AIP | Chaos
An Interdisciplinary Journal of Nonlinear Science

Conditions for efficient chaos-based communication

Murilo S. Baptista, Elbert E. Macau, and Celso Grebogi

Citation: Chaos **13**, 145 (2003); doi: 10.1063/1.1513061
View online: http://dx.doi.org/10.1063/1.1513061
View Table of Contents: http://chaos.aip.org/resource/1/CHAOEH/v13/i1
Published by the American Institute of Physics.

Conditions for efficient chaos-based communication

Murilo S. Baptista
Instituto de Física, Universidade de São Paulo, Caixa Postal 66318, 05315-970 São Paulo, S.P., Brazil

Elbert E. Macau
INPE, Instituto Nacional de Pesquisas Espaciais, Caixa Postal 515,
12227-010 São José dos Campos, S.P., Brazil

Celso Grebogi
Instituto de Física, Universidade de São Paulo, Caixa Postal 66318, 05315-970 São Paulo, S.P., Brazil

(Received 22 May 2002; accepted 16 August 2002; published 21 February 2003)

We find the conditions for a chaotic system to transmit a general source of information efficiently. Transmission of information with very low probability of error is possible if the topological entropy of the transmitted wave signal is greater than or equal to the Shannon entropy of the source message minus the conditional entropy coming from the limitations of the channel (such as equivocation by the noise). This condition may not be always satisfied both due to dynamical constraints and due to the nonoptimal use of the dynamical partition. In both cases, we describe strategies to overcome these limitations. © *2003 American Institute of Physics.* [DOI: 10.1063/1.1513061]

In communication, one requires the source of information to be efficiently transmitted. In other words, the information should be transmitted quickly and with very low distortion. While in traditional communication schemes, the upper bounds for high efficiency is imposed by the channel properties, in communication with chaos this upper bound is dependent on the properties of the dynamical system being used. In this paper, we classify a dynamical system according to its ability to encode a general source of information that can be transmitted and recovered by the receiver with very low distortion. So, in general terms, we argue that transmission of information with very low probability of error can be accomplished if the dynamical rate at which the information is generated by the chaotic system (i.e., the topological entropy of the system) is greater than or equal to the rate at which the source message is being generated (i.e., the Shannon entropy of the source message) minus the conditional entropy associated with channel limitations.

I. INTRODUCTION

We consider a communication system to be efficient if it transmits **quickly** a source message with very low probability of error. In communication, the source message is usually encoded into another message, which is modulated in some sort of wave signal, and then transmitted through the physical medium. In a recent paper,[1] we showed that the encoding and the modulation processes in a chaos-based communication system can be integrated in a single dynamical encoding process. In another words, given a source message, we can find an encoded trajectory which already obeys the constraints of the channel and it is, therefore, the wavesignal to be transmitted. Thus, the encoding trajectory represents a chaotic wave signal which is then transmitted over a channel. It was also shown in Ref. 2 that chaos-based communication is highly *efficient*. In other words, the source message is transmitted carrying the maximum amount of information and with a high level of robustness in the presence of noise.

The fundamental argument that has been emphasized about using a chaotic-based communication system is high efficiency at low cost. In fact, a nonlinear chaotic oscillator that generates a waveform for transmission can be easily and efficiently built, while the electronics that is necessary for encoding the information in the chaotic signal remains as a low-power and inexpensive microelectronic circuit. In addition, chaos-based communication can perform efficiently the main tasks that are expected from a digital communication system nowadays, as we have shown in Ref. 1. In fact, besides transmitting information through a communication channel, a digital communication system must also handle 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. Traditionally, those two functions have to be done independently and each one encodes one bit stream into another. On the other hand, in a communication system based on chaos those functions can be performed in a single shot by the subsystem that executes the modulation of the signal for transmission over the communication channel. Thus, we can have a communication system that inherits the most important advantages of the analog and digital communication system and, at the same time, is much more simple and efficient. This integrated and high efficient scenario is possible because of the intrinsic properties of a chaotic signal, which can be advantageously exploited to carry encoded messages efficiently. This efficient scenario can also be understood in terms of the flexibility that chaotic signals have, allowing one to operate the usual communication functions into the chaotic wavesignal, instead of operating on the bit stream. So, in chaos-based communication, one can perform all the functions at the physical level while digital communication might need to perform the various functions in the software level, which might expend too much time. The flexibility of the chaos-based communication system is advantageously used to create a fast cryptographic chaos-based system.[3] In addition to all these characteristics, we conjecture that the understanding of chaos-based communication can help us in the understanding of biological complex communication processes.

In this paper, we present a general condition that must be obeyed by a particular dynamical system so that it can be used for efficient chaos-based communication. Our main result is that the transmission of information with very low probability of error can be accomplished if the dynamical rate at which the information is generated by the chaotic system (i.e., the topological entropy of the system) is greater than or equal to the rate at which the source message is being generated (i.e., the Shannon entropy of the source message) minus the conditional entropy due to the channel limitations (such as equivocation caused by the noise in the channel). To demonstrate this statement, we establish the connection between the *theory of information*,[4,5] that is used to measure the amount of information of the source, and the *theory of dynamical systems*,[6–10] that is used to measure the amount of information of the encoding trajectories. We treat chaos-based communication as two separate problems: (i) We specify the conditions under which a dynamical system has the potential to create trajectories that encodes the source message. (ii) We specify conditions under which the encoding chaotic trajectory, even in the presence of bounded or unbounded noise in the transmission channel, has the ability to carry the information of the source.

We classify the dynamical system on whether the topological entropy is greater, equal, or smaller than the Shannon entropy. For the case in which it is equal we call the dynamical system as an *optimal encoder*, because of its ability to handle the information of the source just rightly. When the topological entropy is greater than the Shannon entropy, the dynamical system has information to spare—a situation that is necessary when handling noise and dropouts. When the topological entropy is less than the Shannon entropy of the source message, we argue ways to encode the source message such that the nonoptimal dynamical system can still provide the encoding trajectories that are transmitted.

With respect to the encoding of the source, problem (i), it might be common to have a potentially optimal dynamical system, whose capacity is not being fully utilized. In that situation, we say that the system is being misused as it happens when one makes a wrong placement or choice of the phase-space partition (the partition of the phase space that is responsible for the encoding of trajectories into symbolic sequences, the basis for the dynamical process to encode the source message). When that happens, the information of the encoding trajectories is less than the topological entropy of the dynamical system. With respect to the second problem (ii), the same procedure of choosing trajectories robust against unbounded noise could be used in selecting trajectories that could be transmitted over limited bandwidth channels.

II. INFORMATION OF A DYNAMICAL SYSTEM

Dynamically, in communication with chaos, we consider the encoding trajectories to be derived from a discrete-time dynamical process, $x_{i+1}=f(x_i)$, whose state space trajectory $\{x_i\}_{i=0}^{\infty}$, represented by $x\in\Re$, where each x_i takes values on the interval $J=[0,1]$, and each point is obtained from the previous one. Let $\mathcal{R}=\{r_0,r_1,\ldots,r_K\}$ be the $K+1$-symbols each corresponding to one partition element ω_k of the interval J, with $k=0,1,\ldots,K$. By associating symbols to the trajectory x through the state space partition, we create the trajectory symbolic sequence, $\mathcal{Z}$. Let q_k be the probability associated to the symbol r_k. The probability of having the trajectory x within the partition ω_k is $\rho(\omega_k)$.

In chaotic-based communication, the source message is encoded in the trajectories. An encoding trajectory is associated with a symbolic sequence containing the same information as the source message. So, while the symbolic sequence represents the source message (which can serve as a reference with which one has knowledge about how the source message is being encoded), the encoding trajectory is the one that will be transmitted over the channel. Thus, to ensure efficient encoding of the source message, we need to understand how to measure the amount of information contained in the source and, hence, in the symbolic sequence. If no external manipulation is applied to the system f, i.e., if there is no control upon the trajectory x_i, the amount of information generated by the dynamical system is measured by

$$Z(\omega)=\lim_{K\to\infty}\frac{1}{K}\sum_{k=0}^{K}\rho(\omega_k)\ln\left(\frac{1}{\rho(\omega_k)}\right). \tag{1}$$

Note that the above formula is partition dependent. The maximum capacity of information generated by a dynamical system, without external manipulation, is given by the Kolmogorov–Sinai entropy (H_{KS}) (Refs. 6, 7) (also known as metric entropy) defined to be

$$H_{\mathrm{KS}}=\sup_{\omega}[Z(\omega)], \tag{2}$$

where sup is the supreme over all possible partitions. In practice, we calculate H_{KS} by the probabilities Q_e (with $e=1,...,E(P)$) of the number $E(P)$ of possible sequences of P symbols, in the symbolic trajectory Z, by using

$$Q(\omega)=\lim_{P\to\infty}\frac{1}{P}\sum_{e=1}^{E(P)}Q_e\ln\frac{1}{Q_e}. \tag{3}$$

Note that this function is also partition dependent.

An approximately accurate calculation of the the KS entropy is thus given by

$$H_{\mathrm{KS}}=\sup_{\omega}[Q(\omega)], \tag{4}$$

which is now partition independent. We call this quantity the *information rate* of the dynamical system f. The H_{KS} is connected to the metric characteristics of the dynamical system. If the Lyapunov exponents are independent of the trajectory, which is true for Lebesgue almost all initial conditions, then[11]

$$H_{\mathrm{KS}} \leqslant \sum_{\lambda_i > 0} \lambda_i , \tag{5}$$

where each λ_i is a positive Lyapunov exponent of the dynamical system. For ergodic maps, H_{KS} is an invariant quantity for the dynamical system, calculated from its natural invariant measure μ.

In addition to the Kolmogorov–Sinai entropy, which is related to the probability of certain symbolic sequences to appear, we can measure the capacity of the system by the ability it has in generating a certain amount of symbolic sequences. So, the amount of information contained in the symbolic sequence, for a given partition ω, is given by the

$$W(\omega) = \lim_{n\rightarrow\infty} \frac{\ln[E(n)]}{n}, \tag{6}$$

where $E(n)$ is the number of accessible (allowed) symbol sequences of length n. We call this quantity the *information capacity* of the dynamical system for a given partition ω. Thus, Eq. (6), like Eq. (1), is partition dependent. The maximum capacity of information generation of a dynamical system is then the supremum of Eq. (6) over all possible partitions,

$$H_T = \sup_\omega W(\omega), \tag{7}$$

which is now partition independent. We denominate this quantity the *information capacity* of the dynamical system f. This quantity is equivalent and formally the same as the topological entropy[8–10] of the dynamical trajectory. Because of this equivalence, H_T can be appropriately estimated by the number $P(n)$ of unstable periodic orbits of period n embedded in the chaotic attractor. These two quantities are related by $P(n) \sim e^{n * H_T}$ (see Ref. 12 for an efficient method for detection of unstable periodic orbits). In general,

$$H_{\mathrm{KS}} \leqslant H_T . \tag{8}$$

III. INFORMATION OF THE SOURCE

We consider an information source that can be modeled by a discrete memoryless source as the following. Let the random (memoryless) variable X_i be associated to the 2-symbol 0,1 of the alphabet $\mathcal{S}$, through the partition $\Omega_0 = [0,\mathcal{X}[$, and $\Omega_1 = [\mathcal{X},1]$. Furthermore, in this case, once X is uniformly distributed, $p_0 = p(s_0) = \mathcal{X}$ and $p_1 = p(s_1) = 1 - \mathcal{X}$ are the probability functions for the discrete random variable X, considering the partition Ω. We consider the message $\mathcal{M}$ to be a sequence of symbols 0 and 1 that represents the variables X_i. The amount of information, based on the chosen partition, is defined as the average information per source symbol, and is given by the Shannon entropy[4]

$$H_s(\mathcal{S},\Omega) = \sum_{k=0}^{k=K} p_k \ln\left(\frac{1}{p_k}\right). \tag{9}$$

One important property of the entropy H_s is that $0 \leqslant H_s(\mathcal{S},\Omega) \leqslant \ln K$, where the upper limit is reached if and only if $p_k = 1/K$ for all k, which is the case for $\Omega = 0.5$. This upper limit is denoted by $H_s(\mathcal{S})$, where we omit the symbol Ω in this representation. Note that the Shannon entropy is defined through the probabilities p_i of a discrete symbol space. In the approach described in this work, for a better analogy to the dynamical entropies, we define the Shannon entropy through the probabilities p_i with which the random variable X_i $(\in \mathfrak{R})$ visits the different partitions Ω_K within the interval I.

It is often convenient in practice to encode the source message both for security (encryption) and to reduce redundancy (compression). The average code-word length $\langle L \rangle$ for any source encoding is bounded as $\langle L \rangle \geqslant H_s(\mathcal{S})$, according to the source-coding theorem, which states that information cannot be created by the encoding process itself. Another way of looking at the source-coding theorem, better suited when one uses dynamical systems to encode source messages, is by measuring the entropy of the encoded message $\mathcal{M}_c$. This entropy is calculated by the encoded symbolic alphabet $\mathcal{S}_c$ and is defined substituting $\mathcal{S}$ by $\mathcal{S}_c$ in Eq. (9). It is bounded as

$$H_s(\mathcal{S}_c) \leqslant H_s(\mathcal{S}). \tag{10}$$

IV. ENCODING WITH DYNAMICAL SYSTEMS

Analogously to the source-coding theorem, as mentioned in the previous section, a general information source (source message) can be encoded by the chaotic system (dynamic symbolic sequence) with arbitrarily small error probability only if the following condition holds:

$$H_s(\mathcal{S},\Omega) \leqslant H_T . \tag{11}$$

We call this relation as the *dynamical source-coding condition*. If this condition is not satisfied, we may then try to code the message $\mathcal{M}$ using another alphabet $\mathcal{S}_c$ such that $H_s(\mathcal{S}_c) \leqslant H_T$. In fact, this was done in Ref. 13. Otherwise, if the condition is satisfied, there must exist then an encoding scheme that allows the message $\mathcal{M}$ to be encoded by the trajectory $\{x_j\}$.

Let us now use the concepts just outlined, obtained from the Information Theory and the Theory of Dynamical Systems to analyze specific examples of chaotic-based communication systems in order to explore their limits, as spelled out in Eqs. (1)–(10). Let us consider an information source that can be modeled by a discrete memoryless source $\mathcal{X}$, where the random variables X_i are associated to the 2-symbol 0,1 of the alphabet $\mathcal{S}$ through the partition $\Omega_0 = [0,\chi[$ and $\Omega_1 = [\chi,1]$. Furthermore, in this case, once X is uniformly distributed, $p_0 = p(s_0) = \chi$ and $p_1 = p(s_1) = 1 - \chi$ are the probability functions for the discrete random variable X, considering the partition Ω. Consider, as an illustrative example of a chaotic-based communication system, the logistic map

$$x_{n+1} = f_b(x_n) = b x_n (1 - x_n), \tag{12}$$

which is a discrete-time dynamical process, to be used to encode the source information. For the logistic family f_b, the attractive sets, when they exist, are located in the interval $J = [0,1]$. For comparison between the use of information theory in a discrete memoryless source and in a dynamical system, we choose a binary alphabet to represent the variable x, so $\mathcal{R} = [0,1]$, and we divide the interval J in two parti-

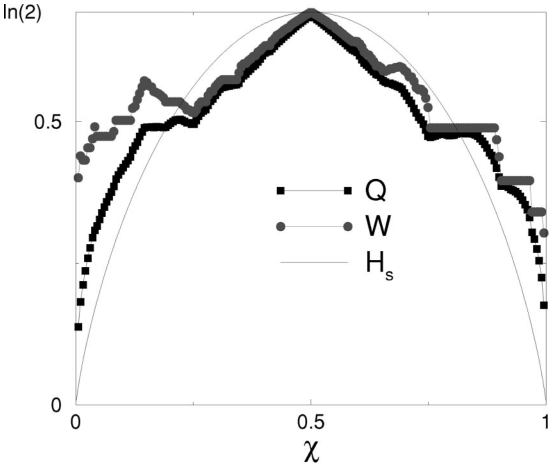

FIG. 1. The Shannon entropy, and the quantities Q and W, the information measure of the symbolic sequence generated by the chaotic system with and without control of the trajectory, respectively. The entropies, as defined by Eqs. (9), (4), and (7), respectively, are shown for $\chi=0.5$. We set $b=4$ in Eq. (12).

tions, $\Omega_0=[0,\chi[$ and $\Omega_1=[\chi,1[$ $(K=1)$. Once x_n is not uniformly distributed in the interval J, $q_0\neq\chi$ and $q_1\neq 1-\chi$.

We now calculate H_s, by using Eq. (9), and the partition dependent quantities $Q(\chi)$ and $W(\chi)$, given by Eqs. (3) and (6), respectively. By varying the partition positions χ, we find how $Q(\chi)$ and $W(\chi)$ approaches H_{KS} and H_T, respectively. Initially, we analyze the $b=4$ case whose logistic map is conjugate to the tent map[14] which behaves as the Bernoulli shift. In this case, the maximum capacity of generating information for a dynamical system takes place, i.e., a trajectory through a generating partition creates all possible symbol sequences. In Fig. 1, we plot H_s, $Q(\chi)$, and $W(\chi)$ versus the partition position χ. We use a trajectory of length 9 000 000 and sequences of length $P=20$ for various possible values of χ. All entropies have the same maximum value ln(2) for $\chi=0.5$, because there $p_0=p_1$, and $q_0=q_1$. For this partition value, $H_{\mathrm{KS}}=Q(\chi)=H_T=W(\chi)=\ln(2)$. Some considerations can be drawn from this figure. For any χ, $Q(\chi)\leqslant W(\chi)$ and $W(\chi)\leqslant\ln(2)$. Note that Eq. (5) is satisfied since the Lyapunov exponent for Eq. (12) with $b=4$ is equal to ln(2). A wrong placement of the partition position, i.e., the $\chi\neq 0.5$, produces symbolic sequences that do not reflect the whole dynamics of the system. In fact, in this case, different orbits of Eq. (12) are coded by the same symbolic sequences, limiting the number of possible sequences, and thus reducing the information per symbol. Analogously, choosing χ such that $p_0\neq p_1$, H_s of the source is smaller than that for $p_0=p_1$ and, thus, reducing the uncertainty about the symbol generated by the source. Another important characteristic of the function $W(\chi)$ in Fig. 1 is that it is nonmonotonic. The reason for this is that, as we change χ, some orbits are destroyed but others might appear in their place. This phenomena is explained in Ref. 15.

For the case in which the system is not a Bernoulli shift $(b<4)$, the system dynamics impose limitations on the possible sequence of symbols that can be generated, and so, $H_T<\ln(2)$. To illustrate this case, we choose $b=3.9$ in Eq. (12), and find $H_{\mathrm{KS}}=0.531\,739\,831$ and $H_T=0.562\,321\,723$ (for $\chi=0.5$). Not all the sequences are generated, since Eq. (12) for $b=3.9$ is not conjugate to a Bernoulli shift. Because of condition (11), the dynamics of Eq. (12) cannot be used to encode a discrete memoryless source for which $p_0=p_1$ and $H_s=\ln(2)=0.693\,147\,180\,6$, for example. When condition (11) is not satisfied, we must code the alphabet $\mathcal{S}$ into $\mathcal{S}_c$ such that $H_T(\mathcal{R})\leqslant H_s(\mathcal{S}_c)$, thus coding the message $\mathcal{M}$ into $\mathcal{M}_c$. That can be done, for example, by eliminating possible sequences of the source, like the authors did in Ref. 13, due to runlength constraints. Thus, say that the binary source has alphabet $\mathcal{S}$ and the characteristics $p_0=p_1=0.5$, so, $H_s(\mathcal{S})=\ln(2)$. Suppose that the trajectories are coded by a binary alphabet $\mathcal{R}$ and the dynamics does not allow for the appearance of two zeros in a row, and that the other possible sequences of two symbols 01,10,11 are equiprobable. Thus, using Eq. (7) one finds $H_T(\mathcal{R})=0.636\,514\,168\,29$. To use such dynamical system to communicate under this condition, it is necessary to encode the source message into code-words that does not allow the two-symbol sequence "00" (code $\mathcal{S}$ into $\mathcal{S}_c$). One encoding is by coding "0" into "01" and "1" into "1." Doing this coding, the probability of appearance of the symbol "0" in the coded source message is $p_0=\frac{1}{3}$ and the probability of appearance of the symbol "1" in the coded source message is $p_0=\frac{2}{3}$. Therefore, $H_s(\mathcal{S}_c)=H_T(\mathcal{R})=0.636\,514\,168\,29$, and then, the dynamical system can now be used to transmit the coded source message $\mathcal{M}_c$. Another way to overcome a forbidden sequence of symbols, that a particular dynamical system might have, is by using a granular partition like the one proposed in Ref. 1. However, the information capacity H_T of a dynamical system that uses a granular partition cannot be larger than the information capacity of the same system when using a generating partition.

V. COMMUNICATION WITH BOUNDED NOISE

Now, we show the limitations on the information transmission imposed by noise of the physical medium. For example, due to the presence of ϵ-bounded noise in the channel, it is advantageous to avoid orbits that are ϵ close to the partition boundary. It makes difficult for the receiver to decode the information of trajectories which eventually pass close to the partition boundary if the trajectories are corrupted by noise during the transmission. So, to have robust encoding trajectories against ϵ-bounded noise,[16,17] we impose a restriction that not all the chaotic attractor, but just a subset of it can be used as the communication system. We discard the orbits that reach the open interval $(\chi-\epsilon,\chi+\epsilon)$. The remaining orbits, the ones used for encoding does not fall in this open interval and in all its preimages. They are, therefore, located in a nonattracting chaotic saddle embedded in the chaotic attractor. The return mapping of the nonattracting chaotic saddle of Eq. (12) is shown in Fig. 2 for $\epsilon=0.05$. Since the chaotic saddle is a subset of the chaotic attractor, its entropy $H_T(\epsilon)$ is smaller than the one of the corresponding chaotic attractor, H_T. For example the entropy of the set shown in Fig. 2 is $H_T(\epsilon=0.05,b=4)=0.534\,824\,014$, while $H_T(\epsilon=0,b=4)=\ln(2)$.

To ensure that the encoding trajectory can be decoded

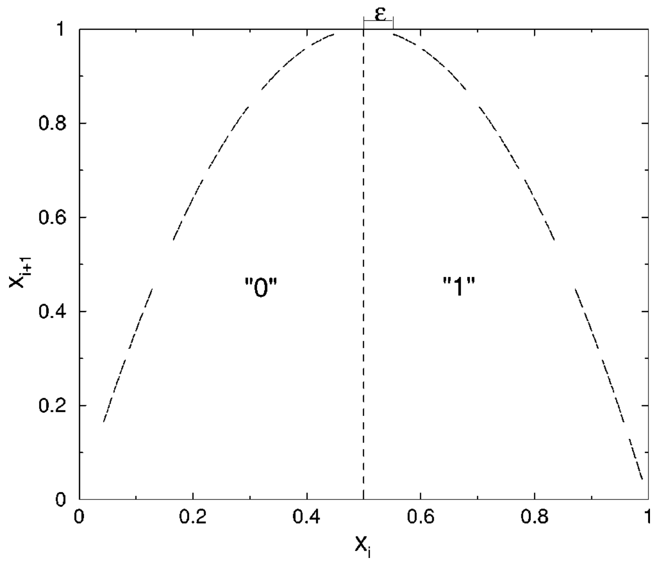

FIG. 2. A numerically calculated trajectory (using the triple PIM triple method) of size 50 000 of the nonattracting chaotic saddle for a gap of size $\epsilon=0.05$. We use $b=4$ in Eq. (12).

with arbitrarily small probability of error, we need

$$H_T(\epsilon)\geqslant H_s(S_c), \tag{13}$$

similar to Eq. (11), but with the topological entropy calculated using the trajectories in the chaotic saddle. These nonattracting orbits have an entropy smaller than the trajectory of the chaotic attractor. Thus, the nonattracting orbits have limited capacity to encode a source of information. Moreover, the derivative of the topological entropy with respect to ϵ is very likely to be zero, since the function $H_T(\epsilon)$ versus ϵ is a devil's-staircase-like function,[16] as shown in Fig. 3. So, slight increases on the gap size does not affect the encoding capacity of the system. In other words, the chosen encoding orbits might be robust against variations of the noise amplitude. The calculation of the nonattracting chaotic set with orbits that are robust against ϵ-bounded noise is performed in practice by eliminating some code-words which are known to lead the orbits to the gap.

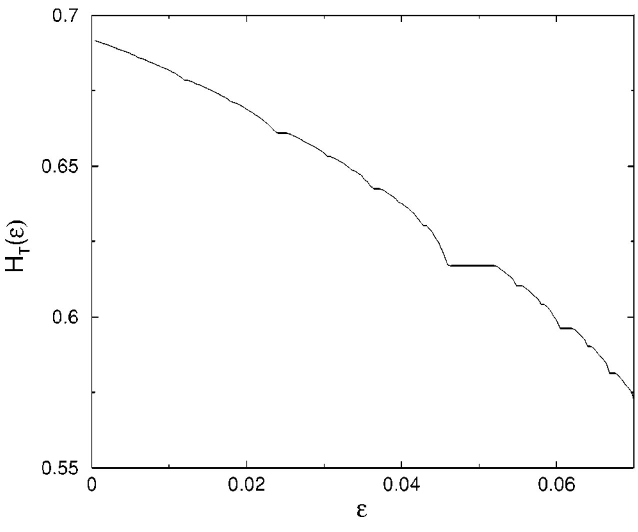

FIG. 3. Topological entropy, $H_T(\epsilon)$ versus the gap size ϵ, using $b=4.0$ in Eq. (12), and nonattracting saddle trajectories of length 200 000.

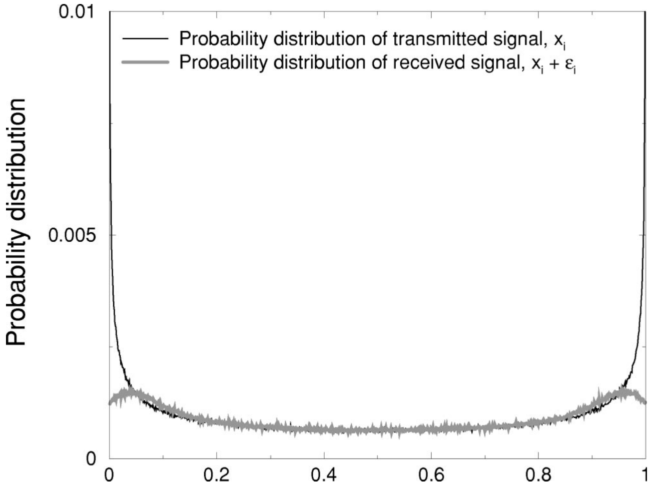

FIG. 4. Probability distribution of the encoding trajectory x (black line) and probability distribution of the received noisy trajectory $\tilde{x}$ (gray line). The horizontal axis represents either x or $\tilde{x}$.

In controlling a dynamical system to obtain a given response, in order to encode a message, it often happens that the perturbation is applied in critical situations. For example, if a small perturbation is applied to Eq. (12) when the trajectory is close to the boundaries of the interval J, the trajectory might go toward the attractor at infinity. So, it is appropriate to work with trajectories that are sufficiently far from the boundaries. This would be another reason for the reduction of information generation in a dynamical system by eliminating additional critical regions of the phase space.

VI. COMMUNICATION WITH UNBOUNDED NOISE

Let us model the channel by adding, to the encoding trajectory points, an independent noisy term η_i with Gaussian probability distribution of variance $\eta=0.05$ and zero mean. So, every point of the transmitted trajectory represented by x_i, is corrupted by noise, i.e., the receiver gets $\widetilde{x_i}=x_i+\eta_i$. Assuming that the source is a random process, whatever is the probability distribution of the source symbols the probability distribution of the encoding chaotic trajectory is given by the probability distribution on the chaotic set. This distribution, numerically obtained, using Eq. (12), for a trajectory of 2 000 000 points, is shown with the black line in Fig. 4. The knowledge of this distribution shape is advantageous when communicating with chaos for the following reasons:

(i) For the purpose of security, the analysis of the distribution of the transmitted encoding chaotic trajectory should not reveal any statistical particular behavior of the source symbols. So, whoever has no knowledge of the partition ω, with which it is possible to convert the trajectory into symbols whose probabilities of appearance should be the same as the source symbols of the message, cannot decode the message.

(ii) The information contained in the chaotic trajectory per point is given by the Kolmogorov–Sinai entropy which can also be obtained through the probability density, $\mu(x)$, of the distribution, $\rho(x)$, shown in this figure. Thus,

$$K_{\mathrm{KS}}=\int_0^1 \sum \lambda_i^+ \mu(x)dx. \tag{14}$$

As discussed before, if the positive Lyapunov exponents (denoted by λ_i^+) of the chaotic system does not depend on the density $\mu(x)$, thus $K_{\mathrm{KS}}=\Sigma\lambda_i^+$, which in the case for the logistic map $H_{\mathrm{KS}}=\ln(2)$.

(iii) For the purpose of filtering, when transmitting the signal through a noisy channel, the noisy trajectory $\widetilde{x_i}$ has a distribution, $\gamma(\widetilde{x_i})$, that differs from $\mu(x)$, as one can see by the gray line of Fig. 4. As the information is corrupted by the noise, the distribution $\mu(x)$ is changed into $\gamma(\widetilde{x_i})$. Any nonlinear filter applied to the trajectory or any other dynamical filter, based on the dynamical system dynamics,[1,2] should work so to make the distribution $\gamma(\tilde{x})$ to be as close as possible to $\rho(x)$.

(iv) To understand how the channel affects the transmitted information, we have to define the condition probability as

$$H_c=-p_{r_0,s_1}\ln(p_{r_0,s_1})-p_{r_1,s_0}\ln(p_{r_1,s_0}), \tag{15}$$

where p_{r_0,s_1} means the probability of sending the symbol "0" and receiving the symbol "1." If the modeled channel is symmetric with respect to the noise distribution, which also means that $p_{r_0,s_1}=p_{r_1,s_0}$, thus $H_c=-2p_{r_0,s_1}\ln(p_{r_0,s_1})$. The condition entropy describes the equivocation caused by the channel, in this case, due to noise. For this particular noise variance (chosen in order to have a distribution of the noisy transmitted trajectory very different from the distribution ρ), the equivocation is very high, $H_c=0.417\,530\,489$. Therefore, in order to be able to transmit information with very low probability of errors (under this noise condition), one needs to encode the source into S_c such that

$$H_T \geqslant H_s(S_c)-H_c, \tag{16}$$

where H_T-H_c is the amount of information that reaches the receiver.

VII. CONCLUSION

In conclusion, by using dynamical systems to generate the encoding trajectories (which are the wavesignals that are transmitted over the channel), one creates a communication system which inherits the characteristics of the respective dynamical system, in addition to the constraints of the source and the channel. The optimal encoding of the source is possible when the the information capacity H_T of the chaotic set used as the encoding wave signal is greater than or equal to the entropy of the source H_s. A nonoptimal encoding arises when $H_T \neq H_s$. When the encoding trajectories are transmitted over a channel with bounded noise, a subset of the chaotic set can be selected, a chaotic saddle, whose orbits are robust to the given noise amplitude, i.e., the noisy encoding trajectories of the saddle can be decoded into the original source message without losses. For this case, the condition for an efficient communication is given by $H_T(\epsilon)\geqslant H_s$, where $H_T(\epsilon)$ is the topological entropy of the saddle constructed for a gap of size ϵ. When the channel has unbounded noise, efficient communication is possible when $H_T \geqslant H_s - H_c$, where H_c is the condition entropy that measures the information losses due to the existence of noise in the channel.

In a channel with other physical restrictions, such as a limited-frequency bandwidth, efficient communication is possible if one finds a subset of the chaotic trajectories whose typical wavelength are high enough to be transmitted over this channel.

Finally, by combining Eqs. (5) and (11), we conclude that a dynamical system can encode a source if $\Sigma_{\lambda_i>0}\lambda_i \geqslant H_s(\mathcal{S})$, what can be used when one does not want to calculate the information capacity. Note that this equation is also valid even for higher dimensional systems.

ACKNOWLEDGMENTS

This work is supported by FAPESP and CNPq.

[1] M. S. Baptista, E. Macau, C. Grebogi, Y.-C. Lai, and E. Rosa, Phys. Rev. E **62**, 4835 (2000).

[2] M. S. Baptista, Phys. Rev. E **65**, 055201 (2002).

[3] R. F. Machado, M. S. Baptista, and C. Grebogi, "Cryptography with chaos at the physical level" (submitted).

[4] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (The University of Illinois Press, Chicago, 1949).

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

[6] A. N. Kolmogorov, Dokl. Akad. Nauk SSSR **119**, 861 (1958).

[7] Ya. G. Sinai, Dokl. Akad. Nauk SSSR **124**, 768 (1959).

[8] S. Newhouse and T. Pignataro, J. Stat. Phys. **72**, 1331 (1993).

[9] I. P. Cornfeld, S. V. Fomin, and Ya. G. Sinai, *Ergodic Theory* (Springer, New York, 1982).

[10] R. C. Adler, A. C. Konheim, and M. H. McAndrew, Trans. Am. Math. Soc. **114**, 309 (1965).

[11] D. Ruelle, *Chaotic Evolution and Strange Attractors* (Cambridge University Press, New York, 1989).

[12] R. L. Davidchack and Y. C. Lai, Phys. Rev. E **60**, 6172 (1999).

[13] S. Hayes and C. Grebogi, SPIE **2038**, 153 (1993); S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3039 (1993); S. Hayes, C. Grebogi, E. Ott, and A. Mark, *ibid.* **73**, 1781 (1994).

[14] D. Gulick, *Encounters with Chaos* (McGraw–Hill, New York, 1992), p. 105.

[15] E. M. Bollt, T. Stanford, Y.-C. Lai, and K. Zyczkowski, Phys. Rev. Lett. **85**, 3524 (2000).

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

[17] I. P. Mariño, E. Rosa, Jr., and C. Grebogi, Int. J. Bifurcation Chaos Appl. Sci. Eng. **9**, 2291 (1999); Phys. Rev. Lett. **85**, 2629 (2000).