Extracting information masked by the chaotic signal of a time-delay system

V. I. Ponomarenko and M. D. Prokhorov

Saratov Department of the Institute of RadioEngineering and Electronics of Russian Academy of Sciences, Zelyonaya Street 38, Saratov 410019, Russia

(Received 5 April 2002; published 27 August 2002)

We further develop the method proposed by Bezruchko et al. [Phys. Rev. E 64, 056216 (2001)] for the estimation of the parameters of time-delay systems from time series. Using this method we demonstrate a possibility of message extraction for a communication system with nonlinear mixing of information signal and chaotic signal of the time-delay system. The message extraction procedure is illustrated using both numerical and experimental data and different kinds of information signals.

DOI: 10.1103/PhysRevE.66.026215 PACS number: 05.45.—a

I. INTRODUCTION

The use of chaotic signals for secure communication has been an active area of research in recent years [1–7]. Chaotic communication systems have attracted a lot of attention due to the broadband power spectrum of chaotic signals, high speed of information transmission, and tolerance to sufficiently high levels of noise. Besides, many chaotic communication schemes are simply realized and demonstrate a rich variety of different oscillating regimes.

Practically all known communication schemes using chaotic signals are based on synchronization of chaotic systems. Different approaches for the transmission of information signals using chaotic dynamics have been proposed, for example, chaotic masking, chaotic modulation, nonlinear mixing, chaotic switching, and others. However, not all chaotic communication schemes are as secure as expected. For example, some communication schemes using low-dimensional chaotic signals can be unmasked by the dynamical reconstruction of the chaotic system from the time series [8–11] or by using suitable return maps [12–14]. The use of hyperchaotic signals of high-dimensional chaotic systems does not always help to improve the security of communication. The hidden message can also be extracted in these cases using the dynamical reconstruction methods [15], surrogate data analysis [16], spectrograms [17], neural networks [18], and wavelet transform [19]. In Refs. [20,21], it has been proposed to employ time-delay systems, demonstrating chaotic dynamics of a very high dimension [22,23], in private communication. However, as it has been shown in Ref. [24] that, for chaotic masking schemes, the hidden information can be extracted even in this case using the methods of reconstruction of time-delay systems from the time series [25–27].

In this paper we propose a method for the reconstruction of the dynamics of a transmitter, which is a chaotic time-delay system, from the transmitted signal. Using this method we unmask a chaotic communication system with nonlinear mixing of chaotic and information signals. The description of the communication scheme is given in Sec. II. In Sec. III the method for the estimation of the parameters of time-delay system is presented. In Sec. IV we extract the hidden information signals using both numerical and experimental data. The obtained results are summarized and discussed in Sec. V.

II. COMMUNICATION SCHEME

A communication scheme with nonlinear mixing of chaotic and information signals has been proposed in Ref. [5] and developed in Ref. [6]. The schemes considered in Refs. [5,6] employed chaotic signals of a low-dimensional ring oscillating system [28] and of a ring scheme based on Chua circuit [29], respectively. In this paper we have chosen the signals of time-delay systems with many positive Lyapunov exponents as chaotic carriers.

A block diagram of the communication system with nonlinear mixing is shown in Fig. 1. In the absence of information signal \( m(t) = 0 \), the transmitter, representing the ring system composed of delay, nonlinear, and inertial elements, can be described in the simplest case by the delay-differential equation

\[
\varepsilon_0 \dot{x}(t) = -x(t) + f(x(t - \tau_0)),
\]

where \( x(t) \) is the system state at time \( t \), function \( f \) defines nonlocal correlations in time, \( \tau_0 \) is the delay time, and parameter \( \varepsilon_0 \) characterizes the inertial properties of the system. The information signal \( m(t) \) is added to the chaotic signal \( x(t) \) with the help of a summator and the signal \( s(t) = x(t) + m(t) \) is transmitted into the communication channel and simultaneously injected into the feedback circuit of the transmitter whose dynamics is described by the equation

\[
\varepsilon_0 \dot{x}(t) = -x(t) + f(x(t - \tau_0) + m(t - \tau_0)).
\]

With this nonlinear mixing the information signal is directly involved in the formation of a complicated dynamics of the chaotic system.
A receiver is composed of the same elements as the transmitter, except that the summatior is replaced by a subtractor breaking the feedback circuit. The receiver equation is

\[ \varepsilon_0 \ddot{y}(t) = -y(t) + f(x(t - \tau_0) + m(t - \tau_0)). \]  

At the output of the subtractor, we have the extracted information signal \( m'(t) = x(t) + m(t) - y(t) \).

If the transmitter and the receiver are composed of identical elements, they become completely synchronized after the transient process. The difference between the oscillations of systems (2) and (3), \( \Delta(t) = x(t) - y(t) \), decreases in time for any \( \varepsilon_0 > 0 \), since \( \Delta(t) = -\Delta/t_0 \). As the result of synchronization, \( x(t) = y(t) \) and \( m'(t) = m(t) \). It should be noted that the quality of the extraction of message \( m(t) \) does not depend on its amplitude and frequency characteristics. By this is meant that the considered communication scheme allows one to transmit complicated information signals without distortion.

If we take away the delay line in the receiver, Eq. (3) will take the form

\[ \varepsilon_0 \ddot{y}(t) = -y(t) + f(x(t) + m(t)). \]  

In this case the receiver synchronizes with the transmitter in such a way that \( x(t) = y(t - \tau_0) \) or, equivalently, \( x(t + \tau_0) = y(t) \). In other words, at time \( t \), the receiver (4) synchronizes with the future state of the transmitter (2) at time \( t + \tau_0 \). This is the case of anticipating synchronization [30]. The delay line will be necessary to extract the information signal. If we delay the signal \( y(t) \) by \( \tau_0 \) and feed the signal \( y(t - \tau_0) \) at the subtractor input, then we receive \( m'(t) = x(t) + m(t) - y(t - \tau_0) = m(t) \) at the subtractor output.

**III. RECONSTRUCTION OF TIME-DELAY SYSTEM USED IN THE TRANSMITTER**

The security of chaotic communication systems is based on the assumption that the parameters of the chaotic transmitter are known only to the authorized receiver having an identical copy of the transmitter. Using the communication scheme considered in Sec. II we show that a hidden message can be extracted by a third party having only the time series of the transmitted signal \( x(t) \). To do this, we have to recover the parameters of the time-delay system (1) generating a masking chaotic signal \( x(t) \). The parameters \( \tau_0 \) and \( \varepsilon_0 \) and the nonlinear function \( f \) are unknown in this case. Various methods for the estimation of the time-delay system parameters from time series have been proposed (see, e.g., Refs. [31–33] and references therein).

To recover the delay time \( \tau_0 \) from the time series we exploit the method proposed recently in Ref. [33], where we have shown that there are practically no extrema separated in time by \( \tau_0 \) in the time series of time-delay system (1). Then, for \( \tau_0 \) definition one has to determine the extrema in the time series, after that one has to define for different values of time \( \tau \) the number \( N \) of pairs of extrema separated in time by \( \tau \), and then one has to construct the \( N(\tau) \) plot. If \( N \) is normalized to the total number of extrema, then for sufficiently large extrema number it can be used as an estimation of probability to find a pair of extrema in the time series, separated by the interval \( \tau \). The absolute minimum of \( N(\tau) \) is observed at the delay time \( \tau_0 \).

The qualitative features of the \( N(\tau) \) plot specified by the delay-induced dynamics are retained in the presence of message in the transmitted signal if the amplitude of the message

**FIG. 2.** (a) Length \( L \) of a line connecting points ordered with respect to \( x(t - \tau_0) \) in the plane \( \{x(t - \tau_0), x(x(t) + x(t))\} \) as a function of \( \varepsilon \). The inset shows \( L(\varepsilon) \) in the neighborhood of the minimum. \( L_{\text{min}}(\varepsilon) = L(10.0) \). (b) The recovered nonlinear function.

**FIG. 3.** Estimation of the parameter \( \varepsilon_0 \) and function reconstruction from the time series of the Mackey-Glass equation with additive Gaussian white noise. (a) The \( L(\varepsilon) \) plot. \( L_{\text{min}}(\varepsilon) = L(9.9) \). (b) Nonlinear function (7) (solid line) and the recovered function (dots).

**FIG. 4.** (a) The frequency-modulated signal for \( A = 0.01, B = 3, f_c = 5 \times 10^{-3}, \) and \( f_m = 5 \times 10^{-4} \). (b) The power spectrum of the frequency-modulated signal \( m(t) \).
is not very large. As it has been shown in Ref. [33], the method is still efficient for a noise level of 10%. However, the level of information signal in the communication schemes with nonlinear mixing must be sufficiently low, otherwise the chaotic signal may not provide enough masking [6].

To recover the parameter \( \varepsilon_0 \) and the nonlinear function \( f \) of system (1) from the chaotic time series, we propose a method that we illustrate at first for the case of message absence. From Eq. (1) it follows that

\[
e_{\varepsilon_0} \dot{x}(t) + x(t) = f(x(t - \tau_0)).
\]  

(5)

Thus, it is possible to reconstruct the nonlinear function by plotting in a plane a set of points with coordinates \([x(t - \tau_0), \varepsilon_0 \dot{x}(t) + x(t)]\). According to Eq. (5), the constructed set of points reproduces the function \( f \). Since the parameter \( \varepsilon_0 \) is a priori unknown, one needs to plot \( \varepsilon \dot{x}(t) + x(t) \) versus \( x(t - \tau_0) \) under variation of \( \varepsilon \), searching for a single-valued dependence in the plane \([x(t - \tau_0), \varepsilon \dot{x}(t) + x(t)]\), which is possible only for \( \varepsilon = \varepsilon_0 \). As a quantitative criterion of single valuedness in searching for \( \varepsilon_0 \) we use the minimal length of a line \( L(\varepsilon) \), connecting all points ordered with respect to \( x(t - \tau_0) \) in the plane \([x(t - \tau_0), \varepsilon \dot{x}(t) + x(t)]\). The minimum of \( L(\varepsilon) \) is observed at \( \varepsilon = \varepsilon_0 \). The set of points constructed for the defined \( \varepsilon_0 \) in the plane \([x(t - \tau_0), \varepsilon_0 \dot{x}(t) + x(t)]\) reproduces the nonlinear function that can be approximated if necessary. In contrast to methods presented in Refs. [25,26], which use only extremal points or points selected according to a certain rule for the nonlinear function recovery, the proposed technique uses all points of the time series. It allows one to estimate the parameter \( \varepsilon_0 \) and to reconstruct the nonlinear function from short time series even in the regimes of weakly developed chaos.

As an example, the \( L(\varepsilon) \) plot is shown in Fig. 2(a) for the time series produced by the Mackey-Glass equation

\[
\dot{x}(t) = -b x(t) + \frac{a x(t - \tau_0)}{1 + x^2(t - \tau_0)},
\]  

(6)

which can be converted to Eq. (1) with \( \varepsilon_0 = 1/b \) and the function

\[
f(x(t - \tau_0)) = \frac{a x(t - \tau_0)}{b(1 + x^2(t - \tau_0))}.
\]  

(7)

The parameters of the system (6) are chosen to be \( a = 0.2, b = 0.1, c = 10, \) and \( \tau_0 = 300 \) to produce a dynamics on a high-dimensional chaotic attractor [23]. The sampling time is set by \( 1. L(\varepsilon) \) is normalized to the most uncorrelated point set. To reduce the computation time one can choose a large initial step of \( \varepsilon \) variation and then reduce it in the neighborhood of minimum \( L(\varepsilon) \). Thus, in Fig. 2(a) the step of \( \varepsilon \) variation is 1 and in the inset this step is reduced to 0.1. The minimum of \( L(\varepsilon) \) takes place exactly at \( \varepsilon_0 = 1/b = 10 \). In Fig. 2(b) the nonlinear function is shown that has been recovered with the defined \( \varepsilon_0 \). This recovered function coincides practically with the true function (7). Note that for the construction of the \( L(\varepsilon) \) plot and for the recovery of the function \( f \) we use only 1000 points of the time series.

The mixing of chaotic signal and information signal of small amplitude does not significantly influence on the accuracy of \( \varepsilon_0 \) estimation. To investigate the robustness of the method to perturbations we apply it to the data produced by adding a zero-mean Gaussian white noise to the time series of Eq. (6). In Fig. 3, the \( L(\varepsilon) \) plot and the recovered nonlinear function are presented for the case where the additive noise has a standard deviation of 3% of the standard deviation of the data without noise. At the reconstruction of the nonlinear function we use \( \varepsilon_0' = 9.9 \), for which the minimum of \( L(\varepsilon) \) is observed. For higher noise levels the accuracy of

FIG. 6. Reconstruction of the Mackey-Glass system for the case of nonlinear mixing of its chaotic signal and frequency-modulated harmonic signal. (a) The \( N(\tau) \) plot. \( N_{\text{min}}(\tau) = N(300.0) \). (b) The \( L(\varepsilon) \) plot. \( L_{\text{min}}(\varepsilon) = L(10.0) \). (c) The recovered nonlinear function.
\( \varepsilon_0 \) estimation becomes worse and a set of points in the plane \([x(t - \tau_0), x'(t) + x(t)]\) is more dispersed.

**IV. EXTRACTING INFORMATION SIGNAL MIXED WITH CHAOTIC SIGNAL**

The information signal \( m(t) \), masked by the chaotic communication system in such a way that its presence is imperceptible in the communication channel, can be extracted by an unauthorized listener from the transmitted signal \( s(t) \). Using the method considered in Sec. III it is possible to estimate the parameters of the chaotic transmitter. Knowing these parameters one can construct the receiver. The more accurate is the estimation of the system parameters, the higher is the quality of synchronous chaotic response of the receiver and, as a consequence, the higher is the quality of the message extraction.

We apply the method to a time series produced by nonlinear mixing of the chaotic signal of the Mackey-Glass system (6) and the frequency-modulated harmonic signal

\[
m(t) = A \sin(2\pi f_c t - B \cos(2\pi f_m t)),
\]

where \( A \) defines the message amplitude, \( f_c \) is the central frequency of the power spectrum of the signal, \( B \) is the frequency modulation index, and \( f_m \) is the modulation frequency. Part of the time series and the power spectrum of frequency-modulated signal are presented in Fig. 4. As a bandpass signal, the frequency-modulated harmonic signal better imitates the structure of speech and music signals than a simple harmonic signal.

Figure 5 shows part of the time series of the transmitted chaotic signal \( s(t) = x(t) + m(t) \) and the power spectrum of \( s(t) \). With a fourth-order Runge-Kutta method for delay-differential equations we record 50,000 points with the sampling interval \( h = 0.5 \). As it can be seen from Figs. 4 and 5,
Figure 6 illustrates the reconstruction of the transmitter parameters. Figure 6(a) shows the number $N$ of pairs of extrema in the time series of $s(t)$, separated in time by $\tau$. To construct the $N(\tau)$ plot we use 20000 points of the time series of $s(t)$. The time series exhibits about 600 extrema and $N(\tau)$ is normalized to their total number. The time derivatives $\dot{x}(t)$ are estimated from the time series by applying a local parabolic approximation. The step of $\tau$ variation in Fig. 6(a) is equal to the integration step $h=0.5$. The location of the absolute minimum of $N(\tau)$ allows one to estimate the delay time $\tau_0=300.0$. Note that we obtain the same values of $\tau_0$ for a time series whose length is shorter by a factor of 3.

To construct the $L(\varepsilon)$ plot [Fig. 6(b)] we use only 2000 points of $s(t)$ realization. The step of $\varepsilon$ variation is set by 0.1. The minimum of $L(\varepsilon)$ takes place at $\varepsilon_0=10.0$ ($\varepsilon_0=1/b=10$). The nonlinear function recovered using the estimated $\tau_0$ and $\varepsilon_0$ is shown in Fig. 6(c). For the approximation of the recovered function we use polynomials of different degree. The approximating function is sufficiently close to the function (7) and ensures a high quality of synchronous response of the receiver if the degree of the polynomial is greater than 11. To increase the accuracy of polynomial approximation we use all points of the time series at the reconstruction of the nonlinear function.

The quality of the recovery of the system parameters can be estimated by the level of the desynchronization noise (Fig. 7) leading to a worse quality of synchronous chaotic response. It follows from Fig. 7 that the level of the desynchronization noise is about 0.1% of the level of the chaotic signal and can achieve 10% of the amplitude of the information signal [Fig. 4(a)] at the receiver output. Parts of the time series and power spectra of the extracted frequency-modulated signal are presented in Fig. 8.

As another example, we consider an experimental communication system using the chaotic signal of an electronic oscillator with delayed feedback. For the case where the filter (see Fig. 1) is a low-frequency first-order $RC$ filter, this oscillator is given by

$$RC\dot{V}(t) = -V(t) + f(V(t - \tau_0)), \quad (9)$$

where $V(t)$ and $V(t - \tau_0)$ are the delay line input and output voltages, respectively; $R$ and $C$ are the resistance and capacitance of the filter elements. Eq. (9) is of the form (1) with $v_0=RC$. In our experiment the nonlinear device has a quadratic transfer function. The chaotic signal $V(t)$ of the system (9) is nonlinearly mixed with the harmonic signal $m(t) = A\sin(2\pi f_c t)$ with amplitude $A$ and frequency $f_c$. The transmitted signal is $s(t) = V(t) + m(t)$. We record the signals $m(t)$ and $s(t)$ using an analog-to-digital converter with the sampling frequency $f_s=4$ kHz. In Fig. 9 parts of the time series and power spectra of these signals are presented.

Figure 10 illustrates the reconstruction of the transmitter. Since the delay time $\tau_0=54.7$ ms is not a multiple of the sampling time $T_s=0.25$ ms, the recovery of $\tau_0$ cannot be absolutely accurate. For the step of $\tau$ variation equal to $T_s$, the minimum of $N(\tau)$ takes place at $\tau'_0=54.75$ ms [Fig. 10(a)]. The $L(\varepsilon)$ plot, constructed with $\tau'_0$ and the step of $\varepsilon$ variation equal to 0.025 ms, demonstrates the minimum at $\varepsilon'_0=4.2$ ms [Fig. 10(b)] ($\varepsilon'_0=4.215$ ms). The recovered nonlinear function is shown in Fig. 10(c). The approximation of this function with a polynomial of degree 2 allows us to obtain a high-quality synchronous response of the receiver and, as the result, a sufficiently qualitative extraction of the hidden message. Parts of the time series and the power spectrum of the extracted harmonic signal are shown in Fig. 11. Thus, the extraction of hidden information is possible in spite of the presence of noise inherent in a real system and the absence of multiplicity between the characteristic tempo-

![FIG. 10. Reconstruction of the electronic oscillator with delayed feedback for the case of nonlinear mixing of its chaotic signal and harmonic signal. (a) The $N(\tau)$ plot. $N_{\text{min}}(\tau)=N(54.75 \text{ ms})$. (b) The $L(\varepsilon)$ plot. $L_{\text{min}}(\varepsilon)=L(4.2 \text{ ms})$. (c) The recovered nonlinear function.](image-url)

![FIG. 11. (a) The extracted harmonic signal. (b) The power spectrum of the extracted message.](image-url)
ral scales of the chaotic transmitter and the sampling time, which result in the inaccurate estimation of the parameters.

V. CONCLUSION

We have proposed the method for reconstructing time-delay systems from time series. This method is based on the statistical analysis of time intervals between extrema in the time series and the projection of the infinite-dimensional phase space of a time-delay system to suitably chosen two-dimensional subspaces. The method allows one to estimate the delay time, the parameter characterizing the inertial properties of the system, and the nonlinear function even in the presence of message signal of small amplitude.

The method considered with systems like Eq. (1) can be extended to a more general class of time-delay systems. As it has been shown in Ref. [33], the procedure of the delay time estimation from the $N(\tau)$ plot can be successfully applied to time series gained from a wide class of time-delay systems including high-dimensional ones. The proposed method of estimation of the parameter $\varepsilon_0$ and the nonlinear function can be also applied to a variety of time-delay systems of order higher than that of Eq. (1). For instance, the dynamics of an electronic oscillator with delayed feedback containing two identical in-series $RC$ filters is described by the second-order delay-differential equation

$$\varepsilon_0^2 \ddot{V}(t) + 2\varepsilon_0 \dot{V}(t) = -V(t) + f(V(t - \tau_0)), \quad (10)$$

where $\varepsilon_0 = RC$. Plotting $\varepsilon^2 \ddot{V}(t) + 2\varepsilon \dot{V}(t) + V(t)$ versus $V(t - \tau_0)$ under variation of $\varepsilon$, we can estimate the parameter $\varepsilon_0$ by the location of the minimum of $L(\varepsilon)$ and recover the function $f$. However, the quality of reconstruction deteriorates, since the procedure involves numerical calculation of the second derivative.

The recovery of the parameters of time-delay systems gives a possibility of message extraction for the communication schemes using chaotic signals of these systems. Hence, the communication systems using chaotic signals of time-delay systems can be successfully unmasked in spite of very high dimension and a large number of positive Lyapunov exponents of chaotic attractors of time-delay systems. We have illustrated the possibility of message extraction for the communication system with nonlinear mixing of information signal and chaotic signal of time-delay system. The extraction of hidden message from the transmitted signal is demonstrated using both numerical data, produced by nonlinear mixing of chaotic signal of the Mackey-Glass system and frequency-modulated harmonic signal, and experimental data, produced by nonlinear mixing of harmonic signal and chaotic signal of the electronic oscillator with delayed feedback. A possible way to improve the level of security of the considered chaotic communication system is to use synchronous retuning of the parameters of the transmitter and the receiver during communication, or to employ high-dimensional time-delay systems.

ACKNOWLEDGMENTS

The authors thank B. P. Bezruchko for stimulating discussions. This work was supported by the Russian Foundation of Fundamental Research, Grant No. 02–02–17578, the Russian Academy of Sciences, Grant No. 23, and the U.S. Civilian Research Development Foundation for the Independent States of the Former Soviet Union, Grant No. REC–006.

[29] R.A. Madan, Chua’s Circuit: A Paradigm for Chaos (World
[31] M.J. Bünner, M. Ciofini, A. Giaquinta, R. Hegger, H. Kantz, R.