Synchronization of Randomly Multiplexed Chaotic Systems with Application to Communication

Shyam Sundar and Ali A. Minai
Department of Electrical & Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, Ohio 45221-0030
(Received 14 June 2000)

Synchronized chaotic systems have recently been applied to the area of secure communications in a variety of ways. At the same time, there have also been significant advances in deciphering messages masked by chaotic signals. It is important, therefore, to explore more secure approaches to using chaos in communication. We show that multiple chaotic systems can be synchronized through a scalar coupling which carries a stochastic signal generated by random multiplexing of the source systems. This approach, which is a variant of the active-passive decomposition method, promises enhanced security in chaos-based communication.

PACS numbers: 05.45.Vx, 07.05.Pj, 05.45.Xt, 43.72.+q

The use of self-synchronizing unidirectionally coupled chaotic oscillators has recently been investigated extensively as a means of secure communications [1–11]. Most of the methods are based on extensions and generalizations of the seminal work by Pecora and Carroll [12,13]. Secure communication is obtained through one of two methods: (1) *masking* of a weak analog message signal by adding it into the strong, chaotic coupling signal from the drive to the response system [1–3,10], or (2) *modulation* of the parameters of the drive system by a digital message signal [2,5,14]. However, it has been shown that both methods are susceptible to attack by a determined intruder using predictive modeling and noise reduction methods from nonlinear dynamics [15–17] (see [18–20] for modeling techniques). One reason for this is that the typical chaotic systems used in the proposed methods are low-dimensional ones, whose attractors have easily identifiable structure. This has fueled interest in the synchronization of hyperchaotic systems [10,21,22] and in synchronization through impulsive coupling [23,24]. One interesting suggestion is the use of volume-preserving maps [11], which do not possess an attractor and have essentially space-filling trajectories.

In this Letter, we present a scheme which allows multiple nonidentical chaotic systems to be synchronized using a scalar signal which is *truly* random by construction. This holds out the possibility of enhanced security since the stochasticity of the carrier (coupling) signal renders it less susceptible to reconstruction using methods developed for deterministic systems. At the same time, the chaotic nature of the underlying generators means that statistical methods also have limited success in breaking system security.

Our method is based on the active-passive decomposition (APD) approach proposed by Kocarev *et al.* [6] and recently applied to multiuser communication by Yoshimura [25]. However, we generate the scalar coupling signal linking transmitters to receivers by switched random multiplexing of the transmitting systems, as described later. In previous reports [26,27], we have shown that a randomly multiplexed scalar coupling can synchronize arrays of chaotic maps. Here we show a similar result for continuous-time systems and apply it to multiuser communication.

Globally Coupled System and Encryption Scheme.— Consider the schematic shown in Fig. 1. The drive system comprises N nonidentical pairs of n-dimensional equations

$$\dot{\mathbf{x}}_i = f(\mathbf{x}_i, s), \qquad i = 1, 2, \ldots, N, \tag{1}$$

$$\dot{\mathbf{y}}_i = f(\mathbf{y}_i, s), \qquad i = 1, 2, \ldots, N, \tag{2}$$

where $\mathbf{x}_i, \mathbf{y}_i \in \mathbf{R}^n$, $s \in \mathbf{R}$, and each $(\mathbf{x}_i, \mathbf{y}_i)$ pair is termed a subsystem. These subsystems are globally coupled by the function

$$s = g(\mathbf{x}_1, \mathbf{y}_1, \mathbf{x}_2, \mathbf{y}_2, \ldots, \mathbf{x}_N, \mathbf{y}_N), \tag{3}$$

as shown in Fig. 1. The response subsystem which is identical to the drive subsystem comprises

$$\dot{\mathbf{x}}'_i = f(\mathbf{x}'_i, s), \qquad i = 1, 2, \ldots, N, \tag{4}$$

$$\dot{\mathbf{y}}'_i = f(\mathbf{y}'_i, s), \qquad i = 1, 2, \ldots, N, \tag{5}$$

It can be shown that the response subsystem will synchronize with the corresponding drive subsystem through

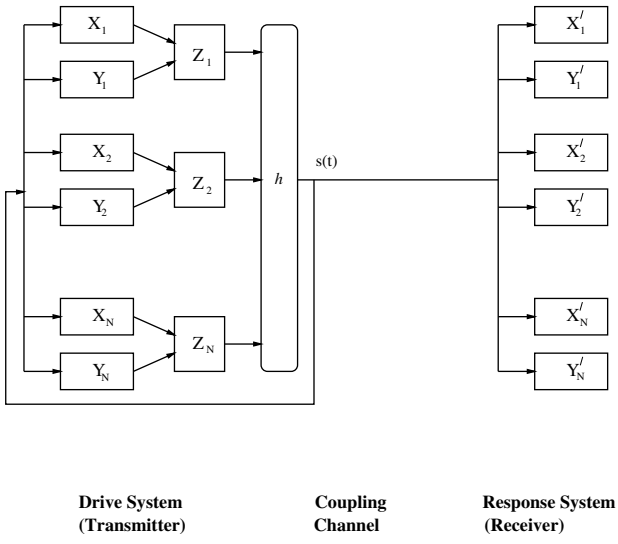

FIG. 1. Globally coupled drive and response systems.

 0031-9007/00/85(25)/5456(4)$15.00 © 2000 The American Physical Society

APD for any arbitrary initial conditions $\mathbf{x}_i(0)$, $\mathbf{y}_i(0)$, $\mathbf{x}'_i(0)$, and $\mathbf{y}'_i(0)$ for all common driving signals s; i.e., $\|\mathbf{x}_i - \mathbf{x}'_i\| \to 0$ and $\|\mathbf{y}_i - \mathbf{y}'_i\| \to 0$ as $t \to \infty$ [6].

Each user i controls subsystem $(\mathbf{x}_i, \mathbf{y}_i)$ at the transmitting end. The corresponding response susbystem $(\mathbf{x}'_i, \mathbf{y}'_i)$ is used for detection at the receiving end. The parameters of the corresponding transmitter and receiver subsystems must match with high precision to achieve adequate detection. Thus, these parameters play the role of the *key* in standard encryption. Their values must either be prearranged between the sender and receiver, or communicated securely in some other way—as is normally assumed for encryption keys.

We assume that user i is communicating information $r_i(t)$ represented in binary 0 and 1. At any time t, this information signal is converted into a *message signal,* $z_i(t)$, as

$$z_i = \begin{cases} x_{ij} & \text{if bit to be transmitted} = 0\,, \\ y_{ij} & \text{if bit to be transmitted} = 1\,, \end{cases} \tag{6}$$

where x_{ij} and y_{ij} are the jth component of $\mathbf{x}_i$ and $\mathbf{y}_i$, respectively. The actual transmitted signal, $s(t)$, is then constructed from these $z_i(t)$. Thus, we get

$$\begin{aligned} s(t) &= g\big(\mathbf{x}_1(t), \mathbf{y}_1(t), \mathbf{x}_2(t), \mathbf{y}_2(t), \ldots, \mathbf{x}_N(t), \mathbf{y}_N(t)\big) \\ &= h\big(z_1(t), z_2(t), \ldots, z_N(t)\big)\,. \end{aligned} \tag{7}$$

All users transmit their bits synchronously, and each transmission cycle has a duration of one bit. Thus, the system must transmit N bits—one for each user—in each cycle. The transmission cycle is divided into MN subintervals of length T, where M is a positive integer. During each subinterval of the transmission cycle, a user i is chosen randomly. The instantaneous value of user i's message signal, $z_i(t)$, is then sampled and transmitted for duration T. This fixed-value signal of length T is called a *chip.* The user selection process is specified so that each user is selected exactly M times over one transmission cycle, albeit in random order. This constraint is not essential for system function if M is reasonably large but allows better performance for small M. Using this scheme, M chips from each user are transmitted over the course of each transmission cycle. This randomly generated signal comprises the system's coupling signal, $s(t)$. Since $s(t)$ drives all the subsystems, the corresponding drive and response subsystems synchronize irrespective of their initial conditions and remain synchronized thereafter.

At the receiver, each response subsystem, i, initializes two accumulator variables, a_i^0 and a_i^1, to zero at the beginning of each transmission cycle. When chip $s(t)$ comes in, receiver i calculates two difference values $d_{ix}(t) = [s(t) - x'_{ij}(t)]$ and $[d_{iy}(t) = s(t) - y'_{ij}(t)]$. It then updates its accumulators as follows:

$$\begin{aligned} a_i^0 &= a_i^0 + 1 \quad \text{if } |d_{ix}| \le \epsilon\,, \\ a_i^1 &= a_i^1 + 1 \quad \text{if } |d_{iy}| \le \epsilon\,. \end{aligned} \tag{8}$$

At the end of the transmission cycle, receiver i decides on its bit as

$$\hat{z}_i = \begin{cases} 0 & \text{if } a_i^0 > a_i^1\,, \\ 1 & \text{if } a_i^0 < a_i^1\,. \end{cases} \tag{9}$$

If $a_i^0 = a_i^1$, the choice is made randomly. In the case when $s(t)$ is communicated with very high precision over a noiseless channel, typically either a_i^0 or a_i^1 will be zero and $a_i^0 + a_i^1 = M$. In these ideal conditions, $M = 1$ and $\epsilon = 0$ suffice for perfect communication. However, when $s(t)$ has lower precision, the signals from different oscillators can interfere, and the quality of detection will depend on N (the number of users) and M (number of chips/user). In noisy channels, $\epsilon > 0$ would be needed for adequate detection.

It should be noted that $s(t)$ serves as both the synchronizing signal *and* the information signal. Thus each binary symbol is encoded with a unique dynamical equation and encryption is achieved by randomly multiplexing amongst the transmitters. Realistically, unless an intruder has access to the precise parameter values being used by the particular user of interest, it is extremely difficult to derive this information from the data stream to break encryption. To do this, an intruder would have to extract the information stream corresponding to that user from $s(t)$. This is made prohibitively difficult by random multiplexing and the fact that no information of this multiplexing is directly transmitted into the channel. The sample and hold for each chip ensures that two adjacent sampled values of any single user have minimum correlation. A further complication for the intruder is the need to estimate the transmitter's parameters with extreme precision, without which decoding is impossible. While this sensitivity to parameter values puts strong accuracy constraints on the legitimate receiver, it is an important factor in ensuring the security of this—and most other—encryption methods. We have discussed this issue in detail for single-user chaotic encryption elsewhere [28].

Example of the Encryption scheme.—In the following, which deals with the model of the scheme with Lorenz system, the communication and encryption scheme discussed earlier is implemented using the well known Lorenz system. Subsystem i at the transmitting end is given by

$$\begin{aligned} \dot{x}_{i1} &= -\sigma_{ix}(x_{i1} - s)\,, \\ \dot{x}_{i2} &= \rho_{ix}x_{i1} - x_{i2} - x_{i1}x_{i3}\,, \\ \dot{x}_{i3} &= x_{i1}x_{i2} - \beta_{ix}x_{i3}\,, \end{aligned} \tag{10}$$

$$\begin{aligned} \dot{y}_{i1} &= -\sigma_{iy}(y_{i1} - s)\,, \\ \dot{y}_{i2} &= \rho_{iy}y_{i1} - y_{i2} - y_{i1}y_{i3}\,, \\ \dot{y}_{i3} &= y_{i1}y_{i2} - \beta_{iy}y_{i3}\,, \end{aligned} \tag{11}$$

and the corresponding subsystem at the receiving end is

$$\begin{aligned} \dot{x}'_{i1} &= -\sigma_{ix}(x'_{i1} - s)\,, \\ \dot{x}'_{i2} &= \rho_{ix}x'_{i1} - x'_{i2} - x'_{i1}x'_{i3}\,, \\ \dot{x}'_{i3} &= x'_{i1}x'_{i2} - \beta_{ix}x'_{i3}\,, \end{aligned} \tag{12}$$

$$\begin{aligned}\dot{y}'_{i1} &= -\sigma_{iy}(y'_{i1} - s),\\ \dot{y}'_{i2} &= \rho_{iy}y'_{i1} - y'_{i2} - y'_{i1}y'_{i3},\\ \dot{y}'_{i3} &= y'_{i1}y'_{i2} - \beta_{iy}y'_{i3}.\end{aligned} \tag{13}$$

We define

$$z_i(t) = \begin{cases} x_{i2}(t) & \text{if transmitted bit} = 0,\\ y_{i2}(t) & \text{if transmitted bit} = 1.\end{cases} \tag{14}$$

In the above equations i indicates the user and varies from 1 to N. The global coupling function and the synchronizing signal is given by

$$\begin{aligned}s(t) &= g\big(x_{12}(t), y_{12}(t), x_{22}(t), y_{22}(t), \ldots, x_{N2}(t), y_{N2}(t)\big)\\ &= h\big(z_1(t), z_2(t), \ldots, z_N(t)\big).\end{aligned} \tag{15}$$

The function h operates as a random multiplexer described in the previous section. It can be shown that the corresponding Lorenz units synchronize for all $s(t)$ [6]. As discussed earlier, transmitting $s(t)$ with low precision can result in detection errors. One way to minimize these is to make the individual Lorenz oscillators in the system as uncorrelated as possible. This can be achieved by making the parameters σ, ρ, and β sufficiently different between the different Lorenz systems. A further decrease in the correlation can be achieved by modifying the Lorenz systems as shown in [25].

The performance of the system was studied through simulation for up to 30 users. To demonstrate that the approach does not depend on a finely tuned selection of parameters, the parameters of the Lorenz systems were chosen randomly in the following ranges: $10 \le \sigma_{ix} \le 20$, $30 \le \rho_{ix} \le 60$, $2.333 \le \beta_{ix} \le 5.333$, $10 \le \sigma_{iy} \le 20$, $30 \le \rho_{iy} \le 60$, and $2.333 \le \beta_{iy} \le 5.333$, where i indicates the user. T was chosen such that consecutive samples of z_i were uncorrelated and one chip was transmitted for each user ($M = 1$). Before detection was started a stream of random bits was transmitted to allow synchronization of the corresponding drive and response subsystems.

The effect of varying precision in $s(t)$ on the bit error rate (BER) as a function of the number of users was evaluated through simulation and is shown in Fig. 2a. The *precision* parameter indicates the number of decimal places to which the transmitted signal $s(t)$ was rounded. 1000 randomly generated bits were transmitted for each user. The simulation shows that with the increase in the number of users BER increased. This is because, with fixed parameter ranges, an increase in the number of users implies closer parameter values for their Lorenz systems. This leads to greater correlation among the subsystems for different users and a higher rate of error. This effect is mitigated by transmitting at higher precision because detection is able to use this information to increase accuracy. Detection performance can also be increased by using a larger M, i.e., transmitting more chips per user in each tramission cycle. This is shown in Fig. 2b. The BER was almost zero when two or more chips were transmitted.

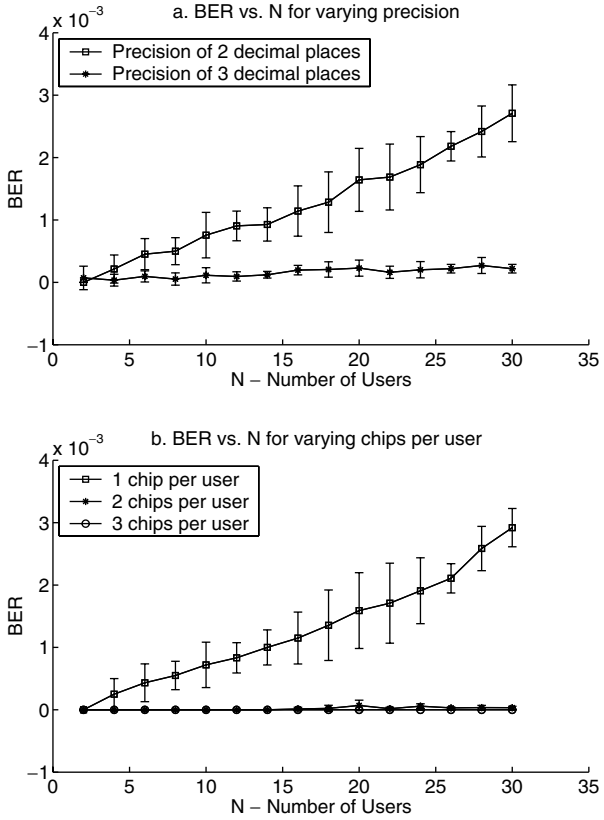

FIG. 2. The figures show the variation of BER as a function of number of users. (a) shows the plot when the signal is transmitted with varying precision for one chip per user. (b) shows the plot when signal is transmitted at a precision of two decimal places with varying chips per user.

Figure 3 shows an example of the transmitted signal, $s(t)$. The random nature of the signal is evident from the plot. Reconstructing the underlying Lorenz systems from this signal is complicated by two facts. (1) While data from all the Lorenz systems is included in $s(t)$ over time, each

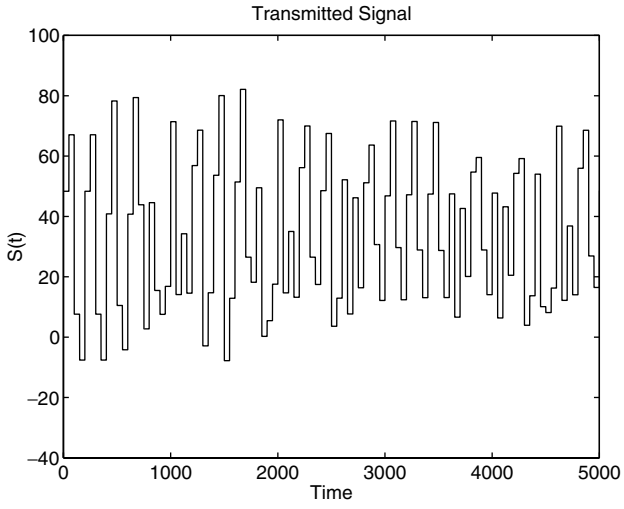

FIG. 3. Plot of the transmitted signal $s(t)$.

individual system is sampled at random intervals, and no information about this is contained in the signal. (2) By choosing the chip length appropriately, many—even most—intervals between the sampling of the same user's signal can be made longer than the correlation time of the Lorenz system, thus making it virtually impossible to identify the origin of individual chips through correlation.

In this paper, we have presented a method for multiuser communication using random multiplexing of chaotic signals. The proposed method overcomes some of the security problems associated with previous schemes for using chaos in communications. While this approach requires much more development before it can be used in practical situations, we believe it provides an intriguing and novel way to combine chaos and randomness into a system with useful functionality. Indeed, the notion of random multiplexing may also have applications in more traditional multiuser communication systems and other distributed systems. We also note that, while the work reported here focuses on continuous-time systems, a similar (and perhaps simpler) arrangement can be implemented using discrete-time chaotic maps. Results on such systems will be presented in future reports.

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

[2] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Trans. Circuits Syst. II **40**, 626 (1993).

[3] C. W. Wu and L. O. Chua, Int. J. Bifurcation Chaos **3**, 1619 (1993).

[4] H. D. I. Abarbanel and P. S. Linsay, IEEE Trans. Circuits Syst. II **40**, 643 (1993).

[5] T. Yang, Int. J. Circuit Theory Appl. **23**, 611 (1995).

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

[7] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E **53**, 4351 (1996).

[8] T. Yang and L. O. Chua, Int. J. Bifurcation Chaos **6**, 2653 (1996).

[9] T. Yang and L. O. Chua, IEEE Trans. Circuits Syst. I **43**, 817 (1996).

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

[11] T. L. Carroll and L. M. Pecora, IEEE Trans. Circuits Syst. I **45**, 656 (1998).

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

[13] L. M. Pecora and T. L. Carroll, Phys. Rev. A **44**, 2374 (1991).

[14] H. Dedieu, M. P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst. II **40**, 635 (1993).

[15] K. M. Short, Int. J. Bifurcation Chaos **4**, 959 (1994).

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

[17] K. M. Short, Int. J. Bifurcation Chaos **6**, 367 (1996).

[18] E. J. Kostelich and J. A. Yorke, Physica (Amsterdam) **41D**, 183 (1990).

[19] T. Sauer, J. A. Yorke, and M. Casdagli, J. Stat. Phys. **65**, 579 (1991).

[20] T. Sauer, Physica (Amsterdam) **58D**, 193 (1992).

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

[22] T. L. Carroll, J. F. Heagy, and L. M. Pecora, Phys. Rev. E **54**, 4676 (1996).

[23] R. E. Amritkar and R. Gupte, Phys. Rev. E **47**, 3889 (1993).

[24] T. Stojanovski, L. Kocarev, and U. Parlitz, Phys. Rev. E **54**, 2128 (1996).

[25] K. Yoshimura, Phys. Rev. E **60**, 1648 (1999).

[26] A. A. Minai and T. Anand, Phys. Rev. E **57**, 1559 (1998).

[27] A. A. Minai and T. Anand, in *Proceedings of the International Joint Conference on Neural Networks, Anchorage, Alaska, 1998* (IEEE, New York, 1998), pp. 1466–1471.

[28] A. A. Minai and T. D. Pandian, Chaos **8**, 621 (1998).