ISSN 1062-8738, Bulletin of the Russian Academy of Sciences: Physics, 2008, Vol. 72, No. 1, pp. 131–135. © Allerton Press, Inc., 2008.
Original Russian Text © A.A. Koronovskii, O.I. Moskalenko, P.V. Popov, A.E. Hramov, 2008, published in Izvestiya Rossiiskoi Akademii Nauk. Seriya Fizicheskaya, 2008, Vol. 72, No. 1, pp. 143–147.

Method for Secure Data Transmission Based on Generalized Synchronization

A. A. Koronovskii, O. I. Moskalenko, P. V. Popov, and A. E. Hramov

Saratov State University, Saratov, 410012 Russia
e-mail: alkor@nonlin.sgu.ru

Abstract—A method for secure data transmission is proposed on the basis of the phenomenon of generalized chaotic synchronization, which is characterized by extremely high stability to noise and fluctuations in a communication channel. The basic concepts of the method proposed are illustrated by numerical simulation of two unidirectionally coupled Róssler systems, chosen as a transmitter and a receiver. Fundamental advantages of the proposed method over the known ones are shown.

DOI: 10.3103/S1062873808010309

INTRODUCTION

The use of chaotic synchronization for secure data transmission is an urgent problem of nonlinear dynamics [1–12]. Currently, a large number of methods for secure data transmission are known. Many of them are based on the phenomenon of complete chaotic synchronization (chaotic masking [1], switching of chaotic modes [2], nonlinear admixing [3], etc.). Generalized [7] and phase [8] synchronizations or simultaneous use of several types of synchronous behavior [7, 13] are more rare.

A fundamental drawback of all schemes known to date is a low stability to noise and fluctuations in the communication channel. When the noise and fluctuation intensity exceeds some threshold value, comparable with the natural noise and distortions, the known data transmission systems become disabled. In addition, a fundamental requirement for almost all such schemes is the presence of highly identical random generators at different sides of the communication channel. This is a very serious technical problem, especially when a device operates for a long time. Another drawback of such schemes (in particular, those using complete chaotic synchronization) is the possibility of reconstruction [14] of the transmitter parameters from a signal transmitted through the communication channel. Due to the presence of an exact copy of the transmitter at the other side of the communication channel, the third side can easily decode an information message in some cases.

In this study, we propose a new method for secure data transmission. It is based on the phenomenon of generalized chaotic synchronization; however, in contrast to the known methods, using both this (see, for example, [7, 13]) and other [1–5] types of synchronous behavior, this method makes it possible to eliminate all the above-mentioned drawbacks. The efficiency of the method proposed is illustrated by numerical simulation of two unidirectionally coupled Róssler systems, chosen as transmitter and receiver. Some statistical estimates of the operating capacity of the proposed scheme in comparison with some known one are reported.

1. GENERALIZED SYNCHRONIZATION AND METHODS FOR ITS DIAGNOSTICS

As was mentioned in the Introduction, the proposed method for secure data transmission is based on the phenomenon of generalized synchronization between random generators at transmitting and receiving sides of the communication channel. Let us briefly dwell on this type of synchronous behavior and the main methods for its diagnostics.

The generalized synchronization mode can be implemented in a system of two unidirectionally coupled chaotic oscillators, master and slave ones. This mode means that, after the end of a transient process, some functional relation $\mathbf{u}(t) = \mathbf{F}[\mathbf{x}(t)]$ is established between their states, $\mathbf{x}(t)$ (master) and $\mathbf{u}(t)$ (slave), whose form may by fairly complex (in particular, fractal [15]). Generally, such a relation can far from always be found, neither analytically nor experimentally. However, there are some effective methods for diagnostics of this mode: the nearest neighbor method, the method for calculating conditional Lyapunov exponents, and the auxiliary-system method. Technical implementation of the first two methods is a fairly difficult problem, which sometimes cannot be solved at all. At the same time, the auxiliary-system method can easily be implemented in practice, but it involves use of an exact copy of the slave generator.

The essence of the auxiliary-system method [16] is as follows: along with the slave system, an identical auxiliary system is considered. The initial conditions for the auxiliary system are chosen to be different from

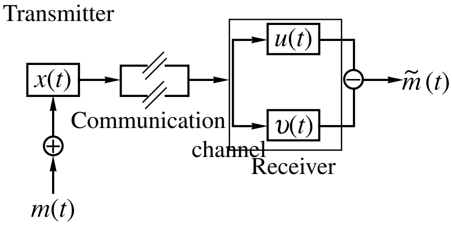

Fig. 1. Schematic of the method for secure data transmission based on the use of generalized chaotic synchronization:$m(t)$ is a binary information signal, $\mathbf{x}(t)$ is the state vector of the transmitter, $\mathbf{u}(t)$ and $\boldsymbol{\upsilon}(t)$ are the state vectors of the receiving generators, and $\tilde{m}(t)$ is a reconstructed signal.

the initial state of the slave system, but lying in the range of attraction of one attractor (in practice, this generally means a small mismatch between the initial conditions, which is automatically implemented due to fluctuations). When generalized synchronization between interacting systems is absent, the state vectors of the slave and auxiliary systems belong to the same chaotic attractor; however, they are different due to the Lyapunov instability of chaotic trajectories. When generalized synchronization occurs, in view of the validity of functional relations between the states of the master and slave systems and, correspondingly, the master and auxiliary ones, the states of the slave and auxiliary systems should become identical after the end of the transient process. Thus, the equivalence of the states of the slave and auxiliary systems after the transient process is a criterion for the existence of generalized synchronization between the master and slave chaotic systems.

2. METHOD FOR SECURE DATA TRANSMISSION

A schematic of secure data transmission based on generalized chaotic synchronization is shown in Fig. 1. This method is as follows. The information signal $m(t)$ is coded as a binary code. One or several control parameters of the transmitter are modulated by a binary signal. The thus obtained signal is transmitted through the communication channel. Here, it is affected by noise and fluctuations, which distort the transmitted signal. The receiver is at the other side of the communication channel. It consists of two identical generators, which can be in the mode of generalized synchronization with the transmitter. It should be noted that the presence of identical generators at one side of the communication channel makes it possible to easily align them. The principle of operation of the receiver is based on the diagnostics of the generalized synchronization mode using the auxiliary-system method (see above). The signal from the communication channel arrives at the receiver generators. The output signals pass through a subtractor and the restored desired signal is detected.

The characteristics of modulation of the transmitter control parameters should be chosen so as to ensure the presence or absence of the generalized synchronization between the transmitter and receiver, depending on the transmitted binary 0/1 bit. For example, let us assume that generalized synchronization is observed when a binary bit 0 is transmitted. Then, both receiver generators will demonstrate identical oscillations, and after transmission through a subtractor, chaotic oscillations will be absent (i.e., we have a binary bit 0). Vice versa, in the case of transmission of a binary bit 1, generalized synchronization is not observed, and oscillations of receiver generators are nonidentical. Then after transmission through the subtractor, chaotic oscillations have a nonzero amplitude (binary bit 1).

3. NUMERICAL IMPLEMENTATION OF THE METHOD FOR SECURE DATA TRANSMISSION

To show the undoubted advantage of the proposed method for data transmission over the known ones, we will perform numerical simulation of the scheme shown in Fig. 1. As both transmitter and receiver, we will use unidirectionally coupled Róssler systems. Such a model is chosen because (i) Róssler system have been fairly well studied (in particular, from the point of view of the generalized synchronization [15–20]) and (ii) a radio generator can be designed, whose dynamics will be described by the equations of the Róssler system [21].

The transmitter is described by the following system of differential equations:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \end{aligned} \tag{1}$$

where $\mathbf{x}(t) = (x_1, x_2, x_3)$ is the state vector of the transmitter; $a = 0.15$, $p = 0.2$, and $c = 10$ are the control parameters; and ω_x is the control parameter characterizing the eigenfrequency of oscillations of the system.

The parameter ω_x is modulated by the useful digital signal as follows. If a binary bit 1 is transmitted within a specified time interval, $\omega_x = 0.95$ during all this interval. When a binary bit 0 is transmitted, $\omega_x = 1$. It should be noted that the above-mentioned values of the control parameter ω_x were chosen only for demonstration; they are related to the character of location of the generalized synchronization boundary, which was investigated in detail in [20]. Actually, the parameter ω_x can take arbitrary values. The only necessary condition is the alternation of regions with asynchronous dynamics and regions of generalized synchronization.

The receiver contains two identical random generators, each described by the following system of equations:

$$\begin{aligned} \dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \\ \dot{u}_2 &= \omega_u u_1 + a u_2, \\ \dot{u}_3 &= p + u_3(u_1 - c). \end{aligned} \qquad (2)$$

Here, $\mathbf{u}(t) = (u_1, u_2, u_3)$ is the state vector of the first receiving generator. Let a vector $\boldsymbol{\upsilon}(t) = (\upsilon_1, \upsilon_2, \upsilon_3)$, also satisfying (2), be the state vector of the second receiving generator (Fig. 1). The control parameters a, p, and c will be chosen the same as for receiving generators. The control parameter ω_u, characterizing the eigenfrequency of receiving generators, will be chosen to be 0.95 during the entire time of signal transmission.

A signal generated by the transmitter passes through the communication channel. In our model, transmission is implemented via coupling of the receiver and transmitter, i.e., through introduction of the component ω_u into the first equation of system (2). Here, $\varepsilon(s(t) - u_1)$ is the so-called signal in the communication channel. The term $s(t) = x_1 + D\xi$ models noise and fluctuation in the communication channel; ξ is the characteristic of a stochastic Gaussian process having the following probability distribution:

$$p(\xi) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right), \qquad (3)$$

where $\xi_0 = 0$ and $\sigma = 1$ are, respectively, the mean and dispersion[1]. The parameter $D\xi$ determines the added noise intensity.

The coupling strength between the transmitter and receiver is characterized by the parameter ε; it was chosen to be 0.14. In this case, it is known that in the absence of noise and fluctuations in the communication channel ($D = 0$), generalized synchronization in system (1), (2) occurs at $\omega_x = 1$, whereas, for $\omega_x = 0.95$, generalized synchronization is not observed (see [20] for details).

The subtractor performs the operation $(u_1 - \upsilon_1)^2$. Hence, according to the auxiliary-system method, absence of oscillations for $\omega_x = 1$ and presence of chaotic oscillations for $\omega_x = 0.95$ should be observed after signal transmission through the subtractor. The reconstructed signal $\tilde{m}(t)$ is a sequence of regions characterized by different types of behavior.

For demonstration, we will choose a simple sequence of binary bits 0/1 as a signal $m(t)$ (Fig. 2, dotted line). Stochastic equation (2) will be integrated using the Euler method with a time discretization step $h = 0.0001$.

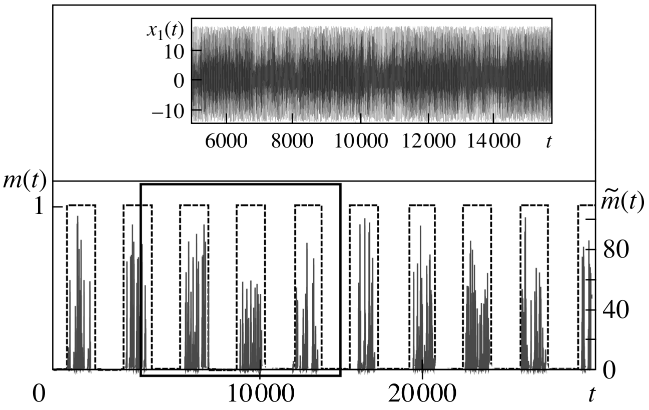

Fig. 2. Transmitted information signal $m(t)$ in the form of a simple sequence of binary bits 0/1 (dotted line) and the reconstructed signal $\tilde{m}(t)$ in the absence of noise and fluctuations in the communication channel ($D = 0$). The inset shows a fragment of a random signal generated by the transmitter in the form of a sequence of three binary bits 0/1 (shown by a rectangle) and transmitted through the communication channel. It can be seen that an information message cannot be decoded by the third side in this case.

Let us first consider the case where noise and fluctuations are absent in the communication channel, i.e., assume that the noise amplitude $D = 0$. Obviously, this case cannot be realized in practice because noise and fluctuations are always present in actual devices. Nevertheless, we will consider first the idealized situation to check the efficiency of the method proposed. The reconstructed signal $\tilde{m}(t)$ for this case is shown in Fig. 2 (solid line). One can see that the desired signal can easily be detected in this case.

It should be noted that a change in the control parameter ω_x does not significantly change the characteristics of a transmitted signal. A fragment of such a signal, containing a sequence of six bits 0/1 is shown in the inset in Fig. 2. Obviously, even in the absence of noise and fluctuations in the communication channel, the third side cannot decode an information message. Introduction of noise into the communication channel distorts a transmitted signal even more. However, the reconstructed signals $\tilde{m}(t)$ are qualitatively similar at different noise amplitudes, up to $D = 400$, as in the absence of noise and fluctuations (Fig. 2, solid line). In this case, we can speak about significant stability of the proposed scheme to noise and fluctuations in the communication channel.

4. COMPARISON OF THE PROPOSED METHOD FOR SECURE DATA TRANSMISSION WITH THE KNOWN METHODS

To show undoubted advantages of our method over the known ones, we will carry out some statistical esti-

[1] It is noteworthy that the character of distribution of the random variable ξ is of no importance, and similar results can be observed for other types of distribution of the probability $p(\xi)$, for example, uniform distribution.)

mations of the operating parameters for the data transmission scheme proposed here and for a number of known schemes (see, for example, [1–3, 7, 13]). Such parameters are as follows:

(i) The signal-to-noise ratio (SNR) at which the scheme becomes disabled; i.e., when there is no possibility of reconstructing the initial useful digital signal $m(t)$ from the output signal $\tilde{m}(t)$. Since noise and fluctuations are inevitably present in a communication channel, estimation of the operating capacity of data transmission schemes in the presence of noise is a very important and urgent problem.

(ii) The maximum mismatch of the control parameters of the generators, which should be initially identical. As was discussed in the Introduction, in most known cases, such generators should be located at different sides of the communication channel. Since it is difficult to realize such devices in practice, the effect of mismatch of their control parameters on the efficiency of the data transmission method is an urgent problem.

Analysis of such characteristics showed that the scheme proposed here becomes disabled at the signal-to-noise ratio SNR = –34.6 dB, whereas for other schemes considered by us this value is positive; i.e., in the presence of noise and fluctuations in the communication channel, whose power is smaller than that of a transmitted signal, all the schemes known to date become disabled. Our scheme has an extremely high stability to noise and fluctuations in the communication channel. Noise, distorting a transmitted signal even more, prohibits decoding of an information message by the third side. In this case, we can speak about constructive role of noise for data transmission, whereas in other cases noise plays a destructive role.

Estimation of the effect of mismatch of control parameters on the efficiency of the method proposed showed that, if the receiving generators are mismatched up to 2% with respect to the parameter ω_x, the scheme under consideration retains its efficiency. Obviously, such a mismatch is not very large, and, in this context, the scheme proposed has analogs (for example, data transmission schemes known as random-mode switching [2] and modulation of control parameters [22]). However, one should take into account that in these cases both generators should be located at different sides of the communication channel (to implement complete synchronization between them). In the case considered here, identical generators are located only at the receiving side of the communication channel, as a result of which they can easily be aligned. In addition, both above-mentioned schemes have limited stability to noise and fluctuations in the communication channel, whereas the stability of the proposed scheme is practically unlimited.

CONCLUSIONS

We have proposed a new method for secure data transmission based on the use of generalized chaotic synchronization. This method has a number of fundamental advantages in comparison with the known methods for secure data transmission. First, it does not require the presence of identical random generators at different sides of the communication channel, and therefore, can easily be implemented in practice. Second, it has an extremely high stability to noise and fluctuations in the communication channel. In this case, we can speak about the constructive role of noise for data transmission. Third, due to the presence of noise in the communication channel, a transmitted signal becomes additionally distorted, as a result of which the third side cannot decode an information message.

ACKNOWLEDGMENTS

This study was supported by the Russian Foundation for Basic Research, project no. 05-02-16273; the Program of the President of the Russian Federation for Support of Leading Scientific Schools of the Russian Federation (project NSh-4167.2006.2) and Young Doctors of Sciences (MD-1884.2007.2); the Research and Educational Center "Nonlinear Dynamics and Biophysics" at the Saratov State University (grant REC-006 of US CRDF); the Foundation of Noncommercial Programs "Dynasty"; and the International Center of Fundamental Physics (Moscow).

REFERENCES

1. Cuomo, M.K., Oppenheim, A.V., and Strogatz, S.H., *IEEE Trans. Circuits Syst.*, 1993, vol. 40, no. 10, p. 626.
2. Dedieu, H., Kennedy, M.P., and Hasler, M., *IEEE Trans. Circuit Syst.*, 1993, vol. 40, p. 634.
3. Dmitriev, A.S., Panas, A.I., and Starkov, S.O., *Int. J. Bifurcation Chaos Appl. Sci. Eng.*, 1995, vol. 5, no. 4, p. 1249.
4. Boccaletti, S., Farini, A., and Arecchi, F.T., *Phys. Rev. E: Stat. Phys., Plasmas, Fluids, Relat. Interdiscip. Top.*, 1997, vol. 55, no. 5, p. 4979.
5. Carroll, T.L. and Johnson, G.A., *Phys. Rev. E: Stat. Phys., Plasmas, Fluids, Relat. Interdiscip. Top.*, 1998, vol. 57, no. 2, p. 1555.
6. Fischer, I., Liu, Y., and Davis, P., *Phys. Rev. A: At., Mol., Opt. Phys.*, 2000, vol. 62, 011 801.
7. Terry, J.R. and VanWiggeren G.D, *Chaos, Solitons Fractals*, 2001, vol. 12, p. 145.
8. Chen, J.Y., Wong, K.W., Cheng, L.M., and Shuai, J.W., *Chaos*, 2003, vol. 13, no. 2, p. 508.
9. Yuan, Z.L. and Shields, A.J., *Phys. Rev. Lett.*, 2005, vol. 94, 048 901.
10. Lucamarini, M. and Mancini, S., *Phys. Rev. Lett.,* 2005, vol. 94, 140 501.
11. Li, Q.S. and Liu, Y., *Phys. Rev. E: Stat., Nonlinear, Soft Matter Phys.*, 2006, vol. 73, 016 218.

12. Fradkov, A.L., Andrievsky, B., and Evans, R.J., *Phys. Rev. E: Stat., Nonlinear, Soft Matter Phys.*, 2006, vol. 73, 066 209.
13. Murali, K. and Lakshmanan, M., *Phys. Lett. A*, 1998, vol. 241, p. 303.
14. Ponomarenko, V.I. and Prokhorov, M.D., *Phys. Rev. E: Stat., Nonlinear, Soft Matter Phys.*, 2002, vol. 66, no. 2, 026 215.
15. Rulkov, N.F., Sushchik, M.M., Tsimring, L.S., and Abarbanel, H.D.I., *Phys. Rev. E: Stat. Phys., Plasmas, Fluids, Relat. Interdiscip. Top.*, 1995, vol. 51, no. 2, p. 980.
16. Abarbanel, H.D.I., Rulkov, N.F., and Sushchik, M.M., *Phys. Rev. E: Stat. Phys., Plasmas, Fluids, Relat. Interdiscip. Top.*, 1996, vol. 53, no. 5, p. 4528.
17. Hramov, A.E. and Koronovskii, A.A., *Phys. Rev. E: Stat., Nonlinear, Soft Matter Phys.*, 2005, vol. 71, no. 6, 067 201.
18. Zheng, Z. and Hu, G., *Phys. Rev. E: Stat. Phys., Plasmas, Fluids, Relat. Interdiscip. Top.*, 2000, vol. 62, no. 6, p. 7882.
19. Hramov, A.E. and Koronovskii, A.A., *Europhys. Lett.*, 2005, vol. 70, no. 2, p. 169.
20. Hramov, A.E., Koronovskii, A.A., and Moskalenko, O.I., *Europhys. Lett.*, 2005, vol. 72, no. 6, p. 901.
21. Rico-Martinez, R., Kreischer, K.E., Flatgen, G., et al., *Phys. D,* 2003, vol. 176, p. 1.
22. Yang, T. and Chua, L.O., *IEEE Trans. Circuits Syst. I*, 1996, vol. 43, p. 817.

SPELL: ok