OPTICAL SECURE COMMUNICATION SYSTEM BASED ON CHAOS SYNCHRONIZATION

Alexander N. Pisarchik and Flavio R. Ruiz-Oliveras
Centro de Investigaciones en Optica, Loma del Bosque 115, Lomas del Campestre, Leon, Guanajuato, Mexico

Keywords: Synchronization, Chaos, Secure communication.

Abstract: We propose a secure optical communication system based on the principles of generalized and complete synchronization of chaotic oscillations. Both a transmitter and a receiver are composed by two chaotic external-cavity semiconductor lasers which are coupled in a master-slave configuration to provide generalized synchronization, while the master lasers in the transmitter and in the receiver are completely synchronized via an optical fiber. A message is added to the slave laser in the transmitter and sent to the receiver to be compared with the output of the receiver slave laser. The system is robust to a small mismatch of the laser parameters or of the coupling between the master and slave lasers, unavoidable in a real system, and can even enable a good communication up to a 5 Gb/s transmission rate using the chaos masking encryption, when the master lasers in the transmitter and in the receiver are coupled bidirectionally.

1 INTRODUCTION

Due to their high relaxation oscillation frequencies (10 GHz and beyond) and direct comparability with existing optical fiber communication technology, semiconductor lasers have attracted much attention from researchers working in optical communications (Shore et al., 2008), especially after successive experiments with the Athens' fiber networks (Argyris et al., 2005). In these lasers, high dimensional chaotic signals with a large information entropy are generated by means of delayed feedback (Mirasso et al., 1996; Ruiz-Oliveras and Pisarchik, 2006). The system performance largely depends on the quality of chaos synchronization, i.e. the synchronization error should be minimized. Depending on the particular application of chaotic optical communication, different encoding and decoding schemes, such as chaos masking, chaos shift keying, and chaos modulation were implemented (Tang et al., 2006). The majority of these schemes are based on complete synchronization (CS) and use only a single channel for both the laser coupling and the signal transmission. A drawback of such schemes is that CS asks for identical systems, very easy to obtain in theory but difficult in practice.

A secure communication system based on the concept of generalized synchronization (GS) (Afraimovich et al., 1986) and its combination with CS was originally suggested by Murali and Lakshmanan (Murali and Lakshmanan, 1998). Since they used a single communication channel, the signal itself created a synchronization error that reduced the communication quality. A different approach (Terry and VanWiggeren, 2001) consisted of two identical pairs of chaotic systems (master and slave); one pair in the transmitter and the other pair in the receiver. A binary message was encrypted in the coupling strength between master and slave in the transmitter and was recovered by analyzing the error dynamics in the receiver; in fact, this method was a modification of a chaos shift keying with an important innovation, it used two channels: one to provide CS between the transmitter and the receiver master systems, and the other channel to compare the two slave trajectories. However, in the chaos shift keying schemes a binary bit message inherently produces a synchronization error, hence limiting the communication rate with the synchronization time because the transmitter and the receiver are not continuously synchronized.

2 COMMUNICATION SCHEME AND LASER MODEL

We propose a new two-channel optical secure communication system shown in Figure 1, which utilizes two pairs of unidirectionally coupled external cavity

N. Pisarchik A. and R. Ruiz-Oliveras F. (2010).
OPTICAL SECURE COMMUNICATION SYSTEM BASED ON CHAOS SYNCHRONIZATION.
In *Proceedings of the International Conference on Data Communication Networking and Optical Communication Systems*, pages 149-153
DOI: 10.5220/0002912001490153

semiconductor lasers, one pair in the transmitter, and the other in the receiver; each consisting of a master laser (ML) and a slave laser (SL), not necessarily identical, but coupled enough to exhibit GS, while the master lasers in the transmitter and in the receiver should be identical (or near identical) and completely synchronized. This scheme is completely symmetric, the optical paths between the master and slave lasers in the transmitter and in the recorder are the same, this provides close similarity between their GS functions. Such a similarity cannot be obtained if only one master laser is coupled with two slave lasers, one in the transmitter and one in the receiver (Yamamoto et al., 2007; Annovazzi-Lodi et al., 2008), giving difficulties for long distance communication.

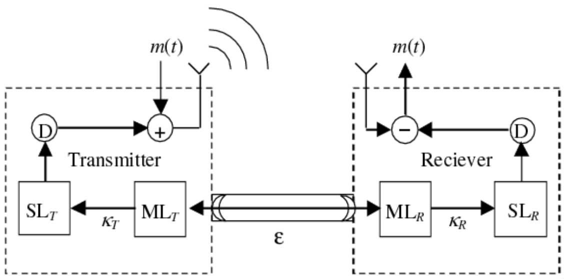

Figure 1: Two-channel optical chaotic communication using chaos masking encryption scheme. ML_T, SL_T and ML_R, SL_R are the master and slave lasers in the transmitter and in the receiver, respectively, κ_T and κ_R are the coupling strengths between the lasers in the transmitter and in the receiver, ε is the coupling strength between the master lasers, and D are the photodetectors.

The external cavity semiconductor lasers can be modeled by the following equations based on the well-known Lang-Kobayashi approach (Mirasso et al., 1996; Lang and Kobayashi, 1980):

$$\dot{E}_{M_{T,R}}(t) = \frac{1}{2}(1+i\alpha)\left[G_{ML_{T,R}}(t) - \frac{1}{\tau_p}\right]E_{M_{T,R}}(t) + \gamma_{M_{T,R}}E_{M_{T,R}}(t-\tau_{M_{T,R}})\exp(-i\varphi_{M_{T,R}}) + \varepsilon E_{M_{R,T}}(t) + \sqrt{2\beta N_{M_{T,R}}(t)}\xi_{M_{T,R}}(t), \quad (1)$$

$$\dot{E}_{S_{T,R}}(t) = \frac{1}{2}(1+i\alpha)\left[G_{S_{T,R}}(t) - \frac{1}{\tau_p}\right]E_{S_{T,R}}(t) + \gamma_{S_{T,R}}E_{S_{T,R}}(t-\tau_{S_{T,R}})\exp(-i\varphi_{S_{T,R}}) + \kappa_{T,R}E_{M_{T,R}}(t) + \sqrt{2\beta N_{S_{T,R}}(t)}\xi_{S_{T,R}}(t), \quad (2)$$

$$\dot{N}_{M,S}(t) = \frac{I}{q} - \frac{N_{M,S}(t)}{\tau_n} - G_{M,S}(t)\left|E_{M,S}(t)\right|^2, \quad (3)$$

$$G_{M,S}(t) = g\frac{N_{M,S}(t) - N_0}{1+\rho\left|E_{M,S}(t)\right|^2}, \quad (4)$$

where the subscripts M and S stand for ML and SL, T and R stand for transmitter and receiver, $E_{M,S}(t)$ is the slow varying electric complex field ($P_{M,S} = |E_{M,S}(t)|^2$ being the laser output power), $N_{M,S}(t)$ is the carrier density, $\alpha = 3$ is the linewidth enhancement factor, $\tau_p = 2$ ps and $\tau_n = 2$ ns are the photon and carrier lifetimes respectively, $\gamma_{M,S}$ is the feedback parameter ($\gamma_{M_{T,R}} = 25$ ns^{-1} and $\gamma_{S_{T,R}} = 20$ ns^{-1}), $\tau_{M,S}$ is the external cavity round-trip time ($\tau_{M_{T,R}} = 1$ ns and $\tau_{S_{T,R}} = 0.5$ ns), $\varphi_{M,S} = \omega\tau_{M,S}$ is the initial phase, $\omega = 1.2\times10^3$ ps^{-1}is the angular frequency for all lasers, $\beta = 1.1$ ps^{-1} is the spontaneous emission rate, $\xi_{M,S}(t)$ is Gaussian white noise of zero mean and unity intensity (Heil et al., 2001), $I = 29$ mA is the pump current, $q = 1.602\times10^{-19}$ C is the electronic charge, $g = 1.5\times10^{-8}$ ps^{-1} is the gain parameter, $N_0 = 1.5\times10^8$ is the carrier density at transparency, $\rho = 10^{-7}$ is the gain saturation coefficient, and $\chi = \eta_{ext}\sqrt{1-R}/(\tau_c\sqrt{R})$ is the coupling parameter ($\chi = \kappa_T, \kappa_R, \varepsilon$) (Mirasso, 2000) varied in the simulations ($R = 0.3$ being the facet laser power reflectivity and $\tau_c = 6.6$ ps being the internal cavity round-trip time, and η_{ext} accounts for losses different than those introduced by the laser facet). $\chi = 100$ ns^{-1} corresponds to the case when approximately 42.8% of the laser output power is injected into the other laser. For the case of unidirectional coupling, ε appears only in ML_R.

2.1 Chaos Synchronization and Information Transmission

To quantitatively measure synchronization, we calculate the normalized cross correlation C between the output powers of two coupled lasers (i and j)

$$C(t) = \frac{\left\langle P_i(t')P_j(t'-t) - \overline{P_i P_j}\right\rangle_{t'}}{\sigma_i\sigma_j}, \quad (5)$$

where $\langle\ldots\rangle$ stands for time average, $\overline{P_i}$, $\overline{P_j}$ and σ_i, σ_j are the mean and standard deviations of the laser powers, respectively. Since in this paper we only take into consideration isochronous synchronization, we only calculate $C(0)$. CS can be quantitatively characterized with the mean synchronization error

$$\langle e\rangle = P_i - P_j. \quad (6)$$

Figure 2 shows C and $\langle e\rangle$ when Eqs. (5) and (6) are used for our system; C_M, $\langle e_M\rangle$ are calculated for ML_R and ML_T [Fig. 2(a)], C_T, $\langle e_T\rangle$ for ML_T and SL_T, C_R, $\langle e_R\rangle$ for ML_R and SL_R [Fig. 2(b)], and C_S, $\langle e_S\rangle$ for SL_R and SL_T [Figure 2(c)], as functions of the coupling strengths for unidirectional and bidirectional coupling between ML_T and ML_R. The qualitative behavior is similar in both cases, however for bidirectional coupling a much smaller ε is required to obtain CS between the masters [Figure 2(a)] and between the slave [Figure 2(c)] lasers. Another advantage of bidirectional coupling, very important for security purposes, is that the transmitter has feedback information about the receiver's behavior, so that if someone tried to enter the synchronization channel in order to obtain part (or all) of the laser light, the feedback signal would be modified. If a hacker was able to connect with the synchronization channel, he would use a part of the laser power to synchronize his own laser, this would reduce the power entering to the authorized receiver and hence the power returning to the transmitter that could be easily identified.

Since ML and SL are not identical, we obtain GS characterized by a relatively small cross-correlation ($C \approx 0.8$) and a high mean error ($\langle e \rangle \approx 0.4$) for even very strong coupling ($\kappa = 100$ ns^{-1}) [Figure 2(b)]. These characteristics indicate a large difference between the laser dynamics preventing a non-authorized person, even when he has access to both channels, to read the message without knowing the function H. The same curves were obtained for both the transmitter and the receiver, since we supposed that their ML and SL were coupled with the same coupling strengths, i.e. $\kappa_T = \kappa_R$. From Figures 2(b) and 2(c), one can see that CS between the master and slave lasers is not needed to obtain CS between SL_T and SL_R, proved even a relatively small coupling strength ($\kappa \approx 50$ ns^{-1}) allows for an excellent correlation.

One way to quantitatively characterize the performance of a communication system is Q-factor, given by

$$Q = \frac{\langle P_1 \rangle - \langle P_0 \rangle}{\sigma_1 + \sigma_0}, \quad (7)$$

where $\langle P_1 \rangle$ and $\langle P_0 \rangle$ are the average optical powers of bits "1" and "0", respectively, while σ_1 and σ_0 are the corresponding standard deviations. We prove the benefits of our system with three encoding methods: (i) chaos modulation, where the message is encrypted by modulating the transmitter's chaotic carrier according to the expression $(1 + m(t))E_S \exp(i\phi_S)$ resembling the type of amplitude modulation (AM), (ii) chaos shift keying, where the message is added to the pump current of SL_T in Eq. (2), $I + m(t)$, inevitably producing an error in synchronization between the slave lasers, and (iii) chaos masking, where the message, completely independent of the electric field, is added to the chaotic carrier as $E_S \exp(i\phi_S) + m(t) \exp(i\phi_m)$ (ϕ_m being the message phase). In all these methods, the message amplitude is set to a 2% of the SL_T amplitude and the length of the encoded message is a 10^4 random bit sequence. The decoded message is filtered with a 5th order Butterworth low-pass filter and

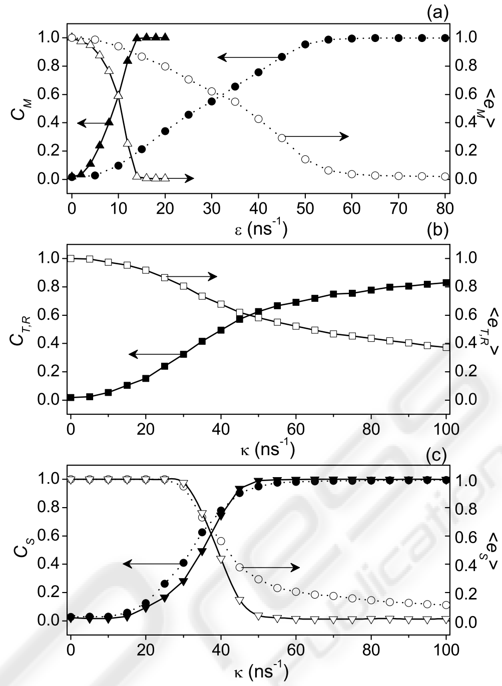

Figure 2: Cross-correlation (filled signs) and mean synchronization error (clean signs) between (a) ML_T and ML_R, (b) ML_T and SL_T, and (c) SL_T and SL_R, when ML_T and ML_R are coupled unidirectionally (dots) ($\varepsilon = 80$ ns^{-1}) and bidirectionally (triangles) ($\varepsilon = 16$ ns^{-1}) as functions of their coupling parameter. All cross-correlations are calculated in the absence of a message.

the eye diagrams from the extracted codes are constructed to evaluate the transmission quality.

For the chaos modulation method, a very low Q-factor is obtained and hence the information transmission is hardly possible. In Figure 3 we plot the values of the Q-factor as a function of the coupling parameter $\kappa = \kappa_T = \kappa_R$ for chaos shift keying [Figure 3(a)] and chaos masking [Figure 3(b)]. We use $\varepsilon = 80$ ns^{-1} for unidirectionally coupled and $\varepsilon = 16$ ns^{-1} for bidirectionally coupled ML_T and ML_R. Note, that 5 Gb/s good signal transmission is only possible for chaos masking in the case of bidirectional coupling.

Finally, we consider the case when the transmitter and the receiver systems are not exactly identical, i.e. either $\kappa_T \neq \kappa_R$ or laser parameters exhibit a small mismatch. Therefore, SL_R and SL_T are partially synchronized by a certain function. Now, GS between ML and SL in the transmitter and in the receiver is characterized by two different functional dependences, that causes a small difference between C_T and C_R, $\delta C = C_T - C_R$, and we are interested in how the mismatch δC affects communication quality. Keeping all laser parameters identical and $\kappa_T = 80$ ns^{-1} for which $C_T = 0.7781$ [Figure 2(b)], we vary κ_R (60 ns^{-1} $\leq \kappa_R \leq 100$ ns^{-1}) giving as a result the variation

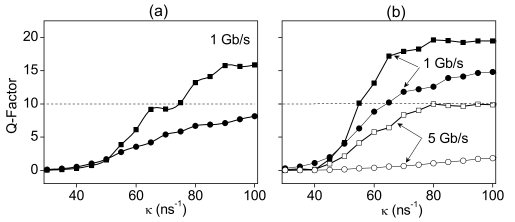

Figure 3: Q-factor as a function of coupling parameter between ML and SL for (a) chaos shift keying and (b) chaos masking for 1 Gb/s (filled signs) and 5 Gb/s (open signs) signal transmission when master lasers are coupled unidirectionally (dots) and bidirectionally (squares) for (a) chaos shift keying and (b) chaos masking. The communication quality is good above the dashed line. For chaos shift keying the 5 Gb/s transmission is not possible.

of C_R ($-0.04 \leq C_R \leq 0.04$). Figures 4(a-c) show $\langle e_S \rangle$ (in %) and Q as functions of δC for 1 Gb/s and 5 Gb/s transmission; Fig. 4(a) was obtained with chaos shift keying and Figs. 4(b) with chaos masking for bidirectionally coupled master lasers with $\varepsilon = 16$ ns^{-1}. The loss of synchronization between slaves due to the chaos shift keying results in the displacement of the maximum C and minimum $\langle e_S \rangle$ from $\delta C = 0$ in Figure 4(a). With the same ε Figure 4(c) represents the results for chaos masking for unidirectional coupling, clearly not as efficient as bidirectional coupling. The communication quality for chaos shift keying with unidirectional coupling is not sufficient ($Q < 10$) [Figure 3(a)]. Although chaos masking allows a 1 Gb/s communication with unidirectional coupling, the error is relatively high ($\langle e_S \rangle > 15\%$) [Figure 4(c)].

We now also consider what happens when the master lasers are not completely identical, keeping $\kappa_R = \kappa_T$. In this case, the most critical parameter for synchronization is the injection current. Figures 4(d-f) show how a small mismatch $\delta I = I_T - I_R$ (I_T and I_R being the injection currents of the master lasers in the transmitter and in the receiver) affects $\langle e_M \rangle$ and Q. One can see that when the master lasers are coupled bidirectionally, the system is more robust to a parameter mismatch, i.e. the 1 Gb/s transmission can be realized in a much larger region of δC or δI, and even a 5 Gb/s rate can be obtained but only for chaotic masking and only when the slave lasers and the master lasers are completely synchronized, i.e. when the identity conditions, $\delta C \approx 0$ and $\delta I \approx 0$, are fulfilled. Figure 4(d) shows that chaos key shifting even for 1 Gb/s is not as efficient as chaos masking.

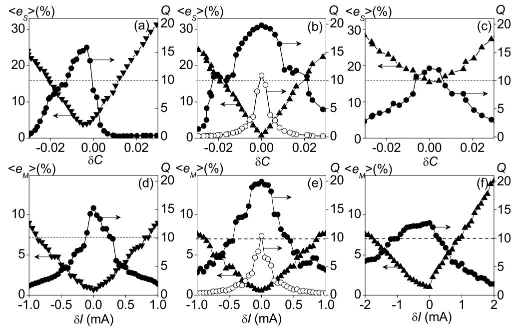

Figure 4: Mean synchronization error (triangles) and Q-factor (dots) as functions of mismatch of (a-c) correlations δC and (e-f) injection currents δI of master lasers for chaos shift keying (left-hand column) and chaos masking (middle and right-hand columns) when the master lasers are coupled either bidirectionally (left-hand and middle columns) or unidirectionally (right-hand column). 1 Gb/s and 5 Gb/s transmission are shown by the closed and open dots, respectively. $\kappa_T = 80$ ns^{-1}, $\varepsilon = 16$ ns^{-1} for bidirectionally and $\varepsilon = 80$ ns^{-1} for unidirectionally coupling, and $I_T = 29$ mA. The communication quality is good above the dashed lines.

3 CONCLUSIONS

We have introduced an efficient optical chaotic communication system which uses the combination of complete and generalized synchronizations. The system contains two channels, one for synchronization and the other for information transmission, and consists of two pairs of external cavity semiconductor lasers each coupled in GS configuration, while the master lasers in the transmitter and in the receiver are completely synchronized. The ability of this system for high-quality communication is demonstrated through numerical simulations with the Lang-Kobayashi model. We have shown that bidirectional coupling between the master lasers provides much better communication quality (up to 5 Gb/s) than unidirectional coupling and makes the system more robust to a mismatch between the ML parameters or the coupling strengths between ML and SL. In the case of bidirectional coupling, the two coupled lasers influence to each other so that the identity requirements for complete synchronization are not as strong as in the case of unidirectional coupling that allows more tolerances. The efficiency of this system is very clear when the encryption method is chaos masking, it can also be used for other methods although the results are not so spectacular.

ACKNOWLEDGEMENTS

This work was supported by Consejo Nacional de Ciencia y Tecnologa of Mexico (project No. 100429).

REFERENCES

Afraimovich, V. S., Verichev, N. N., and Rabinovich, M. I. (1986). Stochastic synchronization of oscillation in dissipative systems. *Quant. Electron.*, 29:795–803.

Annovazzi-Lodi, V., Aromataris, G., Benedetti, M., and Merlo, S. (2008). Secure chaotic transmission on a free-space optics data link. *IEEE J. Quantum Electron.*, 44:1089–1095.

Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., García-Ojalvo, J., Mirasso, C. R., Pesquera, L., and Shore, K. A. (2005). Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature*, 438:343–346.

Heil, T., Fischer, I., Elsässer, W., Mulet, J., and Mirasso, C. R. (2001). Chaos synchronization and spontaneous symmetry-breaking in symmetrically delay-coupled semiconductor lasers. *Phys. Rev. Lett.*, 86:795–798.

Lang, R. and Kobayashi, K. (1980). External optical feedback effects on semiconductor injection laser properties. *IEEE J. Quantum Electron.*, 16:347–355.

Mirasso, C. R. (2000). Applications of semiconductor lasers to secure communications. In *Nonlinear Laser Dynamics: Concepts, Mathematics, Physics, and Applications International Spring School, AIP, Conference Proceedings*, pages 112–127, Washington, DC.

Mirasso, C. R., Colet, P., and Garcia Fernandez, P. (1996). Synchronization of chaotic semiconductor lasers: Application to encoded communications. *IEEE Photon. Tech. Lett.*, 8:299–301.

Murali, K. and Lakshmanan, M. (1998). Secure communication using a compound signal from generalized synchronizable chaotic systems. *Phys. Lett. A*, 241:303–310.

Ruiz-Oliveras, F. R. and Pisarchik, A. N. (2006). Phase-locking phenomenon in a semiconductor laser with external cavities. *Opt. Express*, 14:12859–12867.

Shore, K. A., Spencer, S. P., and Pierce, I. (2008). *Recent Advances in Laser Dynamics: Control and Synchronization*, chapter Synchronization of chaotic semiconductor lasers, pages 79–104. Research Singpost, Kerala.

Tang, S., Chen, H.-F., and Liu, J.-M. (2006). *Digital Communications Using Chaos and Nonlinear Dynamics*, chapter Performance of synchronized chaotic optical communication systems, pages 341–378. Institute for Nonlinear Science. Springer, New York.

Terry, J. R. and VanWiggeren, G. D. (2001). Chaotic communication using generalized synchronization. *Chaos, Solitons and Fractals*, 12:145–152.

Yamamoto, T., Oowada, I., Yip, H., Uchida, A., Yoshimori, S., Yoshimura, K., Muramatsu, J., Goto, S., and Davis, P. (2007). Common-chaotic-signal induced synchronization in semiconductor lasers. *Opt. Express*, 15:3974–3980.