Optics Letters

Signal-to-noise ratio degradation analysis for optoelectronic feedback-based chaotic optical communication systems

Yunhao Xie, Zhao Yang, Mengyue Shi, Weisheng Hu, and Lilin Yi*

State Key Lab of Advanced Optical Communication Systems and Networks, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
**lilinyi@sjtu.edu.cn*

Received 5 June 2023; revised 6 August 2023; accepted 24 August 2023; posted 25 August 2023; published 20 September 2023

Chaotic optical communication encrypts transmitted signals through physical noise; this ensures high security while causing a certain decrease in the signal-to-noise ratio (SNR). Thus, it is necessary to analyze the SNR degradation of decrypted signals after chaotic encryption and the minimum requirements for the SNR of the fiber channel to meet the required bit error rate (BER) performance. Accordingly, an SNR model of decrypted signals for optoelectronic feedback-based chaotic optical communication systems is proposed. Under different channel SNRs, the SNR degradation of 40 Gbit/s phase chaos and intensity chaos models is investigated by simulation and experiment, respectively, with a 15 GHz wideband chaotic carrier. Comparing decrypted signals with original signals, the simulation results show that there is a 2.9 dB SNR degradation for both intensity chaos and phase chaos. Further, in experiments, SNR degradation from 4.5 dB to 5.6 dB, with various channel SNRs for intensity chaos, is analyzed, while there is an SNR degradation from 7.1 dB to 8.3 dB for phase chaos. The simulation and experimental results provide guidance for long-distance transmission chaotic optical communication systems.

https://doi.org/10.1364/OL.497061

Information security of the physical layer remains a challenging subject for fiber communication systems [1]. As a hardware encryption method, chaotic optical communication has attracted the attention of many researchers in the past two decades [2]. Chaotic systems are highly sensitive to initial conditions, which makes them hard to predict and has the potential of providing a high level of privacy in data transmission [3]. Optoelectronic feedback for generating chaos has the advantages of a broadband chaotic carrier, reduced operation complexity, and flexible configuration, and is ideal for secure encryption of high-speed signals [4]. The optoelectronic feedback structure dates from the Ikeda ring cavity, which can exhibit complex dynamics because of the presence of a large delay in the feedback loop and produce chaotic output by nonlinear modulation [5].

Optoelectronic feedback-based chaotic optical communications have been widely studied and developed for improving the transmission rate–distance product of encrypted signals. Based on hardware synchronization, the transmission rate has been increased from 1 Gbit/s to 32 Gbit/s and the transmission distance has been significantly improved, to 200 km [6–8]. At present, it is still a very difficult problem to realize long-distance chaotic synchronization, mainly because well-matched hardware cannot always be guaranteed between the transmitter and the receiver, and the SNR performances of decrypted signals are degraded through fiber channel impairments [9]. We have introduced a neural network (NN) to learn the chaotic nonlinear dynamics of the optoelectronic feedback loop, and apply the trained NN to realize chaotic synchronization in the digital domain, effectively solving the problem of hardware mismatching of transceivers [10]. Moreover, combining NN-based chaotic synchronization with coherent detection and digital signal processing (DSP) algorithms, 30 Gbit/s chaotic encrypted signals over 340 km fiber transmission were experimentally demonstrated [11]. The bit error rate (BER) will rise, owing to the decrease in SNR caused by the chaotic encryption and decryption, together with the damage in the channel. However, there are no studies on this problem. It is necessary to analyze, theoretically, the SNR degradation of decrypted signals after chaotic encryption and the minimum SNR of the fiber channel to meet the BER requirements. This work provides a guidance for further improving the transmission distance of chaotic optical communication.

In this paper, an SNR model of decrypted signals for optoelectronic feedback-based chaotic optical communication systems is proposed. Under different channel SNRs, the SNR degradation of 40 Gbit/s phase chaos and intensity chaos models is analyzed by simulation and experiment, respectively, with 15 GHz chaotic carrier bandwidth. The simulation results show that there is a 2.9 dB SNR degradation with decrypted signals for both intensity chaos and phase chaos. Moreover, in the experiment, after chaos encryption, there is an SNR degradation of 4.5 dB to 5.6 dB on reducing the channel SNR for intensity chaos, while there is an SNR degradation of 7.1 dB to 8.3 dB for phase chaos.

Compared with the digital optical communication system, chaotic optical communication increases the process of chaotic encryption and synchronization, which undoubtedly leads to a decrease in the SNR of the decrypted signals. The SNR model

of the decrypted signals can be described as

$$SNR_{\mathrm{DS}} = \frac{P_{\mathrm{DS}}}{P_{\mathrm{Lin}} + P_{\mathrm{NL}} + P_{\mathrm{ASE}} + P_{\mathrm{TR}}} - SNR_{\mathrm{Syn}}, \tag{1}$$

where $\mathrm{SNR}_{\mathrm{DS}}$ and P_{DS} are the SNR and power of decrypted signals; P_{Lin}, P_{NL}, P_{ASE}, and P_{TR} represent the linear impairments of fiber transmission, nonlinear impairments, amplifier spontaneous emission (ASE) noise superposed by an erbium-doped fiber amplifier (EDFA), and device noise at the transceiver end; and $\mathrm{SNR}_{\mathrm{Syn}}$ denotes the decrease in SNR due to chaotic synchronization error, which consists of two parts. One is caused by the mismatch of physical device parameters, and NN-based chaotic synchronization can minimize this part of the SNR damage. The other is the impairment noise caused by the fiber channel and device noise, superimposed on the encrypted signals, reducing synchronization performance.

Assuming that DSP algorithms can completely compensate for the linear impairments of the chaotic signals [12], by controlling fiber launch power or through nonlinear compensation algorithms, the nonlinear noise can be reduced as much as possible [13]. Then the main sources of system noise are ASE noise and device noise, which are subject to additive white Gaussian noise (AWGN). A study of the quantitative relationship between the SNR of decrypted signals and the SNR of the AWGN channel will provide strong guidance for the next longer-distance fiber transmission experiments. In this way, the residual SNR margin caused by the fiber channel impairments can be analyzed.

First, simulation analysis of the intensity chaos and phase chaos model is carried out based on NN synchronization. Chaotic dynamics follows nonlinear time-delay differential equations; omitting redundant coefficients, we can get

$$\begin{aligned} &\frac{1}{\tau_1}\int_{t_0}^{t} c(\zeta)d\zeta + c(t) + \tau_2\frac{dc(t)}{dt} = f_{\mathrm{NL}}(t,T) \\ &= \beta\cos^2[c(t-T) + m(t-T) + \Phi] \end{aligned}, \tag{2}$$

$$\begin{aligned} &\frac{1}{\tau_1}\int_{t_0}^{t} c(\zeta)d\zeta + c(t) + \tau_2\frac{dc(t)}{dt} = f_{\mathrm{MZI}}(t,T,\delta T) \\ &= \beta\cos^2[c(t-T) - c(t-T-\delta T) + m(t-T) - m(t-T-\delta T) + \Psi] \end{aligned}. \tag{3}$$

Equation (2) corresponds to the intensity chaos model [5] and Eq. (3) is the phase chaos model [11]. A fourth-order Runge–Kutta algorithm is adopted to numerically simulate the process of chaos generation with a sampling rate of 100 GSample/s [14], where $c(t)$ is the chaotic carrier and $m(t)$ is the encrypted signal. The differential nonlinear process governing chaotic dynamics is derived from the bandpass filtering function of the optoelectronic feedback, corresponding to an integral response time with $\tau_1 = 3.18\,\mu\mathrm{s}$ and a differential response time with $\tau_2 = 23.8$ ps, respectively. The amplification factor β is set to 5 and determines the complexity of chaos. The total delay of the feedback loop is $T = 25$ ns. The nonlinear device of the intensity chaotic model is a Mach–Zehnder modulator (MZM) with initial phase $\Phi = \pi/4$. For phase chaos, the nonlinear transformation is performed by a Mach–Zehnder interferometer (MZI), and f_{NL} and f_{MZI} are the response curve functions of the MZM and MZI, respectively. The MZI is governed by a $\cos^2$ transformation with an initial phase of $\Psi = \pi/4$ and imbalanced with a delay of $\delta T \sim 400$ ps, leading to an interference condition determined by the phase difference between times t and $t - \delta T$ [6].

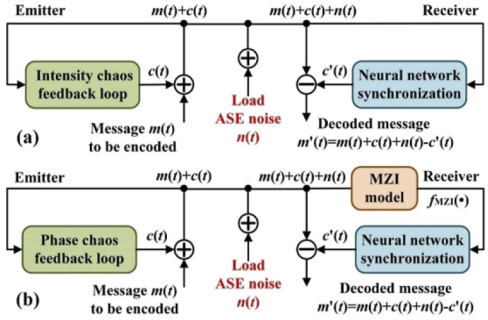

Fig. 1. Simulation setup of NN-based chaotic synchronization under AWGN channel: (a) intensity chaos model; (b) phase chaos model.

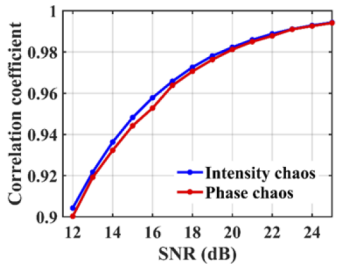

Fig. 2. CC with different channel SNRs in simulation.

The principles of chaos synchronization via a NN and the security of the system have been introduced and studied in detail in previous work [10,11]. Figure 1 shows the simulation setup of NN-based chaotic synchronization under an AWGN channel for intensity chaos and phase chaos systems. The NN describes the relationship between encrypted signals $c(t)+ m(t)$ and chaotic carriers $c(t)$, and $c'(t)$ is the chaos generated by the NN. If the predicted chaotic carrier $c'(t)$ is equal to $c(t)$, the decrypted signal $m'(t)$ will be equal to $m(t)$. The NN is trained at a channel SNR of 25 dB. The well-trained NN is used for chaotic synchronization and decryption under different channel SNRs, and $n(t)$ indicates the noise power.

To quantitatively evaluate the performance of chaotic synchronization, the correlation coefficient (CC) is defined as

$$CC = \frac{\langle [c(t) - \langle c(t)\rangle][c'(t) - \langle c'(t)\rangle]\rangle}{\sqrt{\langle [c(t) - \langle c(t)\rangle]^2\rangle \langle [c'(t) - \langle c'(t)\rangle]^2\rangle}}, \tag{4}$$

where $\langle\cdot\rangle$ denotes an average. We first investigated the CC of $c(t)$ and $c'(t)$ with the channel SNR; the simulation results are shown in Fig. 2. For intensity chaos and phase chaos with a 15 GHz bandwidth, the CC shows a positive correlation with the channel SNR, and the CCs are basically the same for the same channel SNR. When the channel SNR is greater than 15.5 dB, chaos synchronization with a CC greater than 95% can be achieved, and the CC is greater than 98% when the channel SNR is greater than 20 dB.

Figure 3 shows the BER and SNR performance of decrypted signals with different channel SNRs. The red curve shows the BER performance of decrypted signals with channel SNR, and the blue and green curves show the variation of SNR with channel SNR for the SNRs of the original and decrypted signals, where the SNR of the original signal is the same as the channel SNR in the simulation. Figure 3(a) shows the variation

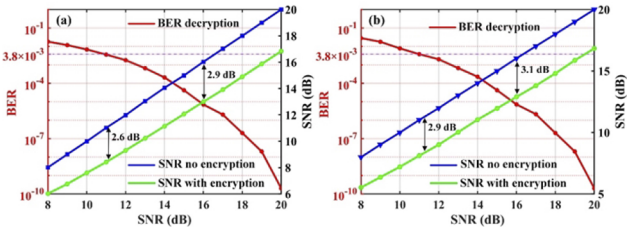

Fig. 3. BER and SNR performance of 40 Gbit/s decrypted signals with different channel SNRs in simulation: (a) intensity chaos model; (b) phase chaos model.

of BER and SNR of 40 Gbit/s decrypted signals with channel SNR after intensity chaos encryption. When the channel SNR is ≈11.2 dB, the BER of the decrypted signals is $\approx 3.8 \times 10^{-3}$, which is the hard-decision forward-error-correction (HD-FEC) threshold [15]. Moreover, the SNR of the decrypted quadrature phase-shift keying (QPSK) signals after chaotic encryption is 8.6 dB at this time, with a 2.6 dB SNR degradation compared with the original signals. With the increase of channel SNR, there is 2.9 dB SNR loss in the decrypted QPSK signals compared with the original signals after intensity chaos encryption. The variation of BER and SNR of 40 Gbit/s decrypted signals with channel SNR for phase chaos encryption in Fig. 3(b) has the same trend. When the channel SNR is ≈11.3 dB, the BER of the decrypted QPSK signals is $\approx 3.8 \times 10^{-3}$, with 2.9 dB SNR degradation compared with the original signals. Additionally, there is 3.0 dB SNR loss in the decrypted QPSK signals compared with the original signals after phase chaos encryption.

After completing the simulation verification, experiments under the AWGN channel in the back-to-back (BtB) case are demonstrated. The experimental setup for intensity chaos is shown in Fig. 4(a). The output light of a continuous wave laser (CW1) with a power of 14 dBm is injected into a Mach–Zehnder modulator (MZM1) with a 3 dB bandwidth of 20 GHz and a half-wave voltage of 4.1 V. The output light of MZM1 is the chaotic carrier $c(t)$, and is divided into two parts through an optical coupler (OC1), where one part is used for training the NN, and the other part is mixed with the QPSK message $m(t)$ from CW2. The mixed signal $c(t) + m(t)$ is amplified by an electric amplifier (AMP) with a 12 V peak-to-peak voltage and a 3 dB bandwidth of 50 kHz to 15 GHz to drive MZM1. MZM2 is driven by a 40 Gbit/s QPSK message generated by an 80 GSample/s arbitrary waveform generator (AWG). The mixture ratio between message $m(t)$ and chaos $c(t)$ is adjusted by variable optical attenuators (VOA1 and VOA2), and the power ratio of the signal and chaotic carrier is 1.5:1. The encrypted carrier $m(t) + c(t)$ is divided into two parts, where one part is used for adding the ASE noise by an EDFA with $n(t)$, and the other part is sent back to the feedback loop for chaos generation. In the feedback loop, after being delayed, the encrypted carrier is converted into electric signals by a photodiode (PD1) with a 3 dB bandwidth of 20 GHz. VOA3 is used to control the feedback strength. The encrypted carrier $m(t) + c(t) + n(t)$ and chaotic carrier $c(t)$ are received by PD2 and PD3, respectively, and collected by an oscilloscope with 100 GSample/s sampling rate. Chaos synchronization can be realized by extracting the chaotic carrier $c(t)$ from the encrypted carrier $m(t) + c(t) + n(t)$.

The experimental setup for the phase chaotic system is shown in Fig. 4(b); a 1550 nm semiconductor laser with a narrow linewidth of 0.1 kHz, followed by an in-phase quadrature

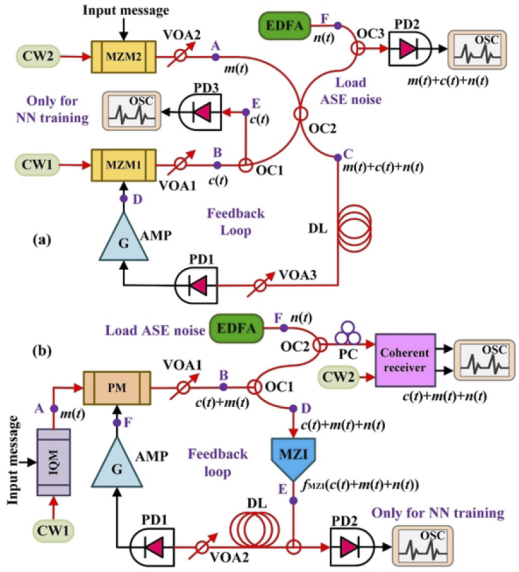

Fig. 4. Experimental structures of optoelectronic feedback-based chaotic optical communication systems in AWGN channel: (a) intensity chaotic system; (b) phase chaotic system. AMP, electrical amplifier; CW, continuous wave laser; DL, optical delay line; EDFA, erbium-doped fiber amplifier; IQM, in-phase quadrature modulator; MZI, Mach–Zehnder interferometer; MZM, Mach–Zehnder modulator; OC, optical coupler; OSC, oscilloscope; PC, polarization controller; PD, photodiode; PM, phase modulator; VOA, variable optical attenuator.

modulator (IQM) with a half-wave voltage of 4.5 V, generates 40 Gbit/s QPSK signals. Most of the devices are identical to those in Fig. 4(a). The differences are that the phase modulator (PM) in the feedback loop is linearly modulated and a MZI with a time-delay difference of 400 ps is used to realize the phase-to-intensity conversion. Since the phase chaos amplitude is constant, the encrypted signal $m(t) + c(t) + n(t)$ is received linearly through a coherent receiver and collected by an oscilloscope with a 100 GSample/s sampling rate at the receiving end.

In the experimental system, both phase chaos and intensity chaos have bandwidths of 15 GHz, and the CC after chaotic synchronization as a function of the channel SNR is shown in Fig. 5. Unlike the simulation results, the device noise and AWGN noise at the transmitter end will affect the synchronization performance at the same time, and we will unify it as the channel SNR in the experiment. Compared with the simulation results, the CC of the experiment is reduced to a certain extent. Under the same channel SNR, the synchronization performance of intensity chaos is significantly better than that of phase chaos,

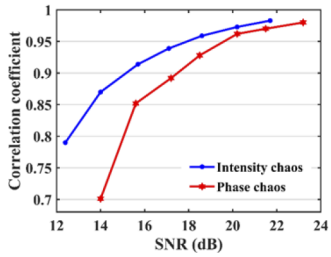

Fig. 5. CC as a function of channel SNR in experiment.

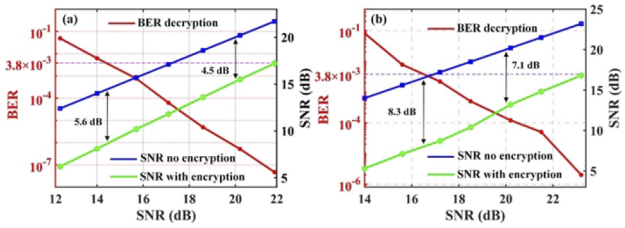

Fig. 6. BER and SNR performance of 40 Gbit/s decrypted signals as a function of channel SNR in the experiment:. (a) intensity chaos model; (b) phase chaos model.

because in the process of NN-based synchronization, the MZI needs to be modeled first for phase chaos, and the modeling error will reduce the performance under the influence of AWGN noise. When the channel SNR is greater than 15.4 dB, intensity chaos can achieve synchronization performance with a CC greater than 90%. For phase chaos, the channel SNR is required to be greater than 17.8 dB. To achieve chaotic synchronization with a CC greater than 95%, intensity chaos requires a channel SNR greater than 18.1 dB, while phase chaos requires a channel SNR greater than 19.6 dB.

The BER and SNR performance of decrypted signals with different channel SNRs in the experiment is shown in Fig. 6. Figure 6(a) shows the variation of BER and SNR of 40 Gbit/s decrypted signals with channel SNR after intensity chaos encryption. When the channel SNR is ≈14.3 dB, the BER of the decrypted signals is the threshold of HD-FEC, and the SNR of the decrypted signals after chaotic encryption is 8.7 dB, with an SNR degradation of 5.6 dB compared with the original signals. When the channel SNR is greater than 14.3 dB, the BER of the decrypted signals is less than the threshold of HD-FEC, and when the channel SNR gradually increases, the SNR gap between the decrypted signals and the original signals will become smaller. When the channel SNR is ≈20 dB, the SNR of decrypted signals is ≈15.5 dB, which has a 4.5 dB SNR degradation with the original signals.

The variation of BER and SNR of 40 Gbit/s decrypted signals with channel SNR for phase chaos encryption is shown in Fig. 6(b). Compared with intensity chaos in the experiment, phase chaos has a larger SNR gap between the decrypted signals and the original signals. For the same reason, the NN-based chaotic synchronization for phase chaos needs to mathematically model MZI first, and the AWGN will reduce the accuracy of the model. When the channel SNR is ≈16.5 dB, the BER of the decrypted signals is the threshold of HD-FEC, and the SNR of the decrypted signals is 8.2 dB, with an SNR degradation of 8.3 dB compared with the original signals. When the channel SNR is 20 dB, the SNR of decrypted signals is 12.9 dB, which has a 7.1 dB SNR degradation of the original signals, and when the channel SNR is 22 dB, the SNR of decrypted signals is 15.3 dB, with a 6.7 dB SNR degradation.

In conclusion, with the NN-based synchronization method, an SNR model of decrypted signals for optoelectronic feedback-based chaotic optical communication systems is proposed. Under different channel SNRs, the SNR degradation of 40 Gbit/s phase chaos and intensity chaos models are analyzed by simulation and experiment, respectively, with 15 GHz chaotic carrier bandwidth. The simulation results show that there is a 2.9 dB SNR degradation with decrypted signals for both intensity chaos and phase chaos. Moreover, in experiment, after chaos encryption, there is a SNR degradation of 4.5 dB to 5.6 dB with varying channel SNR for intensity chaos, while there is a SNR degradation of 7.1 dB to 8.3 dB for phase chaos. The simulation and experimental results provide guidance for long-distance transmission.

Funding. National Natural Science Foundation of China (62025503).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. M. Sciamanna and K. A. Shore, Nat. Photonics **9**, 151 (2015).
2. Y. Fu, M. Cheng, X. Jiang, Q. Yu, L. Huang, L. Deng, and D. Liu, Photonics Res. **7**, 1306 (2019).
3. N. Gastaud, S. Poinsot, and L. Larger, Electron. Lett. **40**, 898 (2004).
4. R. Lavrov, M. Peil, and M. Jacquot, Phys. Rev. E **80**, 026207 (2009).
5. L. Larger, J. P. Goedgebuer, and V. Udaltsov, C. R. Phys. **5**, 669 (2004).
6. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. Mirasso, L. Pesquera, and K. Shore, Nature **438**, 343 (2005).
7. J. Ke, L. Yi, G. Xia, and W. Hu, Opt. Lett. **43**, 1323 (2018).
8. Z. Gao, Q. Li, L. Zhang, B. Tang, Y. Luo, X. Gao, S. Fu, Z. Li, Y. Wang, and Y. Qin, Opt. Lett. **47**, 913 (2022).
9. P. J. Winzer, D. T. Neilson, and A. R. Chraplyvy, Opt. Express **26**, 24190 (2018).
10. J. Ke, L. Yi, Z. Yang, Y. Yang, Q. Zhuge, Y. Chen, and W. Hu, Opt. Lett. **44**, 5776 (2019).
11. Z. Yang, J. Ke, Q. Zhuge, W. Hu, and L. Yi, Opt. Lett. **47**, 2650 (2022).
12. K. Kikuchi, J. Lightwave Technol. **34**, 157 (2016).
13. D. Rafique, J. Lightwave Technol. **34**, 544 (2016).
14. J. R. Dormand and P. J. Prince, J. Comput. Appl. Math **6**, 19 (1980).
15. K. Wang and Z. Ding, IEEE Trans. Wireless Commun. **15**, 8223 (2016).