Extracting messages masked by chaotic signals of time-delay systems

Changsong Zhou[1] and C.-H. Lai[1,2]
[1]Department of Computational Science, National University of Singapore, Singapore 119260
[2]Department of Physics, National University of Singapore, Singapore 119260

(Received 1 October 1998)

We show how to extract messages masked by a chaotic signal of a time-delay system with very high dimensions and many positive Lyapunov exponents. Using a special embedding coordinate, the infinite-dimensional phase space of the time-delay system is projected onto a special three-dimensional space, which enables us to identify the time delay of the system from the transmitted signal and reconstruct the chaotic dynamics to unmask the hidden message successfully. The message extraction procedure is illustrated by simulations with the Mackey-Glass time-delay system for two types of masking schemes and different kinds of messages. [S1063-651X(99)06604-0]

PACS number(s): 05.45.−a

The application of chaotic synchronization systems to secure communication has been a field of great research interest [1–5]. However, it has been shown that in some low-dimensional chaotic systems with only one positive Lyapunov exponent, the hidden message can be unmasked by the dynamical reconstruction of the chaotic signal using nonlinear dynamical forecasting (NLDF) methods [6,7], by using some simple return maps [8], or by using some other methods [9]. It has been suggested that one possible way to improve the security is to employ hyperchaos in communication [5,10,11], based on the consideration that increased randomness and unpredictability of the hyperchaotic signals will make it more difficult to extract a masked message. Lately, it has been shown that messages masked by hyperchaos of six-dimensional systems can also be attacked using NLDF methods [15], showing that going to higher dimensions does not produce a drastic improvement in the security of the system if the local dynamics are still quite low dimensional.

It has been known that very simple time-delay systems [12] are able to exhibit hyperchaos [13]. Therefore, it was proposed in a recent paper that time-delay systems provide alternative simple and efficient tools for chaos communication with low detectability [14]. Chaotic attractors of time-delay systems can have much higher dimensions, and many more positive Lyapunov exponents than the system studied in Ref. [15], and whether the communication is as secure as expected has not been examined yet. In this paper, we will show that messages masked by chaos of a time-delay system, with very high dimensions and many positive Lyapunov exponents, can be extracted successfully, not using some well-established dynamical reconstruction methods [6,7,15], but by using a special, yet simple, embedding approach proposed recently for a time-series analysis of time-delay systems [16–18].

In this paper we focus our attention on scalar time-delay systems of the forms

$$\dot{x}=f(x,x_{\tau_0}),\quad x_{\tau_0}=x(t-\tau_0). \tag{1}$$

For such systems with large time delay τ_0, some well-established nonlinear time-series analysis methods [19–21] run into severe problems [22,23].

An observation of Eq. (1) shows that in a special three-dimensional space $(x_{\tau_0},x,\dot{x})$, the dynamics of the system is restricted to a smooth manifold defined by Eq. (1), namely,

$$\dot{x}-f(x,x_{\tau_0})=0. \tag{2}$$

However, in a similar space $(x_\tau,x,\dot{x})$ with $\tau\neq\tau_0$, the trajectory is no longer restricted to a smooth hypersurface, but fills a great part of the space, resulting in a more complicated structure. This makes it possible to detect the time delay τ_0 of the system by some measures of the complexity as a function of embedding delay τ, and then to recover the dynamics of the system [16–18].

This approach is applied in this paper to extract messages masked by chaotic signals of the above time-delay system. In the context of synchronization, we consider the following communication system with two masking schemes considered in Ref. [14].

Scheme I.

$$\dot{x}=f(x,x_{\tau_0})+kI,$$

$$s=x+I. \tag{3}$$

Scheme II.

$$\dot{x}=f(x,x_{\tau_0})+kIx,$$

$$s=x(1+I). \tag{4}$$

An authorized receiver has an identical copy of the time-delay system that is synchronized with x by the following coupling:

$$\dot{y}=f(y,y_{\tau_0})+k(s-y). \tag{5}$$

In this communication system, the message I, often much lower in amplitude than the chaotic signal x, is injected into the transmitter to modulate the time-delay system. The injection of the message has effectively altered the transmitter dynamics, and has been considered a way to improve the security [5,14] compared with methods where the message is directly added to the chaotic carrier [2]. The masking scheme II is expected to produce securer masking because the message and the chaotic signal couple with each other in a more sophisticated manner. s is the signal transmitted to the receiver to achieve synchronization with a proper coupling parameter k. As a third party, we do not have a receiver system y, but have the time series of the transmitted signal s sampled by a time interval h.

Our message extraction approach consists of the following steps.

(1) We project the time series $\{s^i\}$ to the three-dimensional space $(s^i_\tau, s^i, \dot{s}^i)$ with $\dot{s}^i$ estimated as $\dot{s}^i = (s^{i+1} - s^{i-1})/2h$.

(2) We investigate the complexity of the projected trajectory in the $(s^i_\tau, s^i, \dot{s}^i)$ space by measuring the smoothness. First, we apply a local linear approximation

$$\hat{\dot{s}} = a_i + b_i s + c_i s_\tau \tag{6}$$

to a small neighborhood U_i of a point (s^i_τ, s^i). The fitting parameters a_i, b_i, and c_i are computed by a least-squares fit, and the local fitting error is

$$e_i = \frac{1}{M_{U_i}} \sum_{j \in U_i} (\dot{s}^j - a_i - b_i s^j - c_i s^j_\tau)^2, \tag{7}$$

where M_{U_i} is the number of the neighbor points. The average E of e_i over a number of points (x^i_τ, x^i) provides a measure of the smoothness of the structure in the projected space. If $\tau = \tau_0$, the trajectory is restricted to the close vicinity of the smooth hypersurface for a small enough message I, and E can be rather small if the size ϵ of neighborhood is sufficiently small; otherwise, E can be quite large because there is no unique functional relationship between $\dot{s}$ and (s_τ, s) for $\tau \neq \tau_0$. We can expect a minimum of E at $\tau = \tau_0$. By examining E as a function of embedding delay τ, we can detect the time delay τ_0 of the system by the minimum of E.

(3) After the correct identification of the value of τ_0, we use the local linear approximation

$$\hat{\dot{x}}^i = a_i + b_i s^i + c_i s^i_{\tau_0} \tag{8}$$

as an estimation of $\dot{x} = f(x, x_{\tau_0})$ of the time-delay system in the absence of message I. From Eqs. (3) and (4) we have $\dot{s} = f(x, x_{\tau_0}) + kI + \dot{I}$ for the masking scheme I, and $\dot{s} = f(x, x_{\tau_0}) + kIx + \dot{x}I + x\dot{I}$ for scheme II. For the conditions $|I| \ll |x|$, $|\dot{I}| \ll |kI|$, and $|\dot{x}| \ll |kx|$ with $|\cdot|$ denoting the amplitude, the extracted message can be estimated as

$$kI^i_e = \begin{cases} \dot{s}^i - \hat{\dot{x}}^i, & \text{scheme I} \\ (\dot{s}^i - \hat{\dot{x}}^i)/s^i, & \text{scheme II.} \end{cases} \tag{9}$$

To illustrate the message extraction procedure, we employ the Mackey-Glass (MG) equation as in Ref. [14],

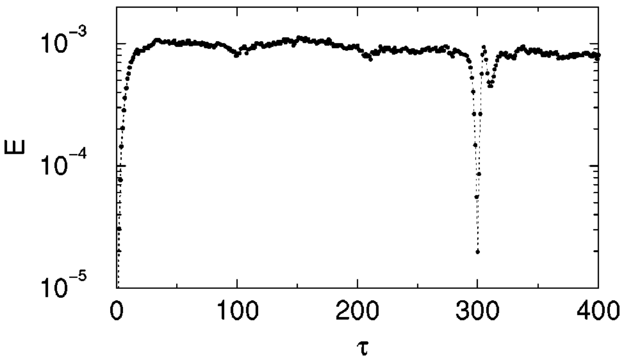

FIG. 1. As a measure of the smoothness, the average fitting error E, as a function of the embedding delay τ, has a pronounced minimum at the value of the time delay of the system.

$$\dot{x} = f(x, x_{\tau_0}) = -bx + \frac{a x_{\tau_0}}{1 + x^c_{\tau_0}}. \tag{10}$$

With parameters $b = 0.1$, $a = 0.2$, and $c = 10$, the system is chaotic for $\tau_0 > 16.8$. In the chaotic regime, the number of positive Lyapunov exponents increases with τ_0 and is about 15 for $\tau_0 = 300$, and the chaotic attractor dimension increases almost linearly with τ_0, for example, the Kaplan-Yorke dimension is roughly 30 for $\tau_0 = 300$ [14]. In our simulation, we take $\tau_0 = 300$ and $k = 1.0$ [14].

In all of the following examples, we record $N = 50\,000$ points with the sample interval $h = 0.5$. The size of the neighborhood is set by $\epsilon = 0.01$.

First, let us consider a simple message signal of the sine wave $I(t) = A \sin(2\pi t/T)$ with $A = 0.005$ and $T = 200$. Figure 1 shows the measure of smoothness E as a function of τ. A pronounced minimum at $\tau = 300$ enables us to identify the time delay of the system correctly, although the system is modulated by the injected message I. This is also true for our other examples in the following, where the results of E are not presented to save space.

With the correct value of the time delay, the message can be extracted successfully, as illustrated in Fig. 2 for the masking scheme I, and in Fig. 3 for the masking scheme II, respectively. A comparison between the time series of s in Fig. 3(a) and that of $\Delta s = \dot{s} - \hat{\dot{x}}$ in Fig. 3(b) reveals that when s is close to zero in a certain period of time, the corresponding Δs is also close to zero in this period of time, indicating that Δs is modulated by s. The demodulated signal $\Delta s/s$ is shown in Fig. 3 as the extracted message. The results show that the masking scheme II does not produce drastic improvement of the security although it can result in a greater distortion of the extracted messages.

Now let us consider an example of a more complicated message signal. In our simulation, we construct a message

$$I(t) = \frac{A}{m} \sum_{i=1}^{m} B_i \sin(2\pi t/T_i), \tag{11}$$

where B_i and T_i are random numbers uniform on (0,1) and (50,500) respectively.

Figures 4 and 5 are results of message extraction for a realization of such a complicated message with $A = 0.01$ and

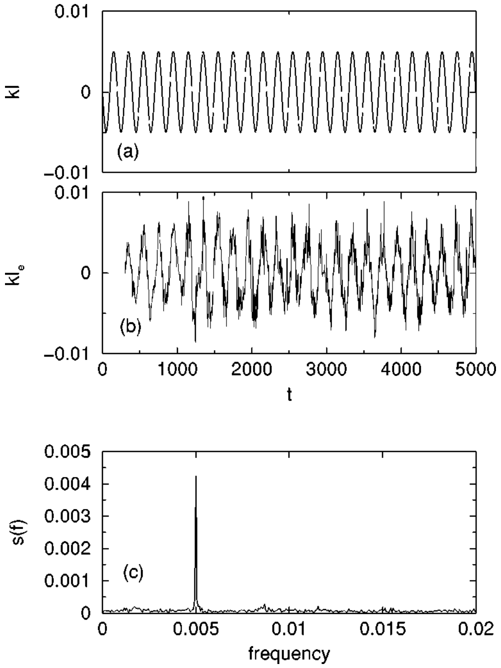

FIG. 2. Illustration of message extraction for a sine wave message masked by scheme I. (a) The original message signal kI, (b) the extracted message, and (c) the power spectrum of the extracted message.

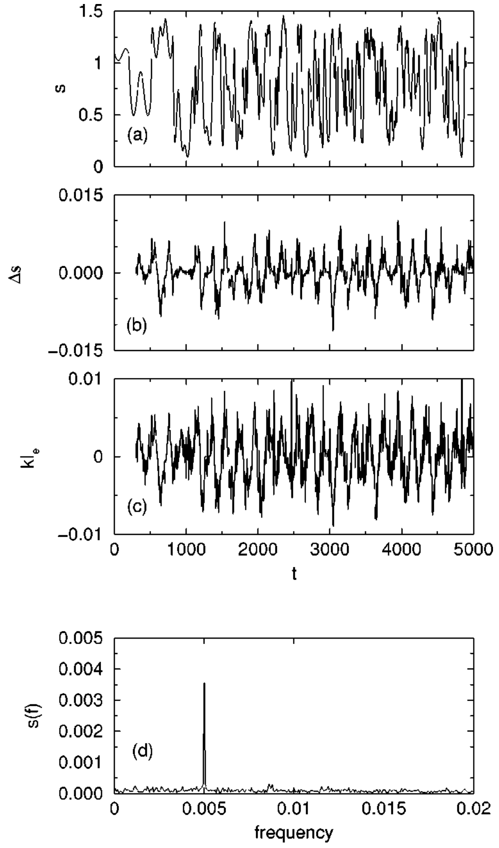

FIG. 3. Illustration of message extraction for the sine wave message masked by scheme II. (a) A time series of the transmitted signal s, (b) $\Delta s=\dot{s}-\dot{\hat{x}}^{i}$, (c) the extracted message, and (d) the power spectra of the extracted message.

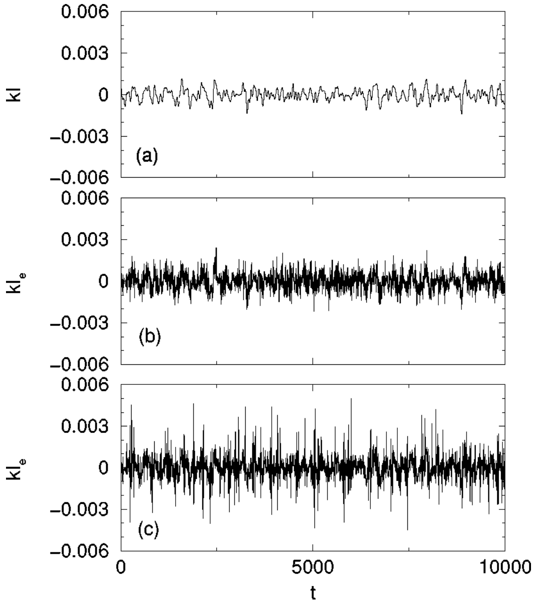

FIG. 4. Illustration of message extraction for a complicated message. (a) The original message, (b) the extracted message for the masking scheme I, and (c) the extracted message for the masking scheme II.

$m=100$. Again, it is seen that the quality of the recovered message deteriorates more when masking scheme II is employed. However, a comparison between the power spectra of the original and extracted messages has shown that unmasking is successful for both masking schemes.

We should point out that the identification of the time delay τ_0 and the quality of the recoved message is not sensitive to the choice of N, h, and ϵ. In general, ϵ should be small enough to apply the local linear approximation, but large enough to average out the fluctuations induced by the message. As a result, if the amplitude of the message is too large, the quality of the recovered message can be quite poor,

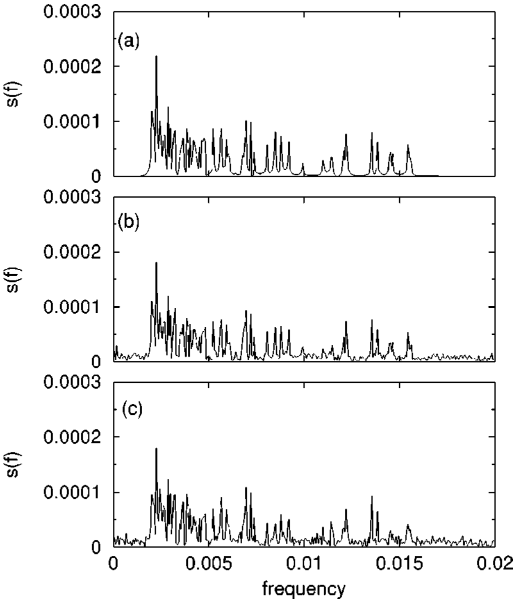

FIG. 5. The power spectra of the original message and the extracted messages in Fig. 4.

and the message extraction becomes more difficult. However, the chaotic signals may not provide enough masking for messages with quite large amplitudes.

For the MG time-delay system studied above, the frequency of the message should be rather low because the power spectrum of the chaotic signal is very low at high frequencies, and is not enough to mask messages with high frequencies. A low frequency of the message means $|\dot{I}| \ll |I|$, which is an advantage for a third party to recover a message with high quality.

In summary, we present a simple method to extract messages masked by a chaotic signal of a time-delay system, which has a very high dimensionality and many positive Lyapunov exponents. Using a special embedding space, the infinite dimensional phase space of the time-delay system is projected onto a three-dimensional space, independent of the actual dimension and the number of positive Lyapunov exponents of the chaotic attractor. The time delay of the system is correctly identified even in the presence of the message, which enables us to extract the message successfully using a simple local reconstruction of the time-delay system in the three-dimensional space.

We come to the conclusion, based on our analysis, that communication using the time-delay system is not as secure as intuitively expected. In general, the security of chaos communication may be spoiled if any reconstruction of the dynamics of the system is possible in some appropriate space, even for very-high-dimensional dynamics.

This work was supported in part by Research Grant No. RP960689 at the National University of Singapore. Dr. Zhou was supported by NSTB.

[1] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[2] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[3] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).

[4] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and Shang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992).

[5] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).

[6] K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959 (1994).

[7] K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 367 (1996).

[8] G. Perez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).

[9] C. S. Zhou and T. L. Chen, Phys. Lett. A **234**, 429 (1997).

[10] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, Phys. Rev. Lett. **76**, 904 (1996).

[11] L. Kocarev, U. Parlitz, and T. Stojanovski, Phys. Lett. A **217**, 280 (1996).

[12] M. C. Mackey and L. Glass, Science **197**, 287 (1977).

[13] J. D. Farmer, Physica D **4**, 366 (1982).

[14] B. Mensour and A. Longtin, Phys. Lett. A **244**, 59 (1998).

[15] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998).

[16] M. J. Bünner, M. Popp, Th. Meyer, A. Kittel, U. Rau, and J. Parisi, Phys. Lett. A **211**, 345 (1996).

[17] M. J. Bünner, M. Popp, Th. Meyer, A. Kittel, and J. Parisi, Phys. Rev. E **56**, 5083 (1997).

[18] R. Hegger, M. J. Bünner, and H. Kantz, Phys. Rev. Lett. **81**, 558 (1998).

[19] P. Grassberger and I. Procaccia, Physica D **9**, 189 (1983).

[20] J. P. Eckmann and D. Ruelle, Rev. Mod. Phys. **57**, 617 (1985).

[21] M. B. Kennel, R. Brown, and H. D. I. Abarbanel, Phys. Rev. A **45**, 3403 (1992).

[22] Th. Meyer and N. H. Packard, in *Nonlinear Modeling and Forecasting*, edited by M. Casdagli and S. Eubank (Addison-Wesley, Redwood City, CA, 1992).

[23] R. Hegger, H. Kantz, and Olbrich, in *Proceedings of the Workshop on Nonlinear Techniques in Physiological Time Series Analysis*, edited by H. Kantz, J. Kurths, and G. Mayer-Kress (Springer-Verlag, Berlin, 1997).