2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Method for Detecting Generalized Synchronization: Application to Secure Communication

Vladimir Ponomarenko†‡ and Mikhail Prokhorov†

†Saratov Branch of the Institute of Radio Engineering and Electronics of Russian Academy of Sciences
38 Zelyonaya Street, Saratov 410019, Russia
‡Department of Nano- and Biomedical Technologies, Saratov State University
83 Astrakhanskaya Street, Saratov 410012, Russia
Email: ponomarenkovi@gmail.com, mdprokhorov@yandex.ru

Abstract– We propose a method for detecting the generalized synchronization which does not exploit an auxiliary system approach. The method is based on using only one response system in the receiver, but this system is driven in turn by the transmitted signal itself and its delayed copy. Using the proposed method we develop a secure communication scheme exploiting the generalized synchronization. The scheme shows very high tolerance to noise in a communication channel.

1. Introduction

Communication systems based on the employment of chaotic synchronization [1] are usually characterized by comparatively low resistance to noise and amplitude distortions of the signal in a communication channel. However, communication systems based on the generalized synchronization are an exception from this rule [2]. They possess very high tolerance to noise and signal distortions. Different methods have been proposed to detect the regime of generalized synchronization in unidirectionally coupled systems. The most popular among them are the auxiliary system approach [3], the conditional Lyapunov exponent calculation [4], and the nearest neighbor method [5]. In the experiment, the generalized synchronization was observed in [6].

The communication systems exploiting the generalized synchronization are based on the following idea. A binary information signal $m(t)$ modulates one or more parameter of the transmitter, i.e. $m(t)$ controls a switch whose action changes the parameter values of the transmitter. The binary 0 corresponds to one parameter set value p_1 of the transmitter and binary 1 corresponds to another parameter set value p_2. The parameters of the receiver should be chosen so as to ensure that the generalized synchronization with the transmitter could take place at a transmission of only one of binary symbols (0 or 1).

The auxiliary system method may be generally considered as the most easy, clear and powerful technique to detect the generalized synchronization regime in chaotic systems. This approach utilizes a second, identical response system to monitor the synchronized motions. If we drive two identical response systems, one the original response system and the other the auxiliary system, with the same input signal from the drive system, then we can identify the presence of the generalized synchronization by observing the stable regime of identical oscillations in auxiliary and response systems [3].

The auxiliary system approach is a promising technique for employing in a physical experiment since it can provide the detection of the generalized synchronization in real time in contrast with other methods requiring the signal recording for further processing. However, the main technical problem of this method is the construction of two identical response systems in the receiver. This problem is especially difficult for solving at high frequencies.

In the present paper, we propose a new method for detecting the generalized synchronization which does not exploit an auxiliary system approach. This method allows one to exploit only one response system in the receiver. Using the proposed method we develop a secure communication scheme exploiting the generalized synchronization.

The paper is organized as follows. In Section 2, the method proposed for the generalized synchronization detection is described. In Section 3, we illustrate the method application to hidden data transmission in a numerical experiment. In Section 4, we consider the operation of the experimental communication scheme based on the generalized synchronization. In Section 5, we summarize our results.

2. Method Description

We propose a method for detecting the generalized synchronization which exploits the idea of auxiliary system approach, but utilizes only one response system which is driven in turn by the transmitted signal itself and its delayed copy.

If we drive the self-oscillating response system twice with the same input signal from the autonomous drive system, then after the transient process it will exhibit identical oscillations in both cases in the presence of the generalized synchronization between the drive and response systems. To ensure the identity of the signal that twice drives the response system we use a delay line.

At first, within the time interval τ we drive the response system in the receiver with the signal incoming from a communication channel. Then, within the same time interval τ we drive the same response system with the delayed signal incoming from the output of the delay line having the delay time τ. At last, we compare the signals of the response system in the considered two cases. With this purpose we calculate the difference between the signal at the response system output and the signal of the response system which is passed through one more delay line with the delay time τ. In the presence of the generalized synchronization, this difference vanishes after the transient process.

A block diagram illustrating the proposed method is shown in Fig. 1. The information signal $m(t)$ representing a sequence of binary 0 and 1 modulates one the transmitter parameters. The chaotic signal $x(t)$ from the transmitter output is transmitted into the communication channel. The receiver is composed of the self-oscillating response system, two delay lines with the same delay time τ, square-wave generator (SWG), commutator, and difference amplifier. The parameters of the receiver are chosen so as to ensure that the generalized synchronization with the transmitter takes place only at a transmission of binary 0.

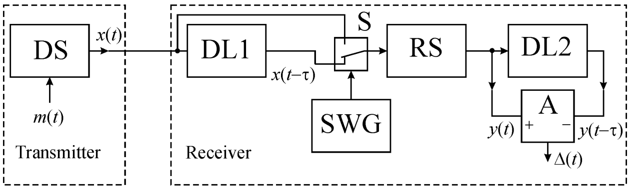

Fig. 1. Block diagram of a communication system based on the generalized synchronization: (DS) drive system, (RS) response system, (DL1 and DL2) delay lines, (SWG) square-wave generator, (S) commutator, and (A) difference amplifier.

The SWG controls a switch whose action changes the signal driving the response system. During the first half of the period of SWG signal, the response system is driven by the signal $x(t)$. During the second half of the period of SWG signal, the response system is driven by the signal $x(t-\tau)$ incoming from the output of the delay line DL1. The period T of SWG signal is chosen so as to ensure that the transient process preceding the regime of generalized synchronization terminates at a time less than $T/2$. The delay times of delay lines DL1 and DL2 are $\tau = T/2$.

In the second half of the period of SWG signal, the difference $\Delta(t) = y(t) - y(t-\tau)$ of the response system signals vanishes after the transient process in the presence of the generalized synchronization between the drive and response systems. In the absence of the generalized synchronization, the difference $\Delta(t)$ shows nonvanishing oscillations within the entire second half of the period of SWG signal.

During the first half of the period of SWG signal, the value of $\Delta(t)$ contains no useful information for the detection of the generalized synchronization. Within this time interval, $\Delta(t)$ shows nonvanishing oscillations similarly to the case of the absence of the generalized synchronization in the second half of the period of SWG signal. For better detection of the generalized synchronization, one could connect detector and low-pass filter to the output of the difference amplifier.

3. Numerical Investigation of Communication System

We study numerically the communication system exploiting the generalized synchronization (Fig. 1) for the case where the drive and response systems represent time-delayed feedback oscillators. A block diagram of the drive system in the transmitter is shown in Fig. 2(a).

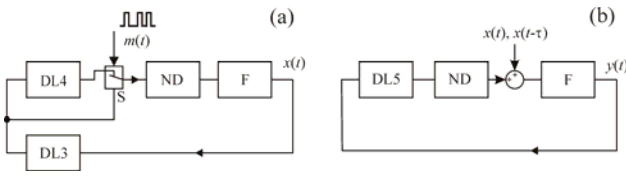

Fig. 2. Block diagrams of the drive (a) and response (b) systems: (DL3, DL4, and DL5) delay lines, (ND) nonlinear devices, (F) filters, and (S) commutator.

The drive system represents a ring system composed of two delay lines DL3 and DL4 with delay times τ_1 and τ_2, respectively, a nonlinear element, and a linear low-pass filter. The binary information signal $m(t)$ switches the delay time in the system in such a way that the delay time is equal to τ_1 at a transmission of binary 0 and it is equal to $\tau_1 + \tau_2$ at a transmission of binary 1. The drive system is described by a first-order delay-differential equation

$$\varepsilon \dot{x}(t) = -x(t) + f_1\left(x\left(t - \left(\tau_1 + m(t)\tau_2\right)\right)\right), \qquad (1)$$

where $x(t)$ is the system state at time t, ε is the parameter that characterizes the inertial properties of the system, and f_1 is a nonlinear function. The signal $x(t)$ from the filter output is transmitted into the communication channel.

A block diagram of the self-oscillating response system in the receiver is shown in Fig. 2(b). The delay line DL5 has the same delay time τ_1 as the delay line DL3. The response system is driven in turn by the signals $x(t)$ and $x(t-\tau)$. It is described by the following equation:

$$\begin{aligned} \varepsilon \dot{y}(t) &= -y(t) + f_2\left(y(t-\tau_1)\right) + \\ & k\left(Z(t)x(t) - \overline{Z(t)}x(t-\tau)\right), \end{aligned} \qquad (2)$$

where f_2 is a nonlinear function, k characterizes the strength of the unidirectional coupling, $Z(t)$ is the signal of the SWG, and $\overline{Z(t)}$ is the inversion of $Z(t)$. A half of the period of $Z(t)$ the response system is driven by the signal $x(t)$. In this case $Z(t) = 1$ and $\overline{Z(t)} = 0$. Another half of the period of $Z(t)$ the response system is driven by the signal $x(t-\tau)$. In this case $Z(t) = 0$ and $\overline{Z(t)} = 1$.

Let us illustrate the efficiency of the proposed communication system for the case where the drive and response systems represent a time-delayed feedback oscillator with quadratic nonlinear function and a low-pass first-order Butterworth filter with cutoff frequency $f_c = 1/\varepsilon$. We choose the following values of the transmitter and receiver parameters: $\tau_1 = 100$, $\tau_2 = 10$, $f_c = 0.2$ $(\varepsilon = 5)$, $f_1(x) = \lambda_1 - x^2$, $f_2(y) = \lambda_2 - y^2$, where $\lambda_1 = 1.7$ and $\lambda_2 = 1.3$ are the parameters of nonlinearity, k=0.13, T=40000 and τ = 20000. With these parameters, the transmitter generates a chaotic signal $x(t)$ (Fig. 3) and the receiver in the absence of coupling $(k = 0)$ oscillates in a periodic regime. It has been shown that the threshold of the generalized synchronization occurrence is smaller in the case of periodic regime of the response system [7].

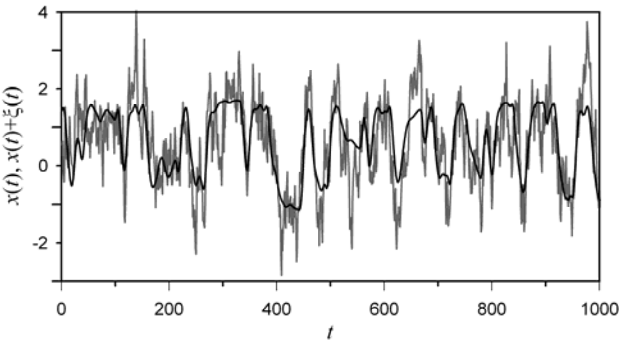

Fig. 3. The time series of the driving chaotic signal $x(t)$ without noise (black color) and corrupted with additive noise (gray color).

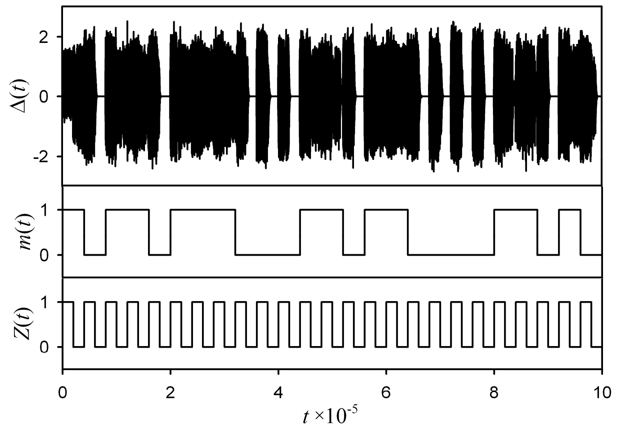

Fig. 4. The time series of the difference signal $\Delta(t)$, information signal $m(t)$, and the signal $Z(t)$ of the SWG.

To investigate the tolerance of the proposed communication system to noise we added a zero-mean Gaussian white noise $\xi(t)$ filtered in the bandwidth of the chaotic carrier to time series of the signal $x(t)$ transmitted into the communication channel. Fig. 3 shows in gray color a part of the time series of $x(t)$ corrupted with noise for the case where the variance of $\xi(t)$ is $\sigma_\xi^2 = 0.63$. The signal $x(t)$ at the output of the drive system has the same variance $\sigma_x^2 = 0.63$. Thus, the signal-to-noise ratio (SNR) in this case is equal to 0 dB.

Fig. 4 shows the results of the scheme operation for the case $\mathrm{SNR} = 0$ dB. At a transmission of binary 0, the difference $\Delta(t)$ oscillates at $Z(t) = 1$ and vanishes at $Z(t) = 0$ indicating the presence of the generalized synchronization between the drive and response systems (Fig. 4). For $m(t) = 1$ the signal $\Delta(t)$ shows nonvanishing oscillations both at $Z(t) = 1$ and $Z(t) = 0$ indicating the absence of the generalized synchronization. Thus, the scheme is still efficient in spite of very high level of noise in the communication channel.

4. Results of the Experimental Scheme Operation

We implemented the proposed secure communication system in a radio physical experiment in which the drive and response systems were constructed using electronic ring oscillators with time-delayed feedback. These oscillators contain analog low-pass first-order *RC* filters and digital delay lines and nonlinear elements implemented using programmable microcontrollers of the Atmel SAM3A family. The nonlinear elements have quadratic nonlinear function.

The drive system is described by Eq. (1) with $\varepsilon = RC = 47$ mcs, $\tau_1 = 930$ mcs, $\tau_2 = 93$ mcs, and $\lambda_1 = 1.7$. With these parameters, the transmitter generates a chaotic signal $x(t)$ (Fig. 5).

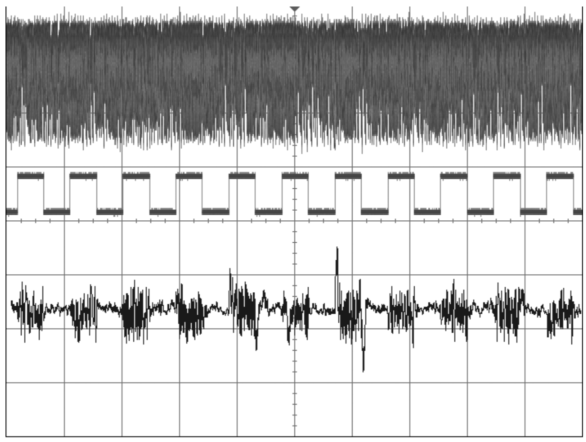

Fig. 5. Oscillograms of temporal realizations of the chaotic signal $x(t)$ in the communication channel (on top), signal $Z(t)$ of the SWG (in the middle), and filtered difference signal $\Delta(t)$ (below) in the case of the transmission of binary 0.

The response system in the receiver is described by Eq. (2) with $\varepsilon = RC = 95$ mcs, $\tau_1 = 930$ mcs, and $\lambda_2 = 1.3$. In the absence of coupling, the response system generates periodic oscillations. The delay lines DL1 and DL2 in the receiver are also implemented using microcontrollers having an integrated 12-bit analog-to-digital converter and digital-to-analog converter. The delay time of these delay lines is set to $\tau = 90$ ms. The period of $Z(t)$ signal is $T = 180$ ms. The coupling coefficient is $k = 0.1$.

Part of the time series of the driving chaotic signal $x(t)$, signal $Z(t)$ of the SWG, and difference signal $\Delta(t)$ passed through a low-pass filter with cutoff frequency $f = 200$ Hz are presented in Fig. 5 for the case of the transmission of binary 0. The time scale over the horizontal axis is 200 ms/div. The scale over the vertical axis is 1 V/div, 5 V/div, and 200 mV/div for the signals $x(t)$, $Z(t)$, and $\Delta(t)$, respectively.

As it can be seen from Fig. 5, at high values of $Z(t)$, the amplitude of oscillations of the signal $\Delta(t)$ is appreciably greater than at small values of $Z(t)$. This abrupt decrease of the amplitude of $\Delta(t)$ indicates the presence of the generalized synchronization between the drive and response systems.

Fig. 6 shows a part of the time series of the signals $x(t)$, $Z(t)$, and $\Delta(t)$ for the case of the transmission of binary 1. As well as in Fig. 5, the difference signal $\Delta(t)$ is passed through a low-pass filter with cutoff frequency $f = 200$ Hz. The scales over the axes are the same as those in Fig. 5.

In contrast to Fig. 5 corresponding to the transmission of binary 0, the amplitude of the difference signal $\Delta(t)$ in Fig. 6 is practically the same within the both halves of the period of the SWG signal $Z(t)$. Such behavior of $\Delta(t)$ indicates the absence of the generalized synchronization between the drive and response systems.

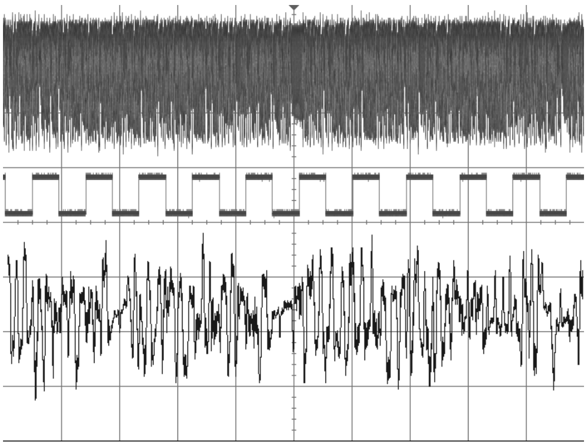

Fig. 6. Oscillograms of temporal realizations of the chaotic signal $x(t)$ in the communication channel (on top), signal $Z(t)$ of the SWG (in the middle), and filtered difference signal $\Delta(t)$ (below) in the case of the transmission of binary 1.

It should be noted that the considered communication scheme has a low rate of data transmission. It is explained by a long time of transient processes that precede the occurrence of the generalized synchronization regime in the time-delayed feedback oscillators used as the drive and response systems in our study. However, one can increase the rate of information transmission by choosing other oscillators as the drive and response systems, which have a short time of transient processes preceding the occurrence of the generalized synchronization.

5. Conclusion

We have proposed the method for the generalized synchronization detection which does not exploit an auxiliary system approach. Using the proposed method we have developed the secure communication system exploiting the regime of generalized synchronization between the transmitter and receiver. The receiver utilizes only one self-oscillating response system which is driven in turn by the transmitted signal itself and its delayed copy. In our communication system, the transmitter and receiver represent time-delayed feedback oscillators.

The proposed communication scheme is studied numerically and realized in the physical experiment. We have illustrated the scheme efficiency for the transmission of binary information signal. It is shown that the proposed scheme possesses high tolerance to noise in the communication channel.

Acknowledgments

This work is supported by the Russian Science Foundation, Grant No. 14–12–00324.

References

[1] L. M. Pecora, T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol.64, pp.821–824, 1990.

[2] A. A. Koronovskii, O. I. Moskalenko, A. E. Hramov, “On the use of chaotic synchronization for secure communication,” *Physics – Uspekhi*, vol.52, pp.1213–1238, 2009.

[3] H. D. I. Abarbanel, N. F. Rulkov, M. M. Sushchik, “Generalized synchronization of chaos: The auxiliary system approach,” *Phys. Rev. E*, vol.53, pp.4528–4535, 1996.

[4] K. Pyragas, “Conditional Lyapunov exponents from time series,” *Phys. Rev. E*, vol.56, pp. 5183–5188, 1997.

[5] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, H. D. I. Abarbanel, “Generalized synchronization of chaos in directionally coupled chaotic systems,” *Phys. Rev. E*, vol.51, pp. 980–994, 1995.

[6] D. Y. Tang, R. Dykstra, M. W. Hamilton, and N. R. Heckenberg, “Observation of generalized synchronization of chaos in a driven chaotic system,” *Phys. Rev. E*, vol. 57 pp. 5247-5251, 1998.

[7] A. A. Koronovskii, O. I. Moskalenko, A. S. Pavlov, N. S. Frolov, A. E. Hramov, “Generalized synchronization in the action of a chaotic signal on a periodic system,” *Tech. Phys.*, vol.59, pp.629–636, 2014.