International Journal of Bifurcation and Chaos, Vol. 25, No. 10 (2015) 1550134 (10 pages)

DOI: 10.1142/S0218127415501345

An Experimental Communication Scheme Based on Chaotic Time-Delay System with Switched Delay

A. S. Karavaev*, D. D. Kulminskiy†, V. I. Ponomarenko‡
and M. D. Prokhorov§
Saratov Branch of Kotel'nikov Institute of Radio Engineering and Electronics of Russian Academy of Sciences, Zelyonaya Street, 38, Saratov 410019, Russia
**karavaevas@gmail.com*
†*kulminskydd@gmail.com*
‡*ponomarenkovi@gmail.com*
§*mdprokhorov@yandex.ru*

Received December 24, 2014; Revised March 20, 2015

We develop an experimental secure communication system with chaotic switching. The proposed scheme is based on time-delayed feedback oscillator with switching of chaotic regimes. The scheme shows high tolerance to external noise and amplitude distortions of the signal in a communication channel.

Keywords: Secure communication scheme; chaotic synchronization; time-delay systems.

1. Introduction

The discovery of the possibility to synchronize two coupled identical chaotic systems [Pecora & Carroll, 1990] stimulated interest in using chaotic signals for confidential transmission of information. Different approaches for the transmission of information signals using chaotic dynamics have been proposed, for example, chaotic masking [Kocarev *et al.*, 1992; Cuomo & Oppenheim, 1993], chaotic switching or chaos shift keying [Parlitz *et al.*, 1992; Dedieu *et al.*, 1993], chaotic modulation [Halle *et al.*, 1993], nonlinear mixing [Volkovskii & Rulkov, 1993; Dmitriev *et al.*, 1995; Dmitriev & Panas, 2002], and others. Based on these approaches, a variety of chaotic communication schemes has been proposed [Van Wiggeren & Roy, 1998; Dmitriev & Panas, 2002; Tao, 2004; Argyris *et al.*, 2005; Koronovskii *et al.*, 2009; Wang *et al.*, 2012; Stankovski *et al.*, 2014]. However, many chaotic communication schemes are not as secure as expected and can be successfully unmasked [Pérez & Cerdeira, 1995; Short, 1997; Zhou & Chen, 1997; Yang *et al.*, 1998; Ponomarenko & Prokhorov, 2002; Alvarez & Li, 2006; Millerioux, 2013]. To improve the security of data transmission, it has been proposed to employ time-delay systems, demonstrating chaotic dynamics of a very high dimension, in private communication [Pyragas, 1998; Kye *et al.*, 2005; Prokhorov & Ponomarenko, 2008; Kye, 2012; Ponomarenko *et al.*, 2012; Ponomarenko *et al.*, 2013]. In particular, special attention has been paid to using optical ring systems with time-delayed feedback for chaotic communication [Goedgebuer *et al.*, 1998; Van Wiggeren & Roy, 1998; García-Ojalvo & Roy, 2001; Udaltsov *et al.*, 2001; Argyris *et al.*, 2005].

Although chaotic communication systems have a lot of merits including broadband power spectrum of chaotic signals, high rates of information

§Author for correspondence

transmission, and simple implementation, they are not devoid of drawbacks restricting their wide use in practice. The main shortcomings of communication schemes based on the employment of chaotic synchronization are their comparatively low interference immunity, low resistance to signal distortion in a communication channel, and stringent requirements imposed on the identity of parameters of transmitter and receiver [Dmitriev & Panas, 2002; Koronovskii *et al.*, 2009]. In our recent paper [Ponomarenko *et al.*, 2013], we have developed an experimental system for secure communication with nonlinear mixing of information and chaotic signals which is devoid of the above mentioned shortcomings because of the use of digital transmission line and employment of programmable microcontrollers to implement a transmitter and receiver.

An original communication scheme with chaotic switching and analog communication channel has been proposed and numerically investigated by Ponomarenko *et al.* [2012]. It possesses a high interference immunity owing to the specific configuration of the receiver. In the present paper, we modified the scheme numerically studied by Ponomarenko *et al.* [2012] and for the first time realized it in a physical experiment.

The paper is organized as follows. In Sec. 2, the proposed communication system is described. In Sec. 3, we illustrate the experimental results of operation of the proposed communication scheme and study the scheme resistance to external noise and amplitude distortions of the signal in a communication channel. Section 4 presents the results of numerical simulation of the proposed scheme. In Sec. 5, we summarize our results.

2. Communication Scheme

Recently we have proposed a secure communication scheme with switching of chaotic regimes and analog communication channel which possesses a high interference immunity [Ponomarenko *et al.*, 2012]. A block diagram of this scheme is presented in Fig. 1. In this scheme, a transmitter represents a ring system composed of two delay lines with delay times τ_1 and τ_2, a nonlinear element, and a linear low-pass filter. The information signal is the binary signal $m(t)$ representing a sequence of binary zeros and units. The signal $m(t)$ switches the delay time in the scheme in such a way that the delay time is equal to τ_1 at a transmission of binary zero and it is equal to $\tau_1 + \tau_2$ at a transmission of binary unity. In the case, where the nonlinear element provides a quadratic transformation, the transmitter is described by a first-order delay-differential equation

$$\varepsilon\dot{x}(t) = -x(t) + \lambda - (x(t - (\tau_1 + m(t)\tau_2)))^2, \qquad (1)$$

where $x(t)$ is the system state at time t, ε is the parameter that characterizes the inertial properties of the system, and λ is the parameter of nonlinearity.

A receiver is composed of two driven time-delay systems, one of which contains a delay line with delay time τ_1 and the other contains a delay line with delay time $\tau_3 = \tau_1 + \tau_2$. The parameters of filters and nonlinear elements in these two systems are identical to the corresponding values in the transmitter. A subtractor placed after the filter breaks the feedback circuit in each driven system of the receiver. The input signal for each time-delay system in the receiver is the chaotic carrier $x(t)$. These systems are described by the following equations:

$$\varepsilon\dot{y}(t) = -y(t) + \lambda - (x(t - \tau_1))^2, \qquad (2)$$

$$\varepsilon\dot{z}(t) = -z(t) + \lambda - (x(t - \tau_3))^2. \qquad (3)$$

The parameters of transmitter and receiver should be chosen so as to ensure that the synchronization with $x(t)$ at every moment of time could take place for only one of the two driven systems.

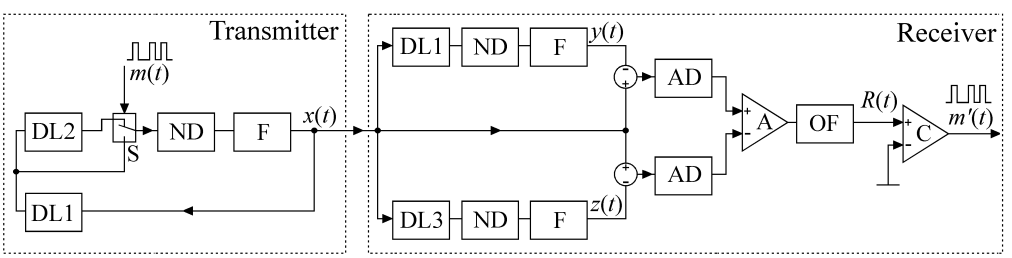

Fig. 1. Block diagram of a communication system with switched delay time: (DL1, DL2, and DL3) delay lines, (ND) nonlinear devices, (F) filters, (S) commutator, (AD) amplitude detectors, (A) differential amplifier, (OF) output filter, and (C) comparator.

When binary zero is transmitted, the output signal $y(t)$ of the first time-delay system in the receiver is synchronized in the absence of noise with the signal $x(t)$. As a result, we have $y(t) = x(t)$ and the signal at the output of subtractor in the first driven system is equal to zero. In this case, there is no synchronization between $x(t)$ and the output signal $z(t)$ of the second time-delay system in the receiver. Since $z(t) \neq x(t)$, the signal at the output of subtractor in the second driven system is not equal to zero. When binary unity is transmitted, $y(t) \neq x(t)$ and $z(t) = x(t)$. As a result, the signal at the output of subtractor in the first driven system is not equal to zero, while the signal at the output of subtractor in the second driven system is equal to zero.

However, the presence of noise in the communication channel impedes the establishment of complete synchronization between the receiver and transmitter. In this case, the signals at the outputs of subtractors in both time-delay systems in the receiver always differ from zero. This fact hampers the extraction of binary message signal. In order to increase the scheme resistance to noise, we have introduced two amplitude detectors, differential amplifier, output filter, and comparator in the receiver, Fig. 1. The output signal of each amplitude detector represents the modulus of an envelope of the input difference signal. Then, the output signals of amplitude detectors are subtracted and smoothed by a low-frequency filter, the output signal of which is $R(t)$. The comparator transforms $R(t)$ into a recovered information signal $m'(t)$, so that the output signal is binary zero for $R(t) \leq 0$ and binary unity otherwise. The signal $R(t)$ has the same sign as that in the absence of noise and, hence, the information signal can be recovered accurately.

In this paper, we modified the scheme (Fig. 1) numerically studied by Ponomarenko *et al.* [2012] and for the first time realized it in a physical experiment. A block diagram of the proposed communication system is shown in Fig. 2. All the transmitter elements are implemented in a digital form using a programmable microcontroller of the Atmel megaAVR family. To increase the speed of response one should use integer calculations in the microcontroller. For this purpose the variables and parameters of Eq. (1) were scaled as follows. For a small ε, the allowable limits of variation of the parameter λ for which system (1) has a periodic or chaotic attractor are from 0 to 2. Within this range of λ variation, the dynamical variable $x(t)$ can take values from -2 to $+2$. Let us pass to integer arithmetic and transform Eq. (1) in such a way that the dynamical variable is placed in a 16-bit memory location, whereby its integer values vary between -2^{15} and 2^{15}. It can be done by substituting variables as $X(t) = cx(t)$ and $\Lambda = c\lambda$, where $c = 2^{14}$ is a scale factor. Then, Eq. (1) takes the

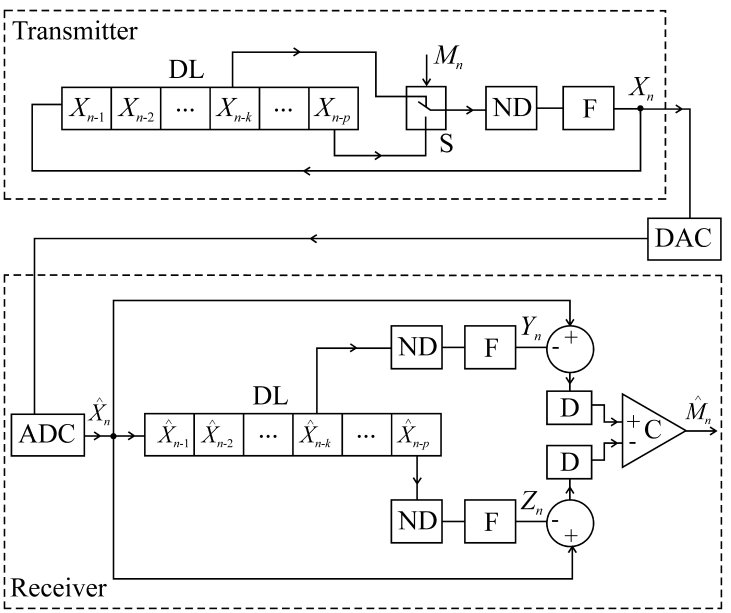

Fig. 2. Block diagram of modified communication system implemented in a digital form: (DL) delay lines, (ND) nonlinear devices, (F) filters, (S) commutator, (DAC) digital-to-analog converter, (ADC) analog-to-digital converter, (D) detectors, and (C) comparator.

following form:

$$\varepsilon\dot{X}(t) = -X(t) + \Lambda - \frac{(X(t-(\tau_1 + m(t)\tau_2)))^2}{c}. \quad (4)$$

Differential equation (4) can be reduced to a difference equation which is more convenient for program implementation on a microcontroller. At a transmission of binary zero, the transmitter is described by difference equation (5), while at a transmission of binary unity, it is described by Eq. (6):

$$X_{n+1} = aX_n + b\left(\Lambda - \frac{X_{n-k}^2}{c}\right), \quad (5)$$

$$X_{n+1} = aX_n + b\left(\Lambda - \frac{X_{n-p}^2}{c}\right), \quad (6)$$

where n is the discrete time, $a = 1-\Delta t/\varepsilon$, $b = \Delta t/\varepsilon$, Δt is the time step, and $k = \tau_1/\Delta t$ and $p = \tau_3/\Delta t$ are the discrete delay times in units of sampling time Δt.

The delay line in the transmitter has two outputs which correspond to the delay times k and p, respectively, Fig. 2. The binary information signal M_n controls a commutator that switches the delay time so that the delay time is equal to k at a transmission of binary zero and is equal to p at a transmission of binary unity. The signal X_{n-k} or X_{n-p} from the delay line output undergoes a quadratic transformation and passes through a digital low-pass first-order Butterworth filter with cutoff frequency $f_c = 1/\varepsilon$. The dynamical variable X_n from the filter output is fed to the delay line input closing the feedback loop. Simultaneously, the signal X_n is fed to the input of external digital-to-analog converter (DAC) and transmitted into a communication channel.

The receiver is implemented on another programmable microcontroller, which is identical to the one used in the transmitter. The incoming analog signal is passed through an analog-to-digital converter (ADC) integrated in the microcontroller of the receiver. A digitization frequency of ADC is set at 1 kHz ($\Delta t = 1$ ms). The signal $\hat{X}_n$ from the ADC output is fed to the input of a delay line which outputs correspond to the delay times k and p, respectively, Fig. 2. The delayed signals $\hat{X}_{n-k}$ and $\hat{X}_{n-p}$ pass through nonlinear elements and filters which are identical to those used in the transmitter. The subtractor placed after the filter breaks the feedback circuit in each of the receiver circuits described by the following equations:

$$Y_{n+1} = aY_n + b\left(\Lambda - \frac{\hat{X}_{n-k}^2}{c}\right), \quad (7)$$

$$Z_{n+1} = aZ_n + b\left(\Lambda - \frac{\hat{X}_{n-p}^2}{c}\right). \quad (8)$$

When binary zero is transmitted, the output signal Y_n of the first circuit in the receiver is synchronized in the absence of noise with the signal $\hat{X}_n$. As a result, we have $Y_n = \hat{X}_n = X_n$ and the signal at the output of subtractor in the first circuit is equal to zero. In this case, there is no synchronization between $\hat{X}_n$ and the output signal Z_n of the second circuit in the receiver. Hence, the signal at the output of subtractor in the second circuit is not equal to zero. When binary unity is transmitted, $Y_n \neq \hat{X}_n$ and $Z_n = \hat{X}_n$. As a result, the signal at the output of subtractor in the first circuit is not equal to zero, while the signal at the output of subtractor in the second circuit is equal to zero.

In the presence of noise in the communication channel, $\hat{X}_n \neq X_n$ and complete synchronization between the receiver and transmitter cannot be achieved. In this case, the signals at the outputs of subtractors in both circuits in the receiver always differ from zero. In the presence of noise, the variance of the signal at the output of subtractor in the synchronized circuit (with the same delay time as in the transmitter) is close to the variance of noise in the communication channel and the variance of the signal at the output of subtractor in the non-synchronized circuit (with the delay time different from the delay time in the transmitter) is close to the variance of chaotic carrier. Taking into account that the level of noise in the communication channel in general case is appreciably less than the level of chaotic carrier, we can extract accurately the message signal even in the case of sufficiently strong noise.

In comparison with the scheme depicted in Fig. 1, we modified the configuration of receiver. Two amplitude detectors, differential amplifier, and output filter are replaced by two elements, Fig. 2, which evaluate the variance of incoming difference signal using 100 values of this signal stored in the circular buffer array in the operative memory of microcontroller. The technical implementation of such elements in a programmable microcontroller is easier. Moreover, this modification results in the

increase of the scheme speed and tolerance to noise. The comparator disposed after detectors calculates the difference R_n between their output signals and transforms R_n into a recovered information signal $\hat{M}_n$, so that the output signal is binary zero for $R_n \leq 0$ and binary unity otherwise.

3. Experimental Results of the Scheme Operation

Let us illustrate the efficiency of the proposed communication scheme for the following values of transmitter parameters: $\lambda = 1.9$, $\Delta t/\varepsilon = 0.5$, $k = 100$, and $p = 110$. Part of the time series of the chaotic signal X_n at the transmitter output is presented in Fig. 3(a). Since the values of k and p are close to each other, the fragments of X_n time series corresponding to k and p are visually indistinguishable, so that it is difficult to determine which binary symbol (zero or unity) is transmitted.

Figure 3(b) shows a part of the time series of the transmitted binary signal M_n. Each bit is transmitted during an interval of 100 ms which corresponds to 100 steps of the discrete time n. The information signal $\hat{M}_n$ extracted at the receiver output is also shown in Fig. 3(b). One can see that the information signal is recovered accurately, but with a delay which value depends on the detector parameters.

To investigate the tolerance of the proposed scheme to noise and amplitude distortions of the signal in the communication channel we have developed a specific electronic scheme which allows us to add a noise with desired intensity formed by noise generator into the communication channel. Figure 4(a) shows the experimental dependence of bit-error rate (BER) of the recovered message on

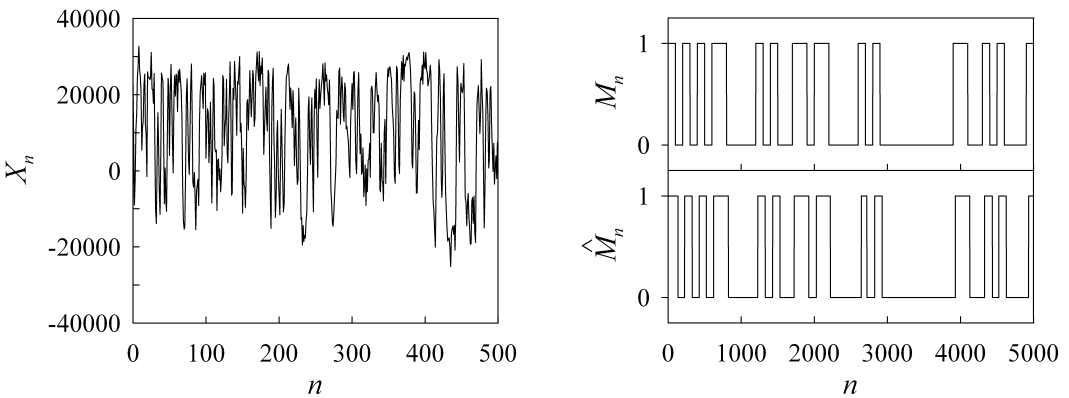

Fig. 3. (a) The time series of chaotic signal X_n and (b) the time series of the transmitted information signal M_n and the information signal $\hat{M}_n$ extracted at the receiver output.

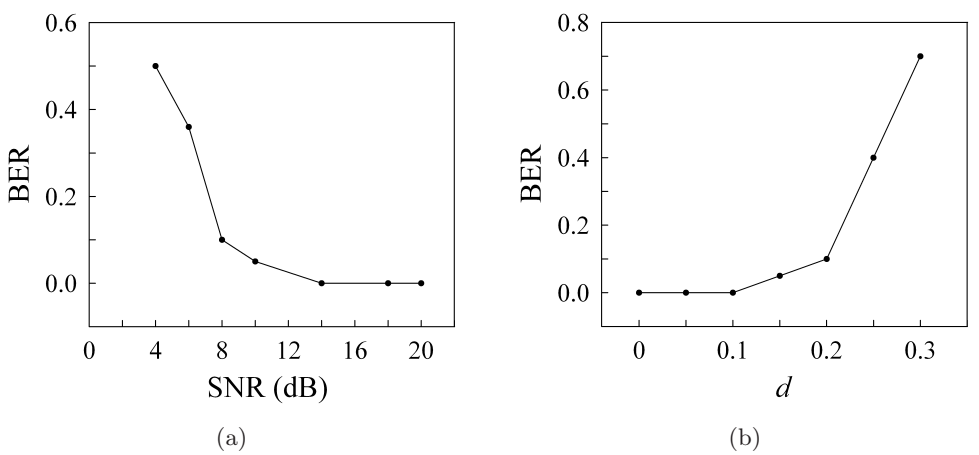

Fig. 4. (a) The experimental bit-error rate as a function of signal-to-noise ratio and (b) as a function of the signal attenuation in the communication channel. In each measuring of BER, 10^5 randomly ordered binary symbols are sent.

the signal-to-noise ratio (SNR). The signal in SNR is the chaotic signal transmitted into the communication channel and noise is an additive zero-mean Gaussian white noise filtered in the bandwidth of the chaotic carrier. For SNR ≥ 14 dB the signal $\hat{M}_n$ is recovered without errors, Fig. 4(a). Thus, the proposed system is more robust against channel noise than most of other communication systems using chaotic synchronization for the transmission of hidden information signal through analog communication channel [Dmitriev & Panas, 2002; Koronovskii *et al.*, 2009].

It should be noted that a real transmission channel always undergoes attenuation effect which may be critical for operation of chaotic communication systems. In fact, many of these systems, especially the systems with chaotic masking and nonlinear mixing, have low resistance to signal distortion in a communication channel. To investigate the resistance of our scheme to amplitude distortions of the signal in the communication channel we control the signal attenuation in the channel using the above mentioned specific electronic scheme. Figure 4(b) depicts the dependence of BER on the parameter $d = (A_t - A_r)/A_t$, where A_t and A_r are the signal amplitudes at the transmitter output and receiver input, respectively. As it can be seen from the figure, for $d \leq 0.1$ the binary information signal at the receiver output is recovered without errors. The value of $d = 0.1$ corresponds to the signal attenuation of about 1 dB. At such level of signal distortion in the communication channel, most schemes with chaotic masking and nonlinear mixing fail [Koronovskii *et al.*, 2009].

Like all other communication systems with chaotic switching, the considered system is characterized by certain limitation of the data transmission rate. This is because of transient processes that take place after every switching of the chaotic regime. After switching of the delay time in the transmitter, a certain time is required for establishing synchronization between the transmitter and one of the driven systems in the receiver. The rate of information transmission can be increased by decreasing the characteristic temporal scales of the system or decreasing the length of time interval during which each bit is transmitted. However, in the last case, the increase of BER of the message recovered in the receiver may take place.

Figure 5 shows for SNR = 8 dB and $d = 0$ the dependence of BER on the length l of the interval during which one bit is transmitted. The values of l are indicated in units of sampling time Δt. The increase of BER is observed as l decreases in the region of its small values. On the other hand, the quality of message recovery at high levels of channel noise can be improved by increasing the value of l which leads to the decrease of BER, Fig. 5. For the considered scheme based on the Atmel megaAVR microcontrollers, the value of $l = 100$ ms seems to be optimal. For smaller l values the scheme has worse resistance to noise. For greater l values, more amount of microcontroller's memory is required and the rate of information transmission decreases.

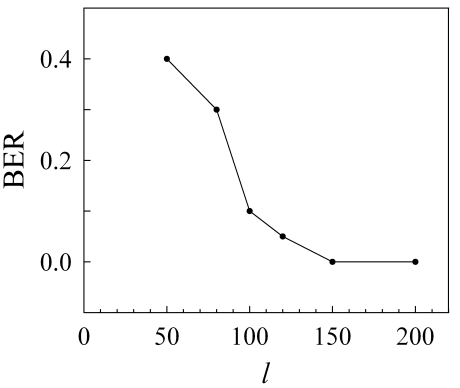

Fig. 5. The experimental bit-error rate as a function of length of time interval during which each bit is transmitted. In each measuring of BER, 10^5 randomly ordered binary symbols are sent.

It is well known that many chaotic communication schemes are not as secure as expected and can be successfully unmasked using the analysis of return maps [Pérez & Cerdeira, 1995; Zhou & Chen, 1997; Yang *et al.*, 1998], dynamical reconstruction of the chaotic transmitter from its time series [Short, 1997; Zhou & Lai, 1999; Ponomarenko & Prokhorov, 2002], and some other techniques [Alvarez & Li, 2006; Millerioux, 2013]. To test the vulnerability of the proposed communication scheme against attacks we applied the method of message extraction based on return maps [Pérez & Cerdeira, 1995].

Let $n = i_{\max}$ be the time when $\hat{X}_n$ gets its ith local maximum S_i, and $n = i_{\min}$ be the time when $\hat{X}_n$ gets its ith local minimum T_i. Then, we construct the return maps S_{i+1} versus S_i, T_{i+1} versus T_i, and V_i versus U_i, where $U_i = (S_i + T_i)/2$ and $V_i = S_i - T_i$. Figure 6 depicts the return map V_i versus U_i constructed from the maxima and minima of a typical experimental time series of $\hat{X}_n$

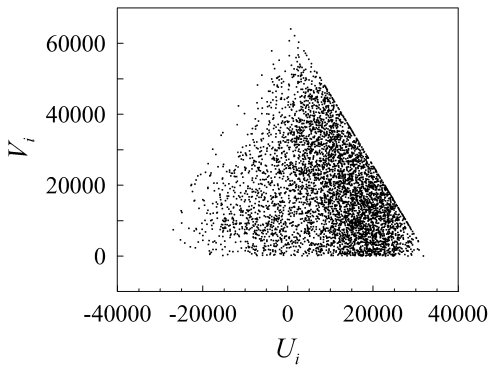

Fig. 6. Return map of the experimental communication system.

for the case where noise is not added intentionally to the signal transmitted through the communication channel. In contrast to the return maps presented by Pérez and Cerdeira [1995], Fig. 6 does not show any 1D curves which could be used for message extraction. The return maps S_{i+1} versus S_i and T_{i+1} versus T_i also do not show 1D curves. Moreover, the return maps are similar in the cases of fixed and switched delay time in the transmitter. Thus, the return map method which is efficient for unmasking low-dimensional chaotic communication systems fails when applied to the proposed communication scheme based on time-delayed feedback oscillator.

Another popular approach for unmasking chaotic communication systems is based on the dynamical reconstruction of the transmitter from its time series. However, even simple time-delay systems can exhibit high-dimensional chaotic dynamics, and a direct reconstruction of such systems using conventional time-delay embedding techniques often fails. Because of this, for a successful recovery of time-delay systems one has to use special methods [Zhou & Lai, 1999; Udaltsov *et al.*, 2001; Ponomarenko & Prokhorov, 2002; Prokhorov *et al.*, 2005; Prokhorov & Ponomarenko, 2008]. One of them is based on the statistical analysis of time intervals between extrema in the time series. It has been shown that time series of first-order time-delay systems practically have no extrema separated in time by the delay time [Prokhorov *et al.*, 2005]. Then, defining, for different values of q, the number of situations N where the points of the chaotic time series separated in time by q are both extremal, one can construct the $N(q)$ plot and recover the delay time as the value at which the absolute minimum of $N(q)$ is observed [Prokhorov *et al.*, 2005]. For the systems with two coexisting delays the $N(q)$ plot exhibits pronounced minima at q values equal to these delay times.

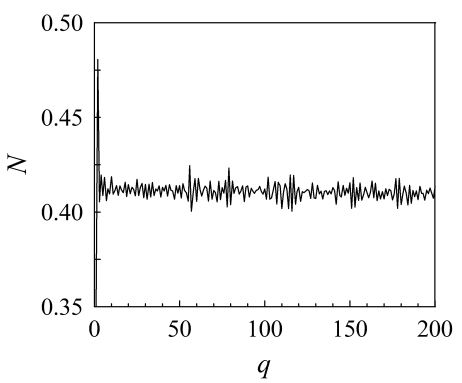

Fig. 7. Number of pairs of extrema N in the experimental time series separated in time by q, as a function of q. $N(q)$ is normalized to the total number of extrema in the time series.

We applied this method to chaotic time series of $\hat{X}_n$. For various q values we count the number N of situations where the derivatives of $\hat{X}_n$ and $\hat{X}_{n-q}$ are simultaneously equal to zero and construct the $N(q)$ plot, Fig. 7, where the step of q variation is equal to one. The time derivatives are estimated from the time series by applying a local parabolic approximation. To construct the $N(q)$ plot we use 30 000 points of time series for the case where noise is not added intentionally to the signal transmitted through the communication channel. The switched delay times $k = 100$ and $p = 110$ cannot be recovered from Fig. 7. The more detailed analysis of the scheme security is the subject of independent investigation.

4. Results of Numerical Simulation of the Scheme

To investigate the limits of the proposed communication scheme we carried out its numerical simulation. The parameters of the simulated scheme were chosen the same as those indicated in Sec. 3 for the experimental setup. To simulate the effect of noise in the communication channel we added a zero-mean Gaussian white noise filtered in the bandwidth of the chaotic carrier to time series of the signal transmitted into the channel. For different levels of noise and three values of l we recovered the binary information signal at the receiver output and constructed the dependences of BER on the SNR, Fig. 8(a). For $l = 100$ and $l = 200$ the message signal is recovered without errors at SNR ≥ 12 dB and SNR ≥ 10 dB, respectively.

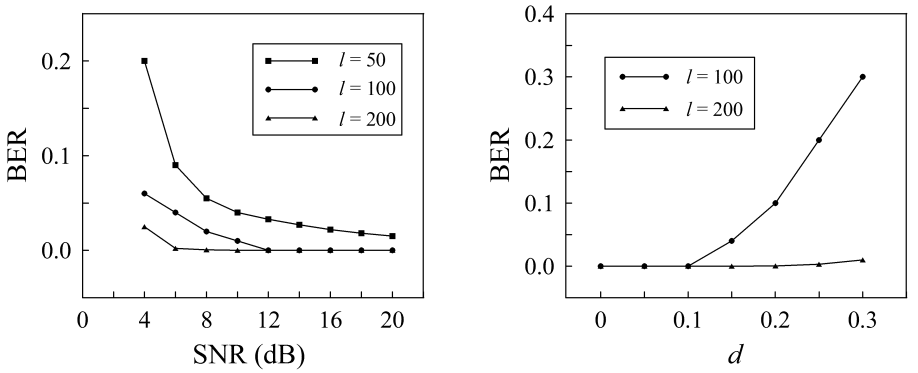

Fig. 8. (a) The bit-error rates as a function of signal-to-noise ratio and (b) as a function of the signal attenuation in the communication channel for the simulated communication system. In each measuring of BER, 10^5 randomly ordered binary symbols are sent.

Figure 8(b) presents for two different values of l, the dependences of BER on the parameter d characterizing the signal attenuation in the communication channel. For $l = 100$ and $l = 200$ the binary information signal at the receiver output is recovered without errors at $d \leq 0.1$ and $d \leq 0.15$, respectively.

As it can be seen from Figs. 4 and 8, the simulated communication system exhibits much higher tolerance to noise and amplitude distortions of the signal than the experimental scheme. We revealed that the reason of deterioration of BER characteristics is the presence of fixed bias of the signal in the communication channel of the experimental scheme. This technical shortcoming will be eliminated in our further research by adjustment of fixed bias.

Figure 9 depicts the dependence of BER on the value of l for the case where SNR = 8 dB and $d = 0$. For small values of l the increase of BER is observed.

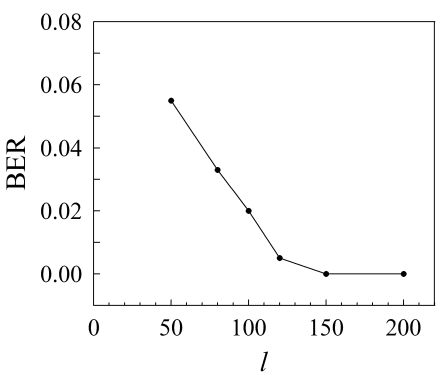

Fig. 9. The bit-error rate as a function of length of time interval during which each bit is transmitted for the simulated communication system. In each measuring of BER, 10^5 randomly ordered binary symbols are sent.

However, the absolute BER values in the region of small l values are by the order of magnitude lower than the corresponding BER values in the experimental scheme, Fig. 5. Hence, without loss of transmission quality the model scheme can provide the higher rates of information transmission than the experimental one by decreasing the length of time interval during which each bit is transmitted. By increasing the resistance of the experimental scheme to noise, one can decrease the values of l without transmission quality loss and therefore increase the rate of data transmission.

The results of the numerical investigation of the proposed communication system indicate that the efficiency of the considered experimental scheme can be sufficiently improved. In particular, the BER of the recovered message under high levels of noise can be potentially decreased several times.

We studied the security of the simulated scheme by applying the return maps and $N(q)$ plots considered in Sec. 3. The return map V_i versus U_i constructed from the maxima and minima of the simulated time series is similar to the one presented in Fig. 6 for the experimental scheme. It does not show any 1D curves and cannot be used for message extraction.

The dependence $N(q)$ with the step of q variation equal to 1 is presented in Fig. 10 for the case of additive noise absence. To construct Fig. 10 we use 30 000 points of time series. The pronounced minima of $N(q)$ are observed at q equal to 100, 103, 110, and 113. Two of these q values coincide with the switched delay times $k = 100$ and $p = 110$. However, in the presence of even small additive noise, the minima at the true values of delay times are

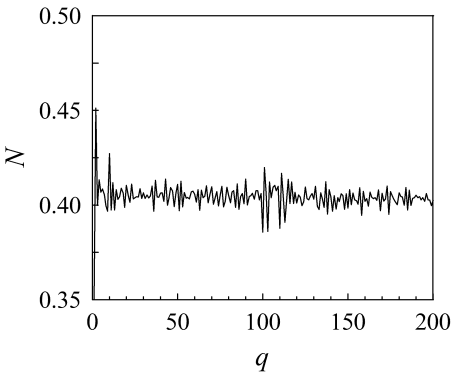

Fig. 10. Number of pairs of extrema N in the simulated time series separated in time by q, as a function of q. $N(q)$ is normalized to the total number of extrema in the time series.

not pronounced. Besides, Fig. 10 indicates only the probable presence of different delays in the system, but it gives no information about the delay time value at the concrete moment which is necessary for hidden message extraction. To recover the current delay time one should analyze short time intervals comparable with the length l of the interval during which one bit is transmitted. In our scheme, the l values are comparable to the delay times. From such short time series it is very difficult to reconstruct the delays using the methods based on the dynamical reconstruction of the chaotic transmitter.

5. Conclusion

We have developed the experimental communication system with chaotic switching and analog communication channel which shows high tolerance to channel noise and attenuation of the signal in the transmission channel. In our scheme, the transmitter and receiver represent time-delayed feedback oscillators implemented in a digital form using programmable microcontrollers. The use of digital elements in the scheme ensures the identity of the receiver and transmitter parameters and increases the quality of hidden message extraction at the receiver output. The proposed configuration of the receiver allows us to increase the scheme resistance to external noise and amplitude distortions of the signal in the communication channel.

We have illustrated the scheme efficiency for the transmission of binary information signal. The experimental dependences of BER on SNR, signal attenuation in the communication channel, and duration of bit transmission are constructed. The possibilities of increasing the rate of information transmission are discussed. The security of the proposed scheme is studied by applying the return maps and the method based on the statistical analysis of time intervals between extrema in the time series.

We have numerically simulated the proposed chaotic communication system and compared the results of simulation with those obtained in the physical experiment.

Acknowledgment

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

References

Alvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation and Chaos* **16**, 2129–2151.

Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., García-Ojalvo, J., Mirasso, C. R., Pesquera, L. & Shore, K. A. [2005] "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature* **437**, 343–346.

Cuomo, K. M. & Oppenheim, A. V. [1993] "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* **71**, 65–68.

Dedieu, H., Kennedy, M. P. & Hasler, M. [1993] "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst.-II* **40**, 634–642.

Dmitriev, A. S., Panas, A. I. & Starkov, S. O. [1995] "Experiments on speech and music signals transmission using chaos," *Int. J. Bifurcation and Chaos* **5**, 1249–1254.

Dmitriev, A. S. & Panas, A. I. [2002] *Dynamical Chaos: New Information Carriers for Communication Systems* (Fizmatlit, Moscow).

García-Ojalvo, J. & Roy, R. [2001] "Spatiotemporal communication with synchronized optical chaos," *Phys. Rev. Lett.* **86**, 5204–5207.

Goedgebuer, J.-P., Larger, L. & Porte, H. [1998] "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.* **80**, 2249–2252.

Halle, K. S., Wu, C. W., Itoh, M. & Chua, L. O. [1993] "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation and Chaos* **3**, 469–477.

Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O. & Parlitz, U. [1992] "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 709–713.

Koronovskii, A. A., Moskalenko, O. I. & Hramov, A. E. [2009] "On the use of chaotic synchronization for secure communication," *Physics — Uspekhi* **52**, 1213–1238.

Kye, W.-H., Choi, M., Kim, C.-M. & Park, Y.-J. [2005] "Encryption with synchronized time-delayed systems," *Phys. Rev. E* **71**, 045202.

Kye, W.-H. [2012] "Information transfer via implicit encoding with delay time modulation in a time-delay system," *Phys. Lett. A* **376**, 2663–2667.

Millerioux, G. [2013] "Cryptanalysis of hybrid cryptosystems," *Int. J. Bifurcation and Chaos* **23**, 1350173-1–13.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 973–977.

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.

Pérez, G. & Cerdeira, H. A. [1995] "Extracting messages masked by chaos," *Phys. Rev. Lett.* **74**, 1970–1973.

Ponomarenko, V. I. & Prokhorov, M. D. [2002] "Extracting information masked by the chaotic signal of a time-delay system," *Phys. Rev. E* **66**, 026215.

Ponomarenko, V. I., Karavaev, A. S., Glukhovskaya, E. E. & Prokhorov, M. D. [2012] "Hidden data transmission based on time-delayed feedback system with switched delay time," *Tech. Phys. Lett.* **38**, 51–54.

Ponomarenko, V. I., Prokhorov, M. D., Karavaev, A. S. & Kulminskiy, D. D. [2013] "An experimental digital communication scheme based on chaotic time-delay system," *Nonlin. Dyn.* **74**, 1013–1020.

Prokhorov, M. D., Ponomarenko, V. I., Karavaev, A. S. & Bezruchko, B. P. [2005] "Reconstruction of time-delayed feedback systems from time series," *Physica D* **203**, 209–223.

Prokhorov, M. D. & Ponomarenko, V. I. [2008] "Encryption and decryption of information in chaotic communication systems governed by delay-differential equations," *Chaos Solit. Fract.* **35**, 871–877.

Pyragas, K. [1998] "Transmission of signals via synchronization of chaotic time-delay systems," *Int. J. Bifurcation and Chaos* **8**, 1839–1842.

Short, K. M. [1997] "Signal extraction from chaotic communications," *Int. J. Bifurcation and Chaos* **7**, 1579–1597.

Stankovski, T., McClintock, P. V. E. & Stefanovska, A. [2014] "Coupling functions enable secure communications," *Phys. Rev. X* **4**, 011026.

Tao, Y. [2004] "A survey of chaotic secure communication systems," *Int. J. Comput. Cogn.* **2**, 81–130.

Udaltsov, V. S., Goedgebuer, J.-P., Larger, L. & Rhodes, W. T. [2001] "Communicating with optical hyperchaos: Information encryption and decryption in delayed nonlinear feedback systems," *Phys. Rev. Lett.* **86**, 1892–1895.

Van Wiggeren, G. D. & Roy, R. [1998] "Communication with chaotic lasers," *Science* **279**, 1198–1200.

Volkovskii, A. R. & Rulkov, N. F. [1993] "Synchronous chaotic response of a nonlinear oscillator system as a principle for the detection of the information component of chaos," *Tech. Phys. Lett.* **19**, 97–99.

Wang, M.-J., Wang, X.-Y. & Pei, B.-N. [2012] "A new digital communication scheme based on chaotic modulation," *Nonlin. Dyn.* **67**, 1097–1104.

Yang, T., Yang, L.-B. & Yang, C.-M. [1998] "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A* **245**, 495–510.

Zhou, C.-S. & Chen, T.-L. [1997] "Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos," *Phys. Lett. A* **234**, 429–435.

Zhou, C. & Lai, C.-H. [1999] "Extracting messages masked by chaotic signals of time-delay systems," *Phys. Rev. E* **60**, 320–323.