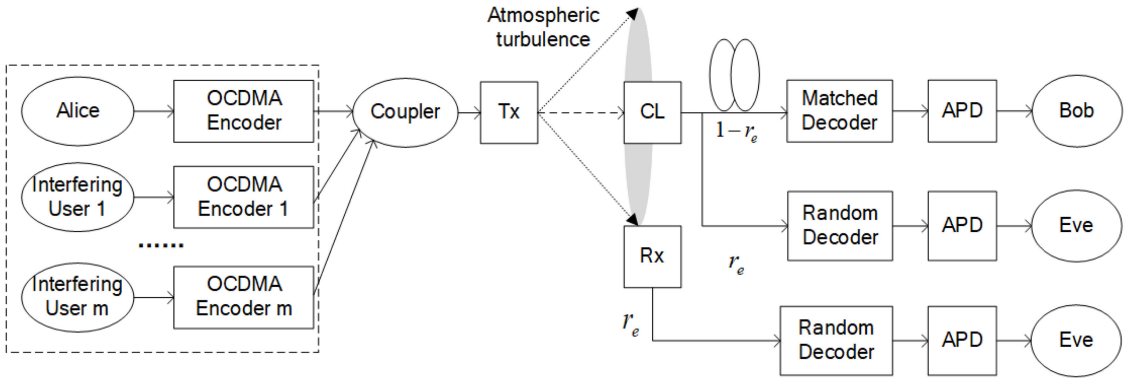


Fig. 1. OCDMA-based hybrid FSO/fiber wiretap channel model.

This paper is organized as follows. In Section 2, we will introduce OCDMA-based hybrid FSO/fiber wiretap channel model. In Section 3, the physical-layer security of OCDMA-based hybrid FSO/fiber wiretap channel will be analyzed. In Section 4, we build an experimental system of OCDMA-based hybrid FSO/fiber wiretap channel. This paper is concluded in Section 5.

2. OCDMA-Based Hybrid FSO/Fiber Wiretap Channel

2.1 OCDMA-Based Hybrid FSO/Fiber Wiretap Channel Model

Fig. 1 shows the OCDMA-based hybrid FSO/fiber wiretap channel model, where the legitimate users Alice and Bob want to communicate over the all-optical transmission link, and the eavesdropper (Eve) observes their transmission on the FSO link or fiber link. The interfering users are employed to prevent Eve from intercepting information by the way of energy detection, and they are independent of each other. The transmission power is P_0, the transmission distance and the attenuation coefficient of FSO link are d_1 and δ, the transmission distance and the attenuation coefficient of fiber link are d_2 and α, respectively.

At the transmitter, the information to be transmitted is OOK modulated and encoded through an optical encoder by using prime frequency hopping codes $(p \times p^2, p, 0, 1)$, where p is the prime number for time spread and frequency hopping. The code length is p^2, the code weight is p and the average cross-correlation value is $\mu_0 = 1/(2p)$ [25]. The encoded signal is transmitted into the atmospheric channel, which is affected by atmospheric attenuation and turbulence. Then the laser beam is directly coupled into the optical fiber through the coupling lens (CL), and is transmitted through the optical fiber. Since the laser beam transmitted in FSO link experiences divergence due to optical diffractions, one possibility for a successful eavesdropping is to locate Eve in the divergence region of the laser beam as suggested in [26]. In addition, Eve can intercept at different positions of the fiber link [18]. We assume that Eve intercepts a fraction r_e of the available power, and Bob receives a fraction $1 - r_e$ [10]. It should be noted that the eavesdropping ratio r_e is the proportion of the signal power intercepted by the eavesdropper to the total signal power at the eavesdropping location. The most ideal eavesdropping situation is that the eavesdropper can collect all the power not captured by the legitimate user. At the receiver, Bob decodes with a matched optical decoder and the signal is received by the avalanche photodiode (APD), while Eve uses a random decoder, including matched and unmatched decoders.

2.2 Atmospheric Turbulence Model

The atmospheric turbulence causes scintillation, which is the major impairment of FSO communications. It's characterized by some models such as log-normal, gamma-gamma, etc. In this paper, we mainly consider the weak turbulence, so the log-normal distribution model is adopted. The

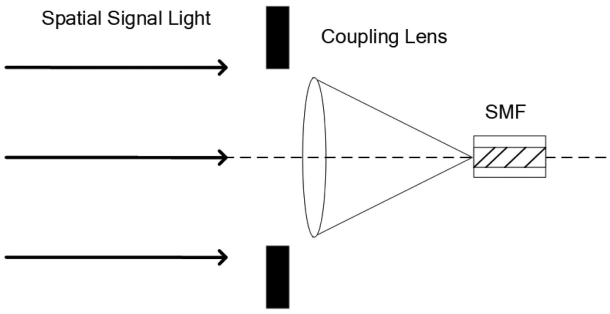


Fig. 2. Apparatus of spatial signal light directly coupling into an SMF.

probability density function (PDF) and the cumulative distribution function (CDF) for the log-normal distribution model are given by [27]

$$f(I) = \frac{1}{I\sqrt{2\pi\sigma^2}} \exp\left[-\frac{\left(\ln I + \sigma^2/2\right)^2}{2\sigma^2}\right] \tag{1}$$

$$F(I) = \frac{1}{2} erfc\left(-\frac{\ln I + \sigma^2/2}{\sigma\sqrt{2}}\right) \tag{2}$$

where $erfc(\cdot)$ is the complementary error function, σ^2 is the log-intensity variance, determined by the parameters of the channel, and can be expressed by

$$\sigma^2 = \exp\left[\frac{0.49\delta^2}{\left(1 + 0.18d^2 + 0.56\delta^{12/5}\right)^{7/6}} + \frac{0.51\delta^2}{\left(1 + 0.9d^2 + 0.62d^2\delta^{12/5}\right)^{5/6}}\right] - 1 \tag{3}$$

where $d = \sqrt{kD^2/4l_{fso}}$, $\delta^2 = 1.23C_n^2 k^{7/6} l_{fso}^{11/6}$, l_{fso} is the transmission distance of FSO link, $k = 2\pi/\lambda$ is the optical wave number, λ is the wavelength of laser source, D is the receiver's aperture diameter, C_n^2 is the altitude-dependent turbulence strength.

2.3 Fiber-Coupling Model

In hybrid FSO/fiber wiretap channel, optical beams transmitted through the FSO link can be directly coupled into the fiber core through a single lens to achieve seamless connection, as shown in Fig. 2. A coupling loss is encountered at the interface between the FSO link and fiber link, thus, a general expression for the fiber-coupling efficiency in a single-mode fiber is given by [28]

$$\eta = 8a^2 \int_0^1 \int_0^1 \left(\exp\left[-\left(a^2 + \frac{A_{RX}}{A_c}\right)\left(x_1^2 + x_2^2\right)\right] \times I_0\left(2\frac{A_{RX}}{A_c} x_1 x_2\right) x_1 x_2\right) dx_1 dx_2 \tag{4}$$

where a is the coupling geometry parameter, $A_{RX} = \pi D^2/4$ is the CL area, $A_c = \pi\rho_c^2$ is the spatial coherence area of the incident wave, with radius $\rho_c = (1.46C_n^2 k^2 l_{fso})^{-3/5}$, $I_0(\cdot)$ is a modified Bessel function of the first kind, order zero.

2.4 Eavesdrop on the FSO Link

First, we consider the case in which Eve is located in the FSO link. As shown in Fig. 1, Eve can collect the power not captured by Bob when Eve is in the divergence region of the laser beam. This is the scenario suggested in [22] as potentially likely to suffer from eavesdropping. Of course, in order not to be noticed by legitimate users, Eve should be as far away from the beam center as possible, while the coupling lens is in the beam center, so the normalized irradiance fluctuations caused by atmospheric turbulence on Bob and Eve are uncorrelated, expressed as I_B and I_E,

respectively. The distance between Eve and Alice is d_{ae}, we assume that $d_{ae} \approx d_1$, because Eve is located in the output terminal of the FSO link.

For the main channel, without considering the turbulence, the receiving chip power of Bob is

$$P_B = p^2 (1 - r_e) P_0 / 10^{\frac{\delta d_1 + \alpha d_2}{10}} \cdot \eta \tag{5}$$

There are some noises at the receiver, such as shot noise, thermal noise and background noise, which can be modeled as zero-mean Gaussian noises. When the receiving power is very small, the background noise and the thermal noise are dominant, but when the receiving power is large enough, the shot noise cannot be ignored. Besides, interfering users using different codes will cause MAI, which may affect the transmission on main channel and wiretap channel. So the average signal current and the noise mean square current can be expressed as

For user data "1",

$$I_{s,1} = RgP_B \left(1 + \frac{1}{2p^2} m\right) I_B \tag{6}$$

$$\sigma_{s,1}^2 = \sigma_{sh-s,1}^2 + \sigma_{b-s}^2 + \sigma_{th}^2 + \sigma_{MAI-s}^2 \tag{7}$$

For user data "0",

$$I_{s,0} = RgP_B \frac{1}{2p^2} m \cdot I_B \tag{8}$$

$$\sigma_{s,0}^2 = \sigma_{sh-s,0}^2 + \sigma_{b-s}^2 + \sigma_{th}^2 + \sigma_{MAI-s}^2 \tag{9}$$

where $\sigma_{sh-s,1}^2 = 2eRF_a g^2 P_B [1 + m/(2p^2)] I_B \cdot \Delta f$, $\sigma_{sh-s,0}^2 = eRF_a g^2 P_B m \cdot I_B \cdot \Delta f / p^2$ represent shot noises, $\sigma_{b-s}^2 = 2eRF_a g^2 P_b \eta \alpha_r \cdot \Delta f$ represents background noise, $\sigma_{th}^2 = 4k_B T \Delta f / R_L$ represents thermal noise, $\sigma_{MAI-s}^2 = m\mu_0(1 - \mu_0)(RgP_B I_B / p)^2$ represents the variance of MAI of Bob. Moreover, R and g are the responsibility and average gain of APD respectively, P_b is the background noise power, e is the electron charge, F_a is the excess noise factor of the APD, k_B is Boltzmann constant, T is the absolute temperature, and R_L is the load resistance. $\Delta f = p^2 \cdot R_b / 2$ is the effective noise bandwidth, where R_b denotes the bit rate. α_r is the attenuation of the background noise power of Bob on the fiber link, expressed as $\alpha_r = 10^{-\alpha d_2 / 10}$ [29].

For the wiretap channel, if Eve uses the unmatched decoder, the range of the code cross-correlation peak value is $1 \leq v < p$. Here, we consider the best case of system security, that is $v = 1$. So the receiving chip power of Eve is

$$P_{F-EU} = p r_e \cdot P_0 / 10^{\frac{\delta d_1}{10}} \tag{10}$$

It's the worst performance for Eve (the upper bound of system security). Hence, the average signal current and the noise mean square current of Eve are represented as

For user data "1",

$$I_{F-eu,1} = RgP_{F-EU} \left(1 + \frac{1}{2p} m\right) I_E \tag{11}$$

$$\sigma_{F-eu,1}^2 = \sigma_{sh-F-eu,1}^2 + \sigma_{b-F-e}^2 + \sigma_{th}^2 + \sigma_{MAI-F-eu}^2 \tag{12}$$

For user data "0",

$$I_{F-eu,0} = RgP_{F-EU} \frac{1}{2p} m \cdot I_E \tag{13}$$

$$\sigma_{F-eu,0}^2 = \sigma_{sh-F-eu,0}^2 + \sigma_{b-F-e}^2 + \sigma_{th}^2 + \sigma_{MAI-F-eu}^2 \tag{14}$$

where $\sigma_{sh-F-eu,1}^2 = 2eRF_a g^2 P_{F-EU} [1 + m/(2p)] I_E \cdot \Delta f$, $\sigma_{sh-F-eu,0}^2 = eRF_a g^2 P_{F-EU} m \cdot I_E \cdot \Delta f / p$ represent shot noises, $\sigma_{b-F-e}^2 = 2eRF_a g^2 P_b \cdot \Delta f$ represents background noise, $\sigma_{MAI-F-eu}^2 = m\mu_0(1 - \mu_0)(RgP_{F-EU} I_E)^2$ represents the variance of MAI of Eve.

However, if Eve uses the matched decoder, the code cross-correlation peak value is $v = p$, so the receiving chip power of Eve is

$$P_{F-EM} = p^2 r_e \cdot P_0 / 10^{\frac{\delta d_1}{10}} \tag{15}$$

In this case, the physical-layer security of the system reaches the lower bound. So the average signal current and the noise mean square current are represented as

For user data "1",

$$I_{F-em,1} = RgP_{F-EM}\left(1 + \frac{1}{2p^2}m\right) I_E \tag{16}$$

$$\sigma^2_{F-em,1} = \sigma^2_{sh-F-em,1} + \sigma^2_{b-F-e} + \sigma^2_{th} + \sigma^2_{MAI-F-em} \tag{17}$$

For user data "0",

$$I_{F-em,0} = RgP_{F-EM}\frac{1}{2p^2} m \cdot I_E \tag{18}$$

$$\sigma^2_{F-em,0} = \sigma^2_{sh-F-em,0} + \sigma^2_{b-F-e} + \sigma^2_{th} + \sigma^2_{MAI-F-em} \tag{19}$$

where $\sigma^2_{sh-F-em,1} = 2eRF_a g^2 P_{F-EM}[1 + m/(2p^2)]I_E \cdot \Delta f$, $\sigma^2_{sh-F-em,0} = eRF_a g^2 P_{F-EM} m \cdot I_E \cdot \Delta f / p^2$ represent shot noises, $\sigma^2_{MAI-F-em} = m\mu_0(1-\mu_0)(RgP_{F-EM} I_E/p)^2$ represents the variance of MAI of Eve.

2.5 Eavesdrop on the Fiber Link

We now consider the case that Eve intercepts information on the fiber link, where Bob and Eve are affected by the same atmospheric turbulence, that is $I_E = I_B$. Therefore, the analysis of the main channel is the same as above. For the wiretap channel, we assume that the eavesdropping distance (distance between Eve and CL) is d_{ce}. If Eve uses the unmatched decoder, and the code cross-correlation peak value is $v = 1$, the receiving chip power of Eve is

$$P_{O-EU} = p r_e \cdot P_0 / 10^{\frac{\delta d_1 + \alpha d_{ce}}{10}} \cdot \eta \tag{20}$$

Hence, the average signal current and the noise mean square current of Eve are represented as

For user data "1",

$$I_{O-eu,1} = RgP_{O-EU}\left(1 + \frac{1}{2p}m\right) I_B \tag{21}$$

$$\sigma^2_{O-eu,1} = \sigma^2_{sh-O-eu,1} + \sigma^2_{b-O-e} + \sigma^2_{th} + \sigma^2_{MAI-O-eu} \tag{22}$$

For user data "0",

$$I_{O-eu,0} = RgP_{O-EU}\frac{1}{2p} m \cdot I_B \tag{23}$$

$$\sigma^2_{O-eu,0} = \sigma^2_{sh-O-eu,0} + \sigma^2_{b-O-e} + \sigma^2_{th} + \sigma^2_{MAI-O-eu} \tag{24}$$

where $\sigma^2_{sh-O-eu,1} = 2eRF_a g^2 P_{O-EU}[1 + m/(2p)]I_B \cdot \Delta f$, $\sigma^2_{sh-O-eu,0} = eRF_a g^2 P_{O-EU} m \cdot I_B \cdot \Delta f / p$ represent shot noises, $\sigma^2_{b-O-e} = 2eRF_a g^2 P_b \eta \alpha_d \cdot \Delta f$ represents background noise, $\sigma^2_{MAI-O-eu} = m\mu_0(1-\mu_0)(RgP_{O-EU} I_B)^2$ represents the variance of MAI of Eve, α_d is the attenuation of the background noise power of Eve on the fiber link, expressed as $\alpha_d = 10^{-\alpha d_{ce}/10}$.

If Eve uses the matched decoder, the receiving chip power of Eve is

$$P_{O-EM} = p^2 r_e \cdot P_0 / 10^{\frac{\delta d_1 + \alpha d_{ce}}{10}} \cdot \eta \tag{25}$$

Hence, the average signal current and the noise mean square current of Eve are represented as

For user data "1",

$$I_{O-em,1} = RgP_{O-EM}\left(1 + \frac{1}{2p^2}m\right)I_B \tag{26}$$

$$\sigma^2_{O-em,1} = \sigma^2_{sh-O-em,1} + \sigma^2_{b-O-e} + \sigma^2_{th} + \sigma^2_{MAI-O-em} \tag{27}$$

For user data "0",

$$I_{O-em,0} = RgP_{O-EM}\frac{1}{2p^2}m \cdot I_B \tag{28}$$

$$\sigma^2_{O-em,0} = \sigma^2_{sh-O-em,0} + \sigma^2_{b-O-e} + \sigma^2_{th} + \sigma^2_{MAI-O-em} \tag{29}$$

where $\sigma^2_{sh-O-em,1} = 2eRF_a g^2 P_{O-EM}[1 + m/(2p^2)]I_B \cdot \Delta f$, $\sigma^2_{sh-O-em,0} = eRF_a g^2 P_{O-EM} m \cdot I_B \cdot \Delta f/p^2$ represent shot noises, $\sigma^2_{MAI-O-em} = m\mu_0(1-\mu_0)(RgP_{O-EM}I_B/p)^2$ represents the variance of MAI of Eve.

3. Analysis Results and Discussion

According to the above analysis, the signal-to-noise ratios (SNRs) of Bob and Eve will be as follows [30]

$$\gamma_b = \frac{(I_{s,1} - I_{s,0})^2}{(\sigma_{s,1} + \sigma_{s,0})^2} \tag{30}$$

$$\gamma_{x-ey} = \frac{(I_{x-ey,1} - I_{x-ey,0})^2}{(\sigma_{x-ey,1} + \sigma_{x-ey,0})^2} \tag{31}$$

where $x = F$ and $x = O$ denote that Eve is located in the FSO link and fiber link, respectively, $y = u$ and $y = m$ denote that Eve uses the unmatched decoder and matched decoder. For the sake of simplicity, we assume a normalized bandwidth $B = 1$, then the channel capacities of the main channel and wiretap channel are given by

$$C_b = \log(1 + \gamma_b) \tag{32}$$

$$C_e = \log(1 + \gamma_{x-ey}) \tag{33}$$

The channel capacity is the maximum transmission rate that the channel can transmit without error, reflecting the maximum amount of information that the channel can transmit. In general, the channel capacity of the main channel is larger than that of the wiretap channel, that is $C_b > C_e$. According to the information theoretic [18], the secrecy capacity is defined as

$$C_S = C_b - C_e = \begin{cases} \log(1+\gamma_b) - \log(1+\gamma_{x-ey}) & \gamma_b \geq \gamma_{x-ey} \\ 0 & \text{otherwise} \end{cases} \tag{34}$$

The secrecy capacity is the maximum transmission rate at which Eve is unable to extract any information. The secrecy outage probability that the instantaneous secrecy capacity C_s is less than a target secrecy rate R_s, is [31]

$$P_{out} = p\,(C_s < R_s) \tag{35}$$

Here, an outage occurs whenever the reliability or the secure of the transmission will not be guaranteed. When Bob's channel cannot support the secrecy rate, i.e., $C_b < R_s$, even if there is no eavesdropper, an outage occurs. However, it is clearly not a failure in achieving perfect secrecy. It is important to provide an outage formulation which gives a more explicit measure of the level of

security. Hence, the conditional secrecy outage probability is defined as [32],

$$\begin{aligned} P_{so} &= p\left(C_s < R_s \,|\, \gamma_b > \gamma_{th}\right) \\ &= p\left(C_b - C_e < R_s \,\middle|\, \gamma_b > 2^{R_s} - 1\right) \\ &= p\left(\gamma_b < 2^{R_s}\left(1+\gamma_{x-ey}\right) - 1 \,\middle|\, \gamma_b > 2^{R_s} - 1\right) \\ &= \frac{p\left(2^{R_s} - 1 < \gamma_b < 2^{R_s}\left(1+\gamma_{x-ey}\right) - 1\right)}{p\left(\gamma_b > 2^{R_s} - 1\right)} \end{aligned} \tag{36}$$

The conditional secrecy outage probability is conditioned upon a message actually being transmitted reliably. An outage occurs only if the transmission is not perfectly secure, so the conditional secrecy outage probability can measure the possibility that the system fails to achieve perfect secrecy more accurately.

3.1 Eavesdrop on the FSO Link

According to Eq. (36), when Eve uses unmatched decoder, the closed-form expression of the conditional secrecy outage probability can be computed as

$$P_{so-u} = \frac{\int_0^{\infty}\left[F_B\left(y_2\right) - F_B\left(y_1\right)\right] f\left(I_E\right) dI_E}{1 - F_B\left(y_1\right)} \tag{37}$$

When Eve uses matched decoder, the conditional secrecy outage probability is expressed as

$$\begin{cases} P_{so-m} = \dfrac{\int_0^{\infty}\left[F_B\left(y_3\right) - F_B\left(y_1\right)\right] f\left(I_E\right) dI_E}{1 - F_B\left(y_1\right)} & R_s = 0 \\ P_{so-m} = \dfrac{\int_0^{y'}\left[F_B\left(y_3\right) - F_B\left(y_1\right)\right] f\left(I_E\right) dI_E}{1 - F_B\left(y_1\right)} + 1 - F_E\left(y'\right) & 0 < R_s \le 1 \end{cases} \tag{38}$$

where $F_B(\cdot)$ and $F_E(\cdot)$ represent the CDF of the normalized irradiance received by Bob and Eve, respectively. R_s is the normalized secrecy rate which is equivalent to spectral efficiency, since the normalized bandwidth is $B = 1$. Using binary modulation, regardless of detection technique, spectral efficiency cannot exceed 1 b/s/Hz [33], so the value range of R_s is $0 \le R_s \le 1$. Moreover, $y_i = (-b_i + \sqrt{b_i^2 - 4a_i c_i})/(2a_i)$, $y' = (-b' + \sqrt{b'2 - 4ac'})/(2a')$, and the parameters are

$$\begin{cases} a_i = \left(2eRF_a g^2 P_B \Delta f\right)^2 - 4m\mu_0\left(1-\mu_0\right)\left(\frac{RgP_B}{p}\right)^2 h_i \\ b_i = -4eRF_a g^2 P_B\left(1 + \frac{1}{p^2}m\right)\cdot \Delta f \cdot h_i \\ c_i = h_i^2 - 4\left(2eRF_a g^2 P_b \eta \alpha_r \cdot \Delta f + \frac{4k_B T}{R_L}\Delta f\right) h_i \end{cases} \tag{39}$$

$$\begin{cases} a' = \left(2eRF_a g^2 P_{F-EM}\,\Delta f\right)^2 - 4m\mu_0\left(1-\mu_0\right)\left(\frac{RgP_{F-EM}}{p}\right)^2 h' \\ b' = -4eRF_a g^2 P_{F-EM}\left(1 + \frac{1}{p^2}m\right)\cdot \Delta f \cdot h' \\ c' = h'^2 - 4\left(2eRF_a g^2 P_b \Delta f + \frac{4k_B T}{R_L}\Delta f\right) h' \end{cases} \tag{40}$$

$$h_1 = \left(2^{R_s} - 1\right)\cdot\left(2eF_a g \Delta f\right)^2 \tag{41}$$

$$h_2 = \left[2^{R_s}\left(1+\gamma_{F-eu}\right) - 1\right]\cdot\left(2eF_a g \Delta f\right)^2 \tag{42}$$

TABLE 1
System parameters and constants

Name	Symbol	Value
Boltzmann constant	k_B	$1.38\times10^{-23}\,W/K/Hz$
Electron charge	e	$1.6\times10^{-19}\,C$
Load resistance	R_L	50Ω
Receiver temperature	T	$300K$
APD responsivity	R	$0.5\,A/W$
Average gain of APD	g	30
Excess noise factor of APD	F_a	16
Background power	P_b	$-40dBm$
Wavelength of laser source	λ	$1550nm$
CL's aperture diameter	D	$0.04m$
Coupling geometry parameter	a	1.12
Refractive structure index	C_n^2	$8.4\times10^{-15}\,m^{-2/3}$
Prime number	p	13
Attenuation coefficient of fiber link	α	$0.2dB/km$
Transmission power	P_0	$10mW$
Bit rate	R_b	$1Gbit/s$

$$h_3 = \left[2^{R_s}\left(1+\gamma_{F-em}\right)-1\right]\cdot\left(2eF_a g\Delta f\right)^2 \tag{43}$$

$$h' = \frac{\left(2eRF_a g^2 P_B\Delta f\right)^2}{4m\mu_0\left(1-\mu_0\right)\left(\frac{RgP_B}{p}\right)^2\cdot 2^{R_s}} + \left(2^{-R_s}-1\right)\left(2eF_a g\Delta f\right)^2 \tag{44}$$

The derivations of Eq. (37) and Eq. (38) are presented in detail in the Appendix A and Appendix B, respectively. Then we analyze the influence of different system parameters on the conditional secrecy outage probability P_{so} through numerical calculation by MATLAB. The system parameters and constants used in the analysis are shown in Table 1.

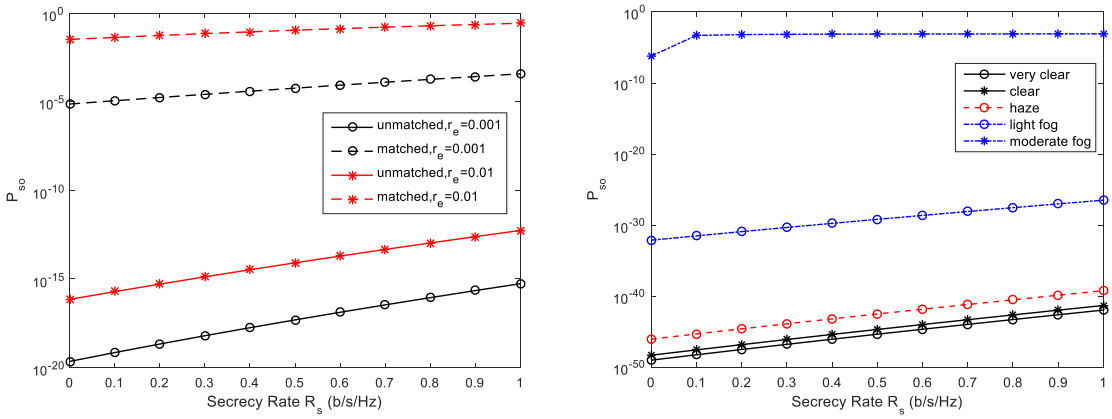


Fig. 3. Conditional secrecy outage probability versus R_s. (a) for different eavesdropping ratios. (b) for various weather conditions.

TABLE 2
Attenuation coefficients and visibility range at 1550 nm for various weather conditions

Weather Conditions	Visibility (km)	Attenuation (dB/km)
Very clear	50.0	0.0647
Clear	20.0	0.2208
Haze	6.0	0.7360
Light fog	2.0	4.2850
Moderate fog	0.6	25.5160

Fig. 3 shows the relationship between the conditional secrecy outage probability P_{so} and the secrecy rate R_s. Here, the transmission distance of FSO link is $d_1 = 2$ km, the transmission distance of fiber link is $d_2 = 50$ km, the number of interfering users is $m = 2$. In Fig. 3(a), the attenuation coefficient of FSO link is $\delta = 10$ dB/km, and the eavesdropping ratios are $r_e = 0.01$ and $r_e = 0.001$. As can be seen from the figure, whether Eve uses matched or unmatched decoder, as R_s increases, the conditional secrecy outage probability P_{so} increases, and the physical-layer security of the system decreases. In addition, the conditional secrecy outage probability P_{so} increases with increasing eavesdropping ratio. In summary, when R_s and r_e increase, the physical-layer security of the system decreases. In Fig. 3(b), Eve uses unmatched decoder, the eavesdropping ratio is $r_e = 0.01$, and the attenuation coefficients for various weather conditions are shown in Table 2 at 1550 nm [34]. As we can see, for a fixed value of R_s, P_{so} is least in the presence of very clear weather condition and increases significantly in the presence of haze and fog. It can be concluded that as the weather conditions deteriorate, the conditional secrecy outage probability P_{so} increases, and the physical-layer security of the system decreases.

Fig. 4(a) shows the relationship between the conditional secrecy outage probability P_{so} and the transmission distance of FSO link d_1. The transmission distance of fiber link is $d_2 = 50$ km. Fig. 4(b)

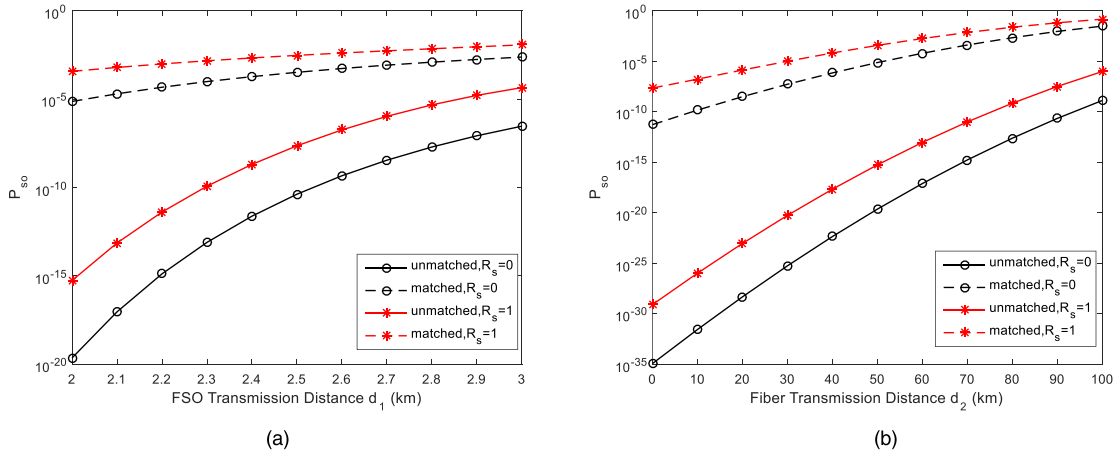


Fig. 4. Conditional secrecy outage probability as a function of (a) the transmission distance of FSO link and (b) the transmission distance of fiber link.

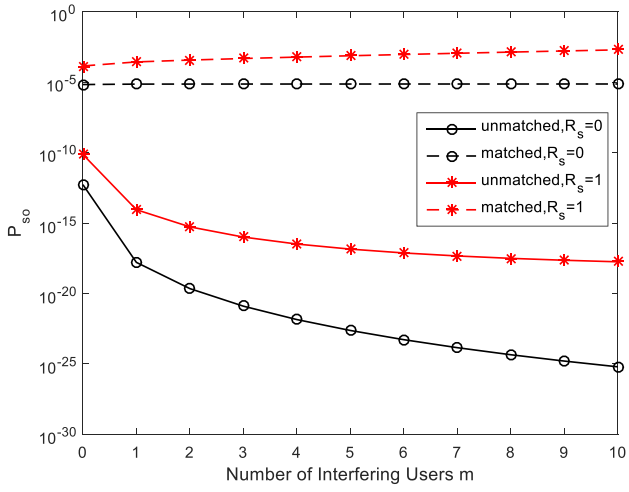


Fig. 5. Conditional secrecy outage probability as a function of the number of interfering users.

shows the conditional secrecy outage probability as a function of the transmission distance of fiber link. The transmission distance of FSO link is $d_1 = 2$ km. Here, the attenuation coefficient of FSO link is $\delta = 10$ dB/km, the number of interfering users is $m = 2$, the eavesdropping ratio is $r_e = 0.001$, and the secrecy rates are $R_s = 0$ and $R_s = 1$. From these figures, it is observed that when R_s is fixed, with the increase of the transmission distance, the conditional secrecy outage probability P_{so} increases, thus the physical-layer security of the system decreases.

The conditional secrecy outage probability as a function of the number of interfering users is shown in Fig. 5. Here, the transmission distance of FSO link is $d_1 = 2$ km, the transmission distance of fiber link is $d_2 = 50$ km, the attenuation coefficient of FSO link is $\delta = 10$ dB/km, the eavesdropping ratio is $r_e = 0.001$, and the secrecy rates are $R_s = 0$ and $R_s = 1$. As can be seen from Fig. 5, when Eve uses matched decoder, the conditional secrecy outage probability P_{so} varies less, which indicates that the impact of the number of interfering users is small, because the shot noise is the dominant factor, and is less affected by the number of interfering users. When Eve uses unmatched decoder, P_{so} decreases with the increase of the number of interfering users, indicating that increasing the number of interfering users can improve the physical-layer security of the system.

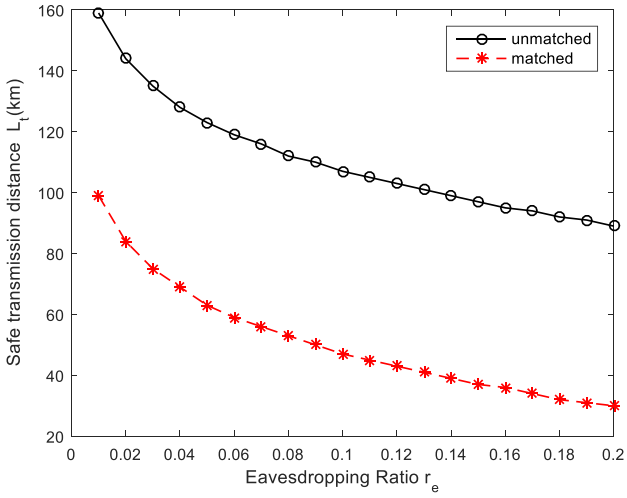


Fig. 6. Relationship between the safe transmission distance and the eavesdropping ratio.

3.2 Eavesdrop on the Fiber Link

When $R_s = 0$, Eq. (36) is simplified to

$$P_{so} = p\left(C_b < C_e\right) = p\left(\gamma_b < \gamma_e\right) \tag{45}$$

The above formulation is the same as the definition of the intercept probability (the probability that the eavesdropper successfully intercepts source signal). According to the analysis of Fig. 3, the conditional secrecy outage probability is the smallest when $R_s = 0$. It shows that the intercept probability is the minimum conditional secrecy outage probability. As long as the channel capacity of the main channel is smaller than that of the wiretap channel, that is $C_b < C_e$, an outage will occur. In this situation, when the transmission distance of FSO link d_1 is fixed, $P_{so} = 0$ always holds for short transmission distance of fiber link or long eavesdropping distance. Therefore, considering the minimum conditional secrecy outage probability $P_{so}^{\min} = 0$, we define the safe transmission distance and interception distance, in order to evaluate the physical-layer security of the system quantitatively.

3.2.1 Safe Transmission Distance: When the transmission distance of FSO link d_1 is fixed, the physical-layer security of the system is affected by the transmission distance of fiber link d_2. So we define the safe transmission distance L_t: when Eve is located anywhere in fiber link, the maximum transmission distance of fiber link under $P_{so}^{\min} = 0$.

$$L_t = \max_{P_{so}^{\min}=0} \{d_2\} \tag{46}$$

Fig. 6 shows the relationship between the safe transmission distance L_t and the eavesdropping ratio r_e. Here, the transmission distance and the attenuation coefficient of FSO link are $d_1 = 1$ km and $\delta = 10$ dB/km, the number of interfering users is $m = 2$. As long as $d_2 \leq L_t$, $P_{so}^{\min} = 0$ always holds when Eve is located anywhere in fiber link, which indicates that the system is absolutely safe when $R_s = 0$. As can be seen from Fig. 6, longer safe transmission distance would be possible by reducing the eavesdropping ratio.

3.2.2 Interception Distance: In the actual communication system, there is a case that $d_2 > L_t$. In this situation, the system cannot guarantee absolute security when Eve is located anywhere in fiber link. Therefore, we define the interception distance L_e: if the eavesdropping distance $d_{ce} < L_e$, $P_{so}^{\min} \neq 0$, and perfect secrecy is compromised.

$$L_e = \min_{P_{so}^{\min}=0} \{d_{ce}\} \tag{47}$$

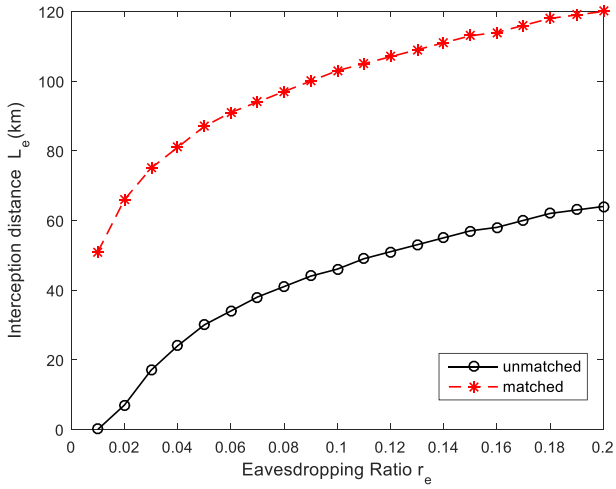


Fig. 7. Relationship between the interception distance and the eavesdropping ratio.

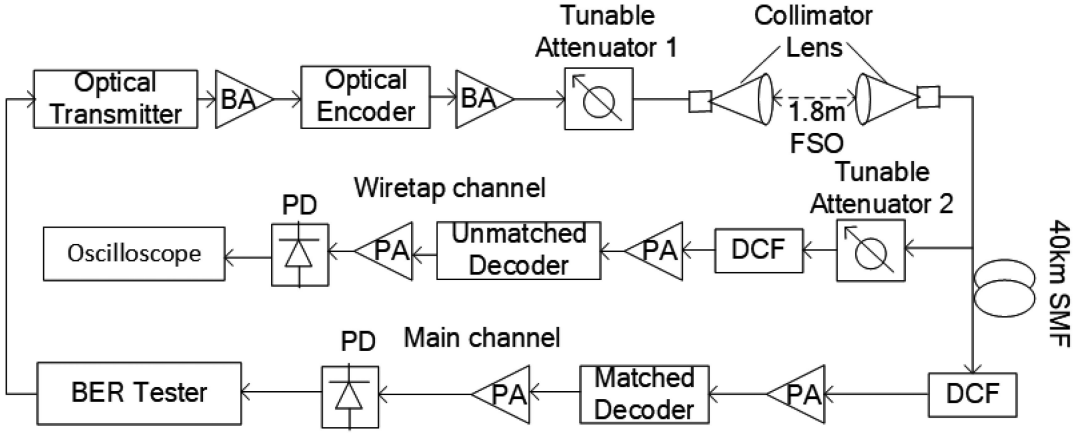


Fig. 8. 10 Gb/s experimental block diagram of OCDMA-based hybrid FSO/fiber wiretap channel.

Fig. 7 shows the relationship between the interception distance L_e and the eavesdropping ratio r_e. Here, the transmission distance and the attenuation coefficient of FSO link are $d_1 = 1$ km and $\delta = 10$ dB/km, the transmission distance of fiber link is $d_2 = 150$ km, the number of interfering users is $m = 2$. As can be seen from Fig. 7, as r_e increases, the interception distance L_e increases. When Eve uses unmatched decoder, if $r_e = 0.01$, the interception distance is $L_e = 0$ km, which indicates that the system is absolute safe when Eve is located anywhere in fiber link. If $r_e = 0.1$, the interception distance is $L_e = 46$ km, indicating that the perfect secrecy will be compromised when $d_{ce} < 46$ km. In order to achieve perfect secrecy, a monitoring device should be set up within the first 46 km range of fiber link, which is used to prevent Eve from eavesdropping.

4. Experimental Investigation

In this section, 10 Gb/s experimental system of OCDMA-based hybrid FSO/fiber wiretap channel is built for the first time. As shown in Fig. 8, FSO channel needs collimation lenses to ensure alignment.

For this experimental design, we can use prime frequency hopping codes {(13,1), (52,2), (65,3)} [35]. Firstly, SeBERT-10G BER tester sends the signal to the SPTX15ps-10G transmitter for OOK

modulation. The pulse width is 15 ps. Then the signal is amplified by Booster-Amplifier (BA). The modulated signal is OCDMA-encoded by optical encoder, and the signal attenuation generated by the encoder is about 17 dB, and the second BA is used to compensate for the attenuation. Then the signal transmits through 1.8 m FSO link and 40 km SMF link. The FVA-600 tunable attenuator 1 is used to simulate the attenuation of FSO link. And the dispersion compensation fiber (DCF) is used to compensate for the fiber dispersion, and the max insertion loss is 2.16 dB. In order to improve the system security, the low power signal is used for transmission, then the signal would be amplified before decoding. For the main channel, the signal is decoded by matched decoder and amplified by the pre-Amplifier (PA), then it is received by the 18.5-ps IR photodetector (PD). For the wiretap channel, the eavesdropper can intercept information at any position of the fiber link and decodes with unmatched optical decoder. Here, the tunable attenuator 2 is used to simulate different eavesdropping ratios. By detecting the receiving power of legitimate user, the total signal power at the eavesdropping location is calculated, and then the tunable attenuator 2 is adjusted to obtain the receiving power of the eavesdropper at a fixed eavesdropping ratio. We assume that the eavesdropper can perfectly compensate for fiber dispersion. Furthermore, we can observe the BER and the eye diagram with BER tester and Tektronix DPO 72004C 20G digital phosphor oscilloscope.

In the system, two-dimensional (2D) OCDMA is used, which performs the frequency spreading in time and wavelength domain simultaneously. 2D OCDMA encoder and decoder can be consisted of wavelength-division multiplexer, optical fiber delay line (ODL) and wavelength-division demultiplexer [36]. The wavelength of the optical pulse is adjusted by wavelength-division multiplexer and demultiplexer, and the position of the optical pulse is adjusted by the ODL. In addition, the wavelength of the optical pulse can also be adjusted by fiber Bragg grating [37]. However, in this experiment, two-dimensional optical encoder and decoder are constructed based on Wavelength Selective Switch (WSS) DROP/ADD and ODLs. Each output port of WSS DROP is connected to a ODL of different length. The length of the ODL is determined by the codeword and data rate. The wavelength of the WSS input terminal is controlled by the computer serial port and can be output to any output port of the WSS DROP. The signals encoded by the ODLs are combined and transmit through the optical links. At the receiving end, the optical signal is divided into three optical signals, and each signal connects with a different length of the ODL, which is matched with the ODL of the encoder. Similarly, the wavelength of each input port of WSS ADD is also controlled by the computer serial port and matches the wavelength setting of the WSS DROP. Then the encoded signal is matched decoded in time domain and frequency domain. For the wiretap channel, the matched length of the ODL and the matched wavelength of each optical pulse are unavailable. Thus we assume that the eavesdropper can guess the position and corresponding wavelength of one optical pulse correctly, achieving unmatched decoding.

In order to improve the modulated rate, the chip rate should be increased in the case of the same code, so a narrower optical pulse is needed. In addition, there are several ways to improve the received sensitivity. On the one hand, the code length of the prime frequency hopping code can be increased to reduce the influence of multiple access interference. On the other hand, an optical filter can be added at the receiving end to filter out-of-band noise, resulting in the improvement of the signal-to-noise ratio, thus improving the received sensitivity.

Firstly, we need to measure the atmospheric turbulence intensity. So we connect an oscilloscope at the output of the FSO channel, in order to observe the waveform and measure the signal amplitude at different times, as shown in Fig. 9. Then we substitute these data into the following equation to calculate the variance [38].

$$\sigma_I^2 = \langle I_1^2 \rangle / \langle I_1 \rangle^2 - 1 \tag{48}$$

where I_1 is the received intensity after passing through the turbulent medium. By calculation, the variance of atmospheric turbulence can be obtained as 0.0029.

Next we get the BER of legitimate user under different receiving power, as shown in Fig. 10(a). It should be pointed out that the receiving power refers to the signal power after dispersion compensation. Fig. 10(b) shows the eye diagram of the legitimate user when the receiving power is

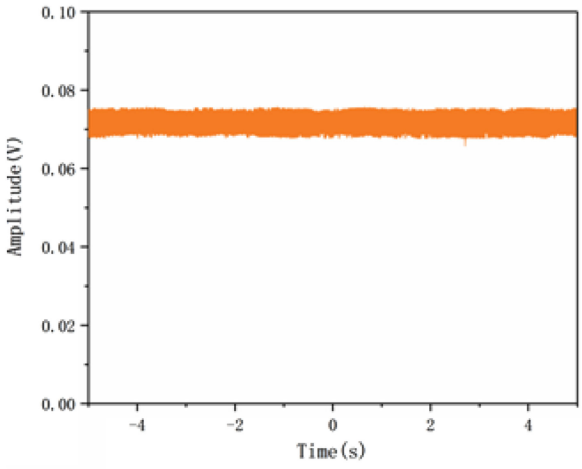
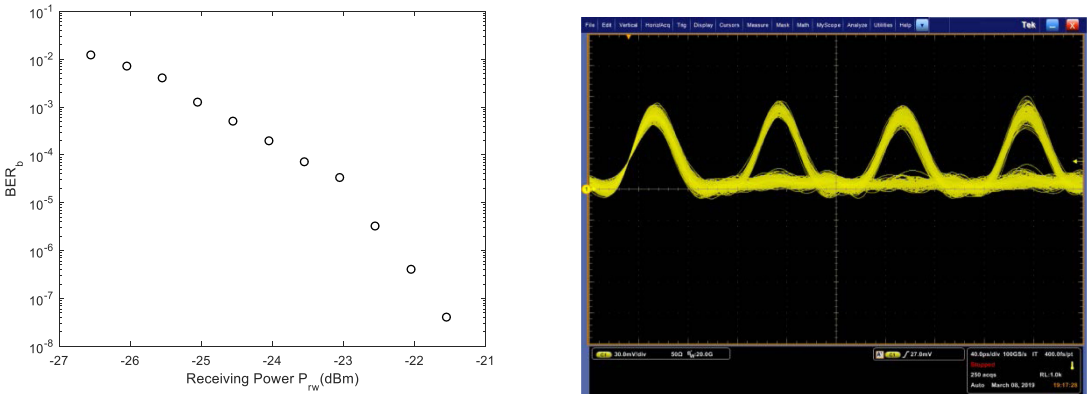


Fig. 9. Signal amplitude after the atmospheric channel.



(a) (b)

Fig. 10. (a) BER of the legitimate user as a function of the receiving power. (b) The eye diagram of the legitimate user.

-21.55 dBm. It can be seen from the figure that the eyes are fully open, indicating that the legitimate user can recover the transmitted signal and reliable transmission can be achieved.

Fig. 11(a) and 11(b) show the eye diagrams of the eavesdropper after unmatched decoding when the eavesdropping distance is $d_{ce} = 30$ km. Here, the eavesdropping ratios are $r_e = 0.5\%$ and $r_e = 1\%$. As can be seen from the figures, the eye diagrams are closed, and the corresponding BERs are 0.187 and 0.094 respectively, which indicates that the eavesdropper can't recover data correctly and the physical-layer security of the system can be guaranteed. However, the perfect secrecy may be compromised when the eavesdropper is located at other positions of the fiber link. According to Eq. (45), when the SNR of eavesdropper is larger than that of legitimate user, that is, the BER of eavesdropper is less than that of legitimate user, the system is unsafe. So the interception distance of the system can be obtained by measuring the BER of eavesdropper and comparing it with the BER of legitimate user.

Fig. 11(c) shows the relationship between the BER of the eavesdropper and the eavesdropping distance. Here, the receiving power of the legitimate user is -21.55 dBm, and the BER of the legitimate user is $BER_b = 4.12 \times 10^{-8}$. When the eavesdropping distance $d_{ce} < L_e$, the BER of the eavesdropper is less than that of the legitimate user, and the system is unsafe. So we can get

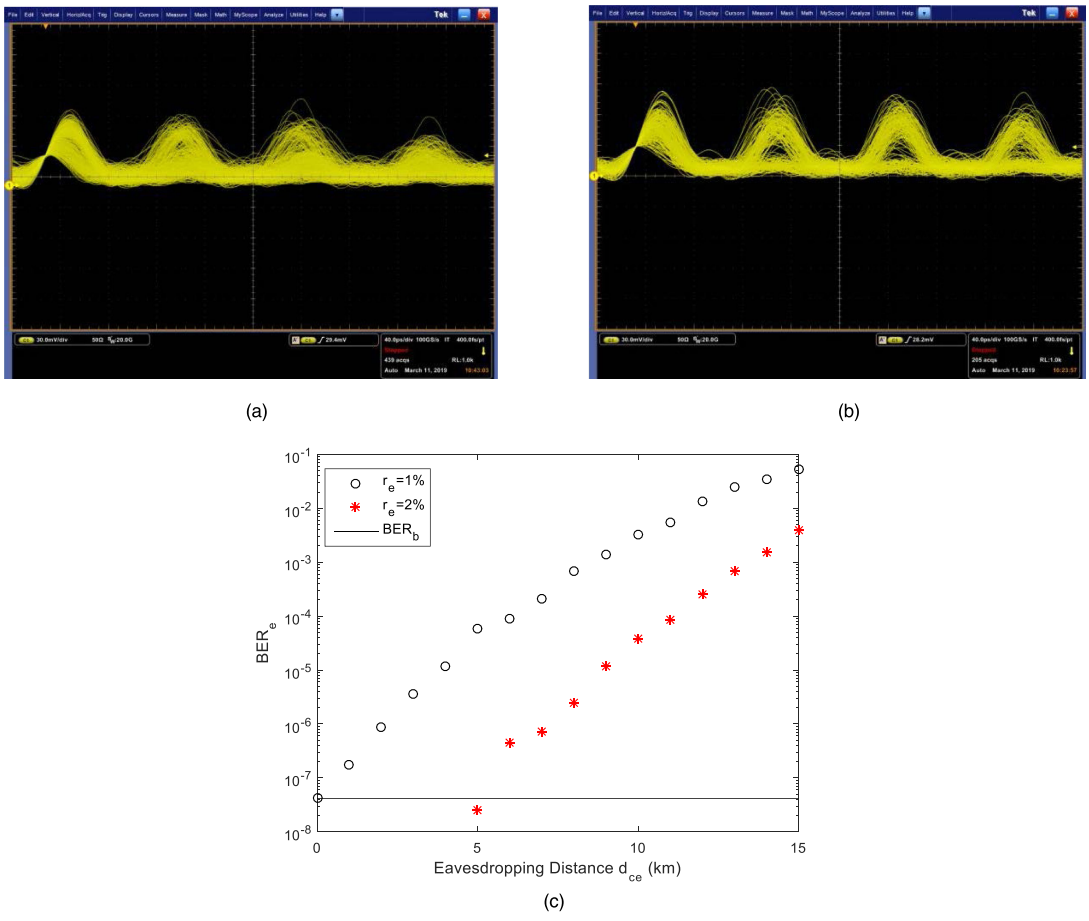


Fig. 11. The eye diagrams and BER of the eavesdropper. (a) The eye diagram of the eavesdropper when $r_e = 0.5\%$. (b) The eye diagram of the eavesdropper when $r_e = 1\%$. (c) The BER of the eavesdropper as a function of the eavesdropping distance.

the interception distance by comparing the BERs of the eavesdropper and legitimate user. As can be seen from the figure, when the eavesdropper uses unmatched decoder, if $r_e = 1\%$, the interception distance is $L_e = 0$ km, which indicates that the system can guarantee absolute security wherever the eavesdropper is located. If $r_e = 2\%$, the interception distance is $L_e = 5$ km.

5. Conclusion

In this paper, the physical-layer security of OCDMA-based hybrid FSO/fiber wiretap channel is discussed, using the conditional secrecy outage probability as the performance metric. The effects of background noise, MAI, shot noise and thermal noise are taken into account. When Eve is located in FSO link, the conditional secrecy outage probability increases with secrecy rate, transmission distance and eavesdropping ratio. As a result, the physical-layer security of the system decreases. Moreover, increasing the number of interfering users can improve the physical-layer security of the system, when Eve uses an unmatched decoder. If Eve intercepts information on the fiber link and the minimum conditional secrecy outage probability is zero, the safe transmission distance and interception distance of the system are definite. When the transmission distance of the FSO link is fixed, if $d_2 \leq L_t$, the system is perfectly secure when Eve is located anywhere in fiber link. If $d_2 > L_t$, a monitoring device should be set up within the interception distance, in order to prevent Eve from eavesdropping.

Furthermore, we build a 10Gb/s experimental system of OCDMA-based hybrid FSO/fiber wiretap channel for the first time. The BERs of the legitimate user and eavesdropper are measured, and the interception distance of the system is obtained. In our research in progress, we will improve and perfect the experiment of hybrid FSO/fiber wiretap channel, pursuing long transmission distance of FSO link and multi-user communication.

Appendix A

1. For $\gamma_b > 2^{R_s} - 1$

By substituting Eq. (30) into $\gamma_b > 2^{R_s} - 1$, we can get

$$\frac{(I_{s,1} - I_{s,0})^2}{(\sigma_{s,1} + \sigma_{s,0})^2} > 2^{R_s} - 1 \tag{49}$$

After rationalizing and simplifying the above formulation,

$$\sigma_{s,1}^2 + \sigma_{s,0}^2 - 2\sigma_{s,1}\sigma_{s,0} > h_1 \tag{50}$$

Here $h_1 = (2^{R_s} - 1) \cdot (2eF_a g \Delta f)^2$, then square on both sides.

$$\left(\sigma_{s,1}^2 - \sigma_{s,0}^2\right)^2 - 2h_1\left(\sigma_{s,1}^2 + \sigma_{s,0}^2\right) + h_1^2 > 0 \tag{51}$$

According to Eq. (7) and (9), we assume that $a_1 = (2eRF_a g^2 P_B \Delta f)^2 - 4m\mu_0(1-\mu_0)(\frac{RgP_B}{p})^2 h_1$, $b_1 = -4eRF_a g^2 P_B(1 + \frac{1}{p^2}m) \cdot \Delta f \cdot h_1$, $c_1 = h_1^2 - 4(2eRF_a g^2 P_b \eta \alpha_r \cdot \Delta f + \frac{4k_B T}{R_L}\Delta f)h_1$.

Then we can get a One-variable quadratic inequality, that is $a_1 I_B^2 + b_1 I_B + c_1 > 0$, and the solution to the inequality is

$$I_B > y_1 = \frac{-b_1 + \sqrt{b_1^2 - 4a_1 c_1}}{2a_1} \tag{52}$$

2. For $\gamma_b < 2^{R_s}(1 + \gamma_{F-eu}) - 1$

By substituting Eq. (30) into $\gamma_b < 2^{R_s}(1 + \gamma_{F-eu}) - 1$, we can get

$$\frac{(I_{s,1} - I_{s,0})^2}{(\sigma_{s,1} + \sigma_{s,0})^2} < 2^{R_s}(1 + \gamma_{F-eu}) - 1 \tag{53}$$

After rationalizing and simplifying the above formulation,

$$\sigma_{s,1}^2 + \sigma_{s,0}^2 - h_2 < 2\sigma_{s,1}\sigma_{s,0} \tag{54}$$

Here $h_2 = [2^{R_s}(1 + \gamma_{F-eu}) - 1] \cdot (2eF_a g \Delta f)^2$, when $\sigma_{s,1}^2 + \sigma_{s,0}^2 - h_2 \leq 0$, $\gamma_b < 2^{R_s}(1 + \gamma_{F-eu}) - 1$ always holds. When $\sigma_{s,1}^2 + \sigma_{s,0}^2 - h_2 > 0$, square on both sides,

$$\left(\sigma_{s,1}^2 - \sigma_{s,0}^2\right)^2 - 2h_2\left(\sigma_{s,1}^2 + \sigma_{s,0}^2\right) + h_2^2 < 0 \tag{55}$$

Then we assume that $a_2 = (2eRF_a g^2 P_B \Delta f)^2 - 4m\mu_0(1-\mu_0)(\frac{RgP_B}{p})^2 h_2$, $b_2 = -4eRF_a g^2 P_B (1 + \frac{1}{p^2}m) \cdot \Delta f \cdot h_2$, $c_2 = h_2^2 - 4(2eRF_a g^2 P_b \eta \alpha_r \cdot \Delta f + \frac{4k_B T}{R_L}\Delta f)h_2$.

So we can get a One-variable quadratic inequality, that is $a_2 I_B^2 + b_2 I_B + c_2 < 0$, and the solution to the inequality is

$$\frac{-b_2 - \sqrt{b_2^2 - 4a_2 c_2}}{2a_2} < I_B < \frac{-b_2 + \sqrt{b_2^2 - 4a_2 c_2}}{2a_2} \tag{56}$$

When $I_B \leq \frac{-b_2-\sqrt{b_2^2-4a_2c_2}}{2a_2}$, $\sigma_{s,1}^2+\sigma_{s,0}^2-h_2 \leq 0$, thus $\gamma_b < 2^{R_s}(1+\gamma_{F-eu})-1$, so the value range of I_B is

$$0 < I_B < y_2 = \frac{-b_2+\sqrt{b_2^2-4a_2c_2}}{2a_2} \tag{57}$$

In summary, the conditional secrecy outage probability is expressed as

$$\begin{aligned} P_{so-u} &= \frac{\int_0^{\infty}\int_{y_1}^{y_2} f(I_B) f(I_E)\, dI_B dI_E}{\int_{y_1}^{\infty} f(I_B)\, dI_B} \\ &= \frac{\int_0^{\infty}[F_B(y_2)-F_B(y_1)] f(I_E)\, dI_E}{1-F_B(y_1)} \end{aligned} \tag{58}$$

Appendix B

For $\gamma_b < 2^{R_s}(1+\gamma_{F-em})-1$, according to Appendix A, we assume that $h_3 = [2^{R_s}(1+\gamma_{F-em})-1]\cdot(2eF_a g\Delta f)^2$, $a_3 = (2eRF_a g^2 P_B \Delta f)^2 - 4m\mu_0(1-\mu_0)(\frac{RgP_B}{p})^2 h_3$, $b_3 = -4eRF_a g^2 P_B(1+\frac{1}{p^2}m)\cdot\Delta f\cdot h_3$, $c_3 = h_2^2 - 4(2eRF_a g^2 P_b \eta\alpha_r\cdot\Delta f + \frac{4k_B T}{R_L}\Delta f)h_3$, so we can get a One-variable quadratic inequality, that is $a_3 I_B^2 + b_3 I_B + c_3 < 0$.

1. When $R_s = 0$, the solution to the inequality is

$$\frac{-b_3-\sqrt{b_3^2-4a_3c_3}}{2a_3} < I_B < \frac{-b_3+\sqrt{b_3^2-4a_3c_3}}{2a_3} \tag{59}$$

When $I_B \leq \frac{-b_3-\sqrt{b_3^2-4a_3c_3}}{2a_3}$, $\sigma_{s,1}^2+\sigma_{s,0}^2-h_3 \leq 0$, thus $\gamma_b < 2^{R_s}(1+\gamma_{F-em})-1$, so the value range of I_B is

$$0 < I_B < y_3 = \frac{-b_3+\sqrt{b_3^2-4a_3c_3}}{2a_3} \tag{60}$$

Hence, the conditional secrecy outage probability is expressed as

$$\begin{aligned} P_{so-m} &= \frac{\int_0^{\infty}\int_{y_1}^{y_3} f(I_B) f(I_E)\, dI_B dI_E}{\int_{y_1}^{\infty} f(I_B)\, dI_B} \\ &= \frac{\int_0^{\infty}[F_B(y_3)-F_B(y_1)] f(I_E)\, dI_E}{1-F_B(y_1)} \end{aligned} \tag{61}$$

2. When $0 < R_s \leq 1$, the solution to the inequality is different when a_3 is positive or negative. Next, we will discuss it in different situations:

1) When $a_3 > 0$, the solution to the inequality is the same as Eq. (60).

2) When $a_3 < 0$, the solution to the inequality is

$$I_B > \frac{-b_3-\sqrt{b_3^2-4a_3c_3}}{2a_3} \tag{62}$$

When $I_B \leq \frac{-b_3-\sqrt{b_3^2-4a_3c_3}}{2a_3}$, $\sigma_{s,1}^2+\sigma_{s,0}^2-h_3 \leq 0$, thus $\gamma_b < 2^{R_s}(1+\gamma_{F-em})-1$, so the value range of I_B is $I_B \in R$.

3) When $a_3 = 0$, the solution to the inequality is

$$I_B > -\frac{c_3}{b_3} \tag{63}$$

When $I_B \leq -\frac{c_3}{b_3}$, $\sigma_{s,1}^2 + \sigma_{s,0}^2 - h_3 \leq 0$, thus $\gamma_b < 2^{R_s}(1+\gamma_{F-em}) - 1$, so the value range of I_B is $I_B \in R$.

Hence, the solution to $\gamma_b < 2^{R_s}(1+\gamma_{F-em}) - 1$ is

$$\begin{cases} 0 < I_B < y_3 & a_3 > 0 \\ I_B \in R & a_3 \leq 0 \end{cases} \tag{64}$$

For $a_3 > 0$, we can get

$$h_3 < \frac{\left(2eRF_a g^2 P_B \Delta f\right)^2}{4m\mu_0 (1-\mu_0)\left(\frac{RgP_B}{p}\right)^2} \tag{65}$$

After simplification,

$$\gamma_{F-em} < \frac{\left(2eRF_a g^2 P_B \Delta f\right)^2}{4m\mu_0 (1-\mu_0)\left(\frac{RgP_B}{p}\right)^2 (2eF_a g\Delta f)^2 \cdot 2^{R_s}} + 2^{-R_s} - 1 \tag{66}$$

By substituting Eq. (31) into the above formulation, we can obtain

$$\sigma_{F-em,1}^2 + \sigma_{F-em,0}^2 - h' < 2\sigma_{F-em,1}\sigma_{F-em,0} \tag{67}$$

Here $h' = \frac{(2eRF_a g^2 P_B \Delta f)^2}{4m\mu_0(1-\mu_0)(\frac{RgP_B}{p})^2 \cdot 2^{R_s}} + (2^{-R_s} - 1)(2eF_a g\Delta f)^2$, then square on both sides,

$$\left(\sigma_{F-em,1}^2 - \sigma_{F-em,0}^2\right)^2 - 2h'\left(\sigma_{F-em,1}^2 + \sigma_{F-em,0}^2\right) + h'^2 < 0 \tag{68}$$

According to Eq. (17) and (19), if $a' = (2eRF_a g^2 P_{F-EM}\Delta f)^2 - 4m\mu_0(1-\mu_0)(\frac{RgP_{F-EM}}{p})^2 h'$, $b' = -4eRF_a g^2 P_{F-EM}(1+\frac{1}{p^2}m)\cdot\Delta f \cdot h'$, $c' = h'^2 - 4(2eRF_a g^2 P_b \Delta f + \frac{4k_B T}{R_L}\Delta f)h'$, we can get a One-variable quadratic inequality, that is $a' I_E^2 + b' I_E + c' < 0$, and the solution to the inequality is

$$0 < I_E < y' = \frac{-b' + \sqrt{b'^2 - 4a'c'}}{2a'} \tag{69}$$

In summary, the conditional secrecy outage probability is expressed as

$$\begin{aligned} P_{so-m} &= \frac{\int_0^{y'}\int_{y_1}^{y_3} f(I_B) f(I_E)\, dI_B dI_E}{\int_{y_1}^{\infty} f(I_B)\, dI_B} + \int_{y'}^{\infty} f(I_E)\, dI_E \\ &= \frac{\int_0^{y'} [F_B(y_3) - F_B(y_1)] f(I_E)\, dI_E}{1 - F_B(y_1)} + 1 - F_E(y') \end{aligned} \tag{70}$$

Acknowledgment

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

References

[1] K. Kazaura, K. Wakamori, M. Matsumoto, T. Higashino, K. Tsukamoto, and S. Komaki, "RoFSO: A universal platform for convergence of fiber and free-space optical communication networks," *IEEE Commun. Mag.*, vol. 48, no. 2, pp. 130–137, Feb. 2010.

[2] I. B. Djordjevic, "Coded-orthogonal frequency division multiplexing in hybrid optical networks," *IET Optoelectron.*, vol. 4, no. 1, pp. 17–28, 2010.

[3] K. Wakamori, K. Kazaura, and M. Matsumoto, "Research and development of a next-generation free-space optical communication system," *Proc. SPIE - Int. Soc. Opt. Eng.*, vol. 7234, 2009, Art. no. 723404.

[4] A. Jurado-Navas *et al.*, "850-nm hybrid fiber/free-space optical communications using orbital angular momentum modes," *Opt. Exp.*, vol. 23, no. 26, pp. 33721–33732, 2015.

[5] C. Y. Li *et al.*, "A flexible two-way PM-based fiber-FSO convergence system," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7901509.
[6] Y. L. Yu, S.-K. Liaw, H.-H. Chou, H. Le-Minh, and Z. Ghassemlooy, "A hybrid optical fiber and FSO system for bidirectional communications used in bridges," *IEEE Photon. J.*, vol. 7, no. 6, Dec. 2015, Art. no. 7905509.
[7] C.-Y. Li *et al.*, "A high-speed and long-reach PAM4 optical wireless communication system," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 7906109.
[8] C.-H. Yeh *et al.*, "Bidirectional free space optical communication (FSO) in WDM access network with 1000-m supportable free space link," *Opt. Commun.*, vol. 435, pp. 394–398, 2018.
[9] C.-H. Yeh *et al.*, "Hybrid free space optical communication system and passive optical network with high splitting ratio for broadcasting data traffic," *J. Opt.*, vol. 20, no. 12, 2018, Art. no. 125702.
[10] A. M. Mbah, J. G. Walker, and A. J. Phillips, "Performance evaluation of turbulence-accentuated interchannel crosstalk for hybrid fibre and free-space optical wavelength-division-multiplexing systems using digital pulse-position modulation," *IET Optoelectron.*, vol. 10, no. 1, pp. 11–20, 2016.
[11] M. A. Esmail, A. Ragheb, H. Fathallah, and M.-S. Alouini, "Investigation and demonstration of high speed full-optical hybrid FSO/fiber communication system under light sand storm condition," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7900612.
[12] H. Xu-Hong *et al.*, "Two-way wireless-over-fibre and FSO-over-fibre communication systems with an optical carrier transmission," *Laser Phys.*, vol. 28, no. 7, 2018, Art. no. 076207.
[13] A. N. Sousa *et al.*, "Real-time dual-polarization transmission based on hybrid optical wireless communications," *Opt. Fiber Technol.*, vol. 40, pp. 114–117, 2018.
[14] 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.
[15] 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.*, 2004, pp. 711–716.
[16] W. Ning, X. Song, J. Cheng, and V. C. M. Leung, "Enhancing the security of free-space optical communications with secret sharing and key agreement," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1072–1081, Dec. 2014.
[17] K. Shimizu *et al.*, "Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area," *J. Lightw. Technol.*, vol. 32, no. 1, pp. 141–151, Jan. 2014.
[18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[19] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in OCDMA," in *Proc. Opt. Fiber Commun. Conf. Nat. Fiber Opt. Engineers Conf.*, 2006, Paper OThT2.
[20] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," *J. Lightw. Technol.*, vol. 23, no. 4, pp. 1652–1663, Apr. 2005.
[21] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.
[22] 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.
[23] K. Sasaki, N. Minato, T. Ushikubo, and Y. Arimoto, "First OCDMA experimental demonstration over free space and optical fiber link," in *Proc. Conf. Opt. Fiber Commun./Nat. Fiber Opt. Engineers Conf.*, 2008, pp. 1–3.
[24] R. M. Nejad, 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.
[25] L. Tancevski and I. Andonovic, "Wavelength hopping/time spreading code division multiple access systems," *Electron. Lett.*, vol. 30, no. 17, pp. 1388–1390, 1994.
[26] M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 6, no. 8, pp. 684–694, Aug. 2014.
[27] A. K. Majumdar, "Free-space laser communication performance in the atmospheric channel," *J. Opt. Fiber Commun. Rep.*, vol. 2, pp. 345–396, 2005.
[28] Y. Dikmelik and F. M. Davidson, "Fiber-coupling efficiency for free-space optical communication through atmospheric turbulence," *Appl. Opt.*, vol. 44, no. 23, pp. 4946–4952, 2005.
[29] E. Bayaki, D. S. Michalopoulos, and R. Schober, "EDFA-based all-optical relaying in free-space optical systems," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3797–3807, Dec. 2012.
[30] P. V. Trinh, N. T. Dang, and A. T. Pham, "All-optical relaying FSO systems using EDFA combined with optical hard-limiter over atmospheric turbulence channels," *J. Lightw. Technol.*, vol. 33, no. 19, pp. 4132–4144, Oct. 2015.
[31] J. M. Romero-Jerez, G. Gomez, and F. J. Lopez-Martinez, "On the outage probability of secrecy capacity in arbitrarily-distributed fading channels," in *Proc. Eur. Wireless; 21st Eur. Wireless Conf.*, 2015, pp. 1–6.
[32] X. Zhou, M. R. Mckay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[33] J. M. Kahn and K. P. Ho, "Spectral efficiency limits and modulation/detection techniques for DWDM systems," *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 2, pp. 259–272, Mar./Apr. 2004.
[34] P. Kaur, V. K. Jain, and S. Kar, "Performance analysis of FSO array receivers in presence of atmospheric turbulence," *IEEE Photon. Technol. Lett.*, vol. 26, no. 12, pp. 1165–1168, Jun. 2014.
[35] 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.
[36] 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, 2017.
[37] M. S Ahmed and I. Glesk, "Mitigation of temperature induced dispersion in optical fiber on OCDMA auto-correlation," *IEEE Photon. Technol. Lett.*, vol. 29, no. 22, pp. 1979–1982, Nov. 2017.
[38] 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.