Unmasking a hyperchaotic communication scheme

Kevin M. Short and Andrew T. Parker
Department of Mathematics, University of New Hampshire, Durham, New Hampshire 03824
(Received 22 January 1998)

This paper will consider the use of nonlinear dynamic forecasting techniques to extract message signals from a six-dimensional, message-modulated hyperchaotic communication scheme. It will be shown that a variety of messages can be successfully extracted using only a three-dimensional reconstruction. Further, the robustness of the signal extraction is demonstrated by extracting a speech message with the speech amplitude varied by over an order of magnitude. In all cases intelligible speech was extracted, so security was not greatly improved by going to a hyperchaotic system or larger amplitude signals. [S1063-651X(98)12207-9]

PACS number(s): 05.45.+b, 89.70.+c

I. INTRODUCTION

The development of chaotic communication techniques has been an active area of research for the past few years. Researchers have primarily focused on the use of synchronizing chaotic circuits to achieve a robust communication channel [1–11]. In these systems, identical transmitter and receiver systems are synchronized by passing a signal from the transmitter to the receiver, where the signal represents the time evolution of one variable in the transmitter system. This produces a chaotic carrier linking the transmitter and receiver. The communication aspect is incorporated either by adding a message signal to the carrier or by modulating some of the parameters of the transmitter with a message signal, which effectively alters the carrier. In several of these schemes, using both additive signals and message-modulated signals, it has been shown that an intercepted signal can be analyzed to detect and extract the hidden messages using nonlinear dynamic (NLD) forecasting [12–15] or other techniques [16]. The primary reason for these weaknesses in security has been the fact the chaotic carrier can be used to create a phase space reconstruction of the transmitter dynamics. Since the message signals perturb the transmitter dynamics, these perturbations are detectable.

It has been suggested that one possible way to make it more difficult to extract a hidden message signal is to increase the dimension of the dynamical system, especially if used with a message-modulated approach to hide the signal. Along these lines there have been several recent reports concerning the synchronization properties of high-dimensional chaotic (hyperchaotic) systems [17,18,11,19–22]. In this paper we will consider a hyperchaotic communication technique developed by Kocarev and Parlitz [11], which uses message modulation and two stages of chaotic scrambling to obscure the presence of the message signal. Further, the technique is perfectly synchronizing, even in the presence of the message, and there are fairly flexible limits on the strength of the message signal, so it is not as restrictive as the additive-message systems, which require that the message be of low amplitude relative to the chaotic carrier. Even so, we will show that going to higher dimensions and using message modulation did not produce a drastic improvement in the security of the system. In fact, even though the system was six-dimensional, we were able to detect and extract signals using only a three-dimensional reconstruction.

In Sec. II we will give a very brief outline of the NLD forecasting approach to signal extraction. Then in Sec. III we will discuss the chaotic communication scheme of Kocarev and Parlitz and in Sec. IV we will present the results of the message extraction. Section V will conclude with some discussion of the implications of these results.

II. NLD FORECASTING

The NLD forecasting will only be outlined here since details can be found in [12]. The first step in NLD forecasting is to reconstruct the phase space dynamics of the underlying dynamical system. This is usually done using a time-delay reconstruction, with the time delay chosen using mutual information techniques [23], although other techniques seem to give similar results [24–26]. Once the reconstruction is obtained, to make a prediction about the future evolution of a given point $\mathbf{x}_\varphi$, we choose neighbors in a local region around the point and base the model on the dynamics exhibited by the neighboring points. That is, if $\{\mathbf{x}_i\}$ is the set of neighbors then we want to find a predictor function $\mathbf{F}$ such that $\mathbf{F}(\mathbf{x}_i)=\mathbf{x}_{i+1}$ for all points in $\{\mathbf{x}_i\}$. We generally choose the model to be an expansion in polynomials up to degree 2 and $\mathbf{F}$ is found by least-squares minimization. Once $\mathbf{F}$ is determined, we predict $\mathbf{F}(\mathbf{x}_\varphi)=\mathbf{x}_{\varphi+1}$. This describes the basic framework for local modeling, but the process needs to be enhanced if it is to be robust in the presence of extraneous noise or if it is to be used to extract hidden signals.

First of all, it often occurs that the reconstructed attractor exhibits self-intersections (and with real-world data, this is almost always the case). To separate out intersecting trajectories, the process is enhanced by the requirement that neighbors must be selected not only on the basis of being physically near in phase space, but also having similar (numerically approximated) tangent vectors. The second enhancement involves choosing local coordinates in the different local regions, so that the coordinates are aligned with the dominant flow directions. The desired transformation matrix is found by using singular value decomposition on a local trajectory matrix R with entries $R_{ij}=(\mathbf{x}_{i+1}-\mathbf{x}_i)_j$, where each row is the vector difference between one of the neighboring points and next point along its trajectory. The decomposition gives $R=UWV^T$ [27], where V is the rotation matrix. The final enhancement in the prediction process is designed to make the predictions more robust by rejecting any perturbations to the local flow that are likely to be

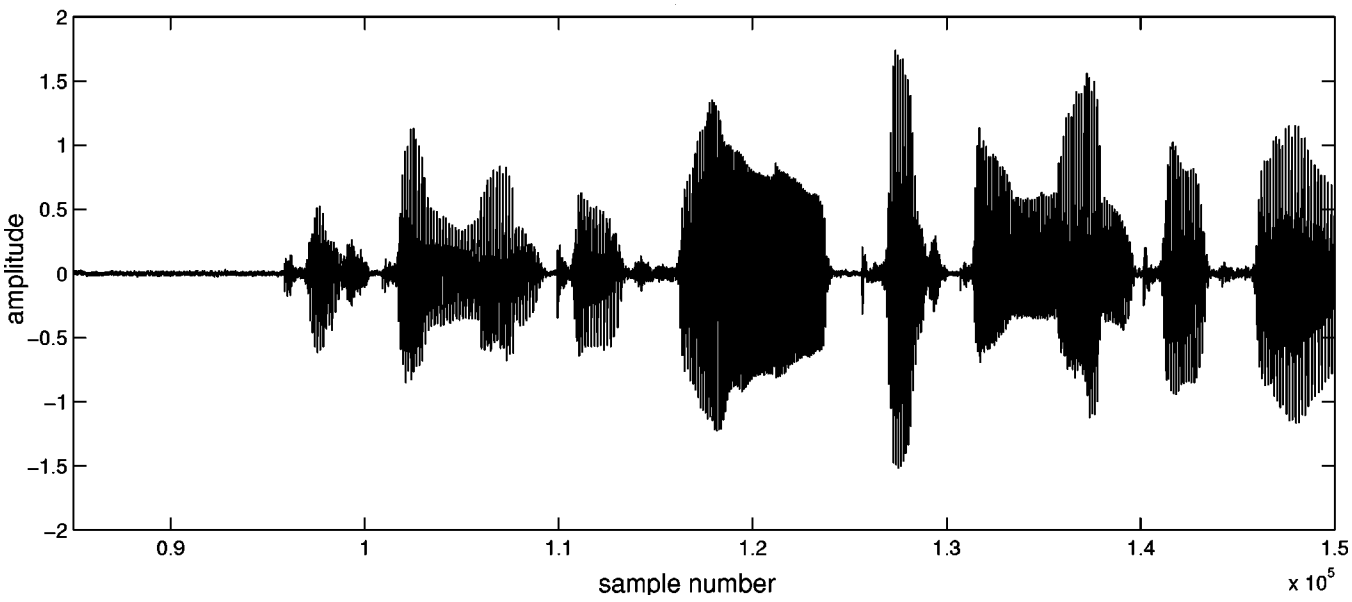

FIG. 1. Original voice trace (''testing 1, 2, 3,...'').

caused by the presence of an interfering signal or a hidden message. This is accomplished by examining the relative magnitudes of the singular values in W and zeroing out any that are below a predetermined threshold. The idea here is that once the new coordinates are chosen, the first principal axis will point in the dominant flow direction, but the other directions may be dominated by the interfering signal or message signal. Consequently, by zeroing out those dimensions, we collapse the problem to a problem of prediction in a subspace of the embedding space. This makes the algorithm more robust and tends to force the predictions to track the chaotic system, while ignoring the interfering signals or hidden messages. Then, when the predicted chaos is subtracted, the interfering signal or hidden message is more evident.

Once the local coordinates are chosen and the collapse to the subspace is effected, the prediction problem is done in the usual way. The predicted value is then converted back to the original coordinate system.

III. HYPERCHAOTIC COMMUNICATIONS

A technique of chaotic communication is developed in [11], where Kocarev and Parlitz use what they call an *active-passive decomposition* (APD). The basic idea is to take a dynamical system

$$\dot{\mathbf{z}}=\mathbf{F}(\mathbf{z})$$

and rewrite it as a nonautonomous system

$$\dot{\mathbf{x}}=\mathbf{f}(\mathbf{x},s(t)),$$

where $s(t)$ is a driving function given by some function $s(t)=h(\mathbf{x})$ or determined independently through a differential equation $\dot{s}=h(\mathbf{x},s)$. If the system for $\dot{\mathbf{x}}$ determines the state of the transmitter in a communications link, then the transmitted signal would be given by $s(t)$. The receiver for the system would be an identical system $\dot{\mathbf{y}}=\mathbf{f}(\mathbf{y},s(t))$ driven by the transmitted signal $s(t)$. The receiver synchronizes exactly with the transmitter as long as the error system, defined by $\mathbf{e}=\mathbf{x}-\mathbf{y}$ and $\dot{\mathbf{e}}=\mathbf{f}(\mathbf{x},s)-\mathbf{f}(\mathbf{y},s)$, has a stable fixed point at $\mathbf{e}=\mathbf{0}$ and we usually demand that the fixed point be globally asymptotically stable.

An important benefit of the approach developed by Kocarev and Parlitz is that an information-bearing message can be incorporated into the function $s(t)$ and this message effectively alters the chaotic dynamics of the transmitter. The synchronization aspect of the communication scheme is extremely robust as long as the error system has the attracting fixed point at the origin, so there is no apparent restriction on the power level of the message signal. This is significantly different from the earliest schemes, where synchronization could only be achieved for low-power message signals. However, in practice we have found that the message signal power must be within a reasonable range; otherwise it may alter the dynamics of the chaotic transmitter so much that the transmitter becomes periodic or quasiperiodic, ruining all hopes of security.

Kocarev and Parlitz go through a number of examples to show that their APD approach is just a generalization of earlier schemes, most all of which have been studied before in [15,14,13,12] and found to have security flaws. However, since the APD scheme is more general, the authors go on to develop an interesting hyperchaotic communication scheme using two different chaotic systems in a cascade, involving six dynamical variables. They expressed the hope that improved communication security would result from the high dimensionality of the system and the fact that the information signal was merely used to modulate the chaotic dynamics. The two chaotic systems were the Lorenz equations and the Rossler equations and the governing equations are

$$\dot{x}_1=2+x_1(x_2-4), \quad \dot{x}_4=-10x_4+s,$$
$$\dot{x}_2=-x_1-x_3, \quad \dot{x}_5=28x_4-x_5-x_4x_6,$$
$$\dot{x}_3=x_2-2.45x_3+s_{aux}, \quad \dot{x}_6=x_4x_5-2.666x_6,$$
$$s_{aux}=i+3x_3, \quad s=10x_5+30s_{aux}/x_6.$$

where i is the information signal and the transmitter has the property that $x_6>0$, so the division causes no problems. Notice that i is only added directly into s_{aux} and then s_{aux} is

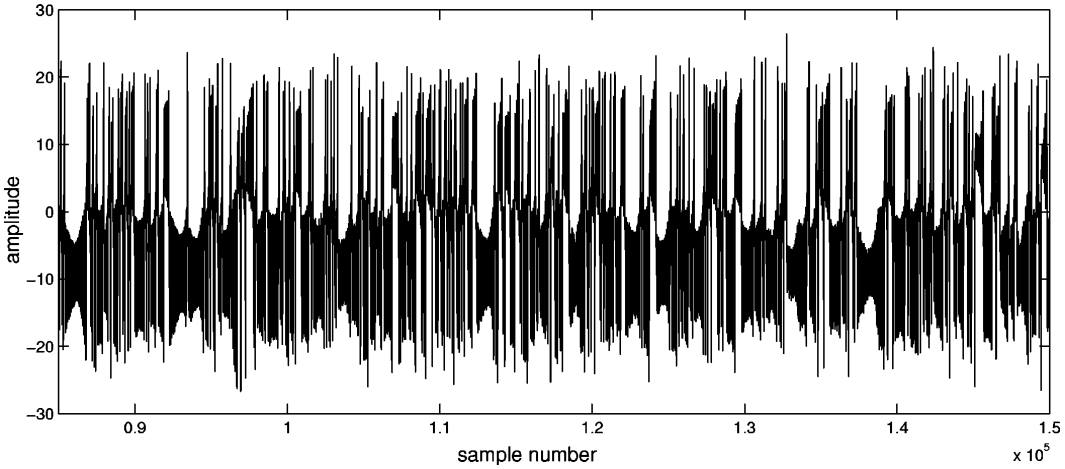

FIG. 2. Hyperchaotic signal carrying voice data.

coupled into the second level of the cascade through s. The transmitted signal is $s(t)$ alone and as will be seen in Sec. IV, the presence of the message is virtually indistinguishable in the dynamics. The equations governing the receiver are essentially the same, but cascaded in the reverse order:

$$\dot{y}_4 = -10y_4 + s, \quad \dot{y}_1 = 2 + y_1(y_2 - 4),$$
$$\dot{y}_5 = 28y_4 - y_5 - y_4y_6, \quad \dot{y}_2 = -y_1 - y_3,$$
$$\dot{y}_6 = y_4y_5 - 2.666y_6, \quad \dot{y}_3 = y_2 - 2.45y_3 + \tilde{s}_{aux},$$
$$\tilde{s}_{aux} = (s - 10y_5)y_6/30, \quad i_R = (s - 10y_5)y_6/30 - 3y_3,$$

where i_R is the recovered information signal. Except for an initial transient, the signal is recovered exactly. We have numerically simulated this communication scheme so that we could generate the transmitted information signal and in the next section we show the results of the analysis of the transmitted signal.

IV. RESULTS

To test the hyperchaotic communication scheme, we used a square wave as a simulated bit stream and also the more complicated case of a speech wave form. In both cases we got good signal extraction, although we will only present the results of the speech extraction here. To generate the data sets, we numerically integrated the system with a time step $\Delta t = 0.01$ using a fourth-order Runge-Kutta scheme. To extract the signal we reconstructed the attractor in three dimensions using a time-delay embedding with $\tau = 10$. In the NLD forecasting, we used second degree polynomials and we chose 25 neighbors in a comparison region of the time series and made predictions based on their behavior.

To test the capability of the NLD forecasting on the speech message, we took a voice trace of the phrase, ''testing, one, two, three, testing, one, two, three,'' sampled at 22 050 Hz, and used it as the information signal in the modulated communication scheme. The original voice trace is shown in Fig. 1. The transmission from the transmitter to the receiver was then modulated by the voice, where the speech begins at sample 95 850 (although a lead-in hiss begins at point 83 850). The resulting signal is shown in Fig. 2. The three-dimensional time-delay reconstruction in Fig. 3 captures much of the behavior of the full six-dimensional system. NLD forecasting was then used to predict the background dynamics. The extracted speech appears in Fig. 4, and although there is some error introduced by the forecasting process, it does not interfere with intelligibility and all listeners found it easy to understand the speech [28]. For the example in Figs. 1–4, the data were scaled so that the range of the chaos was between -25.9 and $+25.1$ and the maximum amplitude in the speech was 1.74. However, the speech extraction could be achieved for a wide range of voice amplitudes since we were able to extract intelligible speech for maximum speech amplitudes of 0.9, 0.32, and 0.16. At amplitudes much greater than 1.74, the speech can be heard unaided in the chaotic transmission and it appears that the speech drives the transmitter out of the chaotic range, although this could be a problem with numerics. Consequently, there does not appear to be a range of values of the speech power that makes the communication approach very secure.

V. DISCUSSION

Our results on the analysis of the hyperchaotic communication scheme are somewhat surprising. Since the communication technique effectively used the message to modulate the dynamics of the chaotic system with the signal never directly added to the transmission, it was unclear at the outset of this investigation that the perturbations introduced by the modulation would in any way resemble the original signals. A potentially more significant result is that the use of

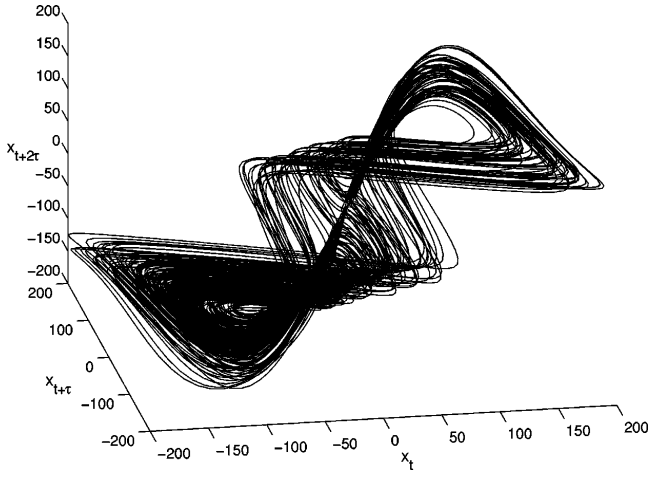

FIG. 3. Three-dimensional reconstruction of signal.

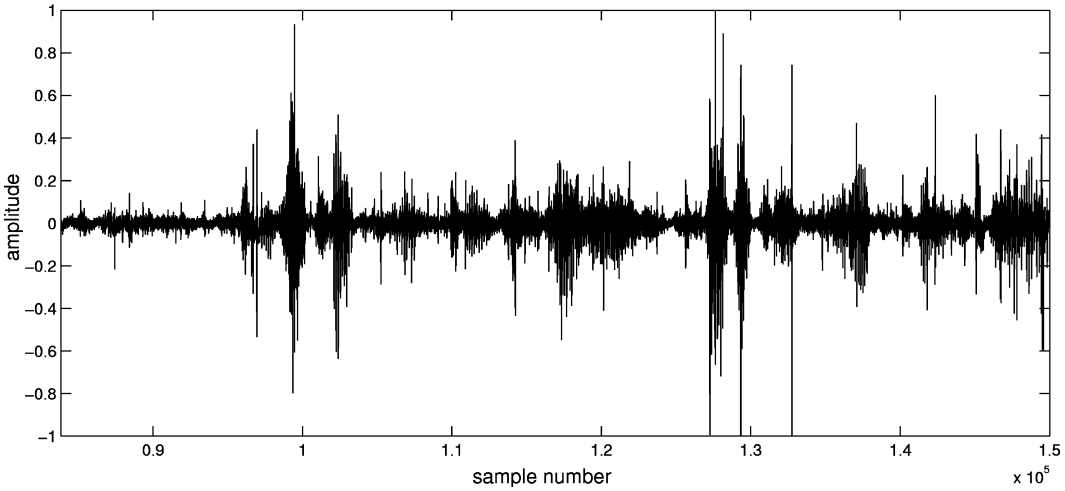

FIG. 4. Extracted speech.

higher-dimensional systems did not make it much more difficult to break the communication scheme, and we were able to use only a three-dimensional reconstruction to analyze a six-dimensional system. We suspect that even though the dynamics are taking place in a six-dimensional space, there is still just a one-dimensional trajectory moving through that space and the local dynamics that are used in the NLD forecasting are still quite low dimensional. If this holds true in general for other higher-dimensional chaotic communication systems, it may be difficult to use higher-dimensional systems as a means to achieve communication security. Conversely, when examining potential higher-dimensional systems, one should concentrate on systems where the local dynamics are also high dimensional.

In all of the hyperchaotic examples presented here, we made explicit use of a region where there was no message being transmitted (except for the low-amplitude hiss in the speech data before the actual speech began). This had the result of giving cleaner results, but we should comment that other experiments have been done where the comparison region was not ''clean.'' For the square wave signal, on a test case where the square wave was present throughout the data, the signal was still successfully extracted; however, there would have been a higher level of bit errors or regions where slight divergences of trajectory would have to be corrected by hand. For the speech example, using a comparison region that overlapped the speech section resulted in only slight reductions in intelligibility.

These investigations provide further evidence that chaotic communication schemes that transmit a chaotic signal that can be used for a phase space reconstruction are very difficult to make secure. Moving to a higher-dimensional chaotic system may provide some benefits, but it is important to consider whether the local dynamics truly reflect significantly more complicated dynamics. Finally, it is important to study how the message modulation of a communication scheme affects the transmitter since if the perturbations to the expected dynamics resemble the message signal, it is likely that they can be extracted.

ACKNOWLEDGMENTS

This work was supported, in part, by a research grant through the Center for Research on Applied Signal Processing at the University of Southern California, (Contract No. 012132).

[1] L. Pecora and T. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[2] L. Pecora and T. Carroll, *Proceedings of the IEEE ICASSP* (IEEE, Piscataway, NJ, 1992).
[3] T. Carroll and L. Pecora, IEEE Trans. Circuits Syst. **38**, 453 (1991).
[4] K. Cuomo and A. Oppenheim, *Proceedings of the IEEE ICASSP* (IEEE, Piscataway, NJ, 1993).
[5] K. Cuomo, A. Oppenheim, and S. Strogatz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1629 (1993).
[6] K. Halle, C. Wu, M. Itoh, and L. Chua, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 469 (1993).
[7] R. He and P. Vaidya, Phys. Rev. A **46**, 7387 (1992).
[8] L. Kocarev *et al.*, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).
[9] U. Parlitz *et al.*, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992).
[10] C. Wu and L. Chua, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1619 (1993).
[11] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
[12] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 957 (1994).
[13] K. Short (unpublished).
[14] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 367 (1996).
[15] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7**, 1579 (1997).
[16] G. Perez and H. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[17] M. K. Ali and J.-Q. Fang, Phys. Rev. E **55**, 5285 (1997).
[18] M. Brucoli, L. Carnimeo, and G. Grassi, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 1673 (1996).
[19] Y.-C. Lai, Phys. Rev. E **55**, R4861 (1997).
[20] U. Parlitz, L. Kocarev, T. Stojanovski, and L. Junge, Physica D **109**, 139 (1997).
[21] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, Phys. Rev. Lett. **76**, 904 (1996).
[22] A. Tamaševičius and A. Čenys, Phys. Rev. E **55**, 297 (1997).
[23] A. Fraser and H. Swinney, Phys. Rev. A **33**, 1134 (1986).
[24] A. Fraser, Physica D **34**, 391 (1989).
[25] A. Albano *et al.*, Phys. Rev. A **38**, 3017 (1988).
[26] A. Mees, P. Rapp, and L. Jennings, Phys. Rev. A **36**, 340 (1987).
[27] W. Press, S. Teukolsky, W. Vetterling, and B. Flannery, *Numerical Recipes in C* (Cambridge University Press, New York, 1992).
[28] See AIP Document No. E-PAPS: E-PLEEE8-58-122807 for electronic versions of the chaotic transmission (km_chaos.au) and extracted speech (km_test123.au). E_PAPS document files may be retrieved free of charge from our FTP server (http://www.aip.org/epaps/epaps.html) or from ftp.aip.org in the directory /epaps/. For further information, e-mail: paps@aip.org or fax: 516-576-2223.