General Approach for Chaotic Synchronization with Applications to Communication

L. Kocarev
Department of Electrical Engineering, St. Cyril and Methodius University, Skopje, P.O. Box 574, Republic of Macedonia

U. Parlitz*
Drittes Physikalisches Institut, Universität Göttingen, Bürgerstrasse 42-44, D-37073 Göttingen, Federal Republic of Germany
(Received 5 July 1994; revised manuscript received 18 November 1994)

A general approach for constructing chaotic synchronized dynamical systems is discussed that is based on a decomposition of given systems into active and passive parts. As a possible application we consider an improved encoding method where the information signal is injected into the dynamical system of the transmitter. Furthermore, we show how to design in a systematic way high-dimensional synchronized systems that may be used for efficient hyperchaotic encoding of information.

PACS numbers: 05.45.+b, 43.72.+q, 47.52.+j

Synchronization of periodic signals is a well-known phenomenon in physics, engineering, and many other scientific disciplines. Recently, synchronization of chaos [1] has aroused much interest in light of its potential applications. In particular, the use of chaotic synchronization in communication systems has been investigated by several authors [2–11]. There, an information signal containing a message is transmitted using a chaotic signal as a broadband carrier, and the synchronization is necessary to recover the information at the receiver. Different implementations of this basic idea have been suggested. For example, in Refs. [2–5] the information signal is added to the chaotic signal and in Refs. [2,6] a parametric modulation is used for the transmission of digital signals. Other approaches to use chaos for the purpose of communication include controlling techniques to encode binary information [12] and methods that make use of the quick decay of the correlation function for chaotic signals [13].

In this Letter we discuss a new approach [8–11] for constructing (chaotic) synchronized systems that may be viewed as a generalization of the method introduced by Pecora and Carroll [1]. This approach and two examples for illustration are presented in the first part of the Letter. In the second part we apply a new method for encoding messages using chaotic dynamics [8–11]. In contrast to most of the schemes proposed in the literature until now we consider cases where the information signal drives the dynamical system that is used in the transmitter. The scalar signal which is transmitted from the transmitter to the receiver is a function of the transmitter state variables and the information signal. If the receiver synchronizes with the transmitter, the information signal can be recovered exactly, i.e., without the reconstruction error that typically occurs with other encoding methods based on synchronization [2,3]. Furthermore, it turns out that this modulation technique not only yields a transmission without errors but also a more secure encoding. Finally, in the third part of the Letter we show that the new synchronization method can be used to construct systematically high-dimensional synchronized systems using low-dimensional systems as building blocks. This possibility is, for example, very useful for the design of communication systems that are based on hyperchaotic signals.

The new synchronization method is based on the fact that it is possible to consider more general decompositions of a given dynamical system

$$\dot{\mathbf{z}} = \mathbf{F}(\mathbf{z}) \tag{1}$$

than the decomposition into subsystems proposed by Pecora and Carroll [1]. Starting from a chaotic autonomous system, for example, one can always formally rewrite it in different ways as a nonautonomous system

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, s(t)) \tag{2}$$

with some driving $s(t) = h(\mathbf{x})$ or $\dot{s} = h(\mathbf{x}, s)$. Let

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}, s(t)) \tag{3}$$

be a copy of the nonautonomous system that is driven by the same signal $s(t)$. If the differential equation for the difference $\mathbf{e} = \mathbf{x} - \mathbf{y}$,

$$\dot{\mathbf{e}} = \mathbf{f}(\mathbf{x}, s) - \mathbf{f}(\mathbf{y}, s) = \mathbf{f}(\mathbf{x}, s) - \mathbf{f}(\mathbf{x} - \mathbf{e}, s), \tag{4}$$

possesses a stable fixed point at $\mathbf{e} = \mathbf{0}$ then there exists for the systems (2) and (3) a synchronized state $\mathbf{x} = \mathbf{y}$ that is stable. This can be proved using stability analysis of the linearized system for small $\mathbf{e}$ or using (global) Lyapunov functions. In general, however, the stability has to be checked numerically using the fact that synchronization occurs if all conditional Lyapunov exponents [1] of the nonautonomous system (2) are negative. In this case system (2) is a passive system that tends to a fixed point when not driven. Therefore, we call the decomposition given by h and $\mathbf{f}$ an *active-passive decomposition (APD)* of the original dynamical system (1). The fact that all conditional Lyapunov exponents of (2) are negative does not exclude chaotic solutions.

 0031-9007/95/74(25)/5028(4)$06.00

To illustrate this synchronization scheme we consider different active-passive decompositions of the well-known Lorenz model. In the first example we choose

$$\begin{aligned} \dot{x}_1 &= -10x_1 + s(t), \\ \dot{x}_2 &= 28x_1 - x_2 - x_1x_3, \\ \dot{x}_3 &= x_1x_2 - 2.666x_3, \end{aligned} \tag{5}$$

with

$$s(t) = h(\mathbf{x}) = 10x_2.$$

To estimate the temporal evolution of the difference $\mathbf{e} = \mathbf{x} - \mathbf{y}$ of the states of the two systems (2) and (3) we note first that the difference $e_1 = x_1 - y_1$ of the first components converges to zero, because $\dot{e}_1 = -10e_1$. Therefore, the remaining two-dimensional system describing the evolution of the differences $e_2 = x_2 - y_2$ and $e_3 = x_3 - y_3$ can for the limit $t \to \infty$ be written as

$$\begin{aligned} \dot{e}_2 &= -e_2 - x_1e_3, \\ \dot{e}_3 &= x_1e_2 - 2.666e_3. \end{aligned}$$

Using the Lyapunov function $L = e_2^2 + e_3^2$ one can show that $\dot{L} = -2(e_2^2 + 2.666e_3^2) < 0$. This means, that the synchronization is globally stable and occurs for all types of driving signals $s(t)$. The conditional Lyapunov exponents of this decomposition are given by $\lambda_1 = -1.805$, $\lambda_2 = -1.861$, and $\lambda_3 = -10$ with respect to the natural logarithm.

Our second example is essentially a decomposition of the Lorenz system into subsystems as suggested by Pecora and Carroll [1]:

$$\begin{aligned} \dot{x}_1 &= 28s(t) - x_1 - s(t)x_2, \\ \dot{x}_2 &= s(t)x_1 - 2.666x_2, \end{aligned} \tag{6}$$

where the function $s(t)$ is now given by the additional differential equation

$$\dot{s} = h(\mathbf{x}, s) = 10(x_1 - s).$$

Using similar arguments as for the first example (5) it is easy to see that the difference $\mathbf{e} = \mathbf{x} - \mathbf{y}$ converges to $\mathbf{0}$ for all $s(t)$ [14]. The conditional Lyapunov exponents are $\lambda_1 = -1.796$ and $\lambda_2 = -1.870$.

This example shows that the Pecora-Carroll method for constructing synchronized systems is included in the more general APD approach. However, our numerical simulations [11] indicate that using the APD any typical chaotic system can be used to implement synchronization using a one-dimensional drive in many ways. The freedom to choose the function h that defines the driving signal therefore leads to a large flexibility in applications. This is different from the synchronization method proposed by Pecora and Carroll [1] where only a finite number of possible couplings exists, that is given by the number of (stable) subsystems of the dynamical system.

What makes the above introduced method for constructing synchronized systems interesting for applications is the fact that in many cases the function $s(t)$ can be rather general. In particular, it may depend not only on the state $\mathbf{x}$ but also on some information signal $i(t)$, i.e., $s = h(\mathbf{x}, i)$ or $\dot{s} = h(\mathbf{x}, s, i)$. This feature can, for example, be used in a communication scheme where $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, s)$ is the (chaotic) dynamical system of the transmitter, $s = h(\mathbf{x}, i)$ is the transmitted and received signal, and $\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}, s)$ constitutes the receiver. In the case of synchronization, i.e., when $\mathbf{y} \to \mathbf{x}$, the information i can be recovered without error from $s = h(\mathbf{x}, i) = h(\mathbf{y}, i)$ if this equation is uniquely solvable for i.

This encoding method has been implemented experimentally using an APD of Chua's circuit [15]. The transmitter and the receiver are given by two copies of the following system:

$$\begin{aligned} C_1 \frac{dV_{C1}}{dt} &= G(V_{C2} - V_{C1}) - g(V_{C1}) - G\alpha(s - V_{C1}), \\ C_2 \frac{dV_{C2}}{dt} &= G(V_{C1} - V_{C2}) + i_L, \\ L \frac{di_L}{dt} &= V_{C2}. \end{aligned} \tag{7}$$

The transmitted signal $s = V_{C1} + i$ is given by the voltage V_{C1} at the capacitor C_1 of the transmitter and the information signal i. The parameters are $C_1 = 10$ nF, $C_2 = 100$ nF, $L = 18$ mH, $G = 1/1700\ \Omega$, $\alpha = 3.4$ and g is a piecewise-linear function defined by $g(V) = m_0V + \frac{1}{2}(m_1 - m_0)[|V + B_p| - |V - B_p|]$ with $m_0 = -0.409$ mS, $m_1 = -0.756$ mS, and $B_p = 1.08$ V. The circuit diagram and other details of this implementation will be given elsewhere [16]. Figure 1 shows as an example the reconstruction of a triangular information signal $i(t)$. Although the parameters of the two coupled circuits are not exactly the same, the quality of the reconstructed signal [Fig. 1(b)] is already quite good. In general this sensitivity of the synchronization on parameter differences may cause difficulties for typical hardware implementations. On the other hand, however, it is a feature that is very welcome for any private communication. This problem and the influence of additional noise in the transmission channel will be discussed in more detail elsewhere.

Of course, the APDs of the Lorenz system introduced above may also be used for encoding. System (5), for example, can be driven by $s = 10x_2 + ix_3$. Note that the above given proof for the synchronization of this system ($\mathbf{e} \to 0$) holds for all driving signals s. Therefore, $\mathbf{y}$ converges to $\mathbf{x}$ for all information signals i (that, of course, have an effect like dynamic noise and thus modify the underlying attractor). Since the variable x_3 is always positive, the information signal can be recovered exactly as $i_R = (s - 10y_2)/y_3$ as soon as the transient of the synchronization process is over. For the second system (6) the transmitted signal s may be generated by the differential equation $\dot{s} = 10(x_1 - s) + i$. To retrieve the

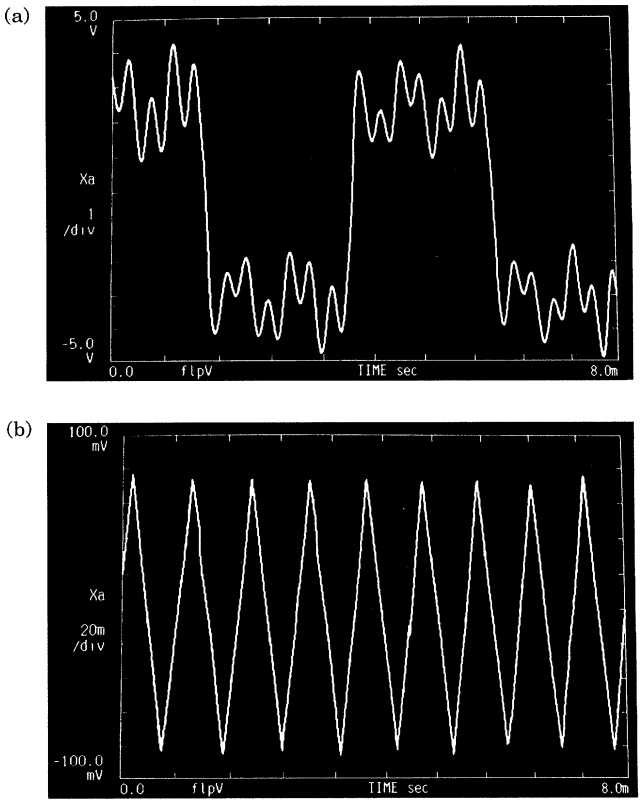

FIG. 1. Experimental implementation of a communication scheme using Chua's circuit (7) with driving $s = V_{C1} + i$ and a triangular information signal i. (a) Transmitted signal s. (b) Recovered signal i_R.

information in the receiver as $i_R = \dot{s} - 10(y_1 - s)$ in this case the derivative $\dot{s}$ has to be computed from s. Of course, other functions h (including linear filters) could also be used to generate the transmitted signal s. The only restriction for the signal s is that it has to be chosen in a way that the transmitter and the receiver remain stable (and chaotic).

The last example shows that the Pecora-Carroll synchronization method can also be used in a more sophisticated way for communication than it was done until now. The communication scheme presented in Refs. [2,3] is based on Pecora-Carroll synchronization and cascaded subsystems in the receiver that are necessary to recover the information signal. Compared to the method discussed in this Letter the main difference consists in the fact that in Refs. [2,3] the information is just added to a chaotic carrier but not injected into the dynamical system constituting the transmitter. In this case, the receiver is forced by a sum of the chaotic signal *and* the information signal whereas the transmitter is just driven by the (pure) chaotic signal. Because of this (slightly) different driving $\mathbf{y}$ does not converge exactly to $\mathbf{x}$ and the information signal can only be recovered including an error that vanishes in the limit $|i| \to 0$. The specific properties of this inevitable error are investigated in Refs. [4,5]. If one uses an information signal with a small amplitude $|i|$ in order to minimize this error, however, the information can be destroyed by noise in the transmission channel. Furthermore, this method is not very secure, because it is possible to fit a nonlinear model to the time series given by the transmitted signal s that consists mainly of the (low-dimensional) chaotic carrier ($|i|$ has to be small to avoid errors). Using this nonlinear model the information signal may then be extracted from s by methods similar to nonlinear noise reduction [17] or other techniques [18]. In contrast, even if we use for our communication scheme just a linear combination like, for example, $s = x_2 + i$, it is difficult to decode the information from the transmitted signal s since the dynamical system of the transmitter is *not autonomous but driven by the information signal* which is in general rather complicated.

The communication method discussed above can also be implemented using high-dimensional systems and transmitted signals that are hyperchaotic. In this case, however, it is in general difficult to find a region in parameter space where hyperchaos exists. Therefore, we propose another method for synthesizing high-dimensional systems in a systematic way, using standard low-dimensional systems with a well-known dynamics, only. For the sake of brevity, only the procedure for designing a six-dimensional transmitter using two three-dimensional systems as building blocks is described in the following. The equations of the transmitter, the transmitted signal, and the receiver are in this case given by

$$\left.\begin{aligned} \dot{\mathbf{x}}_1 &= \mathbf{f}_1(\mathbf{x}_1, s_{\mathrm{aux}}(t)) \\ s_{\mathrm{aux}} &= h_1(\mathbf{x}_1, i(t)) \\ \dot{\mathbf{x}}_2 &= \mathbf{f}_2(\mathbf{x}_2, s(t)) \end{aligned}\right\} \quad \text{transmitter,}$$

$$s = h_2(\mathbf{x}_2, s_{\mathrm{aux}}) \quad \text{transmitted signal,}$$

$$\left.\begin{aligned} \dot{\mathbf{y}}_2 &= \mathbf{f}_2(\mathbf{y}_2, s(t)) \\ \tilde{s}_{\mathrm{aux}} &= h_2^{-1}(\mathbf{y}_2, s(t)) \\ \dot{\mathbf{y}}_1 &= \mathbf{f}_1(\mathbf{y}_1, \tilde{s}_{\mathrm{aux}}(t)) \end{aligned}\right\} \quad \text{receiver,}$$

where we assume that h_1 and h_2 are invertible with respect to i and s_{aux}, respectively. If both pairs of subsystems $(\mathbf{x}_1, \mathbf{y}_1)$ and $(\mathbf{x}_2, \mathbf{y}_2)$ synchronize mutually then at the receiver the information i_R can be recovered as

$$i_R = h_1^{-1}(\mathbf{y}_1, \tilde{s}_{\mathrm{aux}}) = h_1^{-1}(\mathbf{y}_1, h_2^{-1}(\mathbf{y}_2, s)) .$$

The generalization to a communication model with an arbitrary number of low-dimensional subsystems is straightforward [11]. The two low-dynamical systems we use in the following numerical example are the Rössler system and the Lorenz system. The transmitter of our communication model is given by

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

where s is the transmitted signal. The receiver reads

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

The parameters of the Rössler and the Lorenz equations are chosen such that both systems have a chaotic attractor. The information signal shown in Fig. 2(a) is the spoken word "42" recorded with a sampling rate of 8000 Hz and a resolution of 16 bit. Figure 2(b) shows the transmitted signal s. The transmitter and receiver synchronize, and the difference $|i - i_R|$ between the original information signal i and the reconstructed signal i_R is given in Fig. 2(c). The transmitted signal is in this case a sum of two chaotic signals and hyperchaotic. The Lyapunov exponents of the transmitter for $i = 0$ equal $\lambda_1 = 0.710$, $\lambda_2 = 0.177$, $\lambda_3 = 0.000$, $\lambda_4 = -0.006$, $\lambda_5 = -2.59$, and $\lambda_6 = -14.37$. This and other examples of high-dimensional systems with more than one positive Lyapunov exponent [11] show that it is possible to synchronize hyperchaotic systems using a scalar signal, only.

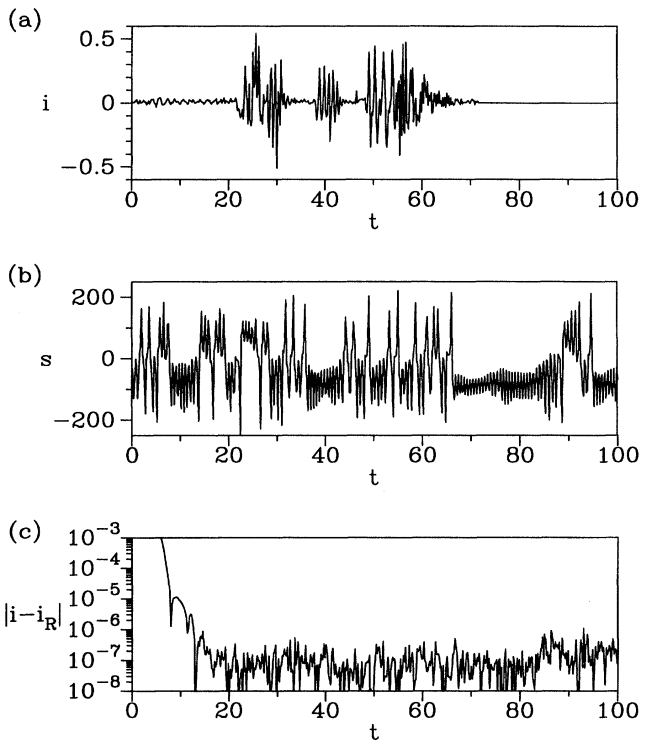

FIG. 2. Numerical simulation of a communication scheme using a combination of Rössler and Lorenz systems. (a) Information signal i given by the spoken word "42." (b) Transmitted signal s. (c) Difference $|i - i_R|$ between the original and the recovered information signal.

In conclusion, we have presented a general approach to construct a large class of synchronized dynamical systems and discussed its application in a communication scheme where the information can be recovered without errors. Furthermore, we introduced a procedure for synthesizing high-dimensional synchronized systems. In this case the transmitted signal is hyperchaotic and therefore yields a more efficient encoding.

The authors thank Professor W. Lauterborn, M. Wiesenfeldt, R. Mettin, and A. Pikovsky for stimulating discussions, and G. Kirschmann-Schröder, K. Lautscham, and H. Hohmann for support with the photographs and the electronic circuit. L. K. thanks the DAAD for a research grant. This work was also supported in part by the Macedonian Ministery of Science and the DFG (SFB 185).

*Electronic address: ulli@physik3.gwdg.de

[1] L. Pecora and T. Carroll, Phys. Rev. Lett. **64**, 821–823 (1990); T. L. Carroll and L. M. Pecora, IEEE Trans. Circuits Syst. **38**, 453–456 (1991).
[2] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65–68 (1993).
[3] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos **2**, 709–713 (1992).
[4] R. Lozi and L. O. Chua, Int. J. Bifurcation Chaos **3**, 1319–1325 (1993).
[5] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, Int. J. Bifurcation Chaos **3**, 1629–1638 (1993).
[6] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos **2**, 973–977 (1992).
[7] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, Int. J. Bifurcation Chaos **3**, 469–477 (1993).
[8] C. W. Wu and L. Chua, Int. J. Bifurcation Chaos **3**, 1619–1627 (1993).
[9] L. Kocarev and U. Parlitz, in Proceedings of Nonlinear Dynamics of Electronic Systems, Krakow, Poland, 1994 (to be published).
[10] L. Kocarev and T. Stojanovski, "A Model for Secret-Key Cryptography using Chaotic Synchronization," in Proceedings of the International Symposium on Information Theory and its Application, Sydney, 1994 (to be published).
[11] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel (to be published).
[12] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031–3034 (1993); S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781–1784 (1994).
[13] U. Parlitz and S. Ergezinger, Phys. Lett. A **188**, 146–150 (1994).
[14] R. He and P. G. Vaidya, Phys. Rev. A **46**, 7387–7392 (1992).
[15] M. P. Kennedy, Frequenz **46**, 66–80 (1992).
[16] U. Parlitz and L. Kocarev (to be published).
[17] P. Grassberger, R. Hegger, H. Kantz, C. Schaffrath, and T. Schreiber, Chaos **3**, 127–141 (1993).
[18] G. Perez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970–1973 (1995).