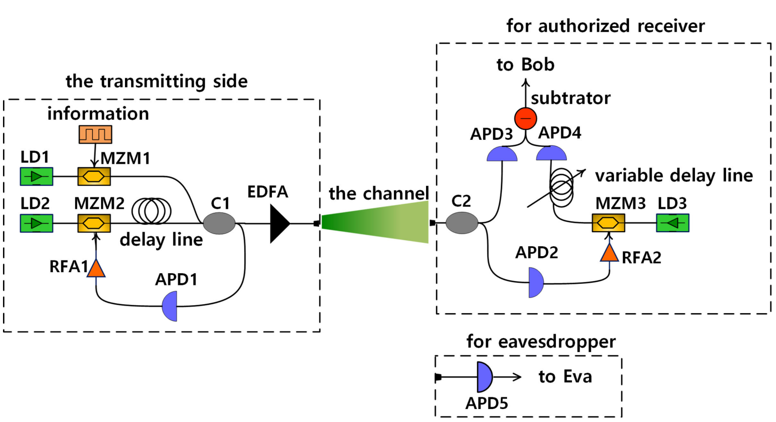
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Prediction Algorithm of Key Design Parameters for Space Chaotic Optical Communication System

Volume 12, Number 4, August 2020

Mi Li
Huihui Zeng
Yufan Yang
You Guo
Jiahan Li



The chaotic optical communication system for the authorized receiver and eavesdropper

DOI: 10.1109/JPHOT.2020.3010838

Prediction Algorithm of Key Design Parameters for Space Chaotic Optical Communication System

Mi Li, Huihui Zeng, Yufan Yang, You Guo, and Jiahan Li

Institute of Optical Communication Engineering, Key Laboratory of Intelligent Optical Sensing and Manipulation, College of Engineering and Applied Sciences, Nanjing University, Nanjing 210093, China

DOI:10.1109/JPHOT.2020.3010838

Manuscript received June 5, 2020; revised July 6, 2020; accepted July 16, 2020. Date of publication July 21, 2020; date of current version August 20, 2020. This work was supported in part by the Joint Funds of Space Science and Technology under Grant 6141B060307, in part by Six talent peaks project in Jiangsu Province (KTHY-003); Fundamental Research Funds for the Central Universities (021314380171 and 021314380152), in part by National Natural Science Foundation of China under Grant 61205045, and in part by Jiangsu Provincial Natural Science Foundation of China (SBK2020021631). Corresponding author: Mi Li (e-mail: limi@nju.edu.cn).

Abstract: Space laser optical communication has been widely investigated to achieve high bit rate information transmission. To enhance the information transmission security in space laser optical communication, chaos-based encryption scheme is adopted. It involves many parameters in designing a space chaotic optical communication system, which a proper tuning of them brings good communication performance. To investigate the key design parameters including the masking efficiency, transmitting optical power and mismatch coefficient, we give the calculation model of the bit error ratio (BER) based on traditional space laser optical communication system from the perspective of the authorized receiver and eavesdropper. Numerical results indicate that the BER for the eavesdropper is sensitive to the masking efficiency but not to the transmitting optical power. By contrast, the transmitting optical power plays a crucial role in the computational formula of the BER for the authorized receiver. A saturate optical power is also proposed at last which helps save the energy. These simulation results can be reference for practical system design.

Index Terms: Space laser optical communication, chaos, bit rate, masking efficiency.

1. Introduction

Space laser optical communication has the advantages of large capacity and good confidentiality compared with traditional space microwave communication. Thus, it has become one of the most popular topics in space optical communication research [1]. Many experiments have been performed through ground-to-satellite optical communication links, achieving a lot of significant advances [2]–[6]. However, since the carrier wave propagates through the long-distance free space, ground-to satellite optical communication scheme is far from safe than ground optical communication using optical fiber. Thus, the chaos-based encryption scheme was induced to enhance the transmission security in space laser optical communication.

Chaotic signal has been applied in encrypted communication systems with the natural characteristic properties, high sensitivity to initial conditions and pseudo-randomness [7]. Chaos synchronization was first evidenced in electronic circuits by Pecora and Carroll, which has become the basis of chaos-based communications [8]. Three years later, Rajarshi Roy first reported the experimental synchronization using two coupled chaotic Nd: YAG lasers [9]. The theoretical studies of chaos synchronization propel the development of practical chaotic optical communication systems. In 1998, Goedgebuer demonstrated chaotic optical communication with erbium-doped fiber ring laser (EDFRL) in experiment, proving that chaotic optical waveforms can be used to mask information at high bandwidths [10]. In 2005, Argyris undertook a long-distance high bit rates field experiment using commercial optical networks, with bit error ratio (BER) below 10^{-7} [11]. After five years later, Argyris and co-workers performed chaotic optical communication experiment that operate in a dense wavelength division multiplexed transmission environment and analyzed the efficiency of data recovery of both the conventional and chaos encrypted channels [12]. To address the bottleneck of chaos synchronization in high-speed chaotic optical communication, Ke *et al.* proposed a deep learning method to achieve the same level of security as the traditional synchronization schemes with implementation difficulty reduced [13]. In order to solve the time delay signature and enhance chaotic dynamics, some significant schemes are analyzed such as vertical-cavity surface-emitting lasers (VCSELs) and phase-modulated Sagnac loop [14]–[16]. And several practical schemes have been proposed to generate broadband chaos [17]–[21]. The fiber chaos-based communication technology has become increasingly mature in recent years.

Although many progresses of chaos-based communication have been made, these works are mainly using optical fiber links. The chaos encryption scheme used in space optical communication has rarely been reported. The important work we only find was carried out in 2002. Rulkov report the results of an experimental analysis of the atmospheric turbulence in the channel and impact of the atmospheric turbulence on the bit-error-rate performance of chaos-based communication system [22]. It verified the feasibility of the application of chaos-based encryption on the space optical communication. However, the BER in 2002's result did not reach 10^{-6} due to the effect of the atmospheric turbulence, which is larger than that of the ground fiber chaotic communication. To improve the BER performance, the key parameters involved in space chaotic optical communication system should be properly tuned. In this paper, we use opto-electronic feedback loop to generate chaotic dynamics and chaos modulation as the information encryption scheme. The masking efficiency, which stands for the amplitude ratio of the information versus chaotic carrier, significantly influence BER performance at the receiver. Larger masking efficiency usually means lower BER, but also make the information more vulnerable to the eavesdropper. The transmitting optical power is also an important parameter. It is well known that increasing the transmitting optical power can improve the BER performance in traditional space laser optical communication. However, considering that the bearable transmitting optical power is limited and the close relationship of the transmitting optical power and synchronization mismatch, it still needs to be clarified what is the most proper value for the transmitting optical power. In order to take both the transmission security and accuracy into account, we give the calculation model of BER in the perspective of the eavesdropper and authorized receiver respectively. Then a prediction algorithm of the key design parameters including the masking efficiency, the transmitting optical power and mismatch coefficient for space chaotic optical communication system has been given through the quantitative analysis. These works will be applicable for field experiment.

2. Principles and Theoretical Analysis

As present in Fig. 1, the whole system can be divided into two subsystems including emitter and receiver [11], [23]. At the emitter, laser diode 2 (LD2), Math-Zehnder modulator 2 (MZM2), delay line, RF amplifier (RFA1) and photo diode 1 (APD1) constitute the chaos generation loop. The electrical signal carrying information is transformed into optical signal and added to carrier wave by optical fiber coupler 1 (C1). An erbium-doped fiber amplifier (EDFA) is used here to compensate the energy attenuation in the free space. At the receiver, the signal at photo diode 3 (APD3) is $m(t) + C_T(t)$, where $m(t)$ is the information amplitude and $C_T(t)$ is carrier wave. Laser diode 3 (LD3), Math-Zehnder modulator 3 (MZM3), photo diode 2 (APD2), RF amplifier (RFA2) and variable delay line constitute the synchronization loop which replicate similar chaotic carrier $C_R(T)$. When the

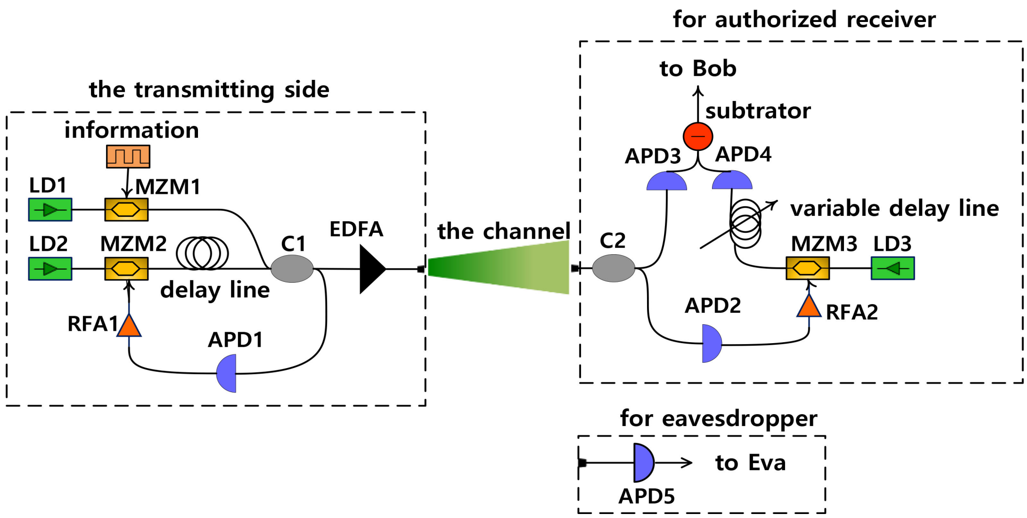


Fig. 1. The chaotic optical communication systems for the authorized receiver and eavesdropper.

parameters of the devices at the receiver are the same as that at the emitter, the replicated chaotic signal $C_R(T)$ is as same as $C_T(t)$ and $m(t)$ can be extracted using subtractor. For eavesdropper, the receiver is only composed of photo diode 5 (APD5). According to Ref. [24], the optical signal received by APD5 is,

$$P_e = \frac{1}{2} P_{\text{in}} \left\{ \cos^2 \left[y\left(t - T\right) + \phi \right] + \alpha \cdot m\left(t\right) \right\} \tag{1}$$

where P_{in} is the receiving optical power. α is masking efficiency. The value of $m(t)$ is "1" or "0". T is the delay time; φ is fixed phase shift associated with the operating point of MZM2. $y(t\text{-}T)$ is variable proportional to the electrical voltage applied to the RF electrodes of MZM2 in the feedback loop. When the dynamical system enters the hyper-chaotic regime, the average nonlinear function $\cos^2[\mathrm{y}(\mathrm{t}-\mathrm{T})+\phi]$ is 1/2 [24].

Accordingly, the average photon counts of APD5 with respect to information of "1" and information of "0" are,

$$K_{e1} = \left\langle P_e \left[m(t) = 1 \right] \right\rangle \frac{\eta T_s}{h\upsilon} = \frac{1}{2} P_{\text{in}} \left(\frac{1}{2} + \alpha \right) \cdot \frac{\eta T_s}{h\upsilon} \tag{2}$$

$$K_{e0} = \left\langle P_e \left[m(t) = 0 \right] \right\rangle \frac{\eta T_s}{h\upsilon} = \frac{1}{4} P_{\text{in}} \frac{\eta T_s}{h\upsilon} \tag{3}$$

where η is the quantum efficiency, T_s the inverse of the bit ratio, h the Planck constant. ν the frequency of laser.

The photodetectors transform the optical signal into electrical signal. According to the working principles of the photodetectors [2], we get the equations of the average current at the output of APD5 with respect to information of "1" and information of "0",

$$m_{e1} = GeK_{e1} + \mathrm{I_{dc}T_s} \tag{4}$$

$$m_{e0} = GeK_{e0} + \mathrm{I_{dc}T_s} \tag{5}$$

where G is the gain factor of APD5, the parameters e, I_{dc} are respectively the elementary charge and dark current.

Compared with traditional space optical communication system, the chaos noise is induced specifically. According to Ref. [7], the chaotic carrier has particular time evolution and frequency spectrum which is similar with noise. Thus, the chaotic carrier will be dealt as normal noise if the transmitting signal is detected directly with photodetector. The chaos noise has been found that it conforms to Gaussian distribution [11]. According to the mathematical definitions of the variance, the chaos noise can be calculated as below,

$$\sigma_{\text{chaos}}^2 = \left\langle \left(P_e\left[m\left(t\right)=0\right] Ge\frac{\eta T_s}{h\nu} - GeK_{e0} \right)^2 \right\rangle$$
$$= \frac{1}{2}\left[\frac{1}{4}P_{\text{in}}T_s\eta\frac{Ge}{h\nu}\right]^2 \tag{6}$$

Therefore, the overall noise can be added with chaos noise as follow,

$$\sigma_{e1}^2 = FG^2e^2K_{e1} + \sigma_T^2 + \sigma_{\text{chaos}}^2 \tag{7}$$

$$\sigma_{e0}^2 = FG^2e^2K_{e0} + \sigma_T^2 + \sigma_{\text{chaos}}^2 \tag{8}$$

where F is the additional noise factor of photodetector, σ_T^2 is the thermal noise, σ_{chaos}^2 is the chaos noise.

Based on the formulas above, we can get the final equations of BER for the eavesdropper [2], where γ_e is the decision threshold,

$$BER_e = \frac{1}{2}\left[1 - \frac{1}{2}erfc\left(\frac{\gamma_e - m_{e1}}{\sqrt{2}\sigma_{e1}}\right)\right] + \frac{1}{4}erfc\left(\frac{\gamma_e - m_{e0}}{\sqrt{2}\sigma_{e0}}\right) \tag{9}$$

For the authorized receiver, the synchronization loop replicates chaotic carrier similar with that generated at the emitter. According to Ref. [2], the average current and the overall variance at the output of the subtractor are,

$$m_{a0} = 2\mathrm{I_{dc}T_s} \tag{10}$$

$$m_{a1} = \frac{1}{2}\alpha P_{\text{in}}\frac{\eta T_S}{h\nu}Ge + 2\mathrm{I_{dc}T_s} \tag{11}$$

$$\sigma_{a0}^2 = FG^2e^2\left(K_{a0} + K_{a0}'\right) + 2\sigma_T^2 + \sigma_n^2 \tag{12}$$

$$\sigma_{a1}^2 = FG^2e^2\left(K_{a1} + K_{a1}'\right) + 2\sigma_T^2 + \sigma_n^2 \tag{13}$$

where σ_T^2 is the thermal noise, G is the gain factor of APD3 and APD4, F is additional noise factor. K_{a0} and K_{a0}' are the average photon counts of APD3 and APD4 respectively for information of "0", K_{a1} and K_{a1}' for information of "1". The overall variance of the noise includes the detector noise and mismatch noise. σ_{a0}^2 corresponds to the information of "0" while σ_{a1}^2 corresponds to the information of "1".

Accordingly, the BER is [2], where γ_a is the decision threshold.

$$\mathrm{BER_a} = \frac{1}{2}\left[1 - \frac{1}{2}\mathrm{erfc}\left(\frac{\gamma_a - \mathrm{m_{a1}}}{\sqrt{2}\sigma_{a1}}\right)\right] + \frac{1}{4}\mathrm{erfc}\left(\frac{\gamma_a - \mathrm{m_{a0}}}{\sqrt{2}\sigma_{a0}}\right) \tag{14}$$

Considering that ground-to-satellite optical communication link is in free space, the influence of the atmospheric turbulence should be taken into account. So the probability distribution of the receiving optical intensity and the final equation of BER are [2],

$$p\left(P_{\text{in}}\right) = \frac{1}{\sqrt{2\pi\sigma_P{}^2}}\frac{1}{P_{\text{in}}}\exp\left[-\frac{\left(\ln\frac{P_{\text{in}}}{P_{aver}} + \frac{\sigma_P{}^2}{2}\right)^2}{2\sigma_P{}^2}\right] \tag{15}$$

$$BER = \int_0^\infty BER_x \cdot p\left(P_{\text{in}}\right) \cdot dP_{\text{in}} \tag{16}$$

where σ_p^2 is the variance of the distribution, x is a or e representing the authorized receiver or the eavesdropper, P_{aver} is the average receiving optical power.

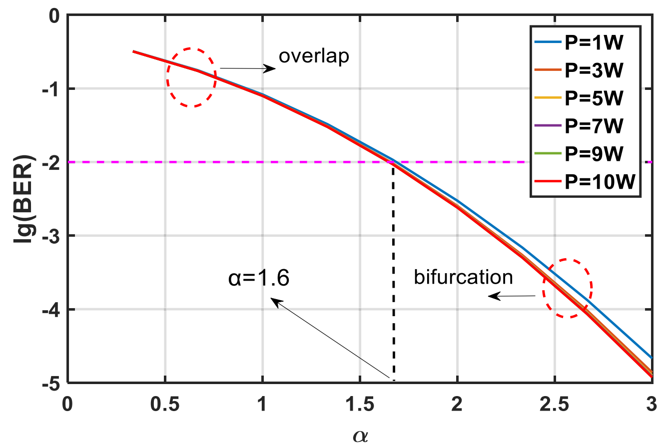


Fig. 2. BER versus masking efficiency of Eva (eavesdropper) under different transmitting optical power.

3. Results

Using the formulas above, we can quantitatively analyze the relationship among masking efficiency, transmitting optical power and mismatch coefficient for both the authorized receiver and the eavesdropper. In further, the advice about how to select these key design parameters in space chaotic optical communication system are given. The parameters used in our model are based on practical space-to-ground optical systems, The zenith angle is 0°, the default divergence angle is $\theta = 30$ μrad, the receiving diameter is 0.25 m, the height of the emitter and the receive are $H = 38\,000$ km, $h_0 = 100$ m, the laser wavelength is $\lambda = 1550$ nm, the photodetector gain factor is $G = 50$, the photodetector quantum efficiency is $\eta = 0.75$, the dark current of the photodetector is $I_{dc} = 10^{-9}$A, The boresight is $A_j = 0$ μrad. The bit rate is 1 Gb/s. The gain factor of EDFA is 30 dB.

Fig. 2 numerically evaluates the BER of the eavesdropper as a function of the masking efficiency for different transmitting optical power, varying from 1 W to 10 W. It shows that the BER varies apparently with the masking efficiency. For example, the BER can even decreases dramatically from 10^{-1} to 10^{-5} when the masking efficiency increases from 0.3 to 3. In addition, Fig. 2 also indicates that when the masking efficiency is relatively small, the curves of the BER for different transmitting optical power overlap. While when the masking efficiency gets larger, the effect of the transmitting optical power appears and the bifurcation will be more obvious. The larger transmitting optical power corresponds to better BER performance. The phenomenon above can be explained through the signal to noise ratio (SNR), shown as below, where the numerator is the output electrical signal of APD3 corresponding to the information signal, the first two terms in the denominator is the detector noise and the latter is chaos noise.

$$\mathrm{SNR_e} = \frac{\frac{1}{2}\alpha \mathrm{P_{in}} \frac{\eta \mathrm{T_s}}{h\nu} \mathrm{Ge}}{\sqrt{\frac{1+2\alpha}{4} \mathrm{FG^2e^2P_{in}} \cdot \frac{\eta \mathrm{T_s}}{h\upsilon} + \sigma_\mathrm{T}^2 + \frac{1}{32}\left(\mathrm{P_{in}Ge}\frac{\eta \mathrm{T_s}}{h\nu}\right)^2}} \tag{17}$$

For the eavesdropper, the detector noise and chaos noise are two main noises. When the masking efficiency is 1, it shows that the chaos noise is 4 orders of magnitude larger than the detector noise. In this way, the detector noise can even be ignored totally in the calculation of the SNR. And further simplification of Eq. (17) is $\mathrm{SNR} = 2\sqrt{2}\alpha$. Namely, the SNR for the eavesdropper rises approximately linearly with the masking efficiency and is virtually the same despite of different transmitting optical power. Thus, the BER for the eavesdropper is greatly influenced by the masking efficiency and not related with the transmitting optical power, due to the inverse relationship of SNR and the BER. When the masking efficiency gets larger, the detector noise will increase. We reasoned that if the masking efficiency gets large enough, 2.5 for example, the detector noise will play a role as substantial as the chaos noise and can not be ignored anymore. Then the

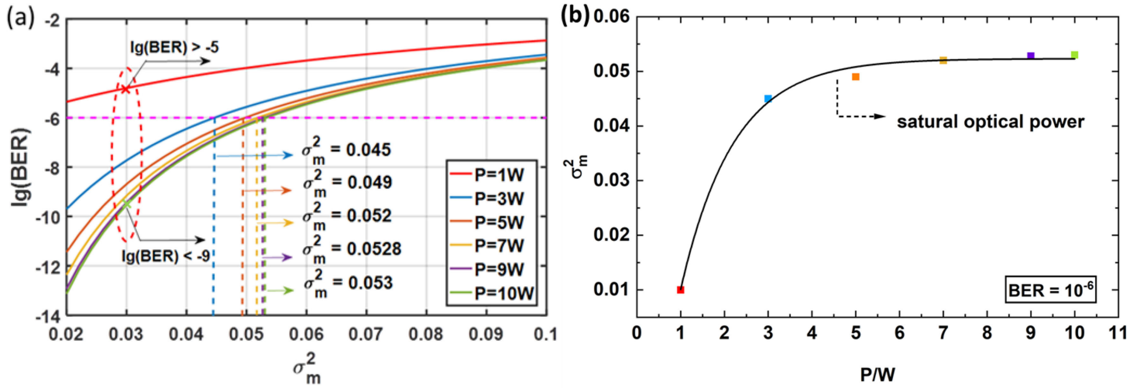


Fig. 3. (a) BER performance versus mismatch coefficient under different transmitting optical power for the authorized receiver. (b) The fitting of the transmitting optical power versus the mismatch coefficient in the case of BER as 10^{-6}.

transmitting optical power is reserved in Eq. (17) and the BER improves as it increases. However, the contribution of the transmitting optical power varying from 1 W to 10 W to the BER is still very tiny even if the making efficiency rises to 3, as shown in Fig. 2.

We have given the reason for the very tiny influence of the transmitting optical power on BER when the optical power varies from 1 W to 10 W in the analysis above. And it suggests that we should focus more on the tuning of the masking efficiency rather than the transmitting optical power if we want to lower the risk of information from eavesdropping. In generally, when the BER for the eavesdropper is evaluated larger than 10^{-2}, it is difficult for the eavesdropper to decode the information. As shown in Fig. 2, here the masking efficiency is approximately 1.6. And in the following, we return to the BER for the authorized receiver with the masking efficiency setting 1.6. By analyzing the relationship of the BER for the authorized receiver versus the transmitting optical power and mismatch coefficient, some guidance about designing the system is further obtained.

For the authorized receiver, the synchronization structure illustrated in Fig. 1 enables the counteraction of the chaotic carriers from the emitter and receiver, so that the information can be extracted conveniently. However, perfect synchronization is rarely possible and mismatch noise is brought inevitably. To measure the mismatch quantitatively, the mismatch coefficient is induced, including amplitude mismatch and phase mismatch [24]. BER performance versus mismatch coefficient under different transmitting optical power for the authorized receiver has been shown in Fig. 3(a). Smaller mismatch coefficient requires more accurate tuning of the communication system, and helps improve the BER performance in the mean time. It seems natural because mismatch coefficient represents the amplitude of the mismatch noise which declines SNR. The numerical results also indicate that, the transmitting optical power has notable influence on BER for the authorized receiver, which is significantly different from that of the eavesdropper, especially when the mismatch coefficient is relatively small. For example, when the mismatch coefficient is 0.03, the BER for the transmitting optical power of 1 W is larger than 10^{-5}, whereas that of 10 W is smaller than 10^{-9}. We can give the explanation from the perspective of SNR likewise,

$$SNR_a = \frac{\frac{1}{4}\alpha P(I)\, Ge\frac{\eta T_s}{h\nu}}{\sqrt{\frac{1+\alpha}{4}P(I)\, FG^2e^2\frac{\eta T_s}{h\nu} + 2\sigma_T^2 + \frac{1}{32}\left(P(I)\, Ge\frac{\eta T_s}{h\nu}\right)^2\sigma_m^2}} \tag{18}$$

where the numerator is the output electrical signal of the subtractor corresponding to the information signal, the first two terms in the denominator is the detector noise and the last one is the mismatch noise.

As we know, the mismatch coefficient indicates the order of the mismatch noise, which value of 1 stands for the transformation of the mismatch noise to the chaos noise. When the mismatch coefficient gets smaller, the mismatch noise reduces and becomes comparable to the detector noise gradually. In this way, the detector noise can not be ignored in Eq. (18). Thus, the SNR for the authorized receiver is proportional to the transmitting optical power. Accordingly, the BER performance for the authorized receiver improves as the transmitting optical power increases. Taken together, these results imply that we can improve the BER performance either by increasing the transmitting optical power or reducing the mismatch noise. Obviously changing the transmitting optical power is a more convenient way while reducing the mismatch noise requires more efforts in system design. More specifically, as shown in Fig. 3(a), to ensure the BER for the authorized receiver smaller than 10^{-6} as well as the coefficient larger than 0.02, 1 W for the transmitting optical power is not enough. In addition, although increasing the transmitting optical power helps to simplify the system design, it becomes less effective as the transmitting optical power continues increasing. For instance, when the transmitting optical power increases from 3 W to 7 W, the corresponding mismatch coefficient for BER of 10^{-6} increases from 0.045 to 0.052. While when the transmitting optical power rises from 7 W to 10 W, the corresponding mismatch coefficient rises only 0.001. It suggests that there is a maximal effective transmitting optical power helping to lower the BER and simplify the system design. Here we call it as the saturate optical power. It can be estimated through the fitting of the transmitting optical power versus the mismatch coefficient. As shown in Fig. 3(b), the saturate optical power in the case of BER as 10^{-6} can be estimated. Generally speaking, the transmitting optical power on the satellite is limited. Given that, the result of the saturate transmitting optical power benefits the optical power design on the satellite.

4. Conclusion

In conclusion, the BER model for both the eavesdropper and the authorized receiver were given and the simulation based on them shows that the BER for the eavesdropper is sensitive to the masking efficiency but not to the transmitting optical power. By properly tuning the masking efficiency, we can protect the information security effectively. By contrast, the transmitting optical power plays a crucial role in the BER for the authorized receiver. We can improve the BER performance by increasing the transmitting optical power with a relative lower masking efficiency ensuring transmission security. Thus, under the same requirement of communication, increasing the transmitting optical power can improve BER performance instead of reducing synchronization mismatch, which helps to reduce the difficulty of system design. Further analysis showed that it is limited to increase the tolerance of the system to synchronization mismatch by increasing the transmitting optical power. Here a saturate optical power is proposed as the most proper value for the transmitting optical power in system design. And the mismatch coefficient corresponding to the saturate optical power represents the required synchronization accuracy of the system. The prediction algorithm above and the simulation results based on it can effectively save much time and efforts for the tuning of the key parameters. It is useful for practical space optical chaotic optical communication system design.

References

[1] M. Toyoshima, W. R. Leeb, H. Kunimori, and T. Takano, “Comparison of microwave and light wave communication systems in space application,” *Opt. Eng.*, vol. 46, 2007, Art. no. 015003.

[2] Y. Jiang, K. Tao, Y. Song, and S. Fu, “Packet error rate analysis of OOK, DPIM, and PPM modulation schemes for ground-to-satellite laser uplink communications,” *Appl. Opt.*, vol. 53, pp. 1268–1273, 2014.

[3] L. C. Andrews, R. L. Phillips, and P. T. Yu, “Optical scintillations and fade statistics for a satellite-communication system,” *Appl. Opt.*, vol. 34, pp. 7742–7751, 1995.

[4] Y. Jiang, J. Ma, L. Tan, S. Yu, and W. Du, “Measurement of optical intensity fluctuation over an 11.8 km turbulent path,” *Opt. Express*, vol. 16, pp. 6963–6973, 2008.

[5] K. Pang *et al.*, “400-Gbit/s QPSK free-space optical communication link based on four-fold multiplexing of Hermite–Gaussian or Laguerre–Gaussian modes by varying both modal indices,” *Opt. Lett.*, vol. 43, pp. 3889–3892, 2018.

[6] S. Lu *et al.*, “Inter-satellite laser communication system based on double Risley prisms beam steering,” *Appl. Opt.*, vol. 58, pp. 7517–7522, 2019.

[7] V. Annovazzi-Lodi, A. Scire, M. Sorel, and S. Donati, “Dynamic behavior and locking of a semiconductor laser subjected to external injection,” *IEEE J. Quantum Electron.*, vol. 34, no. 12, pp. 2350–2357, Dec. 1998.
[8] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.
[9] R. Roy and K. S. Thornburg, “Experimental synchronization of chaotic lasers,” *Phys. Rev. Lett.*, vol. 72, pp. 2009–2012, 1994.
[10] J. P. Goedgebuer, L. Larger, H. Porte, and F. Delorme, “Chaos in wavelength with a feedback tunable laser diode,” *Phys. Rev. E*, vol. 57, pp. 2795–2798, 1998.
[11] A. Argyris *et al.*, “Chaos-based communications at high bit rates using commercial fibre-optic links,” *Nature*, vol. 438, pp. 343–346, 2005.
[12] A. Argyris, E. Grivas, A. Bogris, and D. Syvridis, “Transmission effects in wavelength division multiplexed chaotic optical communication systems,” *J. Lightw. Technol.*, vol. 28, no. 21, pp. 3107–3114, Nov. 2010.
[13] J. Ke *et al.*, “32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization,” *Opt. Lett.*, vol. 44, pp. 5776–5779, 2019.
[14] Y. Ma, S. Xiang, X. Guo, Z. Song, A. Wen, and Y. Hao, “Time-delay signature concealment of chaos and ultrafast decision making in mutually coupled semiconductor lasers with a phase-modulated Sagnac loop,” *Opt. Express*, vol. 28, pp. 1665–1678, 2020.
[15] P. Mu, W. Pan, and N. Li, “Analysis and characterization of chaos generated by free-running and optically injected VCSELs,” *Opt. Express*, vol. 26, pp. 15642–15655, 2018.
[16] S. Xiang, Z. Ren, Y. Zhang, Z. Song, and Y. Hao, “All-optical neuromorphic XOR operation with inhibitory dynamics of a single photonic spiking neuron based on a VCSEL-SA,” *Opt. Lett.*, vol. 45, pp. 1104–1107, 2020.
[17] J. Ohtsubo, “Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1141–1154, Sep. 2002.
[18] N. Jiang, A. Zhao, S. Liu, C. Xue, B. Wang, and K. Qiu, “Generation of broadband chaos with perfect time delay signature suppression by using self-phase-modulated feedback and a microsphere resonator,” *Opt. Lett.*, vol. 43, pp. 5359–5362, 2018.
[19] A. Zhao, N. Jiang, C. Chang, Y. Wang, S. Liu, and K. Qiu, “Generation and synchronization of wideband chaos in semiconductor lasers subject to constant-amplitude self-phase-modulated optical injection,” *Opt. Express*, vol. 28, pp. 13292–13298, 2020.
[20] N. Jiang, A. Zhao, X. Xue, J. Tang, and K. Qiu, “Physical secure optical communication based on private chaotic spectral phase encryption/decryption,” *Opt. Lett.*, vol. 44, pp. 1536–1539, 2019.
[21] J. Ning, A. Zhao, S. Liu, C. Xue, and K. Qiu, “Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback,” *Opt. Express*, vol. 26, pp. 32404–32416, 2018.
[22] N. F. Rulkov, M. A. Vorontsov, and L. Illing, “Chaotic free-space laser communication over a turbulent channel,” *Phys. Rev. Lett.*, vol. 89, 2002, Art. no. 277905.
[23] P. Colet and R. Roy, “Digital communication with synchronized chaotic lasers,” *Opt. Lett.*, vol. 19, pp. 2056–2058, 1994.
[24] Y. C. Kouomou, P. Colet, L. Larger, and N. Gastaud, “Mismatch-Induced bit error rate in optical chaos communications using semiconductor lasers with electrooptical feedback,” *IEEE J. Quantum Electron.*, vol. 41, no. 2, pp. 156–163, Feb. 2005.