IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 22, 2019, accepted January 5, 2020, date of publication January 13, 2020, date of current version January 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965960

Secure Optical Communication Based on Cluster Chaos Synchronization in Semiconductor Lasers Network

SHIQIN LIU, NING JIANG, (Member, IEEE), ANKE ZHAO, YIQUN ZHANG, AND KUN QIU
School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Ning Jiang (uestc_nj@uestc.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61671119 and Grant 61471087, in part by the 111 Project under Grant B14039, and in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2019J003.

ABSTRACT We propose and numerically demonstrate a secure optical communication scheme in a small-world semiconductor lasers network based on cluster chaos synchronization and false-message scrambling. According to the symmetries of network, the semiconductor lasers are divided into sets of heterogeneous coupled clusters. The properties of cluster chaos synchronization, the performance and security of optical chaotic communication, as well as the influence of false message on the synchronization of clusters are systematically investigated. It is demonstrated that, by properly setting the parameters of the lasers network, high-quality chaos synchronization can be achieved between the intra-cluster lasers, whereas incoherent states are observed between inter-cluster lasers. Moreover, by inserting false messages into the inter-cluster couplings, the privacy of chaotic carriers transmitted over the inter-cluster public links can be significantly enhanced, as such secure bidirectional communication among intra-cluster lasers is achievable with a message bit rate of several Gbit/s. Compared with the conventional point-to-point communication systems, the proposed scheme supports multipoint-to-multipoint secure communications.

INDEX TERMS Secure communication, cluster chaos synchronization, semiconductor laser network, false-message scrambling.

I. INTRODUCTION

In recent years, optical chaotic communication based on semiconductor lasers that utilizes the noise-like waveform and broadband-spectrum chaotic signal as carriers for message hiding has attracted great attention, for its potential application in physical-layer secure communication [1]–[5]. Chaos synchronization and communication in coupling lasers systems have been extensively studied in the last two decades [6]–[11]. Argyris and coworkers demonstrated secure chaotic communication over a commercial fiber network in Athen, in virtue of the chaos synchronization of two semiconductor lasers [11], which confirms the feasibility of this technology. After that, several schemes have been proposed to enhance the capacity of chaotic communication systems [12]–[20]. Ke *et al*. experimentally demonstrated high-speed long-distance chaotic optical communication by using the duobinary modulation format and digital signal processing technique [18]. Fu *et al*. proposed a wavelength division multiplexing secure communication case with an optically coupled phase chaos system and phase modulation to intensity modulation conversion mechanism [19]. Our recent work presented a novel high-speed optical communication scheme utilizing the chaos synchronization of distributed semiconductor lasers as the physical key for spectral phase encryption and decryption [20]. Nevertheless, most of these systems mainly focused on the point-to-point scenario, while the multipoint-to-multipoint chaotic communication scenario that is more compatible with the practical communication networks is lack of investigation.

In this paper, we numerically demonstrate the bidirectional secure optical communication in a small-world semiconductor lasers (SLs) network with heterogeneous coupling delays, in virtue of cluster chaos synchronization and false-message scrambling (FMS). By dividing the SLs network into a set of clusters and adjusting the coupling parameters of the network, high-quality cluster chaos synchronization is obtained over a wide dynamic operation range. Taking a nontrivial cluster

The associate editor coordinating the review of this manuscript and approving it for publication was Baile Chen.

composed of three SLs for instance, we demonstrate that the proposed system supports bidirectional transmissions over Gbit/s between intra-cluster SLs. Furthermore, it is indicated that the security of intra-cluster message transmissions can be further significantly enhanced, by embedding false messages into the couplings between inter-cluster SLs to prevent the eavesdroppers from accessing correct chaotic carriers from the inter-cluster public links.

II. NETWORK TOPLOGY AND THEORY MODEL

The small-world network is a typical complex network that lies somewhere between regular and random networks, it has been extensively adopted to simulate the real networks [21]. Since in practical communication networks, the couplings between different entities are heterogeneous, small-world network with heterogeneous delays is discussed in this work to demonstrate the universality of the proposed scheme. Mathematically, the small-world SLs network is defined as a graph $g = [V(g), E(g)]$, where $V(g)$ denotes the vertex set and $E(g)$ presents the edge set. The vertices are adjacent if they are connected by an edge. A symmetry is defined as a permutation of the total vertices in the SLs network that preserves its adjacency. On the basis of the symmetry identification of the SLs network, the SLs can be divided into different clusters by distinguishing the orbits of all symmetries. The orbits are the disjoint sets of SLs in all of the symmetry operations, and the SLs in the same orbit are classified into a cluster. SLs in the same cluster can be permuted to each other without alerting the adjacency of the network, and they are structurally equivalent in the strongest possible sense: the same structural role in the network [22], [23]. Thus, SLs in the same cluster always work under a symmetric operation condition, such that they can synchronize with each other under certain conditions.

Started with a ring of 12 SLs which are connected with its b nearest neighbors by undirected edges, with a probability p, the small world network is generated by reconnecting these edges to other vertices chosen uniformly over these SLs. Fig. 1 shows the topology and the derivative heterogeneous coupling delay clusters of an exemplary small-world SLs network. Here, b and p are respectively set as 10 and 0.1. The mutually coupled SLs in the small world network are divided into a set of clusters referred to as (1, 2, 9), (3, 12), (4, 7), (5, 11), (6), (8, 10), according to the symmetries of the global network. These clusters are respectively referred to as C_A, C_B, C_C, C_D, C_E, C_F, wherein cluster C_A, C_B, C_C, C_D, C_F are non-trivial clusters and cluster C_E is a trivial cluster consisting of only one SL. As shown in Fig. 1(b), the intra-cluster SLs are coupled with each other homogeneously, while the coupling delays among inter-cluster SLs are heterogeneous. Obviously, after setting heterogeneous delays to network, SLs in the same cluster are still symmetric in the aspect of coupling delays, so that the symmetries of the network are still preserved.

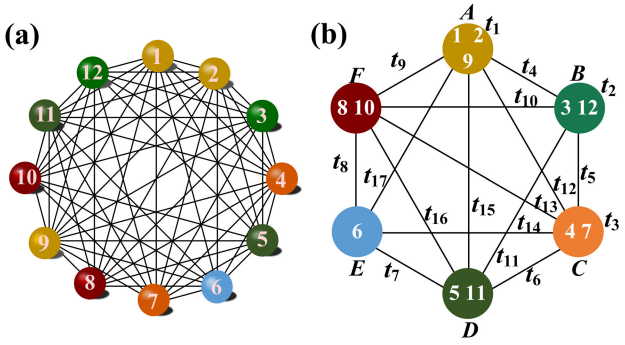


FIGURE 1. (a) Topology of an exemplary small-world network consisting of 12 SLs, (b) mutually-coupled clusters with heterogeneous delays divided from the small-world network. Here, each node of (a) denotes a SL and SLs with different colors belong to different clusters.

For the numerical purpose, the well-known Lang-Kobayashi rate equations are modified by taking the mutual coupling terms into consideration, and are presented as follows [24], [25]:

$$\begin{aligned}\frac{dE_k(t)}{dt} &= \frac{(1+i\alpha)}{2}(G_k(t) - \frac{1}{\tau_p})E_k(t) \\ &\quad +\sigma\sum_{l=1}^{N} A_{kl}E_l(t-\tau_{lk})\exp(-i\omega_l\tau_{lk}) \\ &\quad +\sqrt{2\beta N_k(t)}\chi_k(t) \qquad (1)\end{aligned}$$

$$\frac{dN_k(t)}{dt} = \frac{uI_{th}}{q} - \frac{N_k(t)}{\tau_e} - G_k(t)\,\|E_k\ (t\ )\|^2 \qquad (2)$$

$$G_k(t) = \frac{g(N_k(t)-N_0)}{1+s\,\|E_k\ (t\ )\|^2} \qquad (3)$$

$$A = \begin{pmatrix} 0&1&1&1&1&1&1&1&1&1&1&1\\ 1&0&1&1&1&1&1&1&1&1&1&1\\ 1&1&0&1&1&0&1&1&1&1&1&1\\ 1&1&1&0&1&1&1&1&1&0&1&1\\ 1&1&1&1&0&1&1&1&1&1&0&1\\ 1&1&0&1&1&0&1&1&1&1&1&0\\ 1&1&1&1&1&1&0&0&1&1&1&1\\ 1&1&1&1&1&1&0&0&1&0&1&1\\ 1&1&1&1&1&1&1&1&0&1&1&1\\ 1&1&1&0&1&1&1&0&1&0&1&1\\ 1&1&1&1&0&1&1&1&1&1&0&1\\ 1&1&1&1&1&0&1&1&1&1&1&0 \end{pmatrix} \qquad (4)$$

where the subscripts k and $l(k,\ l\ =\ 1,\ldots,N)$ stand for SL_k and SL_l, respectively; N is the total number of SLs in the small-world network, which indicates the size of the SLs network. The optical gain $G(t)$ is defined in (3), and σ is the homogeneous coupling strength in the whole network. A is an adjacency matrix which is usually used to mathematically describe the connectivity of nodes in the network, $A_{kl} = A_{lk} = 1$ means SL_k and SL_l are mutually coupled with each other and $A_{kl} = A_{lk} = 0$ means no connection between them. The adjacency matrix of the small-world SLs network is expressed in (4). The other intrinsic parameters of SLs are set as the representative values for typical semiconductor laser [5], [10]: the photon lifetime $\tau_p = 2$ ps, the threshold current $I_{th} = 14.7$ mA, the current factor $u = 1.5$, the electric

charge $q = 1.6 \times 10^{-19}$ C, the carrier lifetime $\tau_e = 2$ ns, the linewidth-enhancement factor $\alpha = 5$, the spontaneous emission rate $\beta = 1.5 \times 10^{-6}\text{ns}^{-1}$, the differential gain coefficient $g = 1.5 \times 10^{4}\text{s}^{-1}$, the transparency carrier density $N_0 = 1.5 \times 10^{8}$, the nonlinear saturation coefficient $s = 5 \times 10^{-7}$, the wavelength of SLs is $\lambda_0 = 1550$ nm, and the frequency $\omega_0 = 1.936 \times 10^{14}$rad/s. In addition, the Gaussian noise $\chi(t)$ with unity variance and zero mean is adopted to model the spontaneous emission noise. The values of these parameters do not change unless otherwise stated. τ stands for the coupling delays between different clusters. Without loss of generality, the coupling delays follow the Gaussian distribution (μ, S^2) with $\mu = 6$ns and $S^2 = 0.25$ns, wherein μ denotes the mean of coupling delays, S stands for the standard deviation of coupling delays. The coupling delays are 5.767ns, 5.8ns, 5.67ns, 6.43ns, 5.9ns, 6.93ns, 6ns, 6.93ns, 4.78ns, 6.18ns, 6.14ns, 6.97ns, 6.89ns, 6.95ns, 5.40ns, 6.43ns. In our simulations, the rate equations (1)-(3) are handled with fourth-order Runge-Kutta algorithm with a simulation step of 1 ps [26].

To systematically identify the synchronization quality between the pairwise SLs, the cross-correlation coefficient (CC), which is usually adopted to describe the linear relationship between two signals, is introduced and given by:

$$CC_{k,l} = \frac{\langle (I_k(t) - \langle I_k(t)\rangle) \cdot (I_l(t) - \langle I_l(t)\rangle)\rangle}{\sqrt{\langle (I_k(t) - \langle I_k(t)\rangle)^2\rangle \cdot \langle (I_l(t) - \langle I_l(t)\rangle)^2\rangle}} \quad (5)$$

where $I = |E(t)|^2$ is the intensity time series of chaos outputted by SLs, and $\langle\cdot\rangle$ represents the corresponding time averaging. In this work, two chaotic signals are treated as isochronously synchronous when the corresponding $CC_{k,l} > 0.95$ [27]-[29].

To quantitatively evaluate the synchronization error of each SLs cluster, the time-averaged root-mean square synchronization error (RMS) is further introduced and defined as:

$$RMS = \frac{\sum_{n=1}^{N_c} \sqrt{(I_l(t) - \hat{I}(t))^2/N_e}}{N_c \hat{I}(t)} \quad (6)$$

where subscript $n = 1, \ldots, N_c$, $\hat{I}(t) = \sum_{l=1}^{n_c} I_l(t)/N_c$ stands for average output of a cluster which contains N_c SLs. N_e is the length of $I_l(t)$ ($\hat{I}(t)$). Here, clusters are considered as synchronized when RMS < 0.01 [30].

III. CLUSTER CHAOS SYNCHRONIZATION

Firstly, we investigate the influence of coupling strength on the dynamic behaviors of SLs in the small world network. Since the dynamic behaviors of SLs in the same cluster are very similar for the symmetric configuration, we only show the results of one representative SL for each cluster here. Fig. 2 shows the bifurcation maps of SLs of six clusters. For the SLs in the six clusters, obvious state transitions are observed with the increase of coupling strength. Due to the large degrees of SLs and the small differences of degrees between different-cluster SLs, the coupling strengths for the states changing are small and nearly identical. The states of six clusters change from stable to quasiperiodic (multiple periodic) with coupling strengths below 0.15ns^{-1}, and further change to chaotic states with a slight increasement of coupling strength. Therefore, it is very easy to obtain chaotic carriers by setting a proper overall coupling strength.

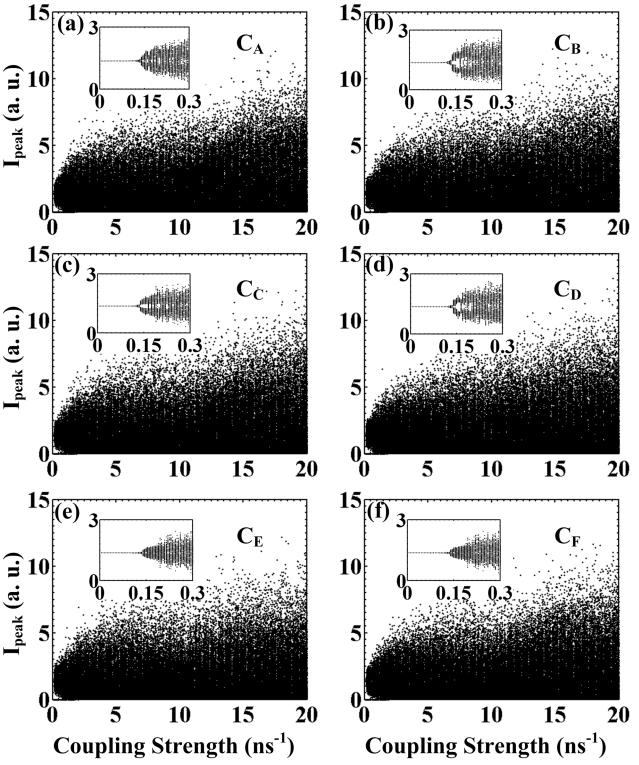


FIGURE 2. Bifurcation diagrams of peak intensity versus coupling strength for representative SLs in cluster (a) C_A, (b) C_B, (c) C_C, (d) C_D, (e) C_E and (f) C_F. The insets in each diagram show the details of bifurcation from 0ns^{-1} to 0.3ns^{-1}.

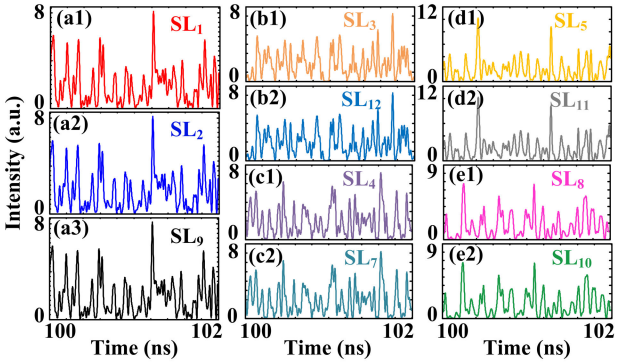


FIGURE 3. Temporal waveforms of the chaotic signals generated by cluster (a1)-(a3) C_A, (b1)-(b2) C_B, (c1)-(c2) C_C, (d1)-(d2) C_D, and (e1)-(e2) C_F with $\sigma = 13\text{ns}^{-1}$. Here, the result for the trivial cluster C_E is not shown for the sake of simplicity.

Fig. 3 shows the temporal waveforms of the chaotic signals outputted by the SLs of the five nontrivial clusters in the

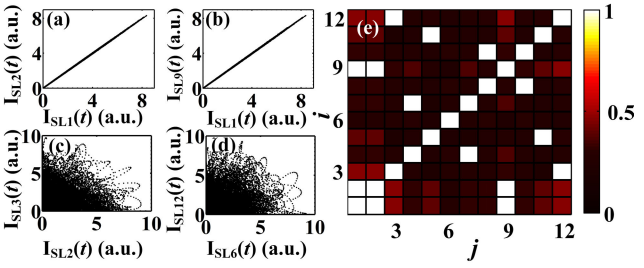


FIGURE 4. Cross-correlations of (a) SL1-SL2, (b) SL1-SL9, (c) SL2-SL3 and (d) SL6-SL12 with coupling strength $\sigma = 13\text{ns}^{-1}$. (e) Pairwise CC of the SLs in the exemplary network with $\sigma = 13\text{ns}^{-1}$.

exemplary network. With coupling strength $\sigma = 13\text{ns}^{-1}$, it is observed that all the SLs are working in chaotic regimes. Moreover, similar waveform fluctuations are observed among intra-cluster SLs, which means the intra-cluster SLs synchronize with each other well. To further investigate the properties of the chaos synchronization, Fig. 4 shows the cross correlations between the intra-cluster SLs and those between inter-cluster SLs, by taking the cluster C_A for instance. Figs. 4(a) and 4(b) indicate that chaos synchronization is achieved among SLs in the exemplary cluster C_A with $CC_{1,2} = 1$, $CC_{1,9} = 1$. Nevertheless, by randomly choosing two pairs of SLs from different clusters, the CC among the inter-cluster SLs are very low as shown in Figs. 4(c) and 4(d) ($CC_{2,3} = 0.17$, $CC_{6,2} = 0.11$). Moreover, Fig. 4(e) gives the pairwise CC of the SLs in the complex network, and it is demonstrated that high-quality chaos synchronization can be easily achieved between intra-cluster SLs, while the CC between inter-cluster SLs are pretty low, which agree with the results shown in Figs. 4(a)-4(d). Thus, cluster synchronization is achieved. Under such a scenario, bidirectional message exchange between intra-cluster SLs is available. The low cross correlations between inter-cluster SLs mean that message exchange is not achievable among different clusters.

Furthermore, in order to investigate the influences of parameters on the quality of cluster chaos synchronization, Fig. 5 presents the dependence of cluster synchronization errors RMS of non-trivial clusters on the coupling strength, under different bias currents. It is shown that the quality of cluster chaos synchronization is particularly sensitive to the coupling strength. When the coupling strength is small, large RMS are observed in five clusters which indicates the non-trivial clusters will lose synchronization in the large-RMS regions. With an appropriate large coupling strength of the network, chaos synchronization (RMS < 0.01) can be realized in five clusters. It is also worth mentioning that, the synchronous parameter range for cluster C_D is wider than those of other clusters which means cluster C_D can keep synchronous even other clusters losing their synchronization. On the other hand, with the increment of I, the parameter regions for synchrony clusters become more and more narrow. For $I = 3I_{th}$, small values of RMS are also found when coupling strength is set around 1ns^{-1}, which correspond to a very narrow synchronization range and are not suitable for

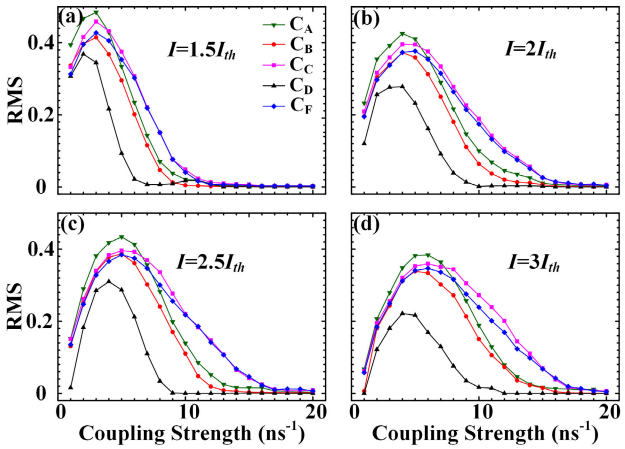


FIGURE 5. RMS of five nontrivial clusters (C_A, C_B, C_C, C_D, C_F) as the function of coupling strength with (a) $I = 1.5I_{th}$, (b) $I = 2I_{th}$, (c) $I = 2.5I_{th}$ and (d) $I = 3I_{th}$.

communications. It can be concluded that the bias current will modify the overall trend of the quality of the cluster chaos synchronization in the small-world SLs network.

In practice, the unavoidable mismatch between the SLs would degrade the synchronization quality of clusters. Therefore, we investigate the influence of intrinsic parameter mismatch on the CC of cluster C_A, C_B, C_C, C_D, and C_F. Here, the mismatch is introduced by fixing the intrinsic parameters of representative SLs in each cluster (SL1, SL2, SL3, SL4, SL5, SL6, and SL8), and changing those of other SLs (SL7, SL9, SL10, SL11, and SL12). The mismatched parameters are: $\alpha' = \alpha(1+u)$, $g' = g(1+u)$, $\tau_p' = \tau_p(1+u)$, $\tau_e' = \tau_e(1-u)$, $N_0' = N_0(1-u)$, $s' = s(1-u)$, where u is the mismatch ratio. For simplicity, the mismatched parameters for different clusters are changed by the same ratio simultaneously. As shown in Fig. 6, with the increase of parameter mismatch, the cross-correlation coefficients of nontrivial clusters decrease gradually. Nevertheless, satisfactory CC ($CC > 0.99$) can be observed over a wide mismatch range, this is mainly contributed to the symmetric couplings of intra-cluster SLs.

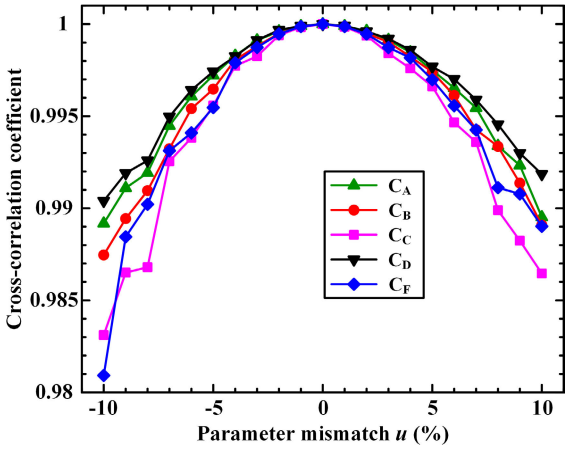


FIGURE 6. Cross-correlation coefficients versus parameter mismatch.

IV. CHAOS COMMUNICATION AND SECURITY DISCUSSION

Based on high-quality cluster chaos synchronization, we investigate the quality and performance of chaos communication in this section. Cluster C_A is taken for instance to demonstrate the chaotic secure communication in the complex SLs network. The theoretical diagram of cluster C_A is illustrated in Fig. 7. The system is composed of three mutually coupled SLs (SL1, SL2, and SL9). The message $m_1(t)$ ($m_2(t)$ or $m_3(t)$) is firstly modulated into the output of the SL1 (SL2 or SL9) by OOK modulation with typical optical intensity modulator (IM), which is mathematically described as $|E_{km}| = |E_k|[1 + d \times m(t)]$, where $E_{km}(t)$ is the modulated carrier, $m(t)$ is the original message, and d is the modulation index which is set as 0.05 to guarantee the effective encryption of message [31]. After that, the modulated chaotic carriers are split into two parts by 50/50 fiber couplers (FC), and then injected to the other two intra-cluster SLs respectively. Due to the symmetric couplings, high quality cluster chaos synchronization is achievable. Based on the cluster chaos synchronization, message transmission can be exchanged between intra-cluster SLs in both clockwise and anti-clockwise directions. To protect the privacy of the chaotic carriers, three false messages $m_f(t)$ are respectively embedded into the injections from SL1, SL2, SL9 to the other-cluster SLs with intensity modulation index $d_f = d$. The $m_f(t)$ are random binary sequences. Under such scenario, eavesdroppers can only get a differential message when they simultaneously attack the intra-cluster public links and the inter-cluster public links. Without $m_f(t)$, it is extremely difficult for eavesdroppers to intercept the correct message. Therefore, in the proposed communication system, the security of message can be guaranteed.

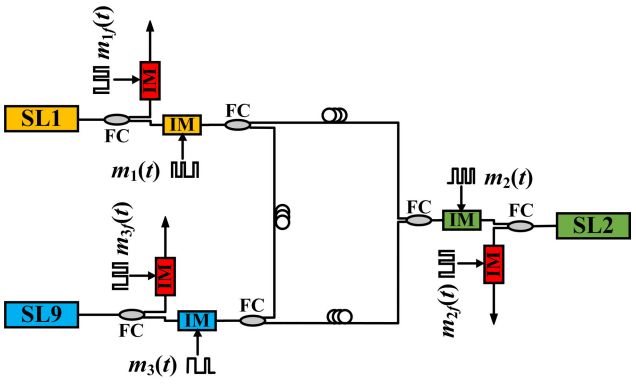


FIGURE 7. Schematic of the chaotic secure communication in an exemplary cluster C_A, wherein SL: semiconductor laser, FC: fiber coupler, IM: intensity modulator, $m(t)$: message, and $m_f(t)$: false message to SLs of other clusters.

The messages are decrypted by the way of direct subtraction decoding which is described as: $m'(t) = \mathrm{LPF}[|E_{km}|^2 - |E_k|^2]$, where LPF denotes a low-pass fourth-order Butterworth filter with a cut-off frequency equal to the message bit rate R which is used to filtering the recovered messages. The communication performance is quantified by calculating the Q-factor of the recovered messages, and the definition of the Q-factor is identical to that in [5].

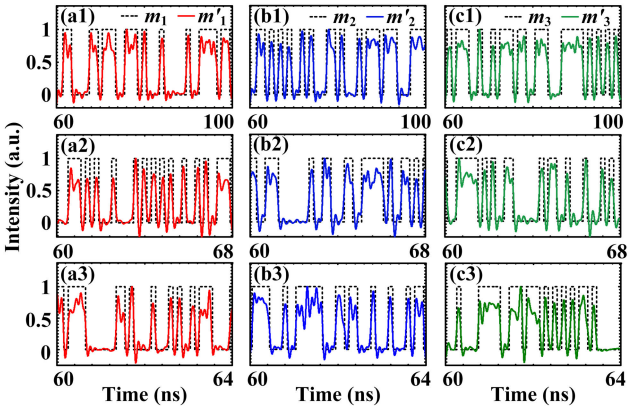


FIGURE 8. Illustrations of message recoveries in the clockwise transmission for the cases of 1 Gbit/s (first row), 5 Gbit/s (second row) and 10 Gbit/s (third row). In these scenarios, $m'_1(t)$, $m'_2(t)$, $m'_3(t)$ are decrypted by SL2, SL9. and SL1, respectively.

Fig. 8 shows the legal recovered messages in the clockwise direction transmission for the cases of different message bit rates, and the results for the anti-clockwise direction scenario are very similar and not shown for simplicity. As shown in Fig. 8, with the synchronous chaotic outputs of SLs in cluster C_A, the messages sent by SL1, SL2, and SL9 are successfully recovered by corresponding receivers SL2, SL9, and SL1 with different transmission cases. For the 5 Gbit/s and 10 Gbit/s transmission cases, more fluctuations are observed in the waveforms of recovered messages compared with those in 1 Gbit/s transmission, which means the influence of message bit rate on the recovery of messages is significant.

In order to evaluate the quality of legal decrypted messages, the eye diagrams of recovered messages $m'_1(t)$, $m'_2(t)$, and $m'_3(t)$ under different R are illustrated in Fig. 9.

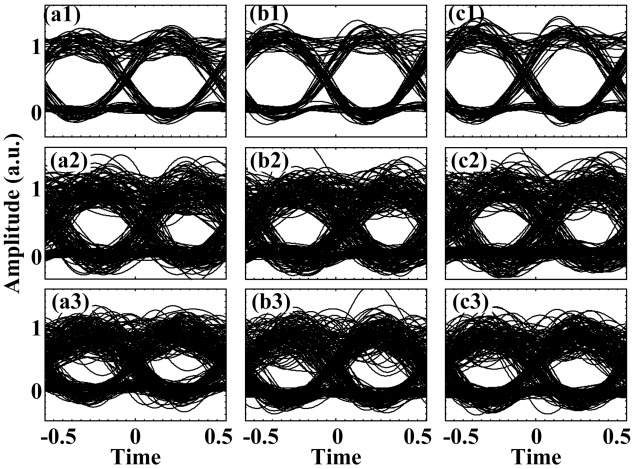


FIGURE 9. (a1)-(a3), (b1)-(b3), and (c1)-(c3) respectively illustrate the eye diagrams of $m'_1(t)$, $m'_2(t)$, and $m'_3(t)$ for the message bit rates of 1 Gbit/s (first row), 5 Gbit/s (second row) and 10 Gbit/s (third row). Here, the eye diagrams correspond to the recovered messages shown in Fig. 8.

The wider the eye, the higher quality the recovered message. Under the legal scenario, the messages are correctly recovered, which is directly indicated by the widely open eye diagrams. It can be seen that the quality of recovered messages under low transmission bit rates are better than those under relatively high transmission bit rates, because the corresponding eye diagrams in low R cases are clearer than those in high R cases. The results are in line with those in Fig. 8. Besides, message security in the communication system is also studied by analyzing the attack on the public links. The illegal interception is carried out by considering a typical attack scenario in chaos communication systems, namely directly filtering the signals transmitted over public links using a low pass filter with a cut off frequency equaling to R [5], [20]. As shown in Fig. 10, for the illegal attack, the eye diagrams of the intercepted messages are completely closed under different transmission bit rates. Therefore, it can be concluded that, the proposed communication system supports chaotic secure transmission over Gbit/s.

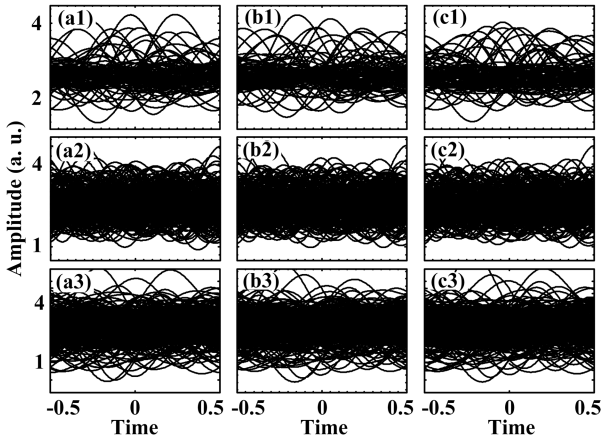


FIGURE 10. Eye diagrams of illegally-intercepted messages on the public transmission links, for the cases of 1 Gbit/s (first row), 5 Gbit/s (second row), and 10 Gbit/s (third row).

We further study the influence of message bit rate R on the performance of bidirectional chaotic communication. Fig. 11 displays the Q-factor of the messages recovered by

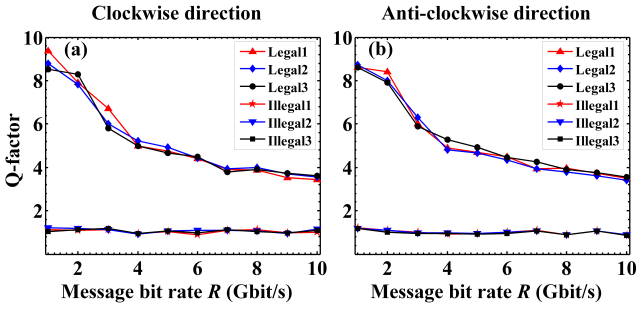


FIGURE 11. The Q-factors of messages recovered by legal decryptions and illegal interceptions in the bidirectional communication of (a) clockwise direction and (b) anti-clockwise direction, versus message bit rate R.

legal decryptions and illegal interceptions versus the bit rate of messages, under clockwise direction and anti-clockwise communication scenarios. Here, the messages are decoded in both directions simultaneously. It is shown that, the Q-factors show similar developing trends in two directions. For the bidirectional chaos communication system, good communication performances (Q-factor larger than 6) are observed when the bit rate is lower than 3 Gbit/s. With the increment of message bit rate, the communication performance is degraded. Q-factors closed to 4 are obtained even when the R is set to 10 Gbit/s. However, the corresponding Q-factors of messages intercepted by eavesdroppers always maintain low values around 1. It is indicated that the eavesdroppers cannot get access to any efficient messages under different transmission rate cases. Thus, message exchanges in cluster C_A are supported with bit rate of messages over Gbit/s, and the security of the communication system is guaranteed simultaneously. Moreover, it is worth mentioning that chaotic secure communication can also be realized in other synchronized clusters, and the communication performance as well as security properties is similar to those in the cluster C_A composed of three SLs. For the sake of simplicity, these results are not given here.

For the small-world SLs network, the coupling links are exposed to the public. To avoid illegal attacks to carrier waves, the FMS is proposed, and the corresponding efficiency is discussed in the above discussion. Without false messages, chaos synchronization in nontrivial clusters is achieved in a wide dynamic operation range as shown in Fig. 5. With FMS, some disturbances along with the false message may affect the performance of cluster chaos synchronization. To explore the influence of FMS on the quality of cluster chaos synchronization, Fig. 12 illustrates the maps of RMS in nontrivial cluster C_B, C_C, C_D, and C_F with different modulation indexes ($d_f = 0, 0.05, 0.1$), in the parameter spaces of coupling strength σ and current factor u. Because the chaos carriers with false messages are not directly coupled to the communication cluster C_A, the effect of FMS on cluster C_A is negligible. Here, the RMS of cluster C_A is not given for simplicity. As shown in Fig. 12, the white dash lines (RMS $= 0.01$) are the boundaries between synchronization regions (denoted by CS) and asynchronization regions. It is observed that, compared with the $d_f = 0$ case, the CS parameter regions of four clusters are negligibly influenced by the FMS when $d_f = 0.05$. With the increasing of modulation index, the optimal parameter ranges for cluster chaos synchronization are slightly narrower in cluster C_B, C_C, and C_F, while cluster C_D is more robust to the FMS due to the little change of its CS region. Therefore, it is concluded that, the influences of false messages on the chaos synchronization quality of other clusters are negligible by properly choosing the modulation index. More importantly, the negligible influence indicates that secure bidirectional communications can be simultaneously supported in the nontrivial clusters C_A, C_B, C_C, C_D, and C_F.

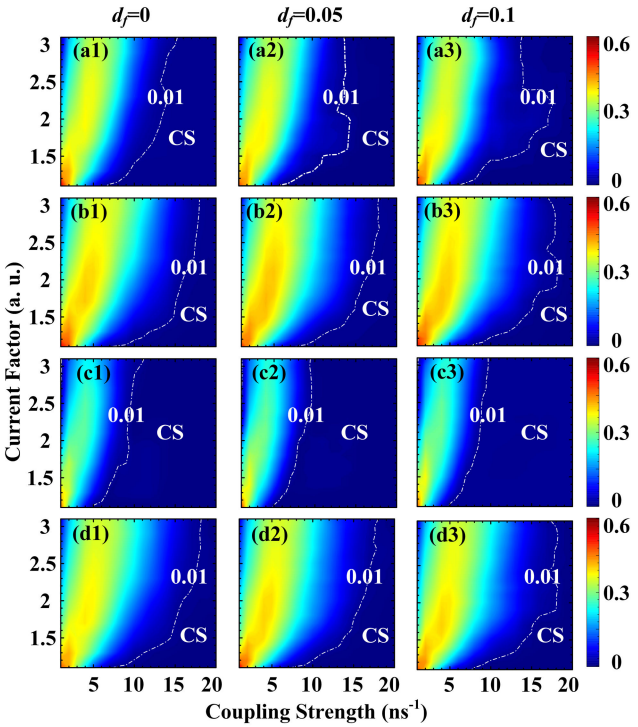


FIGURE 12. Two dimensional maps of RMS in the parameter spaces of coupling strength σ and current factor u with $d_f = 0$ (first column), $d_f = 0.05$ (second column) and $d_f = 0.1$ (third column), (a1)-(a3) cluster C_B, (b1)-(b3) cluster C_C, (c1)-(c3) cluster C_D, (d1)-(d3) cluster C_F.

V. CONCLUSION

In summary, we have proposed and demonstrated a secure optical communication scheme in small world SLs network composed of heterogeneous-delay-coupled semiconductor lasers, in virtue of cluster chaos synchronization and false-message scrambling. The numerical results demonstrated that, high-quality chaos synchronization between intra-cluster lasers can be achieved easily in a wide optimal operation range, due to the symmetric couplings. Based on this, bidirectional secure transmission over Gbit/s between intra-cluster SLs is available. Moreover, we proposed a security-enhanced method by scrambling the inter-cluster couplings with false messages. Under such a scenario, the inter-cluster chaotic carriers in the network are protected privately, and no useful message can be intercepted from the inter-cluster public links, as such the security of messages is further enhanced. This work paves the implementation of network-scenario secure communications using chaotic SLs.

ACKNOWLEDGMENT

S. Liu thanks L. Zhang for her help in the process of simulation.

REFERENCES

[1] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature Photon.*, vol. 9, no. 3, pp. 151–162, Mar. 2015.
[2] J.-M. Liu, H.-F. Chen, and S. Tang, "Synchronized chaotic optical communications at high bit rates," *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1184–1196, Sep. 2002.
[3] N. Li, W. Pan, L. Yan, B. Luo, and X. Zou, "Enhanced chaos synchronization and communication in cascade-coupled semiconductor ring lasers," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 6, pp. 1874–1883, Jun. 2014.
[4] N. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," *Opt. Lett.*, vol. 42, no. 17, p. 3494, Sep. 2017.
[5] N. Jiang, 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, no. 25, p. 32404, Dec. 2018.
[6] A. Uchida, R. McAllister, and R. Roy, "Consistency of nonlinear system response to complex drive signals," *Phys. Rev. Lett.*, vol. 93, no. 24, Dec. 2004, Art. no. 244102.
[7] M. C. Soriano, F. Ruiz-Oliveras, P. Colet, and C. R. Mirasso, "Synchronization properties of coupled semiconductor lasers subject to filtered optical feedback," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 78, no. 4, Oct. 2008, Art. no. 046218.
[8] A. Englert, W. Kinzel, Y. Aviad, M. Butkovski, I. Reidler, M. Zigzag, I. Kanter, and M. Rosenbluh, "Zero lag synchronization of chaotic systems with time delayed couplings," *Phys. Rev. Lett.*, vol. 104, no. 11, Mar. 2010, Art. no. 114102.
[9] S. Xiang, W. Pan, L. Yan, B. Luo, X. Zou, N. Jiang, and L. Yang, "Impact of unpredictability on chaos synchronization of vertical-cavity surface-emitting lasers with variable-polarization optical feedback," *Opt. Lett.*, vol. 36, no. 17, p. 3497, Sep. 2011.
[10] S. Xiang, J. Gong, H. Zhang, X. Guo, H. Wang, Y. Zhang, and A. Wen, "Zero-lag intensity correlation properties in small ring laser network with heterogeneous delays," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 35, no. 2, p. 287, Feb. 2018.
[11] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Nov. 2005.
[12] Y. Hong, P. S. Spencer, and K. A. Shore, "Wideband chaos with time-delay concealment in vertical-cavity surface-emitting lasers with optical feedback and injection," *IEEE J. Quantum Electron.*, vol. 50, no. 4, pp. 236–242, Apr. 2014.
[13] Y. Hong, "Experimental study of time-delay signature of chaos in mutually coupled vertical-cavity surface-emitting lasers subject to polarization optical injection," *Opt. Express*, vol. 21, no. 15, p. 17894, Jul. 2013.
[14] X. Tang, G.-Q. Xia, E. Jayaprasath, T. Deng, X.-D. Lin, L. Fan, Z.-Y. Gao, and Z.-M. Wu, "Multi-channel physical random bits generation using a vertical-cavity surface-emitting laser under chaotic optical injection," *IEEE Access*, vol. 6, pp. 3565–3572, 2018.
[15] S.-S. Li, X.-Z. Li, and S.-C. Chan, "Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation," *Opt. Lett.*, vol. 43, no. 19, p. 4751, Oct. 2018.
[16] P. Mu, P. He, and N. Li, "Simultaneous chaos time-delay signature cancellation and bandwidth enhancement in cascade-coupled semiconductor ring lasers," *IEEE Access*, vol. 7, pp. 11041–11048, 2019.
[17] J. Zhang, M. Li, A. Wang, M. Zhang, Y. Ji, and Y. Wang, "Time-delay-signature-suppressed broadband chaos generated by scattering feedback and optical injection," *Appl. Opt.*, vol. 57, no. 22, p. 6314, Aug. 2018.
[18] J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate," *Opt. Lett.*, vol. 43, no. 6, p. 1323, Mar. 2018.
[19] Y. Fu, M. Cheng, X. Jiang, L. Deng, C. Ke, S. Fu, M. Tang, M. Zhang, P. Shum, and D. Liu, "Wavelength division multiplexing secure communication scheme based on an optically coupled phase chaos system and PM-to-IM conversion mechanism," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 1949–1959, Nov. 2018.
[20] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, p. 1536, Apr. 2019.
[21] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, Jun. 1998.
[22] L. M. Pecora, F. Sorrentino, A. M. Hagerstrom, T. E. Murphy, and R. Roy, "Cluster synchronization and isolated desynchronization in complex networks with symmetries," *Nature Commun.*, vol. 5, Jun. 2014, Art. no. 4079.
[23] L. Zhang, W. Pan, L. Yan, B. Luo, X. Zou, and M. Xu, "Cluster synchronization of coupled semiconductor lasers network with complex topology," *IEEE J. Sel. Topics Quantum Electron.*, vol. 25, no. 6, pp. 1–7, Nov. 2019.

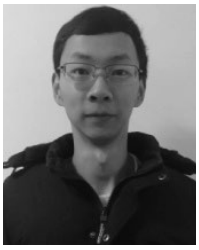
[24] X.-Z. Li, S.-S. Li, and S.-C. Chan, "Correlated random bit generation using chaotic semiconductor lasers under unidirectional optical injection," *IEEE Photon. J.*, vol. 9, no. 5, pp. 1–11, Oct. 2017.
[25] N. Li, H. Susanto, B. R. Cemlyn, I. D. Henning, and M. J. Adams, "Modulation properties of solitary and optically injected phased-array semiconductor lasers," *Photon. Res.*, vol. 6, no. 9, p. 908, Sep. 2018.
[26] T. Deng, J. Robertson, Z.-M. Wu, G.-Q. Xia, X.-D. Lin, X. Tang, Z.-J. Wang, and A. Hurtado, "Stable propagation of inhibited spiking dynamics in vertical-cavity surface-emitting lasers for neuromorphic photonic networks," *IEEE Access*, vol. 6, pp. 67951–67958, 2018.
[27] E. Jayaprasath, Y.-S. Hou, Z.-M. Wu, and G.-Q. Xia, "Anticipation in the polarization chaos synchronization of uni-directionally coupled vertical-cavity surface-emitting lasers with polarization-preserved optical injection," *IEEE Access*, vol. 6, pp. 58482–58490, 2018.
[28] M. Xu, W. Pan, S. Xiang, and L. Zhang, "Cluster synchronization in symmetric VCSELs networks with variable-polarization optical feedback," *Opt. Express*, vol. 26, no. 8, p. 10754, Apr. 2018.
[29] S. Xiang, B. Wang, Y. Wang, Y. Han, A. Wen, and Y. Hao, "2.24-Tb/s physical random bit generation with minimal post-processing based on chaotic semiconductor lasers network," *J. Lightw. Technol.*, vol. 37, no. 16, pp. 3987–3993, Aug. 15, 2019.
[30] M. Xu, W. Pan, and L. Zhang, "Isolated desynchronization and intertwined synchronization in networks of semiconductor lasers," *Opt. Eng.*, vol. 57, no. 04, p. 1, Apr. 2018.
[31] D. Kanakidis, A. Argyris, A. Bogris, and D. Syvridis, "Influence of the decoding process on the performance of chaos encrypted optical communication systems," *J. Lightw. Technol.*, vol. 24, no. 1, pp. 335–341, Jan. 2006.

SHIQIN LIU was born in Sichuan, China, in 1995. She received the B.S. degree in physics from Southwest University, Chongqing, China, in 2017. She is currently pursuing the Ph.D. degree in communication and information system with the University of Electronic Science and Technology of China, Chengdu, China. Her dissertation works focus on the chaos synchronization in semiconductor laser networks, and its applications in secure optical communication and secure key distribution.

NING JIANG (Member, IEEE) was born in Sichuan, China, in 1984. He received the B.S. degree in communication engineering from the University of Electronic Science and Technology of China, in 2005, and the Ph.D. degree in communication and information system from Southwest Jiaotong University, China, in 2012.

He is currently an Associate Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China. He has authored or coauthored more than 80 research articles. His current research works focus on the all-optical secure communication, and energy-efficient optical access networks.

Prof. Jiang is also a member of the Optical Society of America.



ANKE ZHAO was born in Sichuan, China, in 1992. He received the B.Eng. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2016, where he is currently pursuing the Ph.D. degree. His dissertation works focus on the nonlinear dynamics of semiconductor lasers, optical secure communication, and random bit generation.

YIQUN ZHANG was born in Henan, China, in 1997. He received the B.Eng. degree from Xidian University, Xi'an, China, and Heriot-Watt University, Edinburgh, U.K., in 2019. He is currently pursuing the Ph.D. degree with the University of Electronic Science and Technology of China, Chengdu, China. His dissertation works focus on the secure optical communication based on chaos physical encryption.

KUN QIU received the M.S. and Ph.D. degrees from Tsinghua University, Beijing, China, in 1987 and 1990, respectively.

In 1990, he joined the University of Electronic Science and Technology of China, where he was involved in the theories and technologies in optical fiber communications. From 1993 to 1994, he was a Visiting Scholar with the Institution of Optics, University of Rochester. From 2002 to 2006, he was the Director of the State Key Laboratory of the Broadband Optical Transmission and Communication Network. He has finished more than 20 important projects as a Research Team Leader. He has authored more than 200 scientific articles and the book of *Optical Fiber Communication*.

Prof. Qiu was the Chair of the Chengdu Chapter and the IEEE Photonics Society. He received eight awards of science and technology progress from provinces or ministries.