Time delay identification in chaotic cryptosystems ruled by delay-differential equations

V. Udaltsov, L. Larger, J. Goedgebuer, A. Locquet, D. Citrin

Time delay identification in chaotic cryptosystems ruled by delay-differential equations

V. S. Udaltsov,* L. Larger, and J. P. Goedgebuer

GTL-CNRS TELECOM, UMR FEMTO-ST 6174, Georgia Tech Lorraine, 57070 Metz, France

A. Locquet and D. S. Citrin

GTL-CNRS TELECOM, UMR FEMTO-ST 6174, Georgia Tech Lorraine, 57070 Metz, France and School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia, USA

Feedback circuits ruled by time-delayed differential equations (DDE) can be used as the emitters in optical and electronic chaos-based secure communications. The degree of security of communications is limited by the possibility of recovering the parameters of the chaos-generating emitter. We analyze several methods for recovering the time delays in modified DDE systems with two feedbacks. With increasing gain factor of the feedbacks it becomes difficult or even impossible to recover the time delay of the modified circuit.

The history of chaos-based communications started at the beginning of the 1990s, when Pecora and Carroll published their fundamental work on chaos synchronization.[1] Soon after, chaotic waveforms were found to be a possible carrier for confidential information in secure communications.[2] A great number of examples of chaos-based communication systems have been reported since that time. We consider here a specific type of chaos-generating emitter which has a tunable source controlled by a feedback loop with a nonlinear element and a time delay (see, for example, Ref. 3). The dynamics of this circuit can be described by the differential delay equation (DDE) known as Ikeda's equation.[4] Such a circuit is remarkable due to the fact that it is characterized by hyperchaotic dynamics and exhibits high-dimensional attractors (the dimension of chaos reaches values up to 500) with many positive Lyapunov exponents in the case of sufficiently strong nonlinearity of the feedback.[5] Such a circuit can be synchronized easily[6] and provides a high rate of communication, for example, of an order of several Gbits persecond.[7]

In the beginning the high complexity of a chaotic carrier was considered to be a sufficient condition for a high degree of security.[8] However, it was later shown that high dimension by itself does not prevent cracking of a system.[9] Thus the reconstruction of all parameters of a circuit ruled by DDE and the recovery of the transmitted information have been achieved for comparatively low dimensionality of chaos[10–13] and later for a hyperchaotic system despite the high dimensionality of the chaotic carrier.[14] In Ref. 14 we described a way of cracking the parameters of a hyperchaotic system by concentrating mostly on binding the type of nonlinearity and the reconstruction of its parameters.

Nevertheless, the problem of T-recovery is still of great interest and has not been carefully investigated yet. We discuss some aspects of this problem in this Letter.

The block-diagram of the chaos-generating single-feedback circuit is shown in Fig. 1a. It consists of a controlled source (the tunable laser diode in Ref. 3 or the VCO in Ref. 15), a nonlinear element (the birefringent plate placed between two polarizers in Ref. 3 or the set of resonant circuits in Ref. 15), a photodiode[3] or diode,[15] a low-pass filter with a cutoff frequency $f=1/2\pi\tau_1$, and a time delay T. The dynamics of such a circuit are described by the DDE:

$$y(t)+\tau_1\frac{dy(t)}{dt}=\beta F[y(t-T)], \tag{1}$$

where $y(t)$ is the normalized dimensionless variable, β is the feedback gain factor or bifurcation parameter, and F is the function describing the nonlinear element. In the case when the birefringent plate is in use, F is the $\sin^2$ function with the initial phase shift Φ_0: $F[y(t)]=\sin^2[y(t)+\Phi_0]$. It should be noted that Eq. (1) also describes a feedback circuit with controlled nonlinearity and uncontrolled source (for example, the controlled Mach-Zehnder interferometer used in Ref. 16). This system can be attacked successfully.[14] We will consider that system as a classic example for testing known methods of T-recovery.

It was shown that the single-feedback nonlinear delayed circuit with the band-pass filter instead of the low-pass filter also generates hyperchaotic signals.[17] These signals can be used as carriers in the narrow-band transmitting channels. In the case of the $\sin^2$-type nonlinearity and of a band-pass filter formed by a low-pass filter and a high-pass filter, the chaos-generating circuit is ruled by the normalized equation:[17]

$$y(t)\left(1+\frac{\tau_1}{\tau_2}\right)+\tau_1\frac{dy(t)}{dt}+\frac{1}{\tau_2}\times\int_0^t y(t)dt=\beta\sin^2[y(t-T)+\Phi_0], \tag{2}$$

where τ_1 and τ_2 correspond to the cutoff frequencies of the low-pass and high-pass filters. We investigated the possibility of recovering the time delay of that system, too.

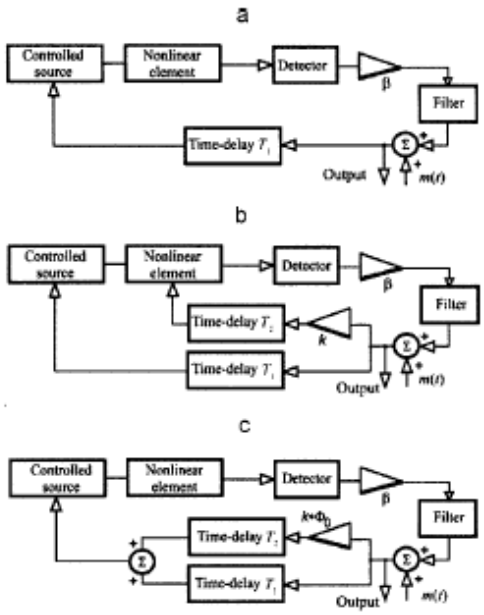

FIG. 1. The block diagrams of chaos-based transmitters: (a) with one feedback on the controlled source, (b) with two feedbacks on the controlled source and the controlled nonlinearity, (c) with two parallel time delays in one feedback and with a controlled source; $m(t)$ is the information signal.

For better security we propose to use two feedback loops with different delays T_1 and T_2: one feedback is controlling the source and another one is controlling the nonlinearity. The block diagram corresponding to that transmitter is shown in Fig. 1b.

We consider here the particular case, in which the nonlinearity is represented by a controlled Mach-Zehnder interferometer (for example, see Ref. 16) that is described by the nonlinear function $F[y(t)]=\sin^2[y(t)+\Phi_0]$. We suppose that the phase shift Φ_0 can be controlled.

In the case of the feedback with the low-pass filter, the dynamics of such a circuit are described by a DDE similar to Eq. (1):

$$y(t)+\tau_1\frac{dy(t)}{dt}=\beta\sin^2\{y(t-T_1)+\Phi_0[1+ky(t-T_2)]\}, \tag{3}$$

where k is the gain in the feedback controlling the nonlinearity (see Fig. 1b).

The band-pass feedback case is ruled by an equation similar to Eq. (2):

$$y(t)\left(1+\frac{\tau_1}{\tau_2}\right)+\tau_1\frac{dy(t)}{dt}+\frac{1}{\tau_2}\int_0^t y(t)dt$$
$$=\beta\sin^2\{y(t-T_1)+\Phi_0[1+ky(t-T_2)]\}. \tag{4}$$

It should be noted that Eqs. (3) and (4) describe also the dynamics of the single-feedback circuit with two parallel time delays; such a circuit is shown in Fig. 1c. The models (1)–(4) were used for numerical simulations and tests of the T-recovery methods.

There are several known methods that can be used by an eavesdropper to recover the value of the time delay T.

1. ANALYSIS OF THE RETURN MAPS OF THE TRANSMITTED SIGNAL

A return map represents the function $y(t)$ versus $y(t-t_0)$, where t_0 is the variable embedding time shift. When $t_0=T$, this function is considered as an analog of a 2D section of the phase trajectory.[18] For $t_0=T$, the return map exhibits some distinguishable structure containing advanced information about the type of the nonlinear function F.[14] In the other cases, the return map represents a series of states with isotropic circular distribution and does not contain any structure.

2. ANALYSIS OF THE AUTOCORRELATION FUNCTION (ACF) OF THE TRANSMITTED SIGNAL

In some cases the ACF of the output signal $y(t)$ has a peak that corresponds to the exact value of T.[14] This method is the least sensitive in comparison with all others; we observed such a peak only for the simple single-feedback circuits shown in Fig. 1a.

3. APPLICATION OF THE AVERAGE MUTUAL INFORMATION TECHNIQUE (THE AMI TECHNIQUE)

The AMI techniques are borrowed from information theory.[19] The AMI is a statistical function that establishes a criterion for mutual dependence between two measurements; such a criterion is based on the notion of information ties between them. The two measurements we consider here are the output signal $y(t)$ and a delayed version of it, $y(t-t_0)$. If $y(t)$ and $y(t-t_0)$ are not completely independent, the AMI function versus the embedding variable t_0 exhibits a sharp peak located at $t_0=T$. It is clear that in our case $y(t)$ and $y(t-t_0)$ are not independent, since they are connected to each other by the DDE.

4. ANALYSIS OF THE TIME DISTRIBUTION OF EXTREMA

The method based on a statistical analysis of time intervals between all pairs of extrema in the time series was described in Ref. 20. We modified this method slightly by using the statistics of a binary function we plot in the time domain. This function is equal to "0" everywhere, except for the moments corresponding to maxima of the sampled time series $y(t)$, where it is equal to "1." Next we simply calculate the sum of many limited series of that binary function, each series having the same duration (longer then expected value of T). Every series begins at arbitrarily chosen moments when the binary function is equal to 1. Such a sum displays a peak located at $t=T$ (see below).

5. RECOVERY OF BY LOCAL LINEAR FITS IN A LOW-DIMENSIONAL SPACE

Bünner[21] *et al.* and Zhou and C.-H. Lai[13] proposed a method which is tailor-made to analyze time series $\{y_i\}$ produced by scalar time-delay systems. Let us first consider the scalar time-delay system described by Eq. (1). They proposed to work in the three-dimensional space $[dy(t)/dt, y(t), y(t-T)]$. In this low-dimensional space, the system is confined to a two-dimensional manifold ruled by the constraint $\tau_1 dy/dt + y(t) - F[y(t-T)] = 0$. In light of the previous properties, Bünner *et al.* proposed, for each time index i, the following discrete local linear model:

$$\dot{y}_i = a_i + b_i y_i + c_i y_{i-t_0}, \tag{5}$$

where $\dot{y}_i$ is an estimate of the time derivative, t_0 is an index corresponding to a time delay, and b_i and c_i are parameters of the local model. The parameters of the model are found by a least-squares fit. From the residual error of the fit, an average fitting error σ can easily be determined for the whole time series $\{y_i\}$.[21] This fitting error σ is minimal when t_0 corresponds to the delay equal to time T, because only in that case do the triples $(\dot{y}_i, y_i, y_{i-t_0})$ fulfill simultaneously the above-mentioned constraint. The unknown value of the delay time thus corresponds to a minimum of the average fitting error σ.

In the case of a time-delay system ruled by a set of coupled delay-differential equations, Hegger *et al.*[22] propose to add a Takens-like embedding to the model used for a scalar system. This leads to a local linear model of the form:

$$\dot{y}_i = a_i + \sum_{j=0}^{M} b_i^j y_{i-j} + \sum_{j=0}^{M} c_i^j y_{i-t_0-j}, \tag{6}$$

where M represents the number of additional delayed variables considered in the model. This model will be used for the systems with band-pass filters since the integro-differential equations describing these systems [Eq. (2)] can be transformed into a set of two coupled delay-differential equations.

We investigated numerically the chaos-generating emitters based on the circuits described by Eqs. (1)–(4). We used the Runge–Kutta procedure to obtain the time series, next applied the T-recovery methods listed above. For the circuit with the low-pass filter, the parameters of the circuit are: $\tau_1 = 5\ \mu$s, $T_1 = 100\tau_1 = 0.5$ ms, $T_2 = 0.77T_1 = 0.386$ ms (arbitrarily chosen), $\Phi_0 = 0.74\pi$ (arbitrarily chosen). For the band-pass filter, we added the value of the second time constant $\tau_2 = 25\ \mu$s. The parameters τ_1 and T_1 are close to the parameters of the experimental setup.[3] The normalized bifurcation parameter β was varied from 0 to 25. The gain k of the feedback loop containing the time delay T_2 was varied from 0.1 to 0.43. The last value corresponds to the "symmetrical" case: $k\Phi_0 = 1$, when the left-hand side of Eqs. (3) and (4) can be written as $\sin^2[y(t-T_1) + y(t-T_2)\Phi_0]$.

We analyzed the time series of the output signals for different duration l: $l = 20T_1$, $l = 100T_1$ and $l = 500T_1$.

The results of the recovery of T for the circuit with the single feedback loop and the $\sin^2$ nonlinearity (Fig. 1a) are shown in Fig. 2. One can see an example of the chaotic output signal (Fig. 2a) and the distribution of the amplitude probability (PDA) (Fig. 2b). It can be seen that the PDA is almost Gaussian for $\beta = 25$, and thus we are dealing with a high-dimensional chaos. The Lyapunov dimension of chaos can be estimated by the equation: $d \approx 0.3\beta T/\tau_1 = 750$. This approximate equation has been derived from a computation of the Lyapunov spectrum based on Farmer's method.[23] It is in agreement with the conjectures on chaos dimension proposed in Ref. 24. Despite that high value of d (the highest value of d reached experimentally is 1.5 times less[5]), all of the methods of T-recovery show that it is possible to determine the value of the time delay. The return map (Fig. 2c) does not represent a series of states with isotropic circular distribution and contains a distinguishable structure (e.g., showing that 3 periods of the nonlinearity participate in the chaos generation). The ACF (Fig. 2d) also exhibits a remarkable peak at $t = T$; sharp peaks are well seen also in the AMI curve (Fig. 2e), in the time distribution of maxima (Fig. 2f), and in the curve representing the average fitting error of the

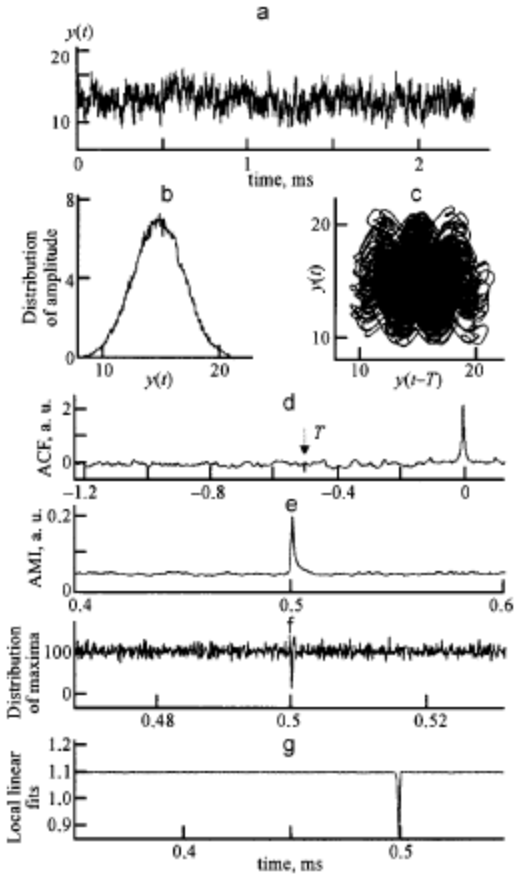

FIG. 2. Recovery of the value of the time delay T for the transmitter with the low-pass filter shown in Fig. 1a for $l = 20T_1$ and $\beta = 25$: (a) an example of the output signal, (b) histogram of the amplitude, (c) the return map, (d) the ACF, (e) the AMI function, (f) the time distribution of maxima, (g) recovery of T by linear fits in a three-dimensional space.

that the system with two delays can be made secure with respect to known attacks based on the identification of the time delay.

The same results were obtained in the case of analysis of the return maps. When β increases, this analysis is not sufficiently sensitive to recover the values of time delays and break the systems with two feedback loops.

Thus we have investigated a chaos-generating circuit ruled by DDE from the point of view of security of the communications when this circuit is in use as an emitter. Despite the possibility of generating hyperchaotic signals, such a circuit had been considered previously to be one that could be successfully attacked and reconstructed by an eavesdropper. Nevertheless, numerical results obtained show that the addition of the second delay can increase the security of the cryptosystem. The modification we propose makes the system essentially more secure than the system based on a single feedback.

Obviously, there are many other possibilities for modifying the system with two feedbacks. We are going to analyze different schemes for chaos-based communications in our next paper.

The participation of V.S. Udaltsov was supported by the Center National de la Recherche Scientifique (CNRS), France.

*E-mail: vladimir.oudaltsov@georgiatech-metz.fr

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**, 821 (1990).
[2] K. M. Coumo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett. **71**, 65 (1993).
[3] J. P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable lased diode," Phys. Rev. Lett. **80**, 2249 (1998).
[4] K. Ikeda and K. Matsumoto, "High-dimensional chaos behavior in systems with time-delayed feedback," Physica D **29**, 223 (1987).
[5] J. P. Goedgebuer, L. Larger, and H. Porte, "Chaos in wavelength with a feedback tunable laser diode," Phys. Rev. E **57**, 2795 (1998).
[6] V. S. Udaltsov, J. P. Goedgebuer, L. Larger, and W. T. Rhodes, "Communicating with optical hyperchaos: information encryption and decryption in delayed nonlinear feedback systems," Phys. Rev. Lett. **86**, 1892 (2001).
[7] J. P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, and W. T. Rhodes, "Optical communication with synchronized hyperchaos generated electrooptically," IEEE Quantum Electron. **38**, 1178 (2002).
[8] L. Kocarev, U. Parlitz, and T. Stojanovski, "An application of synchronized chaotic dynamics arrays," Phys. Lett. A **217**, 280 (1996).
[9] K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," Phys. Rev. E **58**, 1159 (1998).
[10] J. B. Geddes, K. M. Short, and K. Black, "Extraction of signals from chaotic laser data," Phys. Rev. Lett. **83**, 5389 (1999).
[11] B. Mensour and A. Longtin, "Synchronization of delay-differential equations with application to private communication," Phys. Lett. A **244**, 59 (1998).
[12] M. J. Bünner, Th. Meyer, A. Kittel, and J. Parisi, in *Nonlinear Physics of Complex Systems*, edited by J. Parisi, S. C. Müller, and W. Zimmermann, Springer-Verlag, Berlin (1996), p. 229.
[13] C. Zhou and C.-H. Lai, "Extracting messages masked by chaotic signals of time-delay systems," Phys. Rev. E **60**, 320 (1999).
[14] V. S. Udaltsov, J. P. Goedgebuer, L. Larger, J. B. Cuenot, P. Levy, and W. T. Rhodes, "Cracking chaos-based encryption system ruled by nonlinear time delay differential equations," Phys. Lett A **308**, 54 (2003).
[15] L. Larger, V. S. Udaltsov, J. P. Goedgebuer, and W. T. Rhodes, "Chaotic dynamics of oscillators based on circuits with VCO and nonlinear delayed feedback," Electron. Lett. **36**, 199 (2000).
[16] Y. Ch. Kouomou, P. Colet, N. Gastaud, and L. Larger, "Effect of parameter mismatch on the synchronization of electrooptical intensity laser hyperchaos," Phys. Rev. E **69**, 056226 (2004).
[17] V. S. Udaltsov, L. Larger, J. P. Goedgebuer, M. W. Lee, E. Genin, and W. T. Rhodes, "Bandpass chaotic dynamics of electronic oscillator operating with delayed nonlinear feedback," IEEE TCAS-1 **49**, 1006 (2002).
[18] T. Beth, D. E. Lazic, and A. Mathias, "Cryptanalysis of cryptosystem based on remote chaos replication," Lecture Notes in Computer Science (Springer-Verlag, Berlin) **839**, 318 (1994).
[19] H. D. I. Abarbanel, *Analysis of Observed Chaotic Data*, Springer-Verlag, New York (1996).
[20] B. P. Bezruchko, A. S. Karavaev, V. I. Ponomarenko, and M. D. Prokhorov, "Reconstruction of time-delay systems from chaotic time series," Phys. Rev. E **64**, 056216-1 (2001).
[21] M. J. Bünner, Th. Meyer, A. Kittel, and J. Parisi, "Recovery of the time-evolution equation of time-delay systems from time series," Phys. Rev. E **56**, 5083 (1997).
[22] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta, "Identifying and modeling delay feedback systems," Phys. Rev. Lett. **81**, 558 (1998).
[23] J. D. Farmer, "Chaotic attractor of an infinite-dimensional dynamical system," Physica D **4**, 366 (1982).
[24] B. Dorizzy, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Resayre, and A. Tallet, "Statistics and dimension of chaos in differential delay systems," Phys. Rev. A **35**, 328 (1987).

This article was published in English in the original Russian journal. Reproduced here with stylistic changes by AIP.