13 July 1998

PHYSICS LETTERS A

ELSEVIER

Physics Letters A 244 (1998) 59–70

Synchronization of delay-differential equations with application to private communication

Boualem Mensour [1], André Longtin [2]

Département de Physique, Université d'Ottawa, 150 Louis Pasteur, Ottawa, Ontario, Canada K1N 6N5

Received 10 August 1997; revised manuscript received 30 March 1998; accepted for publication 31 March 1998
Communicated by C.R. Doering

Abstract

Unidirectional synchronization of high-dimensional chaos with many positive Lyapunov exponents is demonstrated in first-order delay-differential equations (DDEs) at large delays. Synchronization of this hyperchaotic motion is shown to occur using feedback involving only one scalar variable. An analysis of the potential usefulness of such simple yet infinite-dimensional dynamical systems for broadband signal masking and private communication is also given. A particular feature is the chaotic masking of finite messages encoded onto controlled unstable periodic orbits of the same DDE dynamics used to generate the masking chaos. The difference equation obtained in the singular limit can further be used to transmit digital messages and predict the parameter range over which synchronization in the DDE occurs. Results for systems with a distribution of delays are also presented. © 1998 Elsevier Science B.V.

Keywords: Synchronization; Delay-differential equations; Feedback control; Chaos; Multistability; Private communication; Difference equations; Information storage; Masking

1. Introduction

Synchronization of chaotic systems has received a lot of attention in recent years (see, e.g., Refs. [1–3] and references therein). Apart from exploring the mechanisms by which coupled simple nonlinear elements can entrain one another, there has also been interest in the potential application of chaotic synchronization to signal masking and private communication [4–7]. The basic goal behind chaotic synchronization in this latter context is to recover a given chaotic trajectory from a "driving" system in a usually identical "response" system having an arbitrary initial condition. The idea behind private communication then is to hide a message with the aperiodicity of chaos before transmission, and extracting this chaotic behavior at the receiver through synchronization. The power spectra of chaotic signals are typically broadband, in contrast with those of information-carrying signals (i.e. "messages"). Masking a message with a chaotic carrier, or modulating this carrier with a message signal, both of which are simple forms of spread spectrum communication [8], makes the presence of the signal difficult to detect in either the time or frequency domain.

Two main synchronization techniques have widely been used. The first [1,9] decomposes the system into two subsystems: a master system (transmitter), which has one or more positive Lyapunov exponents,

[1] E-mail: boualem@physics.uottawa.ca.
[2] E-mail: andre@physics.uottawa.ca.

PII S0375-9601(98)00271-0

is used to drive an identical slave system (receiver), which has only negative Lyapunov exponents, into synchronization. In this manner, synchronization has been achieved in various electrical circuits [2,4–6].

The second technique is based on negative feedback proportional to the difference between the outputs of the drive and response systems [10]. It is an extension of methods used to control unstable periodic orbits (UPOs) [11], except that perturbations are instead applied to aperiodic orbits. By varying the strength of the feedback, the Lyapunov exponents of the response system can be made negative; the feedback perturbation then becomes very small in absolute value as time increases, and synchronization is obtained. This method has also been realized experimentally [12–14]. It also appears in many different studies as negative differential feedback or diffusive coupling (see, e.g., Ref. [2,15,16], and also Ref. [17] for a study of this type of synchronization with non-identical response systems). The approach in Ref. [1] can in fact be considered as the infinite coupling strength limit of these feedback approaches, since certain variables in the response dynamics are directly replaced by those of the drive system.

Most investigations of private communication with chaos have focused on the problem of transmitting signals with low-dimensional chaotic systems, such as those generated by the Rössler and Lorenz systems. However, it is desirable to use high-dimensional chaotic carriers with one or many positive Lyapunov exponents to make unauthorized signal unmasking and recovery as difficult as possible. Peng et al. [18] have shown that it is possible to synchronize chaos from a high-dimensional hyperchaotic coupled map lattice using a single scalar variable that is a linear combination of the original phase space variables. Xiao et al. [19] have discussed how high-dimensional spatiotemporal chaos can be used for transmitting and receiving a large number of informative signals simultaneously. Also, Parlitz et al. [6] have constructed a high-dimensional system using a series of low-dimensional "building blocks" of Rössler systems (each block has dimension three). This method has many advantages, but some limitations in its implementation since the sttractor dimension is proportional to the number of blocks.

Delay-differential equations (DDEs) present an alternative simple and efficient tool for chaos communication with low detectability. This is because their simple yet infinite-dimensional dynamics have finite high-dimensional hyperchaotic attractors, and also exhibit multistability when the delay is large (see, e.g., Refs. [20–23]). They are also easily implementable electronically [24,25].

This Letter shows that one-dimensional DDEs are unidirectionally synchronizable using either of the aforementioned techniques. While the feedback method can be applied directly to the receiver as a small perturbation, the master–slave method requires that a proper master–slave decomposition be found. We find in particular that synchronization if possible using the state variable as the single scalar variable, which is interesting in light of the results in Ref. [18]. Further, we demonstrate the potential of such DDEs for private communication. In particular, we present a new masking scheme based on the multistability of the dynamics exhibited by these DDEs at large delay. In this scheme, a finite message (a finite bit string) is first encoded onto one of the many multistable waveforms, either periodic, or made so by UPO control methods. This is done using a specific piecewise constant initial function and feedback control [26] (the different constants in the initial function are mapped to bits in the message). The message is then transmitted using a chaotic DDE carrier generated by an identical system without UPO control, and recovered using synchronization (see Figs. 4 and 5). The spectral features of the signal are then similar to those of the chaotic mask, making unmasking more difficult.

Our work also shows that the simple map obtained in the singular limit of the DDE, especially its maximal Lyapunov exponent, predicts the parameter range where synchronization occurs in the DDE. Finally, the synchronization method based on this limit can be used to synchronize any discrete-time system (i.e. map) and to transmit digital signals.

Our Letter is organized as follows. Section 2 discusses methods of synchronization of the Mackey–Glass DDE and of its singular limit map. Section 3 presents a method of synchronization of distributed delay systems. Section 4 demonstrates the application of chaotic synchronization with DDEs to private communication. Section 5 analyzes the robustness of message recovery to noise and parameter mismatch, and discusses the potential vulnerability of this type of chaos communication to dynamical unmasking tech-

niques. Results and directions for future research are summarized in the conclusion in Section 6.

2. Synchronization of Mackey–Glass DDE

2.1. Synchronization schemes and results

At least two types of chaotic synchronization schemes can be applied to DDEs such as the Mackey–Glass or the Ikeda equations. The first scheme is very simple. It consists of supplying the drive variable $x(t-\tau)$ or $x(t)$ from the driving DDE,

$$\frac{dx(t)}{dt} = -bx(t) + F(x(t-\tau)), \tag{1}$$

to the feedback function of the second "response" DDE to be synchronized,

$$\frac{dy(t)}{dt} = -by(t) + F(x(t-\tau)), \tag{2}$$

or

$$\frac{dy(t)}{dt} = -by(t) + F(x(t)). \tag{3}$$

In both cases, the response system synchronizes very rapidly. We note that, for driving with $x(t)$, the two outputs are shifted from one another in time by the delay τ. Synchronization is expected in both cases since $x(t-\tau)$ or $x(t)$ are driving, via the static nonlinearity F, a linearly stable response system $\dot{y} = -by$, i.e. this response system has a negative conditional Lyapunov exponent. This kind of synchronization would apply to identical first-order systems responding to essentially the same feedback variable.

A second synchronization scheme consists in applying a feedback perturbation proportional to the difference between the two outputs [10],

$$\begin{aligned}\frac{dx(t)}{dt} &= -bx(t) + F(x(t-\tau)),\\ \frac{dy(t)}{dt} &= -by(t) + F(y(t-\tau)) + K[x(t) - y(t)].\end{aligned} \tag{4}$$

The second DDE is identical to the first DDE, except for its coupling to the first via the perturbation $D(t) \equiv K[x(t) - y(t)]$. This could apply to situations where one feedback system is linearly coupled to another identical feedback system, e.g., through some form of crosstalk. Here the linearization of the response subsystem involves time-dependent coefficients, and it is the numerically calculated conditional Lyapunov exponents of the response system that will determine whether or not synchronization occurs.

We focus here on this second type of synchronization in the Mackey–Glass DDE (MG DDE) [27],

$$\frac{dx(t)}{dt} = -bx(t) + \frac{ax(t-\tau)}{1 + x^c(t-\tau)}, \tag{5}$$

with parameters $b = 0.1$ and $c = 10$ (constant throughout our study). Note that the second term on the right hand side of Eq. (5) corresponds to the function F in Eq. (4). The synchronization (i.e. coupling) term is similar to the term used for UPO control in Refs. [11,26,28], i.e. the dynamics are similar to

$$\begin{aligned}\frac{dx(t)}{dt} &= -bx(t) + F(x(t-\tau))\\ &\quad + K[x(t-T) - x(t)],\end{aligned} \tag{6}$$

where T is the period of an UPO. However, aperiodic orbits are now synchronized, as in Ref. [10], rather than UPOs. The aperiodic orbits are thus generated by two similar DDEs evolving from different initial functions.

It is known that this system becomes chaotic for $\tau > 16.8$ with $a = 0.2$, and that in the chaotic regime, the attractor dimension scales roughly linearly with the delay. For the relatively large delay $\tau = 300$ used below, the Kaplan–Yorke dimension is roughly 30 [22,23]. It is also known that the number of positive Lyapunov exponents increases with the delay, and is close to 15 for $\tau = 300$. Interestingly, the metric entropy (sum of the positive Lyapunov exponents) is constant for $\tau > 50$, due to the fact that the values of the Lyapunov exponents scale as τ^{-1} [20]. This has implications for the predictability of the dynamics, and for the multifractal nature of the attractor (see Ref. [29], and Section 5).

Without the unidirectional coupling from the first to the second system, the two trajectories diverge exponentially. By varying the strength of the perturbation, the Lyapunov exponents of the response system can be made negative, causing distances between the orbits of the two systems to decay to zero. This is shown in Figs. 1a,b for two chaotic MG DDEs (Eq. (4))

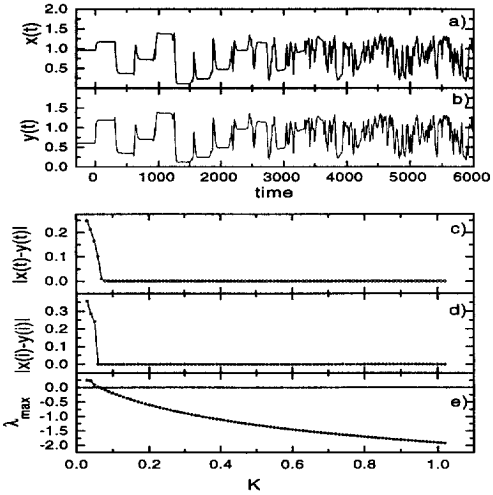

Fig. 1. Synchronization of two MG chaotic DDEs (a = 0.2, τ = 300). (a,b) x versus t and y versus t using Eq. (4) with two different initial conditions. (c) The time average of $|x(t) - y(t)|$ as a function of K for the DDE (Eq. (4)). The average for each K is computed after transients have decayed. (d) The discrete-time average $|x(i) - y(i)|$ as a function of K for the map (Eq. (8)), again computed after transients. (e) The maximum Lyapunov exponent λ_{max} as a function of K for the map (Eq. (8)). We used a fourth-order Runge–Kutta integration algorithm with time step 0.01 throughout this Letter.

for $a = 0.2$ and $\tau = 300$, each of which starts from a different constant initial function on $(-\tau, 0)$. These results show that it is possible to synchronize these chaotic motions, despite the presence of many positive Lyapunov exponents, a large attractor dimension, and a coupling via one scalar variable, namely the state $x(t)$.

We note that the two orbits can remain close yet visibly distinct if the coupling parameter K is misadjusted. Fig. 1c shows the dependence on K of the time average of $|x(t) - y(t)|$. Synchronization occurs for K larger than a certain value ($K > 0.08$). This appears to be always true for the coupling we have chosen. There have been reports in other systems (see, e.g., Ref. [10]) where increasing the coupling strength K destroys the synchronization. This can be caused by multistability. It can also occur without multistability if the feedback is applied to only one variable. The strong perturbation then destabilizes the system because the other variables cannot adjust fast enough to the changes in the variable to which the perturbation is applied. The fact that this asymmetry, where certain variables have feedback and others do not, is not present in the one-dimensional DDE studied here may explain why we do not see loss of synchrony at large K.

2.2. Synchronized singular limit maps

The map obtained in the singular perturbation limit $R = b\tau \to \infty$ of the DDE can be used to study synchronization as in Eq. (4) at large R. First, this limit yields unidirectionally coupled continuous-time difference equations (CTDEs),

$$x(t) = b^{-1}F(x(t-\tau)),$$
$$y(t) = (b+K)^{-1}[F(y(t-\tau)) + Kx(t)]. \qquad (7)$$

If time is discretized in units of τ in Eq. (7), the map dynamics become

$$x(i) = b^{-1}F(x(i-1)),$$
$$y(i) = (b+K)^{-1}[F(y(i-1)) + Kx(i)]$$
$$= (b+K)^{-1}[F(y(i-1)) + Kb^{-1}F(x(i-1))]. \qquad (8)$$

The parameter K can then be adjusted to produce synchronization. We have found that the analysis of this map provides useful information on the parameters that yield synchronization in the DDE from which the map is obtained. The maximum Lyapunov exponent of this two-dimensional map is calculated by applying the QR decomposition method [30,31] to this map (not to the DDE). Typically, only a few QR decompositions are needed for Q to converge to the identity matrix. Figs. 1d,e show the distance $|x(i) - y(i)|$ and the maximum Lyapunov exponent $\lambda_{\max}$ for the map (Eq. (8)) as a function of K. The time average of $|x(i) - y(i)|$ goes to zero and $\lambda_{\max}$ goes negative (indicating synchronization) at $K \approx 0.07$, close to the actual value found for the synchronization of the DDEs (Fig. 1c). Thus, an analysis of Lyapunov exponents for the map is an efficient way to obtain information on synchronization of the DDE itself, while avoiding the difficult numerical determination of the Lyapunov spectrum of the DDE. The underlying reason is that much of the DDE dynamics at large delay are governed by the difference (i.e. map) aspect of the dynamics rather than the differential aspect (the latter

mostly imposes that the solutions be differentiable.) This discrete method of synchronization can of course be applied to a variety of discrete dynamical systems.

3. Synchronization of distributed delay systems

Synchronization can also be studied in the context of systems with a distribution of delays rather than a single fixed delay. Such systems are often encountered in applications, and DDEs are often used to approximate their behavior. Mathematically, the infinite-dimensional DDE can be approximated by an integro-differential equation with a smooth memory kernel, which can be converted into a $(m+2)$-dimensional system of ordinary differential equations (ODEs) such as Eq. (9) below [32,33]. In the chaotic regime with $\tau = 300$, m has to be large ($m > 100$) for the attractors of the DDE and of the distributed delay system to have similar invariants [23]. The method of Pecora and Carroll [1] for synchronizing ODEs can be used here, and one possible decomposition is into a master subsystem governed by

$$\dot{y}_0 = f(y_0, y_{m+1}) = -by_0 + F(y_{m+1}),$$
$$\dot{y}_i = -\alpha(y_i - y_{i-1}), \quad i = 1, \ldots, m+1, \tag{9}$$

and a slave subsystem governed by

$$y_0' = y_0, \tag{10}$$
$$\dot{y}_1' = -\alpha(y_1' - y_0),$$
$$\dot{y}_i' = -\alpha(y_i' - y_{i-1}'), \quad i = 2, \ldots, m+1. \tag{11}$$

Here, the master system drives the slave system through the component y_0. The other components $y_1', y_2', \ldots, y_{m+1}'$ are allowed to have different arbitrary initial conditions. There is of course a finite number of possible decompositions, many of which are expected to yield synchronization [9,6] due to the conditional Lyapunov exponents of the subsystem (see below). The asymptotic stability of the slave subsystem that underlies synchronization can be established by finding a Lyapunov function [4,35]. Let y_i^* be the difference between the desired value y_i and the actual value of the slave variable y_i': $y_i^* = y_i - y_i'$. The y_i^* dynamics are governed by

$$\dot{y}_1^* = -\alpha y_1^*,$$

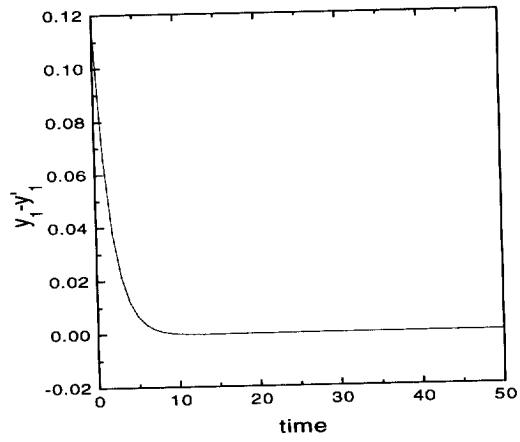

Fig. 2. Synchronization of two MG distributed delay systems ($\alpha = 0.55, m = 54$). The master subsystem drives the slave subsystem with the component y_0. The difference between the two outputs, $y_i - y_i'$ ($i = 1, 2, \ldots, m+1$), shown here for $y_1 - y_1'$, vanishes as $t \to \infty$.

$$\dot{y}_i^* = -\alpha(y_i^* - y_{i-1}^*), \quad i = 2, \ldots, m+1. \tag{12}$$

The y_i^* dynamics are globally asymptotically stable at the origin. This result follows by considering the $(m+1)$-dimensional Lyapunov function defined by

$$E(t) = \tfrac{1}{2}(y_1^{*2} + y_2^{*2} + \ldots + y_{m+1}^{*2}). \tag{13}$$

The time rate of change of $E(t)$ along a trajectory is given by

$$\dot{E}(t) = y_1^*\dot{y}_1^* + y_2^*\dot{y}_2^* + \ldots + y_{m+1}^*\dot{y}_{m+1}^*$$
$$= -\frac{\alpha}{2}[y_1^{*2} + (y_1^* - y_2^*)^2 + \ldots$$
$$+ (y_m^* - y_{m+1}^*)^2 + y_{m+1}^{*2}] \leqslant 0. \tag{14}$$

The Lyapunov function $E(t)$ decreases for all $y \neq 0$. Lyapunov's theorem [34] (see also Ref. [35]) implies that $E(t) \to 0$ as $t \to \infty$. Therefore, the distances y_i^*, along with Eq. (13), go to zero and synchronization occurs as $t \to \infty$ (see Fig. 2).

Synchronization also follows here from the fact that the conditional Lyapunov exponents of the response system are negative. It is straightforward to show that those exponents are the roots of $(-\alpha - \lambda)^{m+1} = 0$. Thus there is only one $(m+1)$-fold degenerate exponent $\lambda = -\alpha$. This exponent is in fact the exponential relaxation rate seen in Fig. 2. We can extend this calculation to arbitrary values of m. In the limit $m \to \infty$ the distributed delay system becomes identical with

the original DDE, and the synchronization is of the simple type seen in Eq. (2).

4. Application to communication with chaos

4.1. Generalities

In this section, we study the potential that simple hyperchaotic high-dimensional DDEs offer for chaos communication. An information signal $m(t)$ containing a message to be transmitted can be masked by the chaotic DDE signal $x(t)$. Chaos synchronization discussed above can then be used to extract the message at the receiver end. Different strategies can be used to make the actual transmitted signal $s(t)$ as broadband as possible, i.e. to make its detection through spectral techniques difficult. As we will see below, the spectrum of the DDE solutions of interest in our Letter have many modes superimposed on a broad background [20,23]. We will focus on strategies in which the signal has low power, i.e. is small in comparison to the chaotic carrier. One strategy is signal masking, where $s(t) = x(t) + \epsilon m(t)$; another is modulation, $s(t) = x(t)m(t)$; there are also combinations of masking and modulation, such as $s(t) = x(t)[1 + \epsilon m(t)]$ [8].

4.2. Communication using signal masking

We propose the following masking technique. A message $m(t)$, multiplied by a small positive number ϵ, drives the chaotic "DDE transmitter" as follows,

$$\frac{dx(t)}{dt} = -bx(t) + F(x(t-\tau)) + K\epsilon m(t). \quad (15)$$

The transmitted signal is $s(t) = x(t) + \epsilon m(t)$. A receiver with an identical copy of the transmitter is used to generate an output $y(t)$ which is synchronized to $x(t)$ using proportional feedback control,

$$\frac{dy(t)}{dt} = -(b+K)y(t) + F(y(t-\tau)) + Ks(t). \quad (16)$$

In the following, the technique is illustrated using $K = b$. If unidirectional chaotic synchronization can be achieved despite the presence of the message $m(t)$, the latter can be recovered as $m(t) = [s(t) - y(t)]/\epsilon$.

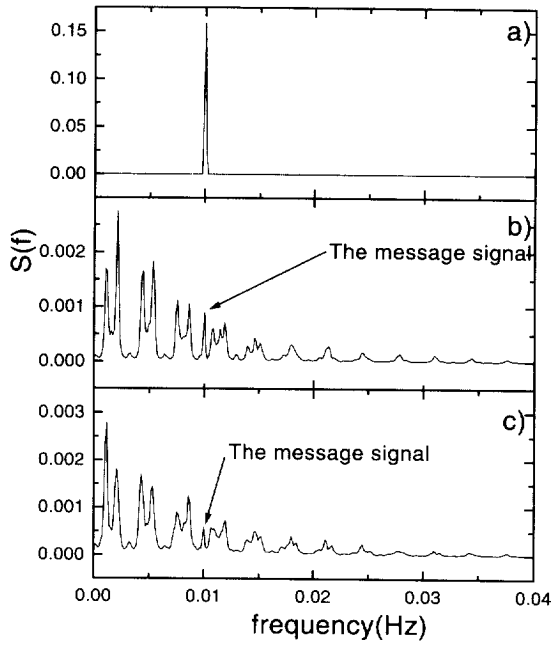

Fig. 3. Transmitting a sine wave signal $m(t) = \sin(2\pi t/100) + 1.5$ with $\epsilon = 0.05$, using an MG carrier with $a = 0.2$ and $\tau = 300$. (a) Power spectrum of the recovered sine wave signal using the masking technique Eq. (15). (b) Power spectrum of the transmitted signal using masking $s(t) = x(t) + 0.05m(t)$ where x is the chaotic carrier. (c) Same as (b) but using masking–modulation $s(t) = x(t)[1 + 0.05m(t)]$, yielding an even smaller power for the sinusoid. Spectra are averages over 20 samples of 4096 points each with sampling time 3.75.

We have found that this recovery is indeed possible. This is illustrated using a simple sine wave for $m(t)$. Fig. 3a shows the power spectrum of the recovered sine wave $m(t) = \sin(2\pi t/100) + 1.5$ after being masked by the chaotic carrier from the MG DDE. The power spectrum (the power is on a linear scale) of the transmitted signal (Fig. 3b) shows only a small peak at $f = 0.01$ Hz, of the same order of magnitude as other peaks in the chaotic broadband. Note that the sine frequency was purposely chosen to produce a peak that stands out from the background, to give an idea of its relative power; of course, it would be advantageous to adjust this frequency so that the peak blends in with the other background structure.

4.3. Communication using chaotic masking–modulation

We now study masking–modulation of the message by a broadband carrier $x(t)$ using $s(t) = x(t)[1 + \epsilon m(t)]$ as the transmitted signal. This masking–modulation technique is used to drive the transmitter in Eq. (15) in the same way as for the masking technique discussed above, but instead of driving with $K\epsilon m(t)$, we drive with $K\epsilon m(t)x(t)$. By synchronizing the receiver to the transmitter, the message can be recovered exactly as $m(t) = [s(t)/y(t) - 1]/\epsilon$. The spectral peak corresponding to the simple "sine wave" message is even smaller in comparison with the masking technique (see Fig. 3c).

4.4. Encoding messages onto UPOs of DDEs

The use of UPOs for private communication has been demonstrated in Ref. [36] using the P_4 orbit of the Hénon map. That method requires an attractor dominated by a few UPOs, near which the system spends more time. We now present a method which suffers less from this constraint. It applies to the transmission of short messages, and relies on a special multistability property of the class of DDEs of interest here when the delay is large.

The idea here is to encode a message, in the form of a finite bit string, directly onto an UPO of the same kind of DDE used to generate the chaotic carrier. To do this, an UPO has to first be stabilized, e.g., by delayed feedback control as in Eq. (6). The message can also be encoded onto a periodic orbit (obtained, e.g., by using a smaller value of a in Eq. (5)), but the UPOs offer a broader choice of orbits to choose from. The encoding technique is described in Ref. [26]. Such controlled UPOs are multistable. They can be given, using an appropriate piecewise constant initial function on the delay interval, a precise periodic form determined by the short message to be transmitted (the different constants in the piecewise constant initial function are mapped to bit groups in the message). The message can be encoded onto any UPO if it can be controlled. Also, different messages can be transmitted and received by simply changing the UPO or the initial function. Since the encoding uses UPOs embedded in the chaotic attractor the transmitted message will have frequencies that match those of the chaotic trajectories.

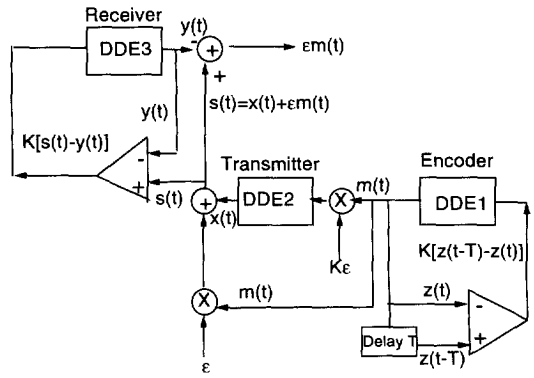

Fig. 4. Block diagram of a chaotic communication system based on the masking technique and UPOs of a DDE. A finite message is stored on a UPO of a DDE stabilized by delayed feedback control (Eq. (6)). This waveform is then masked by the chaotic behavior of a similar but uncontrolled DDE (transmitter), and decoded by another similar DDE with a synchronizing perturbation as in Eq. (4).

In other words, these frequencies will not stand out in the spectrum, and the message has low detectability, as shown in Fig. 5 below.

A block diagram of the method is shown in Fig. 4. The message encoded onto a controlled UPO in the "encoder" is then modulated before transmission with a chaotic carrier of a DDE similar to the one in the encoder. This second DDE can have the same or different feedback parameter (a in Eq. (5)), but has the same other parameters. At the receiver, which contains the exact copy of the transmitter system, the message is extracted using synchronization. Figs. 5a,b show a controlled UPO of a period four orbit P_4 orbit of the MG DDE Eq. (5) and its power spectrum. It is called "P_4" because it is made up of four "plateaus" connected by abrupt transitions. These plateaus are not exactly flat, as they have a bit of structure, especially near their extremities. Yet the average values of these plateaus is well approximated by the four constant values through which the controlled UPO of the singular limit map of the DDE cycles on its corresponding period four orbit.

The initial function on $(-\tau, 0)$ is divided into three pieces, each on an interval (or "bin") of duration $\tau/3$. The ordinate in each of these bins is assigned any one of the four plateau values mentioned above, i.e. it is piecewise constant. Since there are four values, each

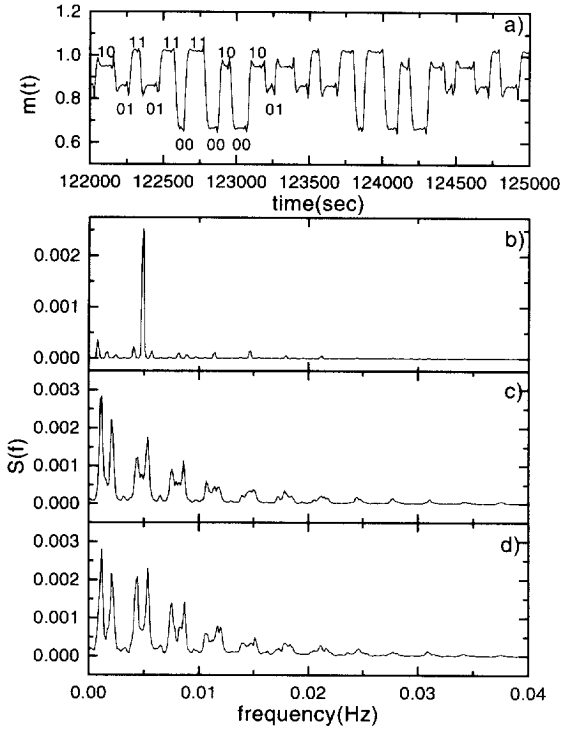

Fig. 5. A message is encoded onto a multistable solution of a controlled P_4 orbit, masked or modulated with a chaotic carrier $x(t)$ using Eqs. (15)–16 ($a = 0.2$, $\tau = 300$), and then transmitted. (a) The controlled multistable solution of P_4 in the DDE obtained from Eq. (6) with $a = 0.145$, $\tau = 300$, $T = 1225$ and $K = 0.05$, on which the message [10, 01, 11, 01, 11, 00, 11, 00, 10, 00, 10, 01] has been encoded [26]. (b) Power spectrum of the waveform in (a). (c) Power spectrum of the masked signal $s(t) = x(t) + 0.1m(t)$. (d) Power spectrum of the masked–modulated signal $s(t) = x(t)[1 + 0.1m(t)]$. Spectra are averages over 20 samples of 4096 points each with sampling time 3.75.

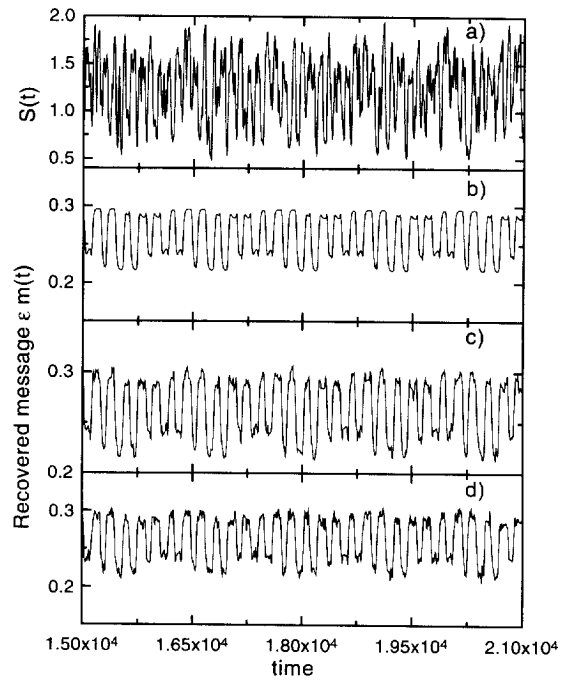

Fig. 6. Transmitting a message using MG DDE for $\tau = 300$, $a = 0.2$, $K = 0.1$, $\epsilon = 0.3$. (a) The transmitted signal $s(t) = x(t) + \epsilon m(t)$. (b) The recovered message $\epsilon m(t) = s(t) - y(t)$ using synchronization of $x(t)$ and $y(t)$. It is a periodic P_4 orbit ($a = 0.1365$) obtained from a piecewise constant initial function with three plateaus in the interval $(-\tau, 0)$. (c) The recovered message $\epsilon m(t)$ using parameter mismatch $a_1 = 0.2$ (transmitter) and $a_2 = 0.198$ (receiver). (d) The recovered message using additive zero-mean Gaussian white noise $\xi(t)$ to the message $s(t) = x(t) + \epsilon m(t) + \xi(t)$. The noise standard deviation is 0.005; the message $\epsilon m(t)$ has a standard deviation of 0.03. The transmitted signal $s(t)$ has mean 1.24 and standard deviation 0.35.

value can be specified by two bits; the map (or DDE at large delay) makes the values cycle as $11 \rightarrow 00 \rightarrow 10 \rightarrow 01 \rightarrow 11$. Actually, to minimize transients, the P_4 orbit was obtained with an initial function defined over $(-4\tau, 0)$, i.e. twelve ordinate values are specified for twelve bins: [10, 01, 11, 01, 11, 00, 11, 00, 10, 00, 10, 01] (see Ref. [26] for details). The last three pairs of bits, 00,10,01, correspond to the actual coded message (arbitrarily chosen). The preceeding three groups of two bits, 11, 00, 10, are the pre-images of 00, 10, 01 under the evolution of the map (i.e. 11 is the pre-image of 00, 00 is the pre-image of 10, and 10 is the pre-image of 01). The other preceeding six groups of two bits are assigned similarly. The message signal is very difficult to pick out in the transmitted signal spectrum in Figs. 5c (masking) en 5d (masking-modulation). Fig. 6b illustrates such a message once recovered from the transmitted signal shown in Fig. 6a; it is virtually identical to the original message (not shown).

4.5. Digital communication

We now show that the continuous-time difference equation (CTDE) obtained in the singular perturbation limit $R \rightarrow \infty$ of Eqs. (15) and (16) can be used for private communication in a digital rather than ana-

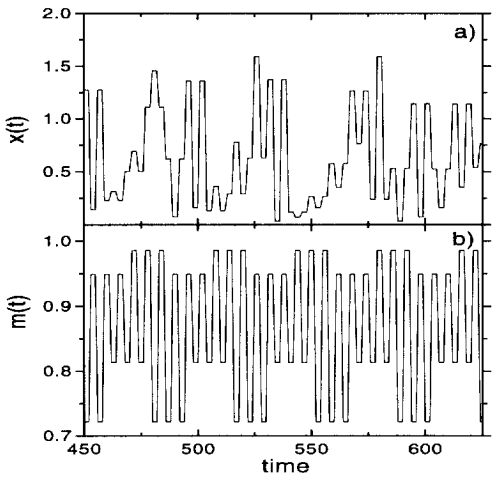

Fig. 7. Transmission of a digital message using chaotic synchronization of continuous-time difference equations with masking–modulation, Eq. (17) ($\epsilon = 0.1$, $\tau = 9$). (a) The transmitted signal. (b) The recovered short periodic message.

log mode. For constant initial functions, such CTDEs exhibit a series of plateaus which follow chaotic orbits. These plateaus are highly unstable; for example, they will not remain "plateaus" in the presence of noise. For example, the dynamics of the masking–modulation technique can be written as

$$x(t) = \frac{F(x(t-\tau))}{b - K\epsilon m(t)},$$

$$y(t) = \frac{1}{b+K}[F(y(t-\tau)) + Ks(t)], \qquad (17)$$

with $s(t) = x(t)[1 + \epsilon m(t)]$. As above, we choose $K = b$. The dynamics for the masking technique can be obtained similarly. If noise is a problem, the method can instead be used in a "map" mode rather than CTDE mode, where each plateau is replaced by only one value (in other words, time is discretized in units of τ, and only one state value is considered per delay interval). Fig. 7 illustrates the method. The digital message is a controlled multistable P_4 solution of the map with piecewise constant initial functions defined on three bins in the delay interval (as for the DDE in Section 4.4 above). The transmission and recovery of this digital message is done here using a masking–modulation (Eq. (17)) as in Section 4.3. We note that another study has reported synchronization and modulation of the singular limit map for the Ikeda equation using an approach as in Ref. [1] rather than that used here [37].

5. Robustness and unmasking

5.1. Parameter mismatch and noise

We now briefly discuss the effect of noise and parameter mismatch between transmitter and receiver on DDE synchronization and message recovery (see, e.g., Ref. [1]). The presence of many positive Lyapunov exponents would intuitively seem to require strict parameter matching and very small noise levels. Our tests show that the DDE synchronization schemes presented here can tolerate a certain level of noise and mismatch, but not too much. We have tested the effect of noise and mismatch on the recovery of the message shown in Fig. 6b (see Section 4.4). This is a stringent test, since the message is encoded onto a P_4 orbit of the DDE using three plateaus within one delay interval (the P_4 used here is actually a periodic orbit rather than a stabilized UPO; same conclusions apply for the stabilized UPO case). More noise and mismatch are tolerable for less complex messages, i.e. for messages that do not vary so quickly in time. Fig. 6c shows the effect of a 1.0% mismatch in the a parameter. It is clear that the basic message waveform with three plateaus per delay is recovered by synchronization; but a further increase in mismatch will make the recognition of the actual succession of plateau values seen in Fig. 6b significantly faulty.

Fig. 6d looks at the effect of additive Gaussian white noise on the message. The message-to-noise ratio is $0.03/0.005 = 6$, and the transmitted signal-to-message ratio is $0.35/0.03 = 11.6$ (note that $\epsilon = 0.3$). We have adjusted the noise standard deviation so that again we are at the limit of recovering the succession of plateau values without significant error. Nevertheless, the basic message waveform is recovered by synchronization as in the mismatch case above.

5.2. Unmasking

We now briefly discuss how dynamical techniques proposed in the recent literature may allow for the

reconstruction of the message without knowledge of the transmitter dynamics, a particular concern in the context of private communication. For example, the method of Short [38,39] applies a state-of-the-art nonlinear prediction algorithm (based on local neighborhood maps) to the signal in which the message is hidden. Predictions on a suitably embedded attractor are used to subtract away the chaotic component of the signal, thus revealing the message. This method has been shown to work well for the low-dimensional Lorenz system. Another method [40], which has also been illustrated on the Lorenz system, uses the fact that the return maps of successive extrema in the time series are shifted when the hidden binary message goes from one state to the other. The application of these techniques to our proposed schemes based on hyperchaotic DDEs and their multistability is beyond the scope of our study, and will be discussed elsewhere. Nevertheless, one can speculate on the success such techniques may have in intercepting the message.

An important condition for the success of nonlinear prediction based on neighborhood maps is that the message only mildly affect the tangent space of the chaotic attractor. These techniques are increasingly difficult to apply as the attractor dimension and metric entropy increase, especially if the data set is limited. It has been shown [41] that nonlinear prediction error scales as $e^{kT_p}N^{-1/D_a}$ where D_a is the attractor dimension, k is the metric entropy, T_p is the prediction time into the future, and N the number of data points. Thus, short data sets containing a message, such as those used here for encoding with UPOs, are difficult to predict if D_a is high; one reason is that more points are required to fill higher-dimensional spaces. Nevertheless, it is usually the case that certain parts of the attractor are more easily reconstructed, such as where the local dimension and Lyapunov exponents are low.

Related issues for successful nonlinear prediction are the disentanglement of trajectories and the proper identification of neighbors. For the chaotic DDE carrier in Section 4 ($\tau = 300$), an application of the false nearest neighbor technique (FNN) [42] may reveal whether good embeddings of the scalar time series can be obtained in the first place. The idea behind the FNN method is to calculate the percentage of neighbors of points in the embedding space which are false, i.e. which do not remain "close" upon going from embedding dimension D_e to $D_e + 1$. This percentage is

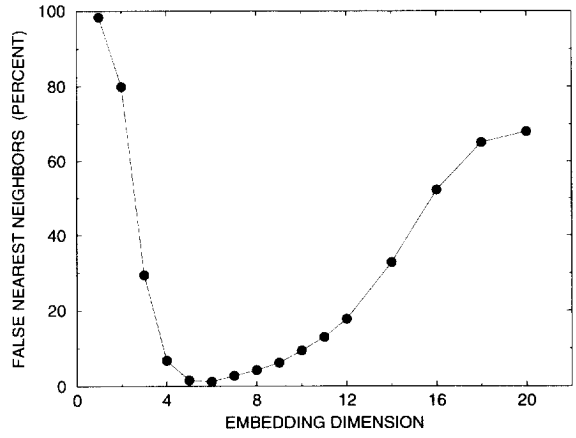

Fig. 8. Percentage of false nearest neighbors as a function of embedding dimension for a chaotic solution of Eq. (5) without a message. The 20 000 point time series was obtained from numerical integration of Eq. (5) with $\tau = 300$ s, an integration time step of 0.01 s, and output every 1.0 s. An embedding delay of 300 s was used; two points in the embedding space whose components were less than 100 s apart in time were discarded as potential nearest neighbors. The algorithm used is described in Ref. [42], with $R_{tol} = 10.0$ and $A_{tol} = 2.0$.

then charted as a function of embedding dimension.

An FNN calculation using the technique in Ref. [42] for our DDE carrier (without a message) with 20 000 points is presented in Fig. 8. The embedding delay T_e used to construct vectors $(x(t), x(t-T_e), x(t-2T_e), \ldots, x(t-(D_e-1)T_e))$ from $x(t)$, was set to $T_e = 300 = \tau$, a natural choice since the singular map (with time discretized in units of τ) is relevant to the understanding the DDE dynamics. For other values of T_e and sampling times of the solution chosen, we have found similar results to those shown in Fig. 8; we chose to show the results for the case yielding the lowest percentage of FNNs over the range of D_e explored. One finds that there is a range of embedding dimensions (5–8) where the percentage of FNNs is low (a minimum at 1.2% for $D_e = 6$), but it does not get any closer to zero. Also, the percentage of FNN increases monotonically for $7 < D_e < 20$, in contrast to the behavior for low-dimensional systems [42], for which the percentage remains very close to zero. More data points would be needed to properly calculate the percentage of FNNs for $D_e > 20$.

A cautious interpretation of this result is that the attractor dimension varies according to the position on

the attractor (i.e. it is a multifractal), as Lyapunov exponents do. This multifractal aspect has been discussed in Ref. [29]. That study further reports that the prediction errors from a genetic algorithm for $\tau = 150$ and $\tau = 30$ (other parameters are as in our study) were surprisingly not very different, but that the $\tau = 150$ case required that more constraints be put on which past states to use for the prediction. This result is possibly linked to the relatively constant metric entropy at large delays. Hence, embedding in 5 to 8 dimensions may reveal the main dynamical features of the attractor. Yet it is likely that finer structure would be missed by a nonlinear prediction algorithm operating on such embedded data.

It remains an interesting open question, whether methods such as those in Refs. [38,39] will nevertheless accurately reconstruct the dynamics to allow for message recovery. More work is also needed to verify the accuracy of nonlinear prediction algorithms for DDEs at large delay. We should point out that previous such attempts have made use of large embedding dimensions for smaller delays than those used here ($D_e = 18$ for $\tau = 100$ in Ref. [41]; $D_e = 50$ for $\tau = 150$ in Ref. [29]; $D_e = 17$ for $\tau = 100$ in Ref. [43]; other equation parameters are the same as here). It also remains to be seen whether the spectral filtering used to separate message and carrier frequencies can be applied to the messages encoded on UPOs of the DDE as proposed in our study, since both have similar spectral features.

Finally, the work of Bünner et al. [44] might be useful to unmask signals masked by DDE chaos. Their technique relies on plots of dx/dt versus $x(t)$ and $x(t-\tau)$, all of which can be obtained from an available signal $x(t)$ (the derivative is numerically estimated). By scanning through values of τ, one can find a value for which the plot neatly falls on the surface $dx/dt(x(t), x(t-\tau))$ determined by the dynamical equations Eqs. (4).

6. Conclusion

In summary, we have shown that the chaotic motion of first-order delay-differential equations and of finite-order distributed delay systems can be unidirectionally synchronized through a negative feedback type of coupling involving only one scalar variable, namely the state variable itself. This synchronization occurs despite the existence of a large number of positive Lyapunov exponents and the high dimensionality of the attractor. We have also achieved DDE synchronization with parametric feedback instead of additive feedback (not shown). Synchronization also occurs in the presence of small amounts of noise or small superimposed information-carrying signals. This makes delay-differential systems appealing for broadband masking applications such as chaos communication. This is especially true when one takes adantage of the multistability feature of these DDEs at large delays. Messages can then be encoded onto stable periodic orbits, or onto controlled unstable periodic orbits of the same kind of DDE dynamics used for the chaotic masking. In this case, the power spectrum of a message-carrying waveform blends in to that of the chaos.

More work is needed to fully quantify the sensitivity of the synchronization to parameter mismatch and noise, and to ensure, in the case of chaos communication, that dynamical unmasking techniques fail. Our results show that synchronization and message recovery can, in the schemes presented, tolerate only a small parameter mismatch ($\approx 3\%$), or Gaussian noise having a standard deviation less than $\approx 33\%$ of the message standard deviation. This sensitivity is presumably a consequence of the attractor invariants and of the coupling schemes studied. Future work should focus on other forms of feedback coupling, such as integral feedback, or feedback based on the system state at many previous times. Another possiblity is of course to choose other DDEs, such as the Ikeda system. Certain parameter choices make the intrinsic feedback function $F(x(t-\tau))$ for this system multipeaked rather than unimodal as for the MG DDE, with the result that the chaotic solutions have statistics very similar to those of nonlinear Langevin equations [45].

Our results also suggest that properly coupled DDE response systems can synchronize to noise as well as any chaotic behavior present in a "drive" system. Thus, aperiodic behavior of deterministic or stochastic origin in one delayed feedback system can entrain the motion of similar systems to which it is unidirectionally coupled. This is relevant to the study of single or multi-loop feedback systems with fixed or distributed delays, such as those occurring in physiology [27,46] and neurobiology [28,47,48]. Future work will also focus on the extension of our results to bi-directional

synchronization of mutually coupled delayed feedback systems.

Acknowledgement

This research was supported by NSERC Canada as well as by a Canadian International Development Agency fellowship to BM.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] N.F. Rul'kov, A.R. Volkovskii, A. Rodriguez-Lozano, E. Del Rio, M.G. Velarde, Int. J. Bif. Chaos 2 (1992) 669.
[3] M.G. Rosenblum, A.S. Pikovsky, J. Kurths, Phys. Rev. Lett. 78 (1997) 4193.
[4] K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[5] L. Kocarev, U. Parlitz, Phys. Rev. Lett. 74 (1995) 5028.
[6] U. Parlitz, L. Kocarev, T. Stojanovski, H. Preckel, Phys. Rev. E 53 (1996) 4351.
[7] N. Gershenfeld, G. Grinstein, Phys. Rev. Lett. 74 (1995) 5024.
[8] M.K. Simon et al., Spread Spectrum Communications Handbook (McGraw-Hill, New York, 1994).
[9] L.M. Pecora, T.L. Carroll, Phys. Rev. A 44 (1991) 2374.
[10] K. Pyragas, Phys. Lett. A 181 (1993) 203.
[11] K. Pyragas, Phys. Lett. A 170 (1992) 421.
[12] A. Kittel, K. Pyragas, R. Richter, Phys. Rev. E 50 (1995) 262.
[13] T.C. Newell, P.M. Alsing, A. Gavrielides, V. Kovanis, Phys. Rev. E 49 (1994) 313.
[14] Y. Hun Yu, K. Kwak, T.K. Lim, Phys. Lett. A 191 (1994) 233.
[15] A. Volkovskii, Sov. Tech. Phys. Lett. 15 (1989) 249.
[16] J.F. Heagy, T.L. Carroll, L.M. Pecora, Phys. Rev. E 50 (1994) 1874.
[17] M. Ding, E. Ott, Phys. Rev. E 49 (1994) 945.
[18] J.H. Peng, E.J. Ding, M. Ding, W. Yang, Phys. Rev. Lett. 76 (1996) 904.
[19] J.H. Xiao, G. Hu, Z. Qu, Phys. Rev. Lett. 77 (1996) 4162.
[20] J.D. Farmer, Physica D 4 (1982) 366.
[21] S. Lepri, G. Giacomelli, A. Politi, F.T. Arecchi, Physica D 70 (1993) 235.
[22] D.E. Sigeti, Physica D 82 (1995) 136.
[23] B. Mensour, A. Longtin, Physica D 113 (1998) 1.
[24] J. Losson, M.C. Mackey, A. Longtin, Chaos (1993) 167.
[25] A. Namajunas, K. Pyragas, A. Tamasevicius, Phys. Lett. A 201 (1995) 42.
[26] B. Mensour, A. Longtin, Phys. Lett. A 205 (1995) 18.
[27] M.C. Mackey, L. Glass, Science 197 (1977) 287.
[28] C. Lourenço, A. Babloyantz, Neural Comput. 6 (1994) 1141.
[29] T.P. Meyer, N.H. Packard, in: Nonlinear Modeling and Forecasting, eds. M. Casdagli, S. Eubank, (Addison-Wesley, Redwood City, CA, 1992), p. 249.
[30] J.P. Eckmann, D. Ruelle, Rev. Mod. Phys. 57 (1985) 617.
[31] H.D.I. Abarbanel, R. Brown, M.B. Kennel, J. Nonlinear Sci. 2 (1992) 343.
[32] D. Fargue, Réducibilité des systèmes héréditaires à des systèmes dynamiques (régis par des équations différentielles aux dérivées partielles), C.R. Acad. Sci. Paris T. 277, No. 17 (Série B, 2e semestre) (1973) 471.
[33] K.L. Cooke, Z. Grossman, J. Math. Anal. Appl. 86 (1982) 592.
[34] D.W. Jordon, P. Smith, Nonlinear Ordinary Differential Equations, 2nd ed. (Oxford University Press, New York, 1987).
[35] R. He, P.G. Vaidya, Phys. Rev. A 46 (1992) 7387.
[36] H.D.I. Abarbanel, P.S. Linsay, IEEE Trans. Circuits Syst. II 40 (1993) 643.
[37] P. Celka, IEEE Trans. Circ. Syst. 42 (1995).
[38] K.M. Short, Int. J. Bifurc. Chaos 4 (1994) 959.
[39] K.M. Short, Int. J. Bifurc. Chaos 6 (1996) 367.
[40] G. Pérez, H.A. Cerdeira, Phys. Rev. Lett. 74 (1995) 1970.
[41] J.D. Farmer, J.J. Sidorowich, Phys. Rev. Lett. 59 (1987) 845.
[42] M.B. Kennel, R. Brown, H.D.I. Abarbanel, Phys. Rev. A 45 (1992) 3403.
[43] M. Casdagli, Physica D 35 (1989) 212.
[44] M.J. Bünner, M. Popp, Th. Meyer, A. Kittel, J. Parisi, Phys. Rev. E 54 (1996) R3082.
[45] M. LeBerre, E. Ressayre, A. Tallet, Y. Pomeau, Phys. Rev. A 41 (1990) 6635.
[46] L. Glass, C.P. Malta, J. Theor. Biol. 145 (1990) 217.
[47] P.C. Bressloff, Phys. Rev. A 50 (1994) 2308.
[48] J. Foss, A. Longtin, B. Mensour, J.G. Milton, Phys. Rev. Lett. 76 (1996) 708.