Security implications of open and closed loop receivers in all-optical chaos-based communications

Miguel C. Soriano, Pere Colet, Claudio R. Mirasso

Abstract—**We numerically find that higher privacy and security in all-optical chaos-based communication systems can be achieved when the closed loop scheme is used in the receiver architecture, instead of the more traditional open loop scheme. Our results show that the extraction of the encoded message demands a larger amplitude of the message when the open loop receiver is used than when the closed loop is implemented. A large amplitude of the encoded message compromises the performance and security of the system.**

Index Terms—**Optical feedback, semiconductor lasers, synchronization, dynamics, chaos.**

I. Introduction

CHAOS-BASED communications have emerged as an alternative technique to improve privacy and security in communication services, especially after the field demonstration in the optical link of the metropolitan area of Athens, Greece [1]. One of the main questions that remains open is how much security can the technique offer?

While in all-optical chaos-based systems the emitter architecture usually includes a semiconductor laser subject to optical feedback from an external or integrated mirror, the receiver system can operate subject to the same feedback architecture (closed loop scheme) or without the optical feedback (open loop scheme) [2], [3]. The main advantages and disadvantages of these schemes can be summarized as follow. Since in the open loop the receiver is not subject to feedback, this configuration is mechanically more stable and easier to implement. The open loop receiver is also very robust against frequency detuning and small parameters mismatch [4], [5], and has a shorter resynchronization time in case the connection is suddenly interrupted [6], [7]. On the contrary, the closed loop is less stable. Therefore, the external or integrated feedback cavities of the emitter and receiver have to be matched within sub wavelength precision, otherwise the synchronization quality is very poor [8]. The closed loop is less robust than the open loop and has a longer resynchronization time [7]. For all these reasons, a receiver with an open loop scheme has been massively used for demonstration purposes [9], [10]. However, there is one point related to the security of the encoding that has not been considered in detail so far [5]. In general, the degree of synchronization in the open loop is worse than that in the closed loop [11], [12], specially when the open loop is working in the strong injection regime [13]. Only if the complete synchronization condition is achieved [7], [11], [12], the correlation of an open loop receiver with an emitter can be larger than that of a closed loop receiver, and can actually amount to almost 1 under certain conditions [15]. Due to the extreme experimental difficulties to attain complete synchronization [14], we assume that the open loop can only work in the strong injection regime. In this regime, the correlation between an emitter and an open loop receiver is not good enough and, although chaos pass filtering properties have been experimentally demonstrated with this scheme [16], [17], messages with large amplitude have to be used. At this point is where the security is compromised. The use of large amplitude modulations makes the message less encrypted and, in many cases, a simple linear filtering process can recover most of the information. Consequently, its performance is strongly limited when a secure transmission is intended.

Security aspects are often associated, by many researchers, directly to the receiver architecture although the security is related only indirectly with the receiver characteristics. Security is related to the difficulty of extracting the message from the chaotic carrier without using the authorized receiver. Two kinds of attacks can be considered. A software attack requires direct information from the signal that is transmitted. If the signal is extracted with enough sampling precision (usually picoseconds precision is required, hardly difficult to be obtained experimentally) time series analysis could be performed and, in some cases, the message could be partially extracted [18]. The second attack is a hardware one. The idea in this case is to use a receiver similar to the authorized one without knowing the specifications of the latter. This is a very difficult task since laser parameters and operating conditions of the emitter are key parameters for the system design and should be kept private. For this second attack, an open loop receiver would be the first and easiest choice. However, as we will show later, the encrypted information cannot be retrieved if the amplitude of the encoded message is small enough.

It is our aim in this letter to show that privacy and security in all-optical chaos-based communication systems can only be achieved when small amplitude messages are used, which can be only recovered with a closed loop receiver.

II. Results and Discussion

We have performed numerical simulations using the standard rate equations model for two emitter and receiver lasers unidirectionally coupled. The equations for the slowly varying

The authors acknowledge financial support from MEC (Spain) and Feder under Projects No. TEC2006-1009/MIC (PhoDECC), No. TEC-2006-28105-E and No. FIS2007-60327 (FISICOS); from EC Project PICASSO Grant No. IST-2005-34551. MCS thanks the MEC for a "Juan de la Cierva" contract.

The authors are with the IFISC (CSIC-UIB) Instituto de Física Interdisicplinar y Sistemas Complejos, Campus Universitat Illes Balears, E-07122 Palma de Mallorca, Spain.

amplitude of the electric field $E(t)$ and the carrier number $N(t)$, assuming single mode operation and low to moderate feedback strengths, read:

$$\begin{aligned}\dot{E}_{M,S}(t) &= \frac{1+i\alpha}{2}\left[G_{M,S}(t)-\frac{1}{\tau_p}\right]E_{M,S}(t) \\ &+ \gamma_{M,S}E_{M,S}(t-\tau)e^{-i\Phi} + \kappa_r\, E_M(t) \quad (1)\\ \dot{N}(t) &= \frac{I}{e}-\frac{N(t)}{\tau_N}-G(t)P(t), \quad (2)\end{aligned}$$

where M (S) refers to the master (slave) laser. The gain $G_{M,S} = g(N_{M,S}-N_o)/(1+sP^2_{M,S}(t))$. $P(t) = |E(t)|^2$ is the laser intensity. For simplicity, we have assumed identical internal laser parameters and operating conditions and neglected noise effects in the lasers. $\alpha = 5$ is the linewidth enhancement factor, $\tau_p = 2$ ps is the is the photon lifetime, $\tau_N = 2$ ns is the carrier lifetime, $g = 1.5\cdot 10^{-8}$ ps^{-1} is the differential gain coefficient, $N_o = 1.5\cdot 10^8$ is the carrier numbers at transparency, $s = 5\cdot 10^{-7}$ is the gain compression coefficient, $I_{th} = 14.7$ mA is the threshold current, $\tau = 1$ ns is the feedback delay time and γ is the feedback strength. The term $\kappa_r E_M(t)$ only appears in the equation for the slave laser (SL) and it accounts for the injection of the master laser (ML) field into the SL. Without loss of generality we consider instantaneous injection from ML to SL and neglect the optical phase in the coupling term since it can be rescaled into $E_S(t)$.

The scheme we have chosen to encode the information is the chaos modulation (CM) scheme, since it is known to be more secure than other encryption methods from the perspective of information theory [19]. Similar results would be obtained if other encoding formats such as chaos shift keying or chaos masking were used, as will be briefly shown later. In the CM scheme the message is encoded by modulating the transmitter's chaotic intensity according to: $P_T(t) = \big(1-\epsilon\, m(t)\big)P_M(t)$, where $P_T(t)$ ($P_M(t)$) is the intensity of the transmitted signal including the message (carrier only), ϵ is the amplitude of the modulation and $m(t)$ is the message being transmitted equal to 0.5 (-0.5) for a "1" ("0") bit. The message can be recovered at the receiver side as $m'(t) = (1-P_M(t)/P_S(t))\,/\epsilon$. The extraction of the message is possible if the SL reproduces mainly the chaotic carrier. For $P_S(t) = P_M(t)$ (ideal synchronization) the message is perfectly recovered. For $P_S(t) = P_T(t)$ (perfect locking) the message cannot be recovered.

To quantify the degree of correlation between two signals the cross-correlation function is typically used. However, we prefer to use the average mutual information (MI) since it is more powerful and gives more useful information. MI is a non-linear measure of the similarities between two quantities x, y and is defined as [20] $J_{xy} = \sum_{i,j} p_{ij}\log_2[p_{ij}/(p_i p_j)]$, where p_{ij} is the joint probability of $x = x_i$ and $y = y_j$, p_i (p_j) is the probability of $x = x_i$ ($y = y_j$). This quantity essentially measures the extra information one gets from a signal when the outcome of the other signal is known. For two independent signals $p_{ij} = p_i p_j$, and J_{xy} is zero. Otherwise, J_{xy} will be positive, taking its maximum value for identical signals. Here we compute the MI between the optical intensity of the ML ($P_M(t)$) and SL ($P_S(t)$), denoted as J_{ms} and the MI between the transmitted signal, $P_T(t)$, and the slave signal $P_S(t)$ (J_{ts}). Both quantities, J_{ms} and J_{ts}, are evaluated when a message of 1Gbit/s is codified in the output of the ML. In the synchronization regime $J_{ms} > J_{ts}$ and the receiver is able to filter out the message.

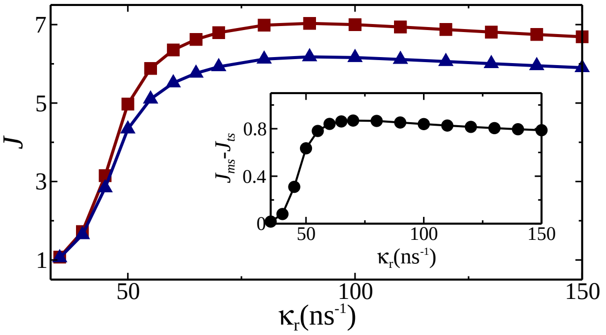

Fig. 1. Color online. Average mutual information between the ML and SL in the closed loop scheme vs. coupling strength (▲ for J_{ts} and ■ for J_{ms}). The inset shows the difference between both MI values. Parameters: $\gamma_M = \gamma_S = 25$ ns^{-1}, $I = 2I_{th}$, $\epsilon = 0.05$.

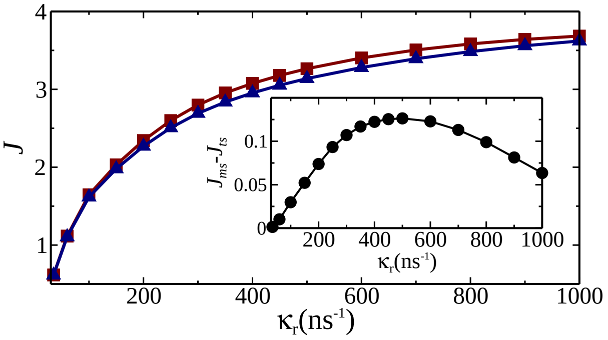

Fig. 2. Color online. Same as Figure 1 but for the open loop ($\gamma_S = 0$).

In Figures 1 and 2 we show the results of the MI computed for the closed loop and open loop, respectively. It can be seen that the discrimination between the master output and the transmitted signal, i.e., $J_{ms} - J_{ts}$ (shown in the insets of the figures), is larger for the closed loop scheme than for the open one. Moreover, only for coupling strengths larger than 100 ns^{-1} the open loop starts to discriminate the two signals [note the different scale of the x and y axis in Figs. 1 and 2]. However, as will be shown below, this discrimination will not be enough for an acceptable performance.

To better quantify the performance of the system we compute the Q-factor defined as $Q = (S_1 - S_0)/(\sigma_1 + \sigma_0)$, where S_1 and S_0 are the average optical power of bits "1" and "0", and σ_1 and σ_0 are the corresponding standard deviations.

In Figure 3 we plot the Q-factor for open (solid line with squares) and closed (solid line with triangles) loop receivers. The results clearly indicate that the closed loop performs much better, reaching much higher Q-factors (larger than 9) even for message amplitudes as small as 2.5%. On the contrary, the open loop can only attain Q-factors of $\sim$5 for message amplitudes of the order of 7.5% that, as will be shown below, are too large to encrypt information. For the sake of completeness, we also show in Fig. 3 the performance of the receivers

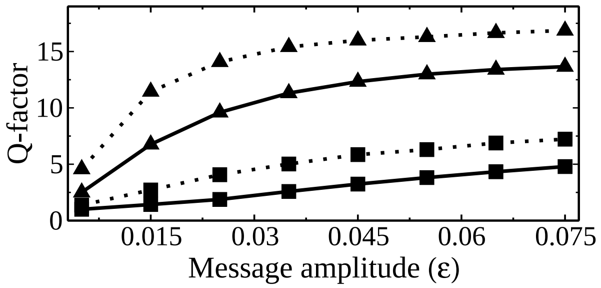

Fig. 3. Q-factor for the open (■) and closed (▲) loop schemes vs. the amplitude of the encrypted message. Solid lines correspond to the CM technique and dashed lines to the CSK method. Parameters: $I = 2I_{th}, \gamma_M = 25$ ns^{-1}; closed loop (open loop) $\gamma_S = 25$ (0) ns^{-1}, $\kappa_r = 80$ (500) ns^{-1}.

for the chaos shift keying (CSK) encryption method. In this encoding scheme the message modulates the injected current of the ML according to the expression $I_T(t) = \big(1 + \epsilon m(t)\big)I$, where $m(t)$ is equal to 0.5 (-0.5) for a “1” (“0”) bit. As in the case of CM, the closed loop receiver (dashed line with triangles) performs much better than the open loop one (dashed line with squares).

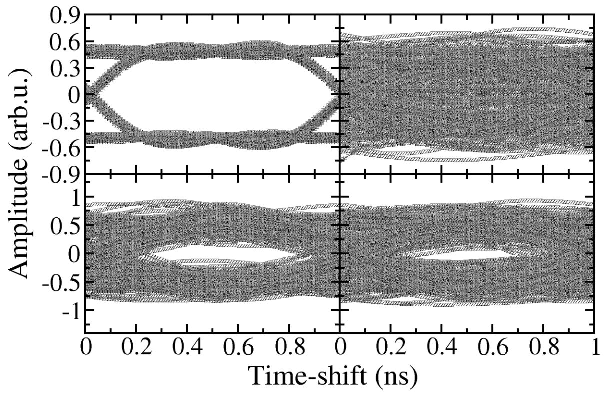

Fig. 4. Left panels: Eye diagram for the closed (top, $\kappa_r = 80$ ns^{-1}) and open (bottom, $\kappa_r = 500$ ns^{-1}) loop receivers for an encoded message amplitude of $\epsilon = 0.05$. Right panels: Eye diagram of $P_T(t)$ filtered by a 5th order butterworth filter and a cut-off frequency of 0.8 GHz for a message of (top) $\epsilon = 0.05$ and (bottom) $\epsilon = 0.075$.

Finally, we show in Figure 4 eye diagrams of the recovered messages using CM with 5% amplitude for the closed loop (left upper panel) and the open loop (left bottom panel) obtained with the authorized receivers. While the closed loop authorized receiver perfectly recovers the message, the quality of the message recovered by the open loop receiver is very poor. On the right side we show the eye diagrams after a simple linear filtering process performed on $P_T(t)$ with (top) a 5% message amplitude and (bottom) a 7.5% amplitude. While for the 5% amplitude the linear filtering is unable to detect the information, the encoded message can be detected for the 7.5% amplitude, highlighting that the information is not sufficiently hidden into the chaotic carrier.

III. Conclusion

We have numerically shown that the best and most efficient way to transmit and recover small amplitude messages, which would guarantee a certain degree of security in all-optical chaos-based communication systems, is to operate with the closed loop scheme in the receiver. On the contrary, the open loop scheme requires large amplitude messages that compromise the security. In practice, the success of chaos-based communications with a closed loop receiver requires the use of stable external or integrated cavities, similar to those that are currently being successfully developed [21].

References

[1] A. Argyris et al., “Chaos-based communications at high bit rates using commercial fiber-optic links”, Nature vol. 438, pp. 343-346, Nov. 2005.

[2] M. W. Lee, J. Paul, S. Sivaprakasam, and K. A. Shore, “Comparison of closed-loop and open-loop feedback schemes of message decoding using chaotic laser diodes”, Opt. Lett. 28, pp. 2168-2170, Nov. 2003.

[3] A. Uchida, F . Rogister, J García-Ojalvo and R. Roy, “Synchronization and communication with chaotic laser systems”, Progress in Optics vol. 48, pp. 203-341, Oct. 2005.

[4] A. Sánchez-Díaz, C. R. Mirasso, P. Colet and P. García-Fernández, “Encoded Gbit/s Digital Communications with Synchronized Chaotic Semiconductor Lasers”, IEEE J. Quantum Electron. vol. 35, pp. 292-297, Mar. 1999.

[5] X. Li, W. Pan, B. Luo, and D. Ma, “Mismatch Robustness and Security of Chaotic Optical Communications Based on Injection-Locking Chaos Synchronization”, IEEE J. of Quantum Electron. vol. 42, pp. 953-960, Sep. 2006.

[6] A. Uchida, N. Shibasaki, S. Nogawa, and S. Yoshimori, “Transient characteristics of chaos synchronization in a semiconductor laser subject to optical feedback”, Phys. Rev. E 69(5), pp. 056201, May 2004.

[7] R. Vicente, T. Pérez, and C. R. Mirasso, “Open vs Closed Loop Performance of Synchronized Chaotic External-Cavity Semiconductor Lasers”, IEEE J. Quantum Electron. vol. 38, pp. 1197-1204, Sep. 2002.

[8] M. Peil, T. Heil, I. Fischer, and W. Elsäßer, “Synchronization of chaotic semiconductor laser systems: A vectorial coupling-dependent scenario”, Phys. Rev. Lett., vol. 88, pp. 174101(1)-(4), Apr. 2002.

[9] A. Argyris, D. Kanakidis, A. Bogris, and D. Syvridis, “Experimental evaluation of an open-loop all-optical chaotic communication system”, IEEE J. Select. Top. in Quantum Electron., vol. 10, pp. 927-935, 2004.

[10] H. F. Chen and J. M. Liu, “Open-loop chaotic synchronization of injection-locked semiconductor lasers with gigahertz range modulation”, IEEE J. Quantum Electron., vol. 36, pp. 27-34, Jan. 2000.

[11] A. Murakami and J. Ohtsubo, “Synchronization of feedback-induced chaos in semiconductor lasers by optical injection” Phys. Rev. A, vol. 65, pp. 033826(1)-(7), Feb. 2002.

[12] A. Locquet, C. Masoller, and C. R. Mirasso, “Synchronization regimes of optical-feedback-induced chaos in unidirectionally coupled semiconductor lasers”, Phys. Rev. E vol. 65, pp. 056205(1)-(12), Apr. 2002.

[13] A. Argyris and D.Syvridis, “Performance of open-loop all-optical chaotic communication systems under strong injection condition” J. Lightwave Tech. vol. 22, pp. 1272-1279, May 2004.

[14] Y. Liu et al., “Experimental observation of complete chaos synchronization in semiconductor lasers”, Appl. Phys. Lett., vol. 80, pp. 4306-4308, Jun. 2002.

[15] J. Revuelta, C. R. Mirasso, P. Colet, and L. Pesquera, “Criteria for Chaos Synchronization of Coupled Chaotic External-Cavity Semiconductor Lasers” IEEE Phot. Tech. Lett. vol. 14, pp. 140-142, Feb. 2002.

[16] I. Fischer, Y. Liu, and P. Davis, “Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication”, Phys. Rev. A, vol. 62, pp. 011801(1)-(4), Jun. 2000.

[17] M. Peil, I. Fischer, and W. Elsäßer, “A short external cavity semiconductor laser cryptosystem”, C. R. Physique vol. 5(6), pp. 633-642, 2004.

[18] K.M. Short and A.T. Parker, “Unmasking a hyperchaotic communication scheme”, Phys. Rev. E vol. 58, pp. 1159-1162, Jul. 1998.

[19] O. A. Rosso, R. Vicente, and C. R. Mirasso, “Encryption test of pseudo-aleatory messages embedded on chaotic laser signals: An information theory approach”, Phys. Lett. A vol. 372, pp. 1018-1023, 2008.

[20] M. Paluš, “Testing for nonlinearity using redundancies: quantitative and qualitative aspects”, Physica D vol. 80, pp. 186-205, Jan. 1995.

[21] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, “Photonic integrated device for chaos applications in communications”, Phys. Rev. Lett. vol. 100, pp. 194101(1)-(4), May 2008.