Communicating with hyperchaos: The dynamics of a DNLF emitter and recovery of transmitted information

V.S Udaltsov, Jp Goedgebuer, L. Larger, J.B Cuenot, P. Levy, W.T. Rhodes

► To cite this version:

V.S Udaltsov, Jp Goedgebuer, L. Larger, J.B Cuenot, P. Levy, et al.. Communicating with hyperchaos: The dynamics of a DNLF emitter and recovery of transmitted information. Optics and Spectroscopy, 2003, 95 (1), pp.114-118. 10.1134/1.1595224 . hal-00094990

HAL Id: hal-00094990

<https://hal.science/hal-00094990>

Submitted on 22 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Communicating with Hyperchaos: The Dynamics of a DNLF Emitter and Recovery of Transmitted Information¹

V. S. Udaltsov*, J. P. Goedgebuer**, L. Larger**, J. B. Cuenot*, P. Levy*, and W. T. Rhodes*

* Centre GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, Metz, 57070 France

** Laboratoire d'Optique PM Duffieux, UMR 6603, Université de Franche-Comté, Besançon CEDEX, 25030 France
e-mail: vladimir.oudaltsov@georgiatech-metz.fr

Abstract—It is reported that signal encoding with high-dimensional chaos produced by delayed feedback systems with strong nonlinearity can be broken. The procedure is described and the method is illustrated with chaotic waveforms obtained from a strongly nonlinear optical system used by the authors previously to demonstrate signal encryption and decryption with wavelength chaos. The method can be extended to any systems ruled by nonlinear time-delayed differential equations.

Many attempts to break the keys of chaos-based cryptosystems have been reported since it was found that chaotic waveforms can be used as carriers of information in secure communications [1]. Some key-breaking methods are based on phase space reconstruction of the emitter dynamics through return map analysis or the use of nonlinear dynamical forecasting (NLDF) [2, 3]. These methods have been applied mostly for breaking communication schemes generating low-dimensional chaotic signals, for example, schemes ruled by the Lorenz and Rössler equations [2, 4]. It was originally thought that chaotic waveforms with a high dimensionality (hyperchaos) could make it more difficult to retrieve the message [5], but Short and Parker later showed that increasing the dimension does not lead to a significant improvement in the security of the system [4].

We consider here one specific class of chaotic systems: delayed nonlinear feedback (DNLF) systems, i.e., systems ruled by nonlinear time-delay differential equations (DDEs) whose dynamics can exhibit high-dimensional attractors with many positive Lyapunov exponents. Over the last few years, researchers have focused on the use of synchronization of such chaotic laser systems to achieve a secure communication channel. In these systems, identical chaotic laser transmitter and receiver setups are synchronized by sending a chaotic signal from the transmitter to the receiver. These systems may represent a significant breakthrough for chaotic communication schemes, since they can provide for signal encryption rates that are greater than 1 Gbit/s. One such laser system that uses a wavelength-tunable laser diode with nonlinear feedback and an appropriately tuned open-loop receiver was reported in

[6]. This experiment was novel in two important aspects: the dynamics appeared to be high-dimensional (~500), and the feedback function was set to be highly nonlinear (with up to five extrema) in the hope of enhancing the privacy of the transmission. The same features were also used in another system (reported by us later) in the radio-frequency domain [7, 8] to enhance the security level. However, the security of these systems is still open for discussion, although chaotic communications based on simpler encryption schemes have been shown to be susceptible to cracking mainly in two cases, as follows: (i) it was shown that information transmitted by a DNLF system with a weak nonlinearity introduced by an erbium optical amplifier in the feedback loop [9] could be successfully unmasked by considering the chaotic waveform as a convolution of the original laser pulses with an “echo” function associated with the delayed feedback loop [10]; (ii) a second type of attacks was proposed for the system with only one extremum Mackey–Glass nonlinear function [11] from time-series analysis [12, 13]. In this paper, we report on our investigation of the security features of systems of this type that exhibit a strong nonlinearity and, thus, a more complex encryption scheme. In order to evaluate the security of a system, we used experimental data sets obtained from the setup reported in [6].

A delay feedback system representative of the systems of concern and used in the experiments reported in [6] is shown in Fig. 1. The transmitter consists of a source (a wavelength-tunable laser diode with a center wavelength $\Lambda_0 = 1550$ nm), a nonlinear element (a birefringent plate with an optical pass difference $D = 11$ mm between its ordinary and extraordinary beams), a detector with a time response $\tau = 8.6$ μ s (shown as a

¹ This article was submitted by the authors in English.

low-pass filter in Fig. 1), and a feedback loop with a delay time $T = 510 \mu\text{s}$.

The message signal $m(t)$ is added to the feedback signal in the transmitter to produce a chaotic transmitted signal, which takes the form of chaos in wavelength. The wavelength fluctuations $\lambda(t)$ around Λ_0 in the transmitted beam can be expressed in the general form [14]

$$x(t) + \tau dx(t)/dt = \beta F[x(t-T)] + f(t) \quad (1)$$

with the output signal $x(t) = K\lambda(t)$ and where β is the bifurcation parameter; $F(x) = \sin^2[x(t) - \Phi]$ is the feedback nonlinear function with multiple extrema; and $f(t) = \gamma[m(t) + \tau dm(t)/dt]$, with $K = \pi D/\Lambda_0^2$, $\Phi = \pi D/\Lambda_0$, and $\gamma = 10^{-2}$ being parameters related to the transmitter. The receiver consists of elements identical to those in the transmitter. The laser diode at the receiver emits light with chaotic fluctuations $\lambda'(t)$ of its wavelength, ruled by

$$y(t) + \tau_R dy(t)/dt = \beta_R F_R[x(t-T_R)] \quad (2)$$

with $y(t) = K\lambda'(t)$. For the authorized receiver, the proper delay time $T_R = T$, response time $\tau_R = \tau$, bifurcation parameter $\beta_R = \beta$, and nonlinear function $F_R = F$ allow recovery of the message by subtracting $y(t)$ from $x(t)$, yielding a difference signal

$$\Delta(t) = x(t) - y(t) = m(t). \quad (3)$$

This is the algorithm we adopted in our experiments [6, 8]. In contrast, for an unauthorized receiver, the difference signal $\Delta(t)$ is a chaotic error signal, which can be expressed as

$$\Delta(t) = \beta F[x(t-T)] - \beta_R F_R[x(t-T_R)] + \tau_R dy/dt - \tau dx/dt + f(t), \quad (4)$$

and direct access to $m(t)$ is clearly impossible without knowing τ , T , and the nonlinear function $\beta F[\cdot]$.

Let us now consider an intruder taping the transmission line. The wavelength fluctuations detected in the transmitted light beam are expressed by Eq. (1). Although message security has not been a primary concern, estimates of the dimensionality of the wavelength dynamics have been made, suggesting a Lyapunov dimension of 500. As mentioned earlier, it is expected that this will allow us to method avoid attacks based on NDLF. Further, the encryption scheme described by Eq. (1) is thought to produce secure encryption compared with methods where the message is directly added to the chaotic carrier [15], because the message and the chaotic signal couple with each other through a more sophisticated process and a strongly nonlinear function. Assuming, however, that the eavesdropper knows that our encryption algorithm relies on a DDE, then only τ , T , and the nonlinear function $\beta F[\cdot]$, at most, are required to recover the message from the transmitted signal (note that changing the nonlinear function

Fig. 1. Block diagram of the DNLF communication system.

$F[\cdot]$ used in [6] can be easily done by using an electro-optic crystal instead of a birefringent plate).

To test the breaking method that will be explained hereinafter, we used a message $m(t)$ formed by the sum of two sine signals with frequencies of 8 and 12 kHz (Fig. 2a). The amplitude of this composite message signal was equal to approximately 0.5% of the amplitude of the chaotic signal in the feedback loop. The output transmitter signal thus obtained and that we used in our simulations is shown in Fig. 2b, was approximately 1 ms in duration, and was sampled at 86-ns intervals to yield $N = 12000$ points.

We start with the assumption that the parameters τ and T can be recovered relatively easily. The value of the time response τ can be estimated by analyzing the spectrum of the tapped signal $x(t)$ and measuring its bandwidth (for example, using the least squares method), which is inversely proportional to τ . The extremes of results obtained in our experiments have shown that the mismatch of τ in the transmitter and the receiver can reach a value of 4–5% without incurring dramatic problems in recovery of the message signal in the receiver, so the value of τ can be known with an accuracy of the order of a few percent. The value of the time delay T can be also obtained. A few methods can be applied here: (i) the analysis of the autocorrelation function (ACF); (ii) the average mutual information (AMI) technique [16]; (iii) the 3D reconstruction of the derivative of $x(t)$ [13]; and (iv) the reconstruction of the return map of $x(t)$ [17]. An example of calculation of the ACF $x(t)$ is shown in Fig. 2c. A narrow peak can be obtained if the sampling step is small enough; the loca-

Fig. 2. Examples of signals: (a) the message signal $m(t)$, (b) the transmitted signal $\lambda(t)$, (c) the ACF of transmitted signal, and (d) the AMI of transmitted signal.

Fig. 3. Examples of return maps and the nonlinear function F : (a, c) return maps and (b, d) nonlinear functions F for (a, b) the system from [6] and (c, d) the system from [7].

tion of the peak gives the value of the time delay T , with an accuracy that increases as the sampling step decreases. The peak corresponding to the time delay T can also be found by observing the AMI of $x(t)$ (Fig. 2d). The value of T can be obtained with an accuracy higher than 1% (see, for example, [13]).

The reconstructed return map $\lambda(t)$ vs. $\lambda(t - T)$ of the transmitter is shown in Fig. 3a; we compared it to the nonlinear function F used in the feedback, which is shown in Fig. 3b. (As another example, we also show, in Figs. 3c and 3d, respectively, the return map and the nonlinear function of the radio-frequency transmitter that were reported in [7], where the nonlinearity was formed by a set of three oscillating resonant circuits.) It can be seen that only a visual judgment of the type of nonlinearity used in the transmitter can be obtained using the data in Figs. 3a and 3c. Another method is thus required to extract the information on the nonlinearity used in the transmitter.

The usual condition of transmitting systems using chaos is that the amplitude of the message signal is much smaller than the amplitude of the chaotic carrier oscillations, i.e., $m(t) \ll x(t)$. We also assume that $dx(t)/dt \ll dm(t)/dt$, which is usually fulfilled in practice, and assume that the dynamics of the variable $x(t)$ can be approximately described by the expression

$$x(t) + \tau dx(t)/dt \approx \beta F[x(t - T)]. \quad (5)$$

Equation (5) is similar to Eq. (1) when a message signal is not injected into the feedback loop; i.e., this approximation means physically that, locally, the dynamics of the system with and without the message are assumed to be the same. This assumption allows us to apply analysis of the local dynamics described by Eq. (5) for reconstruction of Eq. (1). The F forecast can then be made within a very small neighborhood $\{x^i\}$ of every point x^i of the transmitted signal by analyzing the dynamics exhibited by the neighboring points. (If the size of $\{x^i\}$ is not small enough, the trajectories of the systems described by Eqs. (1) and (5) become significantly different with the evolution of the message over time.) Then, knowing the series of the sampled signal $x(t)$ and the delayed signal $x(t - T)$, one can calculate the function $X(t) = x(t) + \tau dx(t)/dt$, and then estimate the forecast of the function F that can be reconstructed using, for example, an expansion in polynomials (up to the second degree in [4]) with the least squares minimization.

In practice, the procedure of key breaking we applied includes the following steps:

1. We choose an arbitrary series of the sampled output signal $x(t)$ with a duration of approximately a few T periods and the corresponding series of the delayed signal $x(t - T)$.

2. We calculate the derivative of the transmitted signal at every point x^i as a vector $dx^i/dt = (x^{i+1} - x^{i-1})/2dh$, where h is the sampling step, and, next, as the vector

$X^i = x^i + \tau dx^i/dt$. Obviously, the sampling step must be at least a few times smaller than τ .

3. For a more accurate approximation, we apply the program choosing the points of the series $x_T = x(t - T)$ surrounded by the set of neighboring points $\{x_T^i\}$ that represents small monotonic (in the time domain) pieces. The size of $\{x_T^i\}$ is arbitrary chosen to equal 5% of the value of the difference $\max(x_T) - \min(x_T)$, where $\max(x_T)$ and $\min(x_T)$ stand for the maximum and minimum values of the series of x_T . In our case, we obtain that the number of neighboring points is from three to five.

4. Next, we estimate the forecast of the function βF^i at every chosen point x_T^i surrounded by a monotonic set $\{x_T^i\}$, using the equation $X^i = \beta F^i(x_T^i)$. In doing so, we apply one of three types of interpolation: a spline linear approximation, a parabolic approximation, or a cubic approximation. In the latter case, an example of such an interpolation made for a sampled series $\lambda_T = \lambda(t - T)$ of 2000 points is shown in Fig. 4a. The projections of βF^i on the plane $\{\beta F^i, \lambda_T\}$ are shown in Fig. 4b. After averaging a number of time series λ_T , we obtain the forecast of $\beta F(\lambda)$ shown in Fig. 4c (solid curve) with the original function $\beta F(\lambda)$ (dashed curve). We obtained qualitatively similar results applying the spline linear and parabolic approximations.

5. However, the forecast of $\beta F(\lambda)$ obtained in Fig. 4c cannot be introduced directly into Eq. (1) to recover the message, due to resulting errors that reach 25% of the original values of $\beta F(\lambda)$. At the same time, attempts to use the forecast of $\beta F(\lambda)$ obtained at this step lead to a chaotic error signal $\Delta(t)$, expressed by Eq. (4), the output of the numerical model of the receiver, with an amplitude at least three times higher than that of the message signal that is to be recovered. A possible way to overcome this problem is to collect statistics and to analyze the signal through a series with duration, for example, between 10 and 100 T periods, but this method would take hours of calculations using a personal computer. We used a faster way to recover the message. The data represented in Figs. 4b and 4c show qualitatively that the function $\beta F(\lambda)$ is a periodic function of the $\sin(\cdot)$, or $\sin^2(\cdot)$ type. We then assume that $\beta F(\lambda)$ can be approximated by the expression $\beta F(\lambda) \approx A \sin^2(B\lambda + C)$, where A , B , and C are the parameters that have to be reconstructed. Then, we calculate the 3D matrix of the fitting error

$$E_{i,j,k} = \sum_{l=1}^N [\beta F_l - A_i \sin^2(B_j \lambda_l^l + C_k)]^2, \quad (6)$$

where N is the number of points used for the estimate of the forecast of the function $\beta F(\lambda)$ in Fig. 4c, doing so within a volume $\{A_i, B_j, C_k\}$ around the expected values

Fig. 4. Reconstruction of the function $\beta F(\lambda)$: (a) the spline cubic approximation as a matrix $\beta F^i(\lambda_T^i)$; (b) the projection of $\beta F^i(\lambda_T^i)$ onto the plane $\{\beta F^i, \lambda_T(t)\}$; (c) the averaged values of βF^i (the dashed curve is the original function describing the nonlinearity involved in the experimental feedback loop).

A , B , and C of the parameters. These values can be obtained in advance using the data shown in Figs. 4b and 4c. Next, we determine the minimum of the error matrix $F_{i,j,k}$. Finally, we obtain $A = 3.44$ nm, $B = 14.2$ nm⁻¹, and $C = 0.78\pi + n\pi$ (the corresponding values for the parameters of Eq. (1) are $\beta = 3.5$ nm, $K = \pi D/\Lambda_0^2 = 14.4$ nm⁻¹, and $\Phi_0 = \pi D/\Lambda_0 = 2.43$). Thus, Eq. (1) is reconstructed. In practice, the procedure of reconstruction takes only a few minutes of calculation.

6. As the last step, the numerical modeling of the receiver with the receiver equations (2) and (4) can be applied for message recovery. We calculated the difference signal $\Delta(t)$, solving Eq. (2) with the obtained values of the parameters A , B , and C . The difference signal $\Delta(t)$ thus obtained is shown in Fig. 5a and can be compared with the original message signal (Fig. 2a). The spectrum of $\Delta(t)$ is shown in Fig. 5b. One can see peaks corresponding to the two components of the original

Fig. 5. Recovery of the information signal: (a) the difference signal $\Delta(t)$ and (b) the spectrum of $\Delta(t)$. The dashed line is the spectrum of the original message signal $m(t)$ shown in Fig. 2a.

transmitted message, showing that the encrypted message is recovered.

Thus, we have shown that our DNLF system is not completely safe and that the key represented by the system parameters can be broken despite the very high dimensionality of the chaotic carrier and the strong nonlinearity involved in the feedback loop.

This raises questions about other high-dimensional chaotic systems of similar design. It seems likely that message security can be enhanced using nonlinear functions that cannot be expressed analytically, since chaotic regimes produced by nonanalytical nonlinear functions seem to be still unsolved mathematically. From that point of view, the possibility of generating more complicated nonlinear functions by using random (and, for example, dynamical) spectral filters in the feedback loop might be a solution to increasing key complexity and making cryptanalysis of such systems very difficult.

ACKNOWLEDGMENTS

The participation of V.S. Udaltsov was supported by the Centre National de la Recherche Scientifique, France. This work was funded by the EEC (contract no. IST-2000-29683, OCCULT).

REFERENCES

1. K. M. Coumo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
2. G. Pérez and H. A. Cedeira, Phys. Rev. Lett. **74**, 1970 (1995).
3. K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7**, 1579 (1997).
4. K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998).
5. L. Kocarev, U. Parlitz, and T. Stojanovski, Phys. Lett. A **217**, 280 (1996).
6. J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).
7. L. Larger, V. S. Udaltsov, J. P. Goedgebuer, and W. T. Rhodes, Electron. Lett. **36**, 199 (2000).
8. L. Larger, J. P. Goedgebuer, V. S. Udaltsov, and W. T. Rhodes, Electron. Lett. **37**, 594 (2001).
9. G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).
10. J. B. Geddes, K. M. Short, and K. Black, Phys. Rev. Lett. **83**, 5389 (1999).
11. B. Mensour and A. Longtin, Phys. Lett. A **244**, 59 (1998).
12. M. J. Brüner, Th. Meyer, A. Kittel, and J. Parisi, Phys. Rev. E **56**, 5083 (1997).
13. C. Zhou and C.-H. Lai, Phys. Rev. E **60**, 320 (1999).
14. V. S. Udaltsov, J. P. Goedgebuer, L. Larger, and W. T. Rhodes, Phys. Rev. Lett. **86**, 1892 (2001).
15. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
16. A. Fraser and H. Swinney, Phys. Rev. A **33**, 1134 (1986).
17. R. Hegger, M. J. Brüner, H. Kantz, and A. Giaquinta, Phys. Rev. Lett. **81**, 558 (1998).