Integrated chaotic communication scheme

Murilo S. Baptista
Institute of Physics, University of São Paulo, P.O. Box 66318, CEP 05315-970, São Paulo, São Paulo

Elbert E. Macau
INPE, Brazilian Institute for Space Research, P.O. Box 515, CEP 12227-010, São José dos Campos, São Paulo

Celso Grebogi
Institute for Plasma Research, Department of Mathematics, University of Maryland, College Park, Maryland 20742

Ying-Cheng Lai
Departments of Mathematics and Electrical Engineering, Arizona State University, Tempe, Arizona 85287-1804

Epaminondas Rosa, Jr.
Department of Physics, University of Miami, Coral Gables, Florida 33146
(Received 18 October 1999; revised manuscript received 2 May 2000)

We present the characteristics and an analysis of a proposed communication scheme fully based on chaos theory. The key point is that the proposed scheme introduces the dynamical system as a way to encode and decode information and as a signal wave generator. In this scheme, all the protocols used to communicate digitally are fully integrated into one single design based on a chaotic modulation process. The chaotic encoder finds a set of trajectories that codes the information into a hard to decode chaotic wave form that carries a large amount of information. We also show how our scheme can handle multiplexing, which is also used as a way to enhance security, and its ability to handle noise.

PACS number(s): 05.45.Vx, 05.45.Gg, 01.20.+x

I. INTRODUCTION

The idea of using chaos as a fundamental building block for constructing communication systems appeared in Ref. [1]. In that work, the authors manipulated a chaotic system, using arbitrarily small time-dependent perturbations, to generate controlled chaotic orbits whose symbolic representation corresponds to the digital representation of a desirable message. Subsequently, this idea was experimentally demonstrated in the scope of an electronic circuit, as reported in Ref. [2]. Recent works, aiming to implement more efficient chaotic-based communication systems, dealt with the synchronization of chaotic trajectories [3], noise filtering from noisy chaotic trajectories [4], chaotic error correcting codes [5], chaos coding [6], and cryptography with chaos [7].

The fundamental argument that has been emphasized about using chaotic-based communication system is its efficiency. In fact, a nonlinear chaotic oscillator that generates a wave form for transmission can be easily built, while all the electronics that is necessary for encoding the information in the chaotic signal remains as a low-power and inexpensive microelectronic circuit. However, so far, it appears that the full meaning of the word ''efficiency'' characterizing the use of chaos for communication is not well understood and fully appreciated.

The purpose of this paper is to show a communication system that uses chaos for performing the main tasks that are expected nowadays from a digital communication system. In fact, more than sending information through a communication channel, a digital communication system must also perform the following two fundamental functions: (i) *source encoding*, which compacts, compresses, and encrypts the source message; and (ii) *channel encoding*, which guarantees that the encoded message is robust against the presence of noise in the channel. Both operations encode one bit stream into another. In a standard digital communication scheme, each of these functions is not only accomplished by different subsystems, but, cumbersomely, the final sequence of bits must be modulated *a posteriori* into a wave form signal that can be adequately transmitted over a channel. This complex and involved scenario can be radically simplified if the communication system is based on chaos instead. All those functions and operations can be performed with the use of only one subsystem, the same one that performs the proper modulation of the signal for transmission over the communication channel. Thus we propose a communication system that inherits the most important advantages of both analog and digital communication systems: simplicity and efficiency (as in the digital system, our communication scheme can transmit information that is compacted, hard to decode, and robust against noise). This integrated communication scheme is attainable especially because a chaotic signal exhibits a kind of short memory that can be exploited to create a scheme where the coding and decoding protocols is not performed in the source but rather in the wave signal. So the signal is not only the carrier but also the message itself.

We now present our scenario of an integrated chaotic communication scheme which uses chaotic dynamics *per se* as a means to address standard communication issues such as encoding, noise reduction, compaction, and so on. For the sake of clarity, the results shown here are derived from a mapping. We assume that this mapping represents the dy-

namics of a chaotic trajectory, obtained from a flow, in a Poincaré section. Thus, from the discrete trajectory, there must exist a continuous trajectory that lies in a higher-dimensional space connecting every point of this mapping in the corresponding section (suspension [8]). Thus, from now on, a chaotic wave signal is, in fact, a set of points obtained through a discreting process (a mapping) of the higher-dimensional continuous trajectory, a trajectory which is the wave signal used to transmit information over a channel.

To find the coding trajectories on which information is sent, we could define a partition of the phase space as done in Ref. [2]. However, we would have to deal with symbolic forbidden transitions, a limitation that is typical in real chaotic dynamical systems. To overcome this limitation, we would need to implement an extra protocol in the communication scheme, a dynamical encoding, as done in Ref. [2], such that the message can be coded into a set of feasible trajectories. Instead, in this work, we look for a dynamical partition for which the coding trajectories, obtained from it, carry a large amount of information efficiently, are hard to decode, and are robust against channel noise. This is all achieved by using a new dynamical partition of the phase space, whose construction is based on the source message itself, and not on the dynamical system as in Ref. [1].

In traditional communication, to make the transmission robust against the presence of noise in the channel, a process that adds redundant information into the encoded source message used. In our proposed scheme, to make the transmission of chaotic signal robust against noise, the length of the coding trajectories must have a minimum length. The determination of the appropriate trajectory length is what we define to be the *chaotic dynamical channel encoder*. Therefore, we create wave signals that carry not only the message itself, but also the dynamic information from which the wave form, in the presence of dropouts and/or transmission noise, can be reconstructed. The length of each trajectory depends on some quantities that we will describe below.

This paper is organized as follows. In Sec. II, we present the proposed integrated scheme. In Sec. III, we describe how to implement this method by giving an example. In Sec. IV, we introduce the notion of entropy to compare this method with a traditional digital system. In Sec. V, we discuss some relevant properties of the proposed method regarding the changing of parameters to adjust the proposed system to function as aimed. In Sec. VI, we discuss the use of this method when a low noise level is present in the channel, and, in Sec. VII, we describe the implementation of a channel dynamical encoder which must be used when there is high noise level in the channel. Finally, in Sec. VIII, we make some general remarks regarding communication with chaos.

II. PROPOSED INTEGRATED COMMUNICATING SCHEME

In this section, we present our ideas by introducing the following communication system. We consider an information source that is modeled by a discrete-time random process $\{X_i\}_{i=-\infty}^{\infty}$, where all X_i's are independent and identically distributed random variables taking values on a discrete set. The source is, therefore, considered to be a *discrete memoryless source* (d.m.s), which means that it is a discrete-time discrete-amplitude random process. Let $\mathcal{S}=\{s_1,s_2,\ldots,s_N\}$ be the *alphabet* set in which the random variable X takes its values, and let the probability mass function for the discrete random variable X be denoted by $p_i=p(X=s_i)$ for all $i=1,2,\ldots,N$. We define as the *message* M or the *information sequence* M an ordered and finite sequence of outputs of the random variable X which is to be transmitted between the source and the destination, or receiver, by using a communication system.

A communication system must perform the following tasks: (a) To convert the information sequence to another more efficient form of representation in order to transmit to the receiver. (b) To introduce redundancy in the information sequence that can be used at the receiver to overcome the effects of noise and other interferences faced by the signal during the transmission over the communication channel. (c) To map the message into a signal wave form that can be properly sent through the communication channel. (d) To recover at the receiver the information sequence that was generated at the source. In this paper, we consider a communication system that codes the information into a hard to break chaotic wave form, robust against noise, and carrying a large amount of information. Our communication system codifies the information sequence on chaotic trajectories of a flow. Furthermore, we assume that we can define a Poincaré section transversal to this flow so that the system dynamics of the flow is well represented by a discrete map on this Poincaré section. We represent an iteration of this Poincaré map as

$$x_{i+1}=F(x_i). \tag{1}$$

Let us assume that we are given a typical message $M=\{m_0,m_1,\ldots,m_{l-1}\}$, $m_i\in S$, where l is large enough so that M_l can be regarded as a good approximation of a *typical sequence* [9] of the information source that we are considering, and $l\gg N$. In fact, it is known that, for l large enough, with a probability approaching 1, every sequence from the source is a typical sequence, i.e., it has the same composition. Consider an arbitrary and fixed initial condition x_0^* that is used to create a trajectory $T_{x_0^*}=\{x_0^*,x_1^*,\ldots,x_{l-1}^*\}$ of length l as a result of $l-1$ iterations of the chaotic map F. The initial condition x_0^* is not necessarily in the invariant chaotic set A. Let us introduce a fixed parameter ϵ so that, to each point x_i^* of the trajectory we associate a hypercube $\beta(x_i^*,\epsilon)$ with center in x_i^* and edge length 2ϵ. Note that since F is *ergodic* on A, the sequence $B(x_0^*,l,\epsilon)=\{\beta(x_0^*,\epsilon),\beta(x_1^*,\epsilon),\ldots,\beta(x_{l-1}^*,\epsilon)\}$ covers part of A for some $l>l_{lm}(\epsilon)$. Given $B(x_0^*,l,\epsilon)$, we consider a subsequence $B_p(x_0^*,l,\epsilon)$ of $B(x_0^*,l,\epsilon)$, so that $\beta(x_i^*,\epsilon)$ does not intersect the previous hypercubes $\beta(x_j^*,\epsilon)$, $j<i$, in the subsequence, i.e., $\beta(x_i^*,\epsilon)\cap\beta(x_j^*,\epsilon)=\varnothing$, for $j<i$. Thus we have

$$B_p(x_0^*,l,\epsilon)=\{\beta(x_{i_1}^*,\epsilon),\beta(x_{i_2}^*,\epsilon),\ldots,\beta(x_{i_q}^*,\epsilon)\}, \tag{2}$$

where one has $q\leqslant l-1$ for sufficiently small ϵ. We introduce a parameter r such that in the sequence $\{x_{i_1}^*,x_{i_2}^*,\ldots,x_{i_q}^*\}$ [the points that are located in the center of the hypercubes of the subsequence $B_p(x_0^*,l,\epsilon)$], $F(x_{i_{k-1}}^*)=x_{i_k}^*$ for $(n-1)r$

$<k\leqslant(n)r$, with $(n=1,2,3,\ldots,q/r)$, but $x^*_{i_{(nr+1)}}$ is not necessarily the forward iteration of $x^*_{i_{nr}}$. Thus, if $r=2, i_2=i_1+1$, and $i_4=i_3$, by definition $i_1=0$, so that $\beta(x_0^*,\epsilon)$ corresponds to the letter m_0 of the message. We say that $B_p(x_0^*,l,\epsilon)$ creates a *pseudopartition* of part of A, which is associated with the units s_i of the alphabet S. Now we associate the message M with $B_p(x_0^*,l,\epsilon)$ by doing the following: for each k from 1 to q, the hypercube $\beta(x^*_{i_k},\epsilon)$ is associated to the letter m_k of the message M. Note that at the end of this procedure we can have the unit $s_i\in S$ associated to many hypercubes of $B_p(x_0^*,l,\epsilon)$. This happens because the set S has only N units s_i, where $N\ll l$. Consequently, as a result of this process we have N subsets P_i, one for each unit of S, where each P_i is formed by the union of the hypercubes $\beta(x^*_{i_k},\epsilon)$ that are associated with the specific unit s_i of S. Thus we create a topological correspondence among the units of the alphabet and the disconnected regions of the invariant chaotic set A.

The preceding paragraph defines formally how to construct the pseudopartition. Such a description might be difficult to understand, so now we present a simple example on how to find such a pseudopartition, say, for $r=2$. Given the initial condition x_0^*, if $x_1^*=F(x_0^*)$ is such that $\beta(x_1^*,\epsilon)$ does not intersect the hypercube $\beta(x_0^*,\epsilon)$, we say that $\beta(x_0^*,\epsilon)$ belongs to the pseudopartition that encodes for the unit s_i, corresponding to the first letter of the message M, which is m_0, and $\beta(x_1^*,\epsilon)$ encodes for m_1. We note that in this case the indexes i_q's are $i_1=0$ and $i_2=1$. Then we iterate x_1^*, obtaining x_2^*. Now two cases must be considered: (1) if x_2^* is such that $\beta(x_2^*,\epsilon)$ does not intersect the hypercubes $\beta(x_0^*,\epsilon)$ and $\beta(x_1^*,\epsilon)$, and $\beta(x_3^*,\epsilon)$ does not intersect all these previous hypercubes, from the previous iterations, then we say that $\beta(x_2^*,\epsilon)$ encodes for m_2, and $\beta(x_3^*,\epsilon)$ codes for m_3. (2) If either $\beta(x_2^*,\epsilon)$ or $\beta(x_3^*,\epsilon)$ intersects the previous hypercubes, then the hypercubes $\beta(x_2^*,\epsilon)$ or $\beta(x_3^*,\epsilon)$ are discarded, and we look for hypercubes $\beta(x_n^*,\epsilon)$ (for $n>3$) that code for the next two ($r=2$) elements of the message M, namely, m_4 and m_5, using the algorithm proposed in case (1). One might say that the letters of messages m_2 and m_3 will not be encoded by our method. We can, however, guarantee that for ϵ not too high, eventually the pair (m_2,m_3) will be encoded by a pair of hypercubes $\beta(x^*_{i_q},\epsilon)$ and $\beta(x^*_{i_{q+1}},\epsilon)$, where i_q will be different from 2 and i_{q+1} will be different from 3. We can also guarantee that, for ϵ not too high, each other pair m_k and m_{k+1} will also be encoded by a pair of hypercubes.

Considering this framework, we now explain how an arbitrary message $M=\{m_0,m_1,\ldots,m_{M-1}\}$ can be codified in a chaotic trajectory. Given this message, we decompose it into consecutive subsequences of r symbols. The value of r, once chosen, remains the same during the operation of the communication system. Some major properties associated with communication systems depend on it, as it will be discussed below. Thus

$$M=M_0\oplus M_1\oplus\cdots\oplus M_{j-1}, \tag{3}$$

where $\oplus$ stands for a concatenation operation, and $M_0=\{m_0,\ldots,m_{r-1}\}$, $M_2=\{m_r,\ldots,m_{2r-1}\}$, and so on. Note that all the subsequences have the same length. If the last subsequence does not have r letters, dummy letters must be added. Suppose that the chaotic trajectory is initially at a point x_0'. We take a unit that corresponds to the letter m_0, say s_j, and look in the subset P_j for some hypercube $\beta(x_{i_k},\epsilon)$ near x_0'. The $r-1$ subsequent iterations of x_{i_k} belong to hypercubes that are associated with the subsequent $r-1$ letters of M_1 in the same order. This procedure generates the trajectory T_1 that codifies the submessage M_1. We repeat the same procedure for M_2, this time having as the initial condition the rth forward iteration of the point x_0'. As a result of this concatenation procedure, trajectories T_i, each with r points, are associated with each the M_i submessages. The forward iteration of the last point of a given trajectory T_i is near to the first point of the subsequent trajectory T_{i+1}. This means that small perturbations are enough to concatenate all the i trajectories corresponding to the i messages. Furthermore, for each trajectory T_i, just its initial condition is enough to generate all the subsequent $r-1$ points of the trajectory. In other words, for each submessage M_i, only the point associated with its first letter needs to be known. The other subsequent $r-1$ symbols of the message M_i appear as a result of the natural dynamical evolution of the chaotic system with the proper initial condition.

To recover the message emitted by the source, the receiver needs to know the dynamical system and its parameters, the value of r, and the fixed initial condition x_0^* which generates the N subsets P_i of the pseudopartitions. Each pseudopartition is associated with a unit s_i of the alphabet S. The receiver decodes the message by identifying the chaotic trajectory with the available information provided by the pseudopartitions P_i. Furthermore, only the initial condition of each trajectory T_i needs to be sent over the communication channel. This means, (and this is quite important) that for each set of r symbols produced by the information source, only one value—the initial condition—needs to be sent over the communication channel in order to recover the message.

III. EXAMPLE OF AN INTEGRATED COMMUNICATION SYSTEM

To illustrate our communication method, we consider an information source to be a *discrete memoryless source*, as defined previously, which means that it is a discrete-time discrete-amplitude random process. Let $S=\{s_1,s_2,s_3,s_4\}$ be an alphabet set composed of four units on which the random variable X takes its values, and let the probability mass function for the discrete random variable X be denoted by $p_i=p(X=s_i)$ with, say, the following values: $p_1=\frac{1}{2}$, $p_2=\frac{1}{4}$, $p_3=\frac{1}{8}$, and $p_4=\frac{1}{8}$. The chaotic mapping F we use to codify the information sequence in its chaotic trajectories is the logistic map

$$x_{i+1}=F(x_i)=bx_i(1.0-x_i), \tag{4}$$

where we choose $b=4.0$. In this case, the hypercubes $\beta(x_i^*,\epsilon)$, generated from an arbitrary and fixed initial condition x_o^*, are the intervals $[x_i^*-\epsilon, x_i^*+\epsilon]$, where the parameter ϵ is fixed. Starting from a typical sequence M_l of the information source with $l\gg N$, and considering an arbitrary

x_o^*, we obtain the pseudopartition, P_j (with $j=1,\ldots,4$) associated with the corresponding units s_j. Each pseudopartition P_j is composed of a collection of intervals, constructed by the following criteria: From the chosen initial condition x_0^*, we generate the sequence $B(x_0^*,\epsilon)=\{\beta(x_0^*,\epsilon),\beta(x_1^*,\epsilon),\beta(x_2^*,\epsilon),\beta(x_3^*,\epsilon),\beta(x_4^*,\epsilon),\beta(x_5^*,\epsilon),\ldots\}$, which corresponds to the intervals $\{[x_0^*-\epsilon,x_0^*+\epsilon],[x_1^*-\epsilon,x_1^*+\epsilon],[x_2^*-\epsilon,x_2^*+\epsilon],\ldots\}$. However, due to overlapping of the intervals β, the subsequence $B_p(x_0^*,\epsilon)$ is created. Let us say, that $B_p(x_0^*,\epsilon)=\{\beta(x_0^*,\epsilon),\beta(x_1^*,\epsilon),-,-,\beta(x_4^*,\epsilon),\beta(x_5^*,\epsilon),\ldots\}$, where the $-$ represents the intervals that overlaps with the previous ones: $\beta(x_0^*,\epsilon)$ and $\beta(x_1^*,\epsilon)$. The typical message M with which we create the pseudopartition is, say, $\{s_1\ s_2\ s_4\ s_1\ s_2\ s_4\ldots\}$. The nonoverlapping intervals of B_p are associated with the message in the following way: m_0 is associated with $\beta(x_0^*,\epsilon)$, m_1 is associated with $\beta(x_1^*,\epsilon)$, m_4 is associated with $\beta(x_4^*,\epsilon)$, and m_5 is associated with $\beta(x_5^*,\epsilon)$. Note that in this example m_2 and m_3 are not associated with any interval β. However, for ϵ sufficiently small, the sequence B_p will eventually have two intervals that can be associated with the pair of letters $(m_2\ m_3)=(s_4\ s_1)$. By definition, the pseudopartition P_j is composed by the intervals of B_p associated with the unit s_j. Thus P_1 is composed of $\{\beta(x_0^*,\epsilon),\ldots\}$, P_2 is composed of $\{\beta(x_1^*,\epsilon),\beta(x_4^*,\epsilon)\ldots\}$, P_3 is composed of $\{,\ldots\}$ (there is not any unit s_3 in M), and P_4 is composed of $\{\beta(x_5^*,\epsilon),\ldots\}$.

Once the pseudopartitions are created, we use them to construct the set of trajectories that encodes the message. In this example, we subdivide the message into consecutive subsequences of two letters each, i.e., we use $r=2$. This implies that every two letters of the message are coded in a two-point trajectory $T_i=\{y_1^i\ y_2^i\}$, where only y_1^i needs to be transmitted. Following our method, in order to find a coding trajectory T_i, we assume that the message M' consists of two pairs of letters, say, $\{s_1\ s_2\ s_2\ s_4\}$, and that the chosen initial condition for the encoding process is x_0'. We look in the pseudopartition for a pair of intervals $[x_n^*-\epsilon,x_n^*+\epsilon]$ and $[x_{n+1}^*-\epsilon,x_{n+1}^*+\epsilon]$ associated with the pair of letters $\{s_1\ s_2\}$. Preferably, we pick the interval that has $x_n^*\approx x_0'$. For the sake of simplicity, we say that $x_0'=x_0^*$. Thus the first pair of letters is encoded by the point $y_1^0=x_0^*$ and the second pair of letters is encoded by $y_1^1=x_n^*$ such that $x_n^*\approx F^2(x_0')$. In general, we code the pair of letters i by a point $y_1^i=x_n^*\approx F^{2(i-1)}(x_0')$.

The coding trajectories are concatenated together to form the signal that is sent over the channel with the information. The concatenated trajectory $\{\ldots,T_i,T_{i+1},\ldots\}$ shadows the trajectory $T_{x_0^*}$ that was used to construct the pseudopartitions P_i. However, any other trajectory obtained from an arbitrary initial condition x_0' could be used. In Fig. 1 we show the trajectory $T_{x_0^*}$ in squares and, in circles, the concatenated trajectory that encodes the message to be transmitted. As we already pointed out, both trajectories are close to each other, which makes it very hard for an intruder to decode them [7,5]. Furthermore, this characteristic reinforces the claim that communication with chaos requires the introduction of a minimum amount of energy (just the imposition of perturbations) to codify the message [2,1].

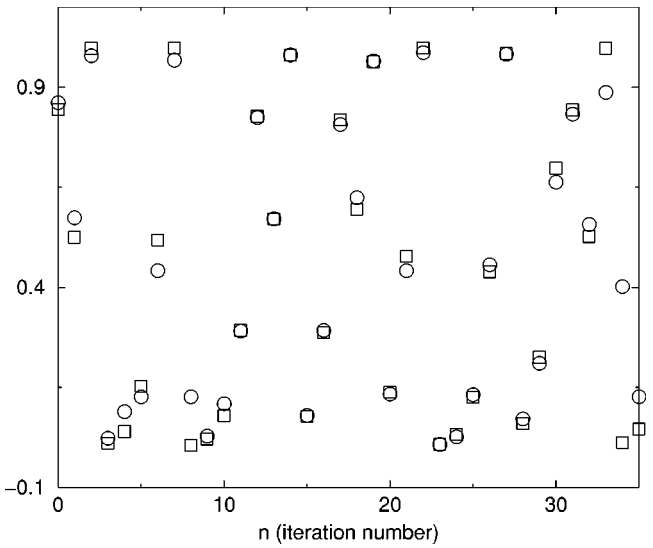

FIG. 1. The concatenated coding trajectory T' in circles, and a trajectory $T_{x_0'}$ in squares for $\epsilon=0.015$.

For $\epsilon=0.0015$, Table I shows a portion of the message to be transmitted (second column), $M'=\{\ldots s_1\ s_1\ s_4\ s_1\ldots\}$. Part of the trajectory $T_{x_0^*}=\{x_0^*,x_1^*,\ldots,x_{l-1}^*\}$ that was used to compute the pseudopartition P_i is shown in the first column, while part of the coding trajectory associated with M' appears in the third column. Remember that just the points y_1^i and y_1^{i+1} are sent over the communication channel to the receiver. Note how the concatenated trajectory $T'=\{\ldots,y_1^i,y_2^i,y_1^{i+1},y_2^{i+1},\ldots\}$ associated with the message M' differs slightly from $T_{x_0^*}$. The trajectories $T_{x_0^*}$ and T', with intervals corresponding to the pseudopartition P_i, are shown schematically in Fig. 2.

IV. ENTROPY OF THE COMMUNICATION METHOD

To compare our proposed communication method with a conventional digital communication method, we use the number of wave signals needed to transmit a message M' in both systems. In the conventional communication scheme, one bit is transmitted using one wave signal modulation. Here we are not adding the redundancy that is typically built in. The number of bits needed to transmit one unit of the message M' is given by the entropy [10]

$$H(S)=\sum_{i=1}^{4} p_i \ln_2\left(\frac{1}{p_i}\right), \tag{5}$$

TABLE I. Coding trajectory $\{y_1^1\ y_1^2\}$ for the message $\{s_1\ s_1\ s_4\ s_1\}$.

Trajectory (partition)	M'	Coding trajectory (partition)
$x_1=0.459028082\ (P_1)$	s_1	$y_1^1(\approx x_1)=0.432921630\ (P_1)$
$x_2=0.993285208\ (P_2)$	s_1	$y_2^1=F(y_1^1)=0.982001969\ (P_1)$
$x_3=0.026678815\ (P_2)$	s_4	$y_1^2(\approx x_3)=0.004890917\ (P_4)$
$x_4=0.103868222\ (P_1)$	s_1	$y_2^2=F(y_1^2)=0.019467984\ (P_1)$

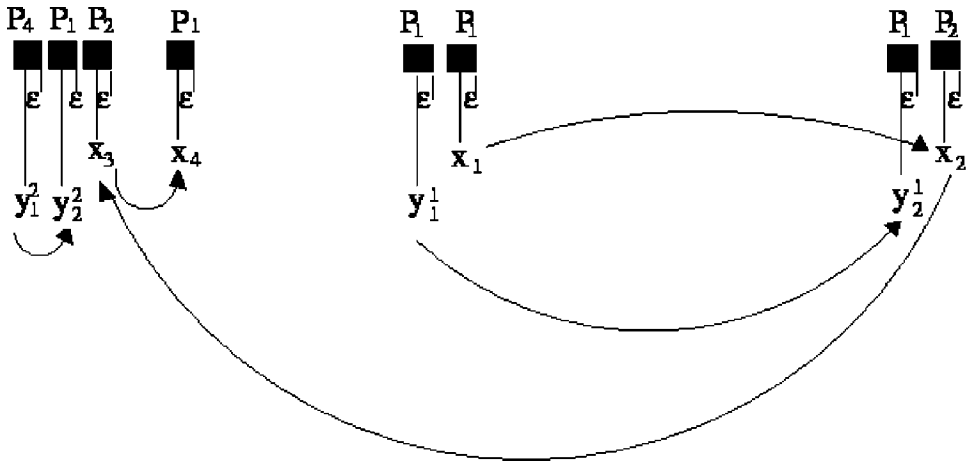

FIG. 2. A representation of the construction of the pseudopartition and the procedure to obtain the concatenated trajectory. A piece of a typical message is $M_l^t=\{s_1,s_2,s_2,s_1,\ldots\}$, and the trajectory used to construct the pseudopartitions is $T_{x_0}^*=\{x_1,x_2,x_3,x_4,\ldots\}$. Every interval $\beta_i=[x_i-\epsilon,x_i+\epsilon]$ is constructed from the points in $T_{x_0}^*$ that do not intersect each other. Thus β_i is associated with M_l^t. Therefore, $\beta_1\in P_1$ (the pseudopartition associated with the symbol s_1), $\beta_2\in P_2$, $\beta_3\in P_2$, and $\beta_4\in P_1$. The message $M'=\{s_1,s_1,s_4,s_1\}$ to be transmitted is codified in the concatenated trajectory $T'=\{y_1^1,y_2^1,y_1^2,y_2^2\}$ using our method.

which gives $H(S)=1.75$ bits for the value of the entropy for the alphabet $S=\{s_1,s_2,s_3,s_4\}$. The entropy of a source S is the average *uncertainty of the receiver* with respect to the letter to be transmitted. The entropy also measures the average amount of information of each letter in a message. The entropy of the source we work with is $H(S)=1.75$ bits, which means that, for each letter transmitted, the receiver obtains 1.75 bits of information. So the amount of information contained in the message M' having 19 000 letters is $19\,000\times H(S)$ bits. When using an optimal compaction method, the traditional digital scheme requires 33 250 wave signals, while, using our scheme, a message composed of 19 000 letters requires only $19\,000/r$ wave signals.

We define the extended alphabet of the source S_e, whose basic units are composed of pairs of units from the alphabet S. It can be shown that $H(S_e)=2H(S)$ [10]. For a low noise level, it will be shown in Sec. VII that we can find a set of trajectories T which codes for every unit of the extended alphabet S_e. From the previous argument, for every unit the receiver obtains 3.5 bits of information. However, as will be argued below in Sec. VI, because of the compaction rate r, only one wave signal is needed to transmit 3.5 bits of information to the receiver. Here we see the basic difference between our proposed scheme and the traditional digital scheme. In the latter, for every unit of the extended alphabet S_e, 3.5 wave signals are necessary. This is so because, for every wave signal transmitted, one bit of information is decoded into a one-bit message. This ''extra'' information contained in the chaotic wave signal allows the receiver to decode the received trajectory if the noise level is of the order of 2ϵ.

In this example, with the use of the parameter r set equal to 2, each set of two symbols of the message is codified in a two-point trajectory $T_i=\{y_1^i\ \ y_2^i\}$, where only y_1^i needs to be transmitted over the channel. We assume that the transmission over the channel of each point of the trajectory requires an interval of time Δ, and that after each such interval there follows an interval of time Δ in which the channel is idle. This idle time could be used for *multiplexing*, i.e., transmitting another different message, as depicted in Fig. 3. In this figure we show a representation of the two wave signals that are obtained by a suspension from the coding discrete trajectories. These two wave signals encode two different messages (Y encodes for message 1, and W encodes for message 2). Within the boxes we show the wave signals that represent the points to be transmitted, $\{Y_1^1\ \ W_1^1\ \ Y_1^2\ \ W_2^2\}$. Thus messages 1 and 2 can be sent multiplexed over the same channel. In a practical application, we require the coding trajectories to be synchronized with the same trajectory x_i, such that $W_1^1\approx F(Y_1^1)$, $Y_1^2\approx F(W_1^1)$, and $W_2^2\approx F(Y_1^2)$. With this synchronization procedure, the full transmitted wave signal is generated by applying small perturbations in only one nonlinear wave generator, and using only one communication channel.

In Fig. 4, we plot the effect of the value of the parameter ϵ over the total number N_T of different trajectories T_i that can be used to codify messages with $r=2$. S_c is the set of all T_i defined for a given value of ϵ. As we increase ϵ, the number N_T decays abruptly and smoothly. As we increase ϵ further, N_T is not smooth any longer. The oscillations observed in N_T are due to the fact that for a larger ϵ, the filling of the phase space by set B_p, is very sensitive to the initial condition x_0^*. At the singular limit $\epsilon=0$, there is only one trajectory, which is the chaotic trajectory.

An identification of the coding trajectory T_i and its characteristics (its length and its frequency of appearance in the transmitted concatenated trajectory) is necessary in order to determine the entropy associated with the set of all coding trajectories S_c. The entropy gives an indication of the average amount of information that can be transmitted by the coding trajectories. This number can be used to quantify how good the encoding process is. For example, when the number of different trajectories is 1, the entropy of the transmitted extended alphabet (the extended alphabet is composed by one single trajectory) is zero. Of course, this is not an interesting situation, since all the information is already known to the receiver. In fact, all the information is contained in the

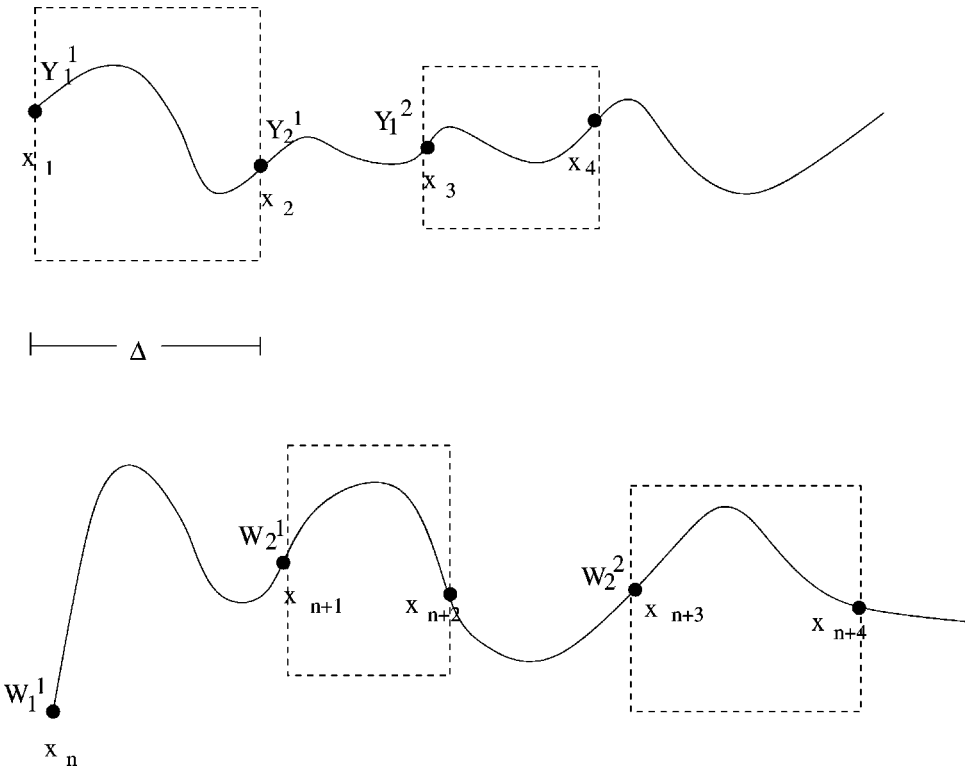

FIG. 3. A representation on how to multiplex two messages using our proposed chaotic integrated communication scheme.

partition of the phase space, information that is already known by both the receiver and the transmitter. Once the initial condition is known, and since the extended alphabet is composed of only one initial condition, there is no need to transmit anything. An extended analysis of entropy of the set S_c is given in Sec. V.

V. PROPERTIES OF THE PROPOSED METHOD

Let us now discuss the main properties of our communication method. The value of the parameter ϵ is straightforwardly related to the ability of our communication method to deal with noise. In principle, the larger this parameter is, the more robust our method against noise will be. This occurs because communication errors due to noise can occur only if the noise strength is large enough to remove a point x_{i_k}, that belongs to a trajectory T_i, out of the hypercube $\beta(x^*_{i_k},\epsilon)$. On the other hand, we should not, choose too large an ϵ. The larger the value of ϵ, the smaller the subsequence $B_p(x_0^*,l,\epsilon)$ of hypercubes, with only $\beta(x_i^*,\epsilon)$ not intersecting the previous hypercubes $\beta(x_j^*,\epsilon)$, where $j<i$. However, with a small number of hypercubes, fewer terms of the *typical sequence* M_l are considered when creating the pseudopartitions $\{P_i\}_{i=1}^N$, and so the statistical properties of the information source is not adequately probed. Our communication method is optimized for subsequences with a value of r that is not too small. Thus there is a trade-off between the robustness of our communication method to deal with low noise levels and the maximum value to be used for the parameter r. This parameter should not be too small for the trajectories to be long enough or to ''feel'' the statistical properties of the source. One important property of our partition creation procedure can be understood when ϵ is set equal to zero. The pseudopartition in this case is composed of a collection of points, corresponding to a zero area set. The probability density of the points in T_i that make up the pseudopartition associated with the alphabet symbols s_i is equal to p_i for all $i=1,\ldots,4$. The probability density of two-iteration trajectories $T_i \oplus T_j$ that code for a pair of symbols $\{s_i s_j\}$ is equal to $p_i \times p_j$, and so on. This statistical equivalence between the probability density of the coding trajectories, which are associated with the sequence of symbols, and the statistics of the symbols in the message is very important. It allows for a construction of a pseudopartition that is optimal in making a good correspondence between the trajectory and the message, in the sense that optimal coding trajectories for the message are constructed. This property

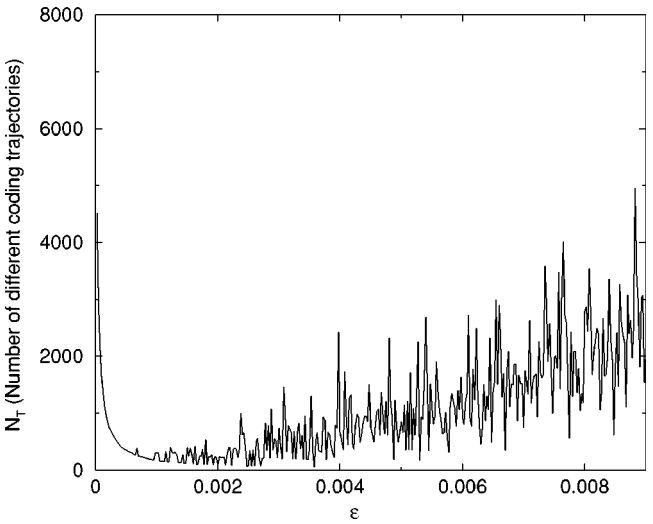

FIG. 4. Number of different trajectories, N_T, of the set of coding trajectories S_c as one varies the parameter ϵ, which is the half-length of the interval in x.

was explored in Ref. [7]. One consequence of this statistical equivalence is that any message can be subdivided into a set of sequences of r symbols.

The parameter r is also associated with another characteristic of our method: the compaction rate. Since we have a deterministic system for each sequence of r symbols of the message, only the initial condition of the associated trajectory T_i needs to be sent over the communication channel. This initial condition is sufficient for the receiver to recover the whole original sequence of r symbols. In a traditional digital scheme, the more compacted the message, the faster the transmission. For the proposed scheme, the larger the value of r, the higher the speed of the transmission. Thus we say that the larger the value of r, the higher should be the level of compaction achieved. It must be clear that while in a traditional digital scheme the compaction is implemented in the source, in this scheme the compaction is implemented into the wave signal.

In communication, one needs to address problems related to the channel such as the noise level and the damping of the wave signal. Due to the binary nature of digital communication, the periodical reinforcing of the signal and the error correction are performed by relatively simple systems. In our work, as we will show and argue in Secs. VI and VII, the dynamics not only guides the encoding of the message (source encoding and channel encoding) but is also responsible for the recovery of a message corrupted by noise [5]. Even though we did not address the issue of dealing with the damping of the wave signal in this work, based on some previous experiments and also on some preliminary theoretical work of ours, a chaotic amplification scheme may be possible to be implemented by using a chaotic system. For now, we propose that the damping can be resolved by the usage of a series of receiving stations, separated by a distance such that the upper bound in the damping of the wave signal is lower than 2ϵ. Those stations do recover the original message using the ideas presented in Sec. VII.

VI. COMMUNICATION WITH LOW NOISE LEVELS

Using the calculation of the entropy for the set of trajectories S_c, we want to clarify the placement of the dynamical system in the proposed communication scheme. The entropy of S_c is

$$H(S_c)=\sum_{n=1}^{N_T} p_{T_n} \ln_2\left(\frac{1}{p_{T_n}}\right), \tag{6}$$

where p_{T_n} is the probability of appearance of the trajectory T_n, and the length of the trajectories is $\langle l_n\rangle=2$.

Equation (6) measures the average amount of information contained in the r-point trajectories T_n. In the transmission, due to the memory properties of the chaotic dynamics, there is no need to transmit the two point trajectory, but rather only one point. Every point represents a wave signal in a real application. Thus, for each pair of letters transmitted, the receiver obtains a half wave signal that has $H(S_c)$ bits, quantity shown in Fig. 5. We see that, for all values of ϵ, the average amount of information transmitted is higher than the information retrieved, that is 3.5 bits. This ''extra'' information is actually provided by the dynamical system to allow

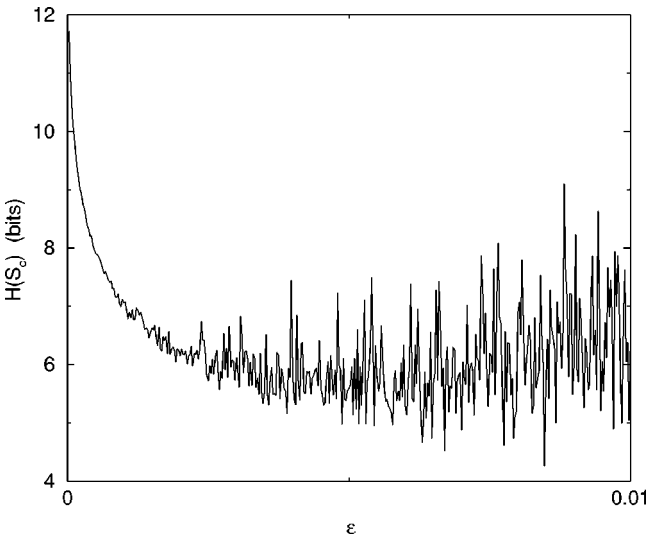

FIG. 5. The entropy of the set S_c in bits with respect to the parameter ϵ. The coding trajectories are calculated considering a message M' composed of 19 000 letters from the alphabet S.

the receiver to reconstruct the coding trajectory. That is a major point in this paper. The chaotic wave signal is not only the carrier of the information, but contains information in itself. That is possible because the chaotic wave signal has memory, or, in other words, is redundant.

An important characteristic of our method is its ability in making use of the deterministic redundancy of chaotic dynamics in order to overcome the effects of noise, interference, and dropouts encountered in the transmission of the signal over the communication channel. This mechanism is also related to the value of the parameter r. Let us suppose that we can use a maximum value for this parameter, say r_{lm}. Using values smaller than r_{lm} results in smaller sequences that are consequently more tolerant to noise and less affected by correlational effects of noise, like bias for example. Thus the smaller the value of the parameter r, the higher the level of redundancy introduced in the wave signal.

With regard to the security issue, we can show that our communication method codifies the messages in a way that is hard to decode by someone (an *intruder*) that is not either the sender or the receiver. In fact, the receiver decodes the message by associating the received trajectory with the information provided by the pseudopartition $\{P_i\}_{i=1}^N$, where the hypercubes are associated with the symbols of the alphabet. The fixed initial condition x_0^*, which is used to create the trajectory $T_{x_0^*}$ associated with the message M_l and to generate the pseudopartition $\{P_i\}_{i=1}^N$, is the method's secret key. Security relies on the secrecy of this initial condition. When, for security reasons, the pseudopartitions need to be changed, a new initial condition x_0^* must be used. Furthermore, since the concatenated trajectories that are used to send any particular message shadow the same trajectory $T_{x_0^*}$, all those trajectories are quite similar, making it rather improbable for an intruder to decode the message based on the statistical analysis.

As a result of our analysis, our proposed communication scheme works for the following reasons: (a) The assumptions made about the information source imply the existence

of a typical sequence M_l that embeds with probability 1 all the allowable subsequences of length r produced by the information source. (b) The smoothness of deterministic systems implies that solutions from neighboring initial conditions remain close over short time intervals. (c) The ergodicity property of the chaotic dynamics and the existence of an invariant measure on those systems allow for our definition of a pseudopartition on the chaotic invariant set in correspondence with the transition probability among the symbols of the alphabet in subsequences of length r generated by the information source. (d) The sensitive dependence on initial conditions, the main characteristic of chaotic systems, makes possible a smooth concatenation among the trajectories T_i by using small perturbations.

VII. COMMUNICATING WITH HIGH NOISE LEVEL

In this section, we consider a scenario where the level of noise is considerably higher, so that it can drive a point belonging to a trajectory T_i out of the hypercube $\beta(x_i^*,\epsilon)$. In this case, using the method previously discussed, the receiver would not be able to identify properly the trajectory received and, consequently, it will associate a wrong sequence of symbols with the trajectory. Let us suppose that the transmitter sends a trajectory $T=\{x_0,x_1,\ldots,x_n\}$, where x_0 is the initial condition and the other points are found through $x_{i+1}=F(x_i)$. Because of the noise, this trajectory arrives at the receiver as $\tilde{T}=\{\tilde{x}_0,\tilde{x}_1,\ldots,\tilde{x}_n\}$, where $\tilde{x}_i=x_i+\eta_i$, and the noise $\{\eta_i\}_{i\in\mathbf{N}}$ is an independent and identically distributed random variable with zero mean and variance η^2.

In Ref. [4], the authors devised a method for filtering, at the receiver, *in-band* noise present in the signal that was generated by a chaotic system and further transmitted over a communication channel. This method, which uses some fundamental properties from chaotic dynamics, can be embodied in our communication method after some modifications. From $\tilde{T}$ it produces a trajectory $\hat{T}$, which allows for the adequate recovery of the original sequence of symbols of the transmitted message. Before demonstrating how this can be accomplished, we first review the fundamental ideas about that method. To simplify our discussion, we only consider the case where the function F is a one-dimensional map. However, the argument can be extended to higher-dimensional maps without difficulty.

Let us consider the trajectory T and the perturbed trajectory $\tilde{T}$. We can visualize the effect of the noise as a force acting on each point of the original trajectory, sending it to a new point that belongs to a nearby orbit. At each point x_i of the trajectory T, the distance between the orbit T and the orbit of a nearby point x is changed by the factor $|F'(x)|>1$ on the average under forward iterations, since F is chaotic. Consequently, under backward iteration, that distance is changed by the factor $|1/F'(x)|$. Now consider a point $\widetilde{x_{j+m}}$ of the perturbed trajectory $\tilde{T}$. This point is located approximately η units away from the point x_{j+m} of the unperturbed trajectory T, so that $\widetilde{x_{j+m}}$ could be located outside the proper hypercube associated with x_{j+m}. If we start from $\widetilde{x_{j+m}}$ and iterate it m times in the backward direction, the distance between the point $F^{-m}(\widetilde{x_{j+m}})$ and the point x_j can be estimated to be given by the factor $|1/(\Pi_{k=1}^{m}F'^{k}(x_{j+k-1}))|<1$ for $m\geqslant 1$. This equation can be used to estimate the number of backward iterations m necessary for the distance between the point $F^{-m}(\widetilde{x_{j+m}})$ and x_j to be less than ϵ,

$$\left|\frac{1}{\left(\prod_{k=1}^{m}F'^{k}(x_{j+k-1})\right)}\right|\times\eta<\epsilon, \tag{7}$$

where $\widetilde{x_{j+m}}-x_{j+m}\leqslant\eta$ for $x_{j+m}\in T$. Decoding the message means revealing the meaning of the received trajectory $\tilde{T}$. This is possible if the receiver is able to identify the magnitude of the noise, η_j. This allows it to determine that the transmitted point x_j was received as $\tilde{x}_j$ $(\tilde{x}_j=x_j+\eta_j)$. Thus the receiver identifies if x_j is within some hypercube $\beta(x_j^*)$, which represents some unit s_k. However, due to the unpredictability of the noise magnitude, this decoding process is impractible. What the receiver can do is to take m backward iterations of the last received point $\widetilde{x_{j+m}}$, such that $|F^{-m}(\widetilde{x_{j+m}})-x_j|\leqslant 2\epsilon$. Therefore, the decoding boils down to determining whether $F^{-m}(\widetilde{x_{j+m}})$ is within the same hypercube as the point x_j. This decoding process is shown schematically in Fig. 6, where the backward iterations are represented by triangles, the noisy trajectory by squares, and the noiseless trajectory by circles.

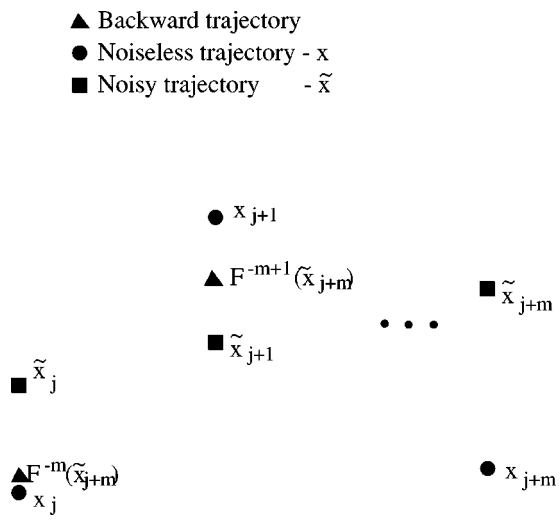

FIG. 6. A representation of the decoding process, where the receiver applies m backward iterations (triangles) on the noisy trajectory (squares) in order to obtain $x_j-F^{-m}(x_{j+m})\leqslant 2\epsilon$, where x_j is the noiseless trajectory (circles).

So, given a point x_j in a trajectory, the transmitter must estimate the number m of forward iterations, starting from x_j, that the coding trajectory must have.The length of the coding trajectory is thus $m+1$. For a specific $x_j\in T$, we try successive values of m until finding one that satisfies Eq. (7). As the value of m depends in general on the specific point, we denote it $m(x_j,\eta,\epsilon)$. In Ref. [4], m was considered to be constant and only a function of η.

Motivated by Eq. (7), we introduce the parameter $\mathcal{G}$, called the *gap-to-noise ratio*, which is defined by the following relation:

$$\mathcal{G}=\frac{\epsilon}{\eta}. \tag{8}$$

For the integrated scheme that we are presenting here, $\mathcal{G}$ is as important as the *signal-to-noise ratio*—a quantity that defines how much noise is in the channel [10] for a conventional communication scheme. Combining Eqs. (7) and (8), we have the following result:

$$\left|\frac{1}{\left(\prod_{k=1}^{m} F'^{k}(x_{j+k-1})\right)}\right|<\mathcal{G}. \tag{9}$$

The procedure for finding out the size of the coding trajectories, such that they are robust against noise, is done by the *dynamic channel encoder*. The modification in regard with the low level noise case is that, instead of just transmitting the initial point x_0^j for each trajectory T_i, we transmit x_0^j and its m subsequent iterations $\{x_0^j, F(x_0^j), \ldots, F^m(x_0^j)\}$, where the value of m is calculated such that relation (9) is obeyed. We call this new trajectory T_i', and its length $l_i'=m+1$. The set that contains the dynamically encoded trajectories is now S_c'. With this sequence of points, the receiver iterates the last received point of this sequence m times in the backward direction. As a result, it determines a point $\widehat{x_0^j}$ which is ϵ close to x_0^j, making it possible to properly recover the associated message M_j' by using the same procedure described in Sec. VII. Thus the other $r-1$ symbols of the message M_j are then recovered by the receiver using the hypercubes at each of the $r-1$ iterations of x_j, where x_j is obtained by finding the hypercube $\beta(x_j,\epsilon)$ that contains $\tilde{x}_0^j$.

Now we show a practical implementation of our chaotic communication scheme when a dynamical channel encoder has to be applied. Assume that $\eta=0.1$. For this value of η the noise level corresponds to 10% of the magnitude of the signal. Using Eq. (9), the m forward iterations resulting from a large number of uniformly distributed set of initial condition are shown in Fig. 7(a). As seen in this figure, the coding trajectory, that has an initial point at $y_1^i=0.43292163$ and encodes the pair of units s_1 and s_1, needs to have a length $l_c'=5$. Thus the coding trajectory T_i' (see Table II, column 3) is not given only by the point $y_1^i=0.43292163$, but also by the next four iterations of this point by applying Eq. (4). Consequently, $y_2^i=F(y_1^i)$, $y_3^i=F(y_2^i)$, $y_4^i=F(y_3^i)$, and $y_5^i=F(y_4^i)$. The next pair of units is encoded by a three-point trajectory given by y_1^{i+1}, y_2^{i+1}, and y_3^{i+1}, and hence $m=2$.

The concatenation of the trajectories T_1' with T_2' is discontinuous. However, the discontinuity may be only slight, if we construct a concatenated trajectory for which the point y_1^2 is close to the forward iteration of the point y_2^1. This is accomplished by the dynamical channel encoder, if the following constraint is obeyed when constructing set S_c': $F(y_m^n)\approx y_0^{n+1}$. We do not use this constraint to construct set S_c' in this work because, as we shall see below we want set S_c to have the same entropy as the S_c', so that we can analyze the effect caused by the noise in the dynamical channel encoder. To be able to control the trajectory or the wave signal by using only very small perturbations (small consumptions of energy), it is desirable that the concatenated trajectories be only slightly discontinuous. In addition, the transmitted concatenated trajectory will also be secure, as previously discussed, if it shadows the trajectory x_i.

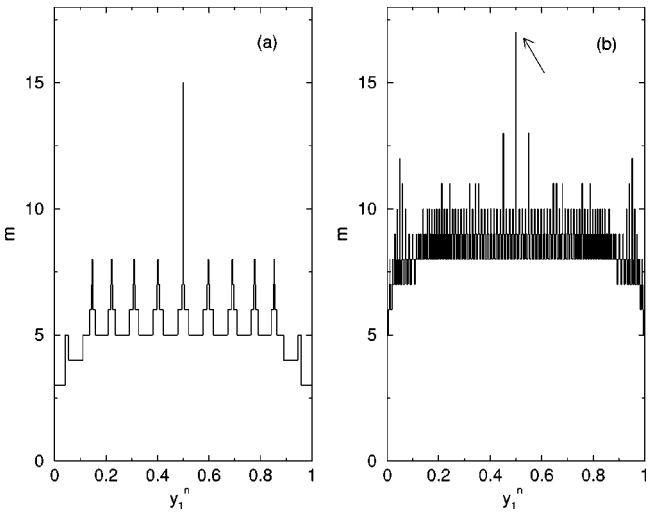

FIG. 7. (a) The m forward iterations, which indicate the lengths of coding trajectories, as a function of y_1^n (in units of x) for $\mathcal{G}=0.1$. (b) The same plot, but for $\mathcal{G}=0.01$.

We can quantify how efficient our communication scheme is with respect to the parameter $\mathcal{G}$. As $\mathcal{G}$ decreases its nominal value, m increases, and the steps seen in Fig. 7(a) become sharper. This results in a more complex diagram, as shown in Fig. 7(b). In this figure, the arrow indicates a point that represents the m forward iteration for a point very close to $y_1^j=0.5$. This point has a very large Lyapunov time that is proportional to the inverse of the left-hand side of Eq. (9), yielding a higher value of m. In practice, it is desirable to avoid points for which the value of m is high. If we compute the average value of m for a large number of uniformly distributed initial conditions in the interval [0,1], taking into account the value of $\mathcal{G}$, we can estimate the typical number of points of a coding trajectory for a particular value of the $\mathcal{G}$. This is shown in Fig. 8. As seen in this figure, if $\mathcal{G}$ is 0.01, we expect coding trajectories with an average length of 3.

In Fig. 9, we plot the entropy S_c' and the average length of the coding trajectory as a function of ϵ, for $\eta=0.1$. The entropy of the set S_c' for all different trajectories T_i used to codify messages for $r=2$ is

TABLE II. Coding trajectory with dynamical channel encoding for the message $\{s_1\ s_1\ s_4\ s_1\}$.

Trajectory	Message	Coding trajectory
$x_1=0.459028082$	s_1	$y_1^1(\approx x_1)=0.432921630$
$x_2=0.993285208$	s_1	$y_2^1=F(y_1^1)=0.982001969$
		$y_3^1=F(y_2^1)=0.0706964067$
		$y_4^1=F(y_3^1)=0.262793699$
		$y_5^1=F(y_4^1)=0.774932666$
$x_3=0.026678815$	s_4	$y_1^2\ (\approx x_3)=0.004890917$
$x_4=0.103868222$	s_1	$y_2^2=F(y_1^2)=0.0194679844$
		$y_3^2=F(y_2^2)=0.0763559241$

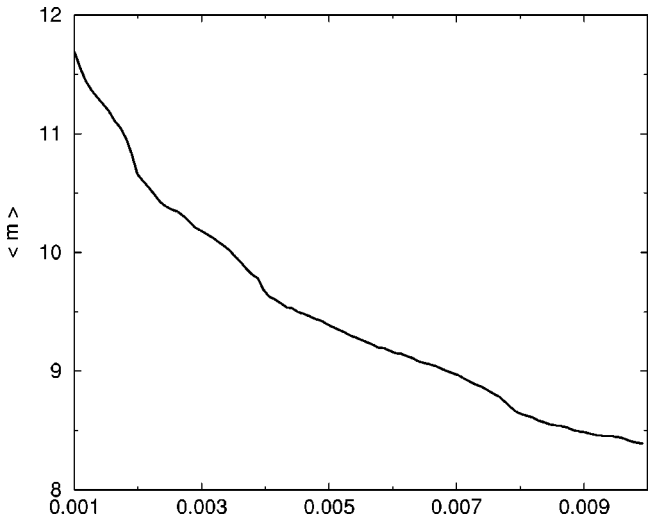

FIG. 8. Average forward time $\langle m \rangle$ as $\mathcal{G}$ (in the horizontal axis) is varied.

$$H(S_c') = \sum_{n=1}^{N_T} p_{T_n'} \ln_2 \left(\frac{1}{p_{T_n'}} \right), \tag{10}$$

and the average length $\langle l_n' \rangle$ of the coding trajectories is

$$\langle l_n' \rangle = \sum_{n=1}^{N_T} p_{T_n'} \times l_n', \tag{11}$$

where $p_{T_n'}$ is the probability of appearance of the trajectory T_n'. Note that $H(S_c') = H(S_c)$, if $p_{T_n'} = p_{T_n}$, and $N_T = N_T'$. The quantity $\langle l_n' \rangle$, computed using Eq. (11), can be estimated approximately by the predicted average forward time m given in Fig. 8.

To understand how a high noise level affects the efficiency of the proposed scheme, we use Fig. 9 to compare the

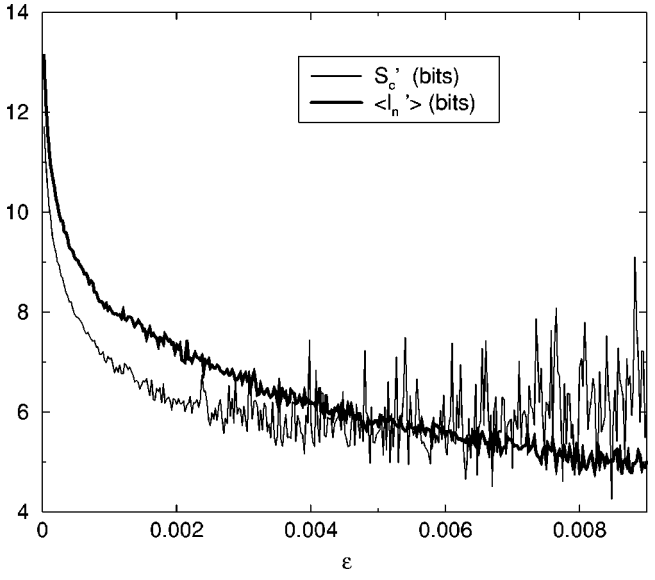

FIG. 9. The curve shows the entropy of the set S_c' in bits, and the thick lines represent the average length of the coding trajectory $\langle l_n' \rangle$, both with respect to the parameter ϵ. In this figure, $\eta = 0.1$ $(\mathcal{G} = \epsilon/0.1)$.

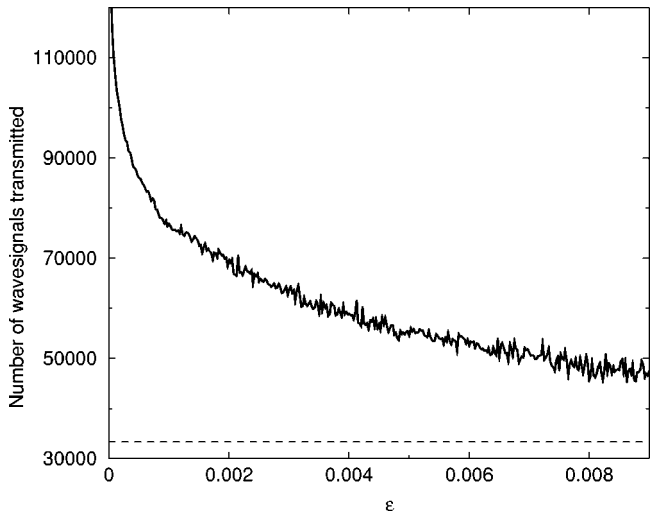

FIG. 10. Total number of wave signals used to transmit the message M' with respect to the parameter ϵ (continuous line). The dashed line indicates this number when information is encoded using the perfect compaction method, and then transmitted using a traditional digital communication scheme when no channel encoder is used. In this figure, $\eta = 0.1$ $(\mathcal{G} = \epsilon/0.1)$.

ratio between $H(S_c')$ and the average length $\langle l_n' \rangle$ of the trajectories of set S_c', with the ratio between $H(S_c)$ and $\langle l_n \rangle$ for $r = 2$. For a low noise level, this ratio is equal to $H(S_c')/r$ with $[H(S_c) = H(S_c')]$. Thus a large amount of information in bits is transmitted per wave signal. For a high noise level, the curve $H(S_c')$ follows closely the curve $\langle l_n' \rangle$, which results in a ratio close to one bit per wave signal. Therefore, the noise is responsible by a decrease in the amount of information carried by each wave signal as compared to the transmission with low noise level. This is a consequence of the fact that $\langle l_n' \rangle > r$. Thus more dynamical information is being sent if the trajectories are longer, which makes the transmission more slower.

Another result shown in Fig. 9 is that for small ϵ, $H(S_c)$ is large, meaning that the certainty of the receiver to obtain some particular wave signal is small (or the uncertainty of the receiver is large). In other words, there is a large number of coding trajectories for every pair of symbols. For ϵ large, one notes that the entropy curve decreases as ϵ increases, but oscillates as ϵ increases. This signifies a decrease in the *uncertainty of the receiver* for expecting incoming wave signals or it signifies a lower number of possible coding trajectories for every pair of letters.

The number of wave signals used to transmit a message M' composed of 19 000 letters, as we vary ϵ, is shown in Fig. 10, for a noise level $\eta = 0.1$. In this figure, the dashed horizontal line represents the number of wave signals used to transmit the same message with a conventional digital communication scheme when the message has gone through the perfect compaction encoder and the codeword is not redundant (the codeword produced contains the minimum possible amount of information). Therefore, we see that even for a high level of noise (10% of the signal), the proposed method introduces a low redundancy into the coding trajectories, which, in other words, means that the coding trajectories do not need to have a large length in order to allow the receiver to fully decode the message.

VIII. CONCLUSIONS

Conventional communication systems used nowadays are expected to reliably transmit a large amount of information over a communication channel. In order to fulfill the reliability objective, a digital system introduces redundancy in the message in order to allow for the detection and correction of transmission errors. Since the channel imposes limitations on the amount of data that can be transmitted, compression and compaction algorithms are used to allow the transmission of the maximum possible amount of information. In order to preserve the confidentiality of the message, cryptography methods must be used. Finally, the message is converted to a signal that is compatible with the transmission media that physically implements the communication channel. The implementation of all these features results in complex and expensive systems made up of a chain of sophisticate subsystems, each one responsible for the accomplishment of a specific task. These systems use a considerable amount of energy to operate.

We argued in this work that this evolved scenario can be simplified considerably with the use of a communication system based on chaos. In fact, we presented an integrated scheme of implementation that performs all the functions that are expected from a conventional and efficient digital communication system using a simple chaotic modulation process. The encoder subsystem codifies the message in a chaotic wave signal, and this codification operation embodies the tasks of compaction, cryptography, and noise and dropout robustness. Furthermore, the resulting codified chaotic signal is perfectly suitable for the transmission channel. This is accomplished due to the dynamical properties of the chaotic signal.

Our communication method can be used with efficiency even in situations where the noise level is extreme. In this case, we defined the parameter $\mathcal{G}$, which guides the receiver on the implementation of a trustful dynamic channel encoder to find the coding trajectories.

More than just arguing for a chaotic based communication system, we claim that the efficiency of the communication system *per se* favors this technology. One has the ability to implement all the features that are expected to be accomplished by a digital communication system using just one operation, chaotic modulation, which is done by using small perturbations and with a minimum consumption of energy. In addition, the proposed scheme introduces the usage of a chaotic wave signal generator as a type of source encoding and decoding. For the encoding, the dynamical system is a wave signal generator. For the decoding, the dynamical system is an information generator.

The results presented here give us a foundation for the construction of a theory of communication based on the proposed scheme. Specifically, the channel capacity, which measures the maximum amount of information to be transmitted over a channel, depends not only on the channel bandwidth, the power of the source signal, and the noise magnitude, but also on the dynamical properties of the considered chaotic wave signal generator.

ACKNOWLEDGMENTS

This work was partially supported by FAPESP, ONR (Physics) and a joint CNPq/NSF-INT grant.

[1] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993); S. Hayes and C. Grebogi, in *Structure and Properties of Interfaces in Materials*, edited by W.A.T. Clark, V. Oahmen, and C. L. Briant, MRS Symposia Proceedings No. 238 (Materials Research Society, Pittsburgh, 1993), p. 153. S. Hayes and C. Grebogi, Proc. SPIE **2038**, 153 (1993).

[2] S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781 (1994).

[3] L.M. Pecora and T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); K. Cuomo and A.V. Oppenheim, *ibid.* **71**, 65 (1993); L. Kocarev and U. Parlitz, *ibid.* **74**, 5028 (1995); M. Hasler, Int. J. Bifurcation Chaos Appl. Sci. Eng. **8**, 647 (1998).

[4] E. Rosa, S. Hayes, and C. Grebogi, Phys. Rev. Lett. **78**, 1247 (1997).

[5] M.S. Baptista, E. Rosa, C. Grebogi, Phys. Rev. E **61**, 3590 (2000).

[6] E. Bollt, Y.-C. Lai, and C. Grebogi, Phys. Rev. Lett. **79**, 3787 (1997).

[7] M.S. Baptista, Phys. Lett. A **240**, 50 (1998).

[8] D. K. Arrowsmith and C. M. Place, *An Introduction to Dynamical Systems* (Cambridge University Press, New York, 1994).

[9] By typical we mean that M_l^t contains the most frequent sequences of letters (words) that appear in the different messages m' that will be transmitted.

[10] S. Haykin, *Communication Systems* (Wiley, New York, 1994); C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (The University of Illinois Press, Champaign, 1964).