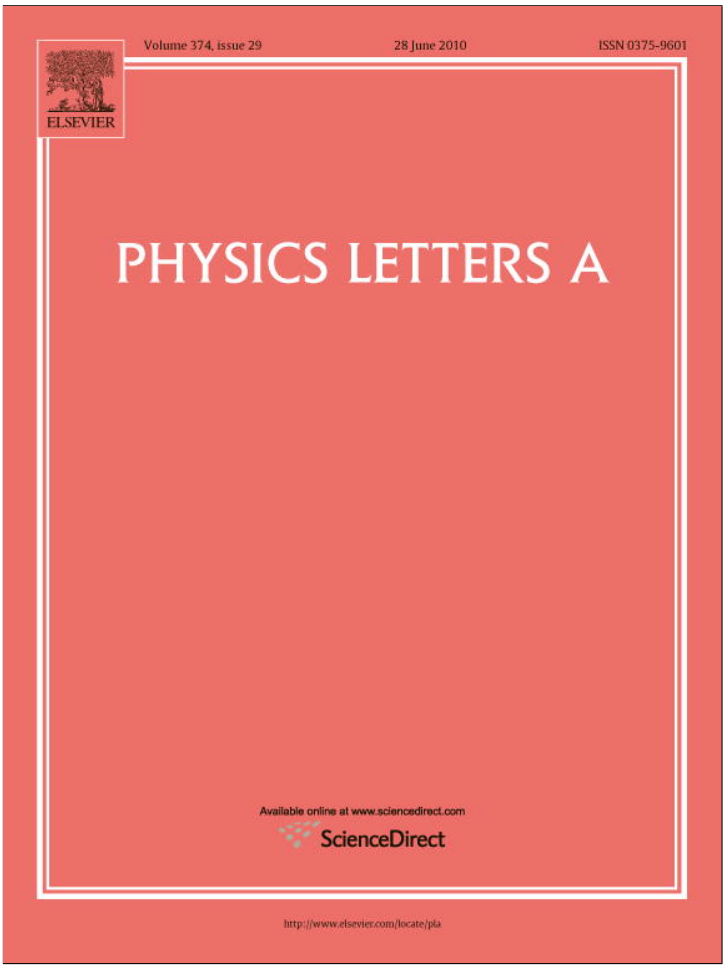

Physics Letters A 374 (2010) 2925–2931

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Generalized synchronization of chaos for secure communication: Remarkable stability to noise

Olga I. Moskalenko *, Alexey A. Koronovskii, Alexander E. Hramov

Faculty of Nonlinear Processes, Saratov State University, 83, Astrakhanskaya, Saratov, 410012, Russia

ARTICLE INFO

Article history:
Received 3 September 2008
Received in revised form 18 February 2010
Accepted 7 May 2010
Available online 12 May 2010
Communicated by A.P. Fordy

Keywords:
Synchronization
Chaotic oscillators
Dynamical system
Generalized synchronization
Noise
Chaotic communication
Secure information transmission

ABSTRACT

A new method for secure information transmission based on generalized synchronization is proposed. The principal advantage of it is a remarkable stability to noise. To reveal this peculiarity of the proposed method the effectiveness of the detection of the information signal from the transmitted one in the presence of noise in the communication channel is examined both for the proposed scheme and for the schemes of chaotic communication known already. The main ideas of the proposed method are illustrated by the example of coupled Rössler systems used both transmitter and receiver.

0. Introduction

The use of chaotic signals for information transmission attracts great attention of modern scientists [1–11]. Along with the theoretical studies, the chaos based systems are used in the practical applications [12–14]. Among of the works devoted to this subject there are a lot of papers devoted to the secure communication [15–20]. Several methods for secure information transmission are known. Some of them are based on the synchronization of chaotic oscillators [21–28]. Recently, the practical implementation of the chaotic synchronization for the secure information transmission have been reported [29].

One of the most important problems connected with the secure communication based on the chaotic synchronization phenomenon is the distortions of signals caused by the influence of noise (first of all, in the communication channel) that results in the loss of the transmitted information, with the ability of the secure communication systems to be stable to the external perturbations being limited [30]. All known schemes based on the chaotic synchronization phenomenon prove to be characterized by the weak robustness to noise [31–33].

In this Letter we report a new method for secure information transmission possessing remarkable stability to noise. As it would be shown below, our scheme demonstrates the great resistance to noise in comparison with the other ones known hitherto. Moreover, we use the subsidiary source of noise in the proposed scheme to provide the additional masking of the information signal. The scheme is based on the generalized synchronization phenomenon [34–36], with several other disadvantages inherent in the already known systems for secure communications being overcome. At the same time, as well as other communication schemes based on chaotic synchronization it is characterized by the low rate of information sending.

The structure of the Letter is the following. Section 1 describes a theoretical background leading to the new method for secure information transmission. It contains brief description of the generalized synchronization regime, with principal advantages of its use for secure communication being briefly discussed. In Section 2 a new method for secure information transmission based on this type of the synchronous chaotic system behavior is proposed. General requirements for such secure communication scheme are considered. Section 3 presents results of numerical simulation of the proposed method. In Section 4 the stability of our communication scheme (as well as a series of another ones) to noise is discussed. Quantitative characteristics of the efficiency of the secure communication schemes are introduced. Our scheme is shown to possess the remarkable stability to noise. Section 5 discusses the other advantages of the proposed secure communication scheme. The

* Corresponding author.
E-mail addresses: moskalenko@nonlin.sgu.ru (O.I. Moskalenko), alkor@nonlin.sgu.ru (A.A. Koronovskii), aeh@nonlin.sgu.ru (A.E. Hramov).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2010.05.024

influence of the control parameter mismatch of generators which have to be identical firstly and the effect of nonlinear distortions in the communication channel on the efficiency of the proposed and already known communication schemes are also considered in this section. Final discussions and remarks are given in Conclusions.

1. Theoretical background of the method to be proposed

The generalized synchronization regime (GS) in two unidirectionally coupled chaotic oscillators means the presence of a functional relation $\mathbf{u}(t) = \mathbf{F}[\mathbf{x}(t)]$ between the drive $\mathbf{x}(t)$ and response $\mathbf{u}(t)$ system states [34,37]. This relation may be rather complicated and even fractal, with the form of this relation being not usually found in most cases, that seems to be very important if it is used for secure communication.

To detect the GS regime the conditional Lyapunov exponent computation [37], the nearest neighbor [38] and auxiliary system methods [39] are frequently used. At the same time, only the last of them can be easily realized in practice. According to this method the behavior of the response system $\mathbf{u}(t)$ is considered together with the auxiliary system $\mathbf{v}(t)$ one. The auxiliary system is equivalent to the response one by the control parameter values, but starts with other initial conditions belonging to the same basin of chaotic attractor (if there is the multistability in the system). In practice it means the small distinctions in the initial conditions that are realized automatically because of the presence of fluctuations in the constructive elements of generators. If GS takes place, the system states $\mathbf{u}(t)$ and $\mathbf{v}(t)$ become identical after the transient is finished due to the existence of the relations $\mathbf{u}(t) = \mathbf{F}[\mathbf{x}(t)]$ and $\mathbf{v}(t) = \mathbf{F}[\mathbf{x}(t)]$. Thus, the coincidence of the state vectors of the response and the auxiliary systems $\mathbf{v}(t) \equiv \mathbf{u}(t)$ is considered as a criterion of the GS regime presence.

Except for the complicated character of the functional relation between the drive and response system states the GS regime has several other advantages in comparison with the other types of chaotic synchronization usually used for the secure information transmission (e.g., the complete synchronization one). First, this regime can be observed in the nonidentical and even different dynamical systems (including the systems with the different dimension of the phase space), that makes possible transmitting and receiving generators to be nonidentical (see Sections 2 and 5 for detail). Second, the location of the boundary of the GS regime onset on the "parameter mismatch – coupling strength" plane differs radically from the other synchronization types. In particular, there are known examples of unidirectionally coupled dynamical systems for which the coupling strength corresponding to the onset of the GS regime in the case of the small parameter mismatch is twice as much as for the same oscillators with parameters detuned sufficiently [40,41]. This peculiarity allows to provide the appearance and destruction of the synchronous regime at small modulation of the control parameter value that ensures the effective parameter modulation at the information transmission. Third, the noise is known to do not affect on the threshold of the GS regime onset, i.e. the GS regime appears in unidirectionally coupled dynamical systems in the absence and presence of noise for the same values of the coupling parameter strength [42]. As a consequence, noise may be used to provide the additional masking of the information signal. Indeed, this regime has many similarities with the noise-induced synchronization regime both in the mechanisms of the synchronous regime arising and methods for its detection [43].

All arguments mentioned above results in the conclusion that GS can be effectively used for secure information transmission.

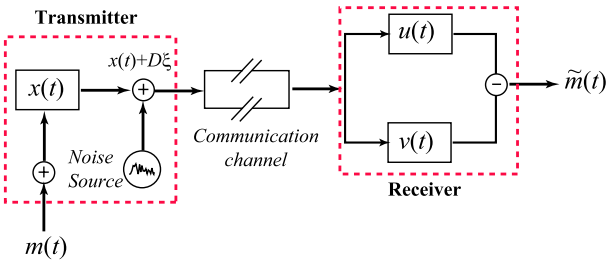

Fig. 1. (Color online.) The scheme for secure information transmission based on GS. Here $m(t)$ is a binary information signal, $x(t)$ is a vector-state of the transmitting generator, $u(t)$ and $v(t)$ are of the receiving one, respectively; $\tilde{m}(t)$ is a recovered signal.

2. A method for secure information transmission

The scheme for secure information transmission based on the GS phenomenon is shown in Fig. 1. Information signal $m(t)$ is encoded in the form of a binary code. One or more control parameters of the chaos generator are modulated slightly by the information binary signal in such a way that the characteristics of the chaotic signal (i.e., its amplitude and frequency both in time realization and power spectrum) are not changed noticeably. To provide the additional masking of the information signal as well as the variation of the characteristics of the transmitted signal the source of noise is used.

The obtained signal is transmitted through the communication channel (where the noise is supposed to be also observed) to the receiver located on the other side of the communication channel. It represents two identical chaos generators capable to be (or not to be) in the GS regime with the transmitting one. The principle of operation of the receiver is based on the GS regime detection by means of the auxiliary system method [39]. At the output of the receiver the transmitted signal passes on the subtractor and the recovered signal $\tilde{m}(t)$ is detected.

The character of modulation of the control parameters of the transmitting generator should be chosen in such a way that depending on the transmitting binary bit "0"/"1" the existence or nonexistence of the GS regime between the transmitter and receiver chaos generators would be observed. In order the variation of the characteristics of the transmitted signal remains unnoticeable for the non-authorized third party, the location of the GS boundary on the "control parameter mistuning – coupling parameter" plane must have the peculiarity discussed in Section 1, i.e. at the small variation of the control parameter the critical coupling parameter value corresponding to the threshold of the GS regime onset must change sharply. Then, if the GS regime is chosen to take place when binary bit "0" is transmitted, due to the existence of the functional relation between the chaotic system states both generators of the receiver would demonstrate identical oscillations. Therefore, upon passing the subtractor the absence of chaotic oscillations, i.e. the binary bit "0", would be observed. On the contrary, when the binary bit "1" is transmitted the GS regime does not take place. Thus, the oscillations of the receiver generators in this case would be non-identical. Upon passing the subtractor the chaotic oscillations of non-zero amplitude, i.e. the binary bit "1", would be detected.

It should be noted, that the particularity of the boundary of the GS regime mentioned above provides interchange of regions with synchronous and asynchronous behavior on the receiving side of the communication channel depending on the transmitting binary bit at negligible changes of the transmitting signal characteristics. Furthermore, due to the presence of the noise source these changes become completely unnotice-

able, especially in the time representation. That leaves non-authorized third party no possibility to decode the message signal by the one transmitting through the communication channel.

3. Numerical simulation of the proposed method

The efficiency of the proposed method can be verified with the following numerical example. Transmitting and receiving generators are chosen to be unidirectionally coupled Rössler systems. Such choice is connected with the facts that (i) Rössler system is studied in detail (including in the view of GS, see e.g. [40,44,35,41]), (ii) the location of the GS boundary fulfills the requirements given in Sections 1–2 (see also [41]), (iii) it is possible to construct electronic generator which dynamics is described by such equations [45].

The transmitting generator is given by:

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

where $\mathbf{x}(t) = (x_1, x_2, x_3)^T$ is its vector-state, $a = 0.15$, $p = 0.2$ and $c = 10$ are the control parameter values, ω_x defines the natural frequency of the system oscillations.

The control parameter ω_x is modulated by the message binary signal in the following way. If in the given time interval the binary bit "1" is transmitted, then the control parameter $\omega_x = 0.91$ in that time internal. At transmission of the binary bit "0" parameter ω_x is chosen randomly in the range $[0.9; 0.9099]$ providing the relative maximal value of the ω_x-parameter mismatch to be less that 1.1%. Such a choice of the control parameter ω_x is caused by the character of the GS boundary location studied in [41]. It provides slight modulation of characteristics of the transmitting signal both in time and frequency representations. In fact, we can modulate this parameter quite arbitrary and even use modulation of any or several parameters, but the key condition in this case is the interchange of regions with the asynchronous dynamics and the GS regime in the time series of the transmitted signal.

The receiver consists of two identical chaos generators each of which is described by the following system:

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

Here $\mathbf{u}(t) = (u_1, u_2, u_3)^T$ is the vector-state of the first receiver generator. Let $\mathbf{v}(t) = (v_1, v_2, v_3)^T$, also satisfying (2), be the vector-state of the second generator (see Fig. 1). Control parameters a, p and c are selected identical to the transmitter generator ones. The control parameter $\omega_u = 0.95$ characterizing the natural frequency of the receiver generators is chosen to be fixed for all time.

Signal from the transmitting generator after the summing with the noise signal produced by the noise source (see Fig. 1) passes through the communication channel. In our model it is realized by the coupling between the transmitting and receiving generators, i.e. by adding the component $\varepsilon(s(t) - u_1)$ in the first equation of (2). Here $s(t) = x_1 + D\xi$ is the so-called signal of the communication channel.[1] The term $D\xi$ simulates the noise both appeared in the communication channel and produced by the noise source.

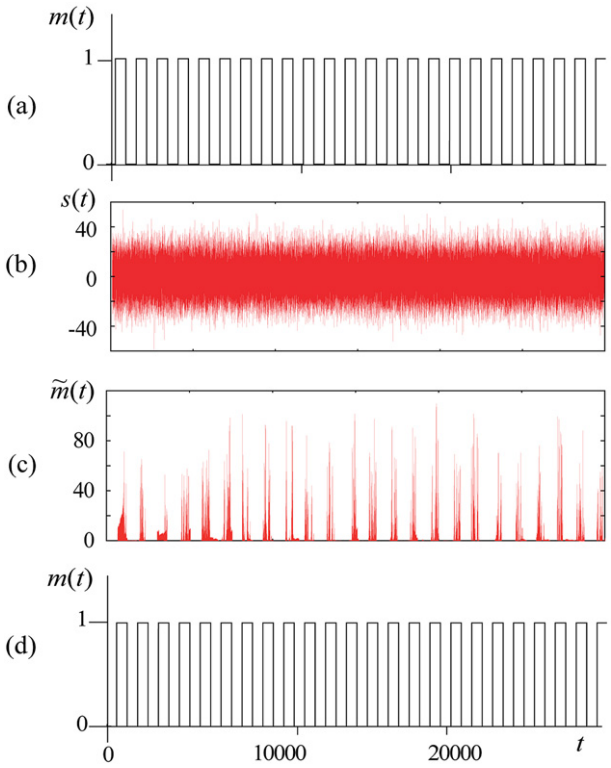

Fig. 2. (Color online.) (a) Transmitted message signal $m(t)$ represented by the sequence of the binary bits "0"/"1", (b) the signal $s(t)$ transmitted through the communication channel, (c) recovered signal $\tilde{m}(t) = (u_1 - v_1)^2$ and (d) the signal recovered by low-pass filtering and thresholding for value of the noise amplitude $D = 10$.

Here ξ is the stochastic Gaussian process which is described by the following probability distribution:

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

where $\xi_0 = 0$ and $\sigma = 1.0$ are the mean value and variance.[2] Parameter D defines the total intensity of the noise.

The coupling strength between the transmitter and receiver generators is characterized by the parameter ε. It is chosen to be equal to $\varepsilon = 0.14$. In that case, in the absence of the noise ($D = 0$) the GS regime in (1)–(2) is known to take place if $\omega_x < 0.91$ or $\omega_x > 0.97$, whereas for $\omega_x \in [0.91; 0.97]$ GS is not observed (see [41] for detail).

The subtractor (see Fig. 1) realizes operation $(u_1 - v_1)^2$. Then upon passing it due to the auxiliary system method the absence of oscillations for $\omega_x \in [0.9; 0.9099]$ and the presence of chaotic oscillations for $\omega_x = 0.91$ should be observed. The recovered signal $\tilde{m}(t)$ would represent the sequence of regions with the different behavior.

For the demonstrating purposes a simple sequence of the binary bits "0"/"1" presented in Fig. 2a, is chosen to be a message signal $m(t)$. To integrate stochastic equation (2) we have used Euler method with time discretization step $\Delta t = 0.0001$. It should be noted, that the use of Euler method is not principal. In particular, the similar results have also been obtained by us with the four order Runge–Kutta method adapted for the stochastic differential equations [46].

[1] It should be noted that the signal transmitting through the communication channel comes to the receiver generators with certain delay. But due to unidirectional coupling between the transmitting and receiving generators this delay does not matter.

[2] It is important to note that the character of the distribution of the random variable ξ does not matter and the similar results have been obtained both for uniform distribution of the probability density $p(\xi)$ and Gaussian distribution with different values of the mean value and variance.

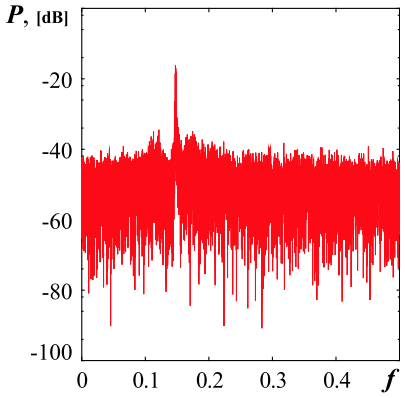

Fig. 3. (Color online.) Power spectrum of signal $s(t)$ transmitting through the communication channel for the value of the noise amplitude $D = 10$. One can easily see only one narrow spectral component in it. That makes decoding information signal difficult without full information about characteristics of the receiver.

Figs. 2b–d illustrate the operation of the scheme in the presence of noise. We have chosen the noise intensity to be great enough, e.g. $D = 10$. In Fig. 2b the signal transmitting through the communication channel is shown. One can easily see that modulation of the parameter ω_x does not change the characteristics of the transmitting signal noticeably. Furthermore, the noise of the great intensity still more distorts the transmitting signal, first of all increasing its amplitude. Power spectrum of such signal contains only one very narrow distinct spectral component (see Fig. 3), with it being become almost indistinguishable with further increasing of the noise intensity. In this case the non-authorized third party has no possibility to decode the information signal without a full information about characteristics of the receiver generators. In particular, our calculations show that application of the windowed Fourier transform or continuous wavelet transform [47] does not permit to detect useful information from the transmitted signal. Fig. 2c shows the recovered signal $\tilde{m}(t) = (u_1 - v_1)^2$. The message signal is seen to be easily recovered by the low-pass filtering and the thresholding the signal $\tilde{m}(t)$. It is shown in Fig. 2d.

Other principal question connected with the secure communication scheme operation is the rate of the information transmission. As we have discussed in the Introduction, the rate of the proposed method as well as other ones (transmitting digital information) based on chaotic synchronization due to the presence of the transient processes in switching is a low one. To illustrate this fact numerically we estimate the rate of the information sending for our scheme. It is clearly seen from Fig. 2 that for a time of 10 000 units 18 bits of information have been transmitted, i.e. the rate of the proposed method is $1.8 \cdot 10^{-3}$ bits/unit of time.

The analogous results could be obtained for different values of the noise intensity till $D = 400$. Moreover, the recovered signals $\tilde{m}(t)$ look qualitatively identical for different D, i.e. the noise do not destruct the GS regime. In this case one can say about the remarkable stability of our communication scheme to noise despite of the fact that the stability of all schemes proposed early [2,48,14,49,25,50] is limited. At that, the rate of the information sending would be the same low as for other schemes transmitting digital information on the basis of chaotic synchronization.

4. Stability of secure communication schemes to noise

As it was mentioned in Introduction, we assume that the stability of communication schemes to noise is one of the most important features of secure communication schemes. To quantify the degree of their stability the quantitative characteristics of their efficiency in the presence of noise should be introduced. For digital secure communication schemes such characteristics is an average energy of chaotic radio pulse per transmitted information bit E_b related to the noise spectral density N_0, up to which the secure communication scheme remains efficient [51]. The energy per bit is described by:

$$E_b = \mathrm{P}_{\mathrm{sign}} T, \tag{4}$$

where $\mathrm{P}_{\mathrm{sign}}$ is the power of transmitted signal (without noise), T is a time spent for transmission of one bit of information. The noise spectral density is defined as:

$$N_0 = \frac{\mathrm{P}_{\mathrm{noise}}}{B}, \tag{5}$$

where $\mathrm{P}_{\mathrm{noise}}$ is a power of noise in the communication channel, B is the bandwidth of the channel.

The power of the signal (independently of the fact whether it is deterministic or stochastic) has been computed by its time realization. In our calculations the channel bandwidth has been chosen to be $B = f_2 - f_1 = 0.2$, where $f_1 = 0.05$, $f_2 = 0.25$ are its boundary values.

To compare the effectiveness of our communication scheme in the presence of noise with the several other ones we have estimated the value of E_b/N_0, up to which secure communication scheme remains efficient, for our scheme and a series of another schemes proposed in earlier publications [2,48,14,49,25,50]. Certainly, we could not consider all schemes known at present but we have tried to choose schemes most close to our one and touch upon all well-known communication schemes which have already become classical, i.e. chaotic masking, chaotic shift keying, nonlinear mixing and others. In all cases the unidirectionally coupled Rössler systems with the control parameter values being closed to the values given in Section 3 have been chosen to be a transmitter and receiver.

Table 1
The values of an average energy of chaotic radio pulse per transmitted information bit related to the noise spectral density (E_b/N_0, [dB]) corresponding to the cases when there are no possibility to recover the information signal.

No.	Scheme	Ref.	E_b/N_0, [dB]
1	Chaotic masking	[2]	56.48
2	Chaotic shift keying	[48]	30.76
3	Nonlinear mixing	[14]	64.99
4	Chaotic parameter modulation	[49]	30.76
5	GS scheme	[25]	23.66
6	Scheme based on CS and GS	[25]	39.52
7	Scheme with compound signal	[50]	39.24
8	Our scheme		−10.01

The E_b/N_0 values corresponding to the cases when there are no possibility to recover the information signal as well as the names of schemes and references to the papers, where they are described, are shown in Table 1. It is clearly seen that all considered schemes become fully inoperative for the positive values of E_b/N_0, i.e. for the noise power less than the power of signal transmitted through the communication channel. The radically different situation takes place when our scheme is considered. Our scheme remains efficient until E_b/N_0 is less than zero (see Table 1). In the other words, our scheme possesses a remarkable stability to noise. Even if the noise intensity considerably exceeds the transmitting signal one, our scheme is capable of working.

To explain such behavior of our communication scheme we should refer to the following discussions. As we have already mentioned in Section 1, the GS regime on the basis of which our communication scheme has been proposed, has many similarities with the noise-induced synchronization one [43], i.e. we can achieve GS both by the deterministic and stochastic signal influence. Due to the fact that both transmitter generators have been affected by the

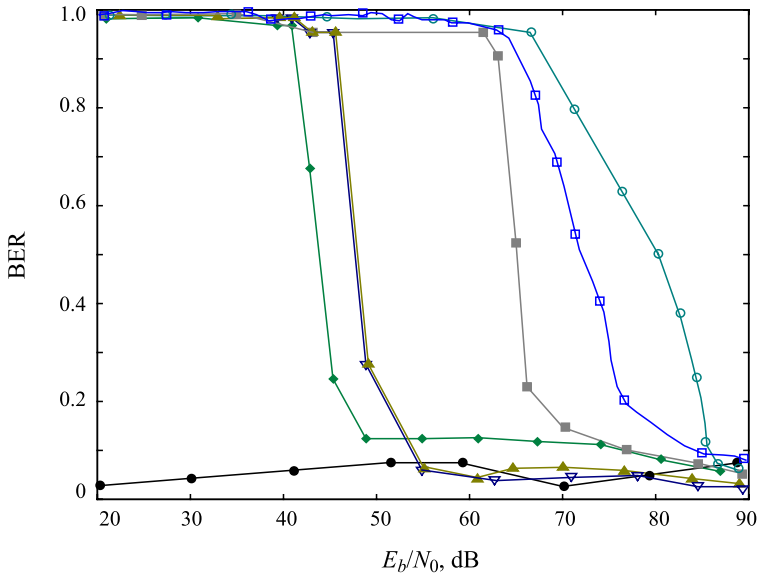

Fig. 4. (Color online.) Dependence of the bit error rate (BER) on the average energy of chaotic radio pulse per transmitted information bit related to the noise spectral density (E_b/N_0) for different secure communication schemes, i.e. ○ – chaotic masking, ◆ – chaotic switching (chaotic parameter modulation), ■ – nonlinear mixing, ▲ – scheme on the basis of GS described in [25], △ – scheme on the basis of GS and CS described in [25], □ – scheme with compound signal [50], ● – our secure communication scheme.

influence of the same signal, the character of signal (is it deterministic or stochastic one) is not crucial. The key role belongs to the presence of the main spectral components which are almost undistinguishable (see Fig. 3). When intensity of noise is such a great one that spectral components disappear, our method become failed because of the noise-induced synchronization regime realization. Therefore our scheme possess a remarkable stability to noise.

A radically different situation takes place in the other schemes for secure communication mentioned above. All of them demands the presence of identical generators in the different sides of the communication channel, at that in all of them the recovered signal is obtained as a difference between signal in the communication channel and response of the receiver generator on it. It is clear that in the case of the influence of stochastic (random) signal on the deterministic receiver generator the obtainment of the same stochastic signal is impossible. Therefore for such secure communication schemes their efficiency in the presence of noise is limited by the amount of noise which the transmitter generator itself could support. In the case of the use of Rössler generators (with control parameter values closed to the last one presented in Section 3) in the transmitter and receiver such amount in accordance with analogue of Shannon theorem for digital signals [51] is $E_b/N_0 = -1.46$ dB. It is clearly seen that our numerical estimations are in a full agreement with the theoretical prediction results.

Correctness of the arguments mentioned above could be also confirmed by the dependence of the bit error rate (BER) [52] on the E_b/N_0 value for different communication schemes mentioned above. Such dependencies are shown in Fig. 4. At computation of the bit error rate the threshold value allowing to detect the original information binary signal from the signal $\tilde{m}(t)$ has been chosen to be fixed independently on the noise intensity affected on the transmitting generator whereas it has been changed for the characteristics presented in the Table 1. At the same time, it is clearly seen that for different secure communication schemes (except the our one) BER becomes equal to 1 quickly, whereas for our scheme it is closed to 0 independently on the noise intensity. Such results are in a good agreement with the last one presented above in Table 1.

It should be noted, that the change of the control parameter values and equations of generators could result in the variation of the quantitative values of the average energy per bit related to the noise spectral density, but the order of these magnitudes, relation between them and the qualitative behavior of BER vs E_b/N_0 would always remain the same.

5. The other advantages of the proposed method

Except of the problem connecting with the influence of noise in the communication channel, all schemes considered in Section 4 have some other disadvantages and difficulties for practical purposes. The most part of schemes (e.g., schemes 1–4 in Table 1) uses the complete synchronization of chaotic oscillators [53,54] that, first of all, requires an identity of the transmitting and receiving generators being located in the different sides of the communication channel. It is a very big conceptual problem, especially for a long time of operation of the devices. Second, in some cases the parameters used in the transmitter can be estimated from the transmitting signal, and, therefore, the information signal can be extracted from it [55].

The scheme proposed in [25] (system 5 in Table 1), as well as our one, is based on the generalized synchronization. Despite of the fact that its stability to noise is greater than in several other schemes (e.g., in schemes 1 and 3 from Table 1), the problem of the identity of the generators on both sides of the communication channel still remain unsolved. Furthermore, such scheme demands realization of the complementary communication channel that produces additional problems for practical realization.

In schemes 6 and 7 (see Table 1) both types of the synchronous chaotic system behavior mentioned above, i.e., the generalized and complete synchronization, are used for the information transmission. In the first case both of them are touched in this process directly whereas in the second one generalized synchronization is used for the creation of the compound signal to be transmitted through the communication channel. Certainly, such schemes are supposed to be more secure in comparison with the other schemes mentioned above, but they demand the presence of additional identical generators on different sides of the communication channel and, in some cases, realization of the complementary communication channel. Therefore, the practical realization of these

Table 2
Maximal value of ω_u parameter mismatch (PM, %) and level of nonlinear distortions (ND, dB) in the communication channel for which secure communication schemes remain efficient.

No.	Scheme	Ref.	PM	ND
1	Chaotic masking	[2]	0.30	1.03
2	Chaotic shift keying	[48]	2.00	23.3
3	Nonlinear mixing	[14]	0.30	0.26
4	Chaotic parameter modulation	[49]	2.00	23.3
5	GS scheme	[25]	1.00	7.75
6	Scheme based on CS and GS	[25]	0.50	4.83
7	Scheme with compound signal	[50]	0.20	2.63
8	Our scheme		2.00	27.2

schemes is a very big problem. Moreover, the stability to noise, especially, for the scheme 7, is a very low (see Table 1).

Contrary to all schemes mentioned above, our one does not require an identity of chaotic generators on both sides of the communication channel, and, therefore, it is a simple enough for the practical realization.

Other important characteristic of the secure communication schemes is their robustness to the parameter mismatch (PM). As it was mentioned above, almost all known communication schemes demand the presence of two or more identical generators on one or different sides of the communication channel. Due to the problems connected with the technical realization of such schemes the influence of the control parameter mismatch of generators, that have to be identical firstly, is a topical problem of the secure communication. To realize the parameter mismatch in numerical simulation we should replace any control parameter A by $A(1 \pm \eta)$ in one of identical generators. Then η would be the value of the parameter mismatch (PM). We have estimated the relative values of the ω_u parameter mismatch up to which the considered schemes remain efficient. Since the choice of sign of the parameter mismatch does not matter, we have used the sign "+" in our calculations. The obtained results are presented in Table 2 (column 4) for all schemes considered above. It is easy to see, that in that case our scheme has analogous. For example, the chaotic switching and chaotic parameter modulation schemes (i.e., schemes 2 and 4 in Tables 1 and 2, respectively) are capable of working if control parameter values are detuned up to 2%. The degree of robustness of our communication scheme to the parameter mismatch is the same. But in our scheme such generators are located on the one side of the communication channel, so their adjustment to identical state can be easily realized.

Except the presence of noise, transmitting signal can undergo the changes of another character in the communication channel. One of such changes is the nonlinear distortions of the signal. Transmitting signal $x(t)$ is most frequently supposed to have a transformations in the form of cubic nonlinearity [31]. So, after the transmission through the communication channel the signal $y(t) = x(t)(1 - \alpha x^2(t))$, where α is a small enough, would pass at the input of the receiver.

To estimate the influence of nonlinear distortions in the communication channel the following quantitative characteristic has been introduced:

$$\mathrm{ND} = 10 \lg \frac{P_x}{P_y} \ [\mathrm{dB}]. \tag{6}$$

Here P_x and P_y are the powers of signals $x(t)$ and $y(t)$, respectively, computed by the time realization of the signal. In that way

$$P_x = \int_0^T x^2(t)\,dt, \quad P_y = \int_0^T y^2(t)\,dt, \tag{7}$$

where T is the time of the signal transmission. The quantity mentioned above characterizes the maximal level of nonlinear distortions for which secure communication scheme remains efficient. The more there would be this value, the more the signal would be distorted, therefore the more would be the maximal level of the nonlinear distortions up to which the methods for secure information transmission would still remain efficient.

The results of the influence of the nonlinear distortions in the communication channel on the efficiency of the secure communication schemes mentioned above are shown in Table 2 (column 5). It is easy to see that our scheme proposed in Sections 2 and 3 exceeds all considered analogues according to this characteristic. The maximal level of the nonlinear distortions for it is equal to ND = 27.2 dB. The most close characteristics correspond again to the chaotic switching and chaotic parameter modulation schemes (schemes 2 and 4 in Table 2). At the same time, they are found to be rather less than the last one for our secure communication scheme. Furthermore, both schemes mentioned above possess the limited stability to noise whereas the stability of our scheme is almost unrestricted for the real limits.

It is necessary to emphasize that the quantitative characteristics of the efficiency of the secure communication schemes presented in Tables 1 and 2 are obtained for unidirectionally coupled Rössler systems with control parameters values equal or closed to the last ones described in Section 3 and Gaussian distribution of noise in the communication channel. The change of parameters and equations of generators and characteristics of the noise source could result in variation of the quantitative values of all considered characteristics, but their order as well as the relation between them would always remain the same. In particular, the similar results have been obtained by us for Chua [56] and Rulkov [57] generators used both the transmitter and receiver and different kinds of the noise distribution in the communication channel.

6. Conclusions

In conclusion, we have developed a new method for secure information transmission possessing a remarkable stability to noise. It enables to use additional source of noise in our communication scheme providing a big distortions of the transmitted signal, with decoding the information signal by non-authorized third party being become difficult. Moreover, it does not require an identity of the chaotic generators on both sides of the communication channel because of using the generalized synchronization instead of the complete one. Therefore, it is simple enough for the practical realization. Instead, the additional receiver generator is used for the possibility of the generalized synchronization regime detection. To demonstrate the principal advantages of our method in comparison with the early developed ones the signal to noise ratio and influence of the control parameter mismatch of firstly identical generators and nonlinear distortions in the communication channel are estimated numerically both for our scheme and for the series of the other ones.

Acknowledgements

We thank Dr. Svetlana V. Eremina for the English language support. We are grateful to the Referees of our Letter for the useful comments and remarks. This work has been supported by Russian Foundation for Basic Research (projects 08-02-00102) and Federal special-purpose programme "Scientific and educational personnel of innovation Russia".

References

[1] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, A. Shang, Int. J. Bifur. Chaos 2 (4) (1992) 973.
[2] M.K. Cuomo, A.V. Oppenheim, S.H. Strogatz, IEEE Trans. Circuits Systems 40 (10) (1993) 626.
[3] L. Kocarev, U. Parlitz, Phys. Rev. Lett. 74 (25) (1995) 5028.
[4] J.H. Peng, E.J. Ding, M. Ding, W. Yang, Phys. Rev. Lett. 76 (6) (1996) 904.
[5] V.S. Anishchenko, A.N. Pavlov, Phys. Rev. E 57 (1998) 2455.
[6] M.C. Eguia, M.I. Rabinovich, H.D.I. Abarbanel, Phys. Rev. E 62 (5) (2000) 7111.
[7] I. Fischer, Y. Liu, P. Davis, Phys. Rev. A 62 (2000) 011801(R).
[8] N.F. Rulkov, M.A. Vorontsov, L. Illing, Phys. Rev. Lett. 89 (27) (2002) 277905.
[9] Z.L. Yuan, A.J. Shields, Phys. Rev. Lett. 94 (2005) 048901.
[10] Q.S. Li, Y. Liu, Phys. Rev. E 73 (2006) 016218.
[11] A.L. Fradkov, B. Andrievsky, R.J. Evans, Phys. Rev. E 73 (2006) 066209.
[12] P.B. Larsen, L.M. Earley, R.M. Wheat, J.H. Booske, Secure chaos communications using driven traveling wave tube amplifiers with delayed feedback, in: Proceedings of Vacuum Electronics Conference, 2006, held Jointly with 2006 IEEE International Vacuum Electron Sources, IEEE International, 2006, pp. 521–522.
[13] A.S. Dmitriev, B.Y. Kyarginsky, A.I. Panas, S.O. Starkov, Int. J. Bifur. Chaos 13 (6) (2003) 1495.
[14] A.S. Dmitriev, A.I. Panas, S.O. Starkov, Int. J. Bifur. Chaos 5 (4) (1995) 1249.
[15] R. Roy, Nature 438 (2005) 298.
[16] H. Jaeger, H. Haas, Science 304 (2008) 78.
[17] A.S. Dmitriev, M. Hasler, A.I. Panas, K.V. Zakharchenko, Complex Systems 6 (1) (2003) 1.
[18] B. Cessac, J.A. Sepulchre, Chaos 16 (2006) 013104.
[19] G.K. Rohde, J.M. Nichols, F. Bucholtz, Chaos 18 (2008) 013114.
[20] D. Materassi, M. Basso, Int. J. Bifur. Chaos 18 (2) (2008) 567.
[21] K. Murali, M. Lakshmanan, Phys. Rev. E 48 (3) (1993) R1624.
[22] S. Boccaletti, A. Farini, F.T. Arecchi, Phys. Rev. E 55 (5) (1997) 4979.
[23] T.L. Carroll, G.A. Johnson, Phys. Rev. E 57 (2) (1998) 1555.
[24] A.S. Dmitriev, A.I. Panas, L.V. Kuzmin, Complex Systems 2 (3) (1999) 91.
[25] J. Terry, G. VanWiggeren, Chaos Solitons Fractals 12 (2001) 145.
[26] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.
[27] W. Xiang-Jun, Chaos 16 (2006) 043118.
[28] C. Cruz-Hernandez, N. Romero-Haros, Communications in Nonlinear Science and Numerical Simulation 13 (2008) 645.
[29] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. Mirasso, L. Pesquera, K. Shore, Nature 438 (7066) (2005) 343.
[30] S. Li, G. Alvarez, G. Chen, X. Mou, Chaos 15 (1) (2005) 013703.
[31] A.S. Dmitriev, A.I. Panas, Dynamic Chaos: Novel Type of Information Carrier for Communication Systems, Fizmatlit, Moscow, 2002.
[32] T. Yang, Int. J. Comput. Cognition 2 (2) (2004) 81.
[33] H. JinFeng, G. JingBo, Chaos 18 (2008) 013121.
[34] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring, H.D.I. Abarbanel, Phys. Rev. E 51 (2) (1995) 980.
[35] A.E. Hramov, A.A. Koronovskii, Phys. Rev. E 71 (6) (2005) 067201.
[36] S. Boccaletti, J. Kurths, G.V. Osipov, D.L. Valladares, C.T. Zhou, Phys. Reports 366 (2002) 1.
[37] K. Pyragas, Phys. Rev. E 54 (5) (1996) R4508.
[38] L.M. Pecora, T.L. Carroll, J.F. Heagy, Phys. Rev. E 52 (4) (1995) 3420.
[39] H.D.I. Abarbanel, N.F. Rulkov, M.M. Sushchik, Phys. Rev. E 53 (5) (1996) 4528.
[40] Z. Zheng, G. Hu, Phys. Rev. E 62 (6) (2000) 7882.
[41] A.E. Hramov, A.A. Koronovskii, O.I. Moskalenko, Europhys. Lett. 72 (6) (2005) 901.
[42] A.A. Koronovskii, P.V. Popov, A.E. Hramov, JETP 103 (4) (2006) 654.
[43] A.E. Hramov, A.A. Koronovskii, O.I. Moskalenko, Phys. Lett. A 354 (5–6) (2006) 423.
[44] A.E. Hramov, A.A. Koronovskii, Europhys. Lett. 70 (2) (2005) 169.
[45] R. Rico-Martinez, K.E. Kreischer, G. Flätgen, J.S. Anderson, I.G. Kevrekidis, Physica D 176 (2003) 1.
[46] N.N. Nikitin, S.V. Pervachev, V.D. Razevig, Automation and Telemechanics 4 (2008) 133 (in Russian).
[47] A.A. Koronovskii, A.E. Hramov, Continuous Wavelet Analysis and its Applications, Fizmatlit, Moscow, 2003 (in Russian).
[48] H. Dedieu, M.P. Kennedy, M. Hasler, IEEE Trans. Circuits Systems I 40 (1993) 634.
[49] T. Yang, L.O. Chua, IEEE Trans. Circuits Systems I 43 (1996) 817.
[50] K. Murali, M. Lakshmanan, Phys. Lett. A 241 (1998) 303.
[51] B. Sklar, Digital Communication. Fundamentals and Application, Prentice Hall PTR, New Jersey, 2001.
[52] A. Abel, W. Schwarz, Proc. IEEE 90 (5) (2002) 691.
[53] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (8) (1990) 821.
[54] L.M. Pecora, T.L. Carroll, Phys. Rev. A 44 (4) (1991) 2374.
[55] V.I. Ponomarenko, M.D. Prokhorov, Phys. Rev. E 66 (2) (2002) 026215.
[56] L.O. Chua, M. Komuro, T. Matsumoto, IEEE Trans. Circuits Systems 33 (11) (1986) 1073.
[57] N.F. Rulkov, Chaos 6 (1996) 262.