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

Communication System Based on Time-Delayed Feedback Oscillator with Switching of Chaotic Regimes

Mikhail Prokhorov†, Anatoly Karavaev†‡, Danil Kulminskiy†‡, and Vladimir Ponomarenko†‡

†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: mdprokhorov@yandex.ru, karavaevas@gmail.com, kulminskydd@gmail.com, ponomarenkovi@gmail.com

Abstract– 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 experimental dependences of bit-error rate on the signal-to-noise ratio, signal attenuation in a communication channel, and duration of bit transmission are constructed. The scheme shows high tolerance to external noise and amplitude distortions of the signal in the communication channel.

1. Introduction

The use of chaotic signals for secure communication has been an active area of research since the early 1990s. Many methods involving synchronization of chaotic systems have been proposed to scramble the transmission of information [1–3]. The most popular among them are chaotic masking, chaotic switching or chaos shift keying, chaotic modulation, and nonlinear mixing. However, many chaotic communication systems, especially the systems using low-dimensional chaotic signals, are not as secure as expected and can be successfully unmasked [4]. 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 [5].

Although chaotic communication systems have a lot of merits including broadband power spectrum of chaotic signals, high rates of information transmission, and simple implementation, they are not devoid of drawbacks restricting their wide use in practice. The main shortcomings of communication schemes based on 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 [3].

In the present paper, we propose a new communication system with chaotic switching which is devoid of above mentioned shortcomings owing to the specific configuration of the receiver and employment of programmable microcontrollers to implement a transmitter and receiver in the experimental scheme.

The paper is organized as follows. In Section 2, the proposed communication system is described. In Section 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. In Section 4, we summarize our results.

2. Communication Scheme

A block diagram of the proposed communication scheme based on a time-delay system with switching of chaotic regimes is shown in Fig. 1. 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.

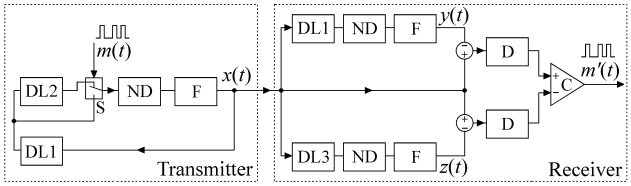

Fig. 1. Block diagram of a communication system: (DL1, DL2, and DL3) delay lines, (ND) nonlinear devices, (F) filters, (S) commutator, (D) detectors, and (C) comparator.

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

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

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 that is placed after the filter breaks the feedback circuit in each driven system of the receiver. These systems are described by the following equations:

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

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

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.

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 the 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 the 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.

The operation of the most of communication schemes with chaotic switching is based on the described above concept [1–3]. 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 system resistance to noise, we have modified the classical scheme taking onto account the following considerations. In the presence of noise, the variance of the signal at the output of subtractor in the synchronized system is close to the variance of noise in the communication channel and the variance of the signal at the output of subtractor in the nonsynchronized system is close to the variance of chaotic carrier. Since the level of noise in the communication channel in general case is appreciably less than the level of chaotic carrier, we can recover accurately the hidden message even in the presence of sufficiently strong noise.

We added two detectors and comparator in the receiver in order to increase the scheme tolerance to noise (Fig. 1). The detectors evaluate the variance of incoming difference signal and the comparator calculates the difference $r(t)$ between the output signals of detectors and 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.

We realized the proposed communication system in a physical experiment. To achieve the complete identity of the transmitter and receiver parameters in the experimental setup we implemented all the transmitter and receiver elements in a digital form using programmable microcontrollers of the Atmel megaAVR family.

In order 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 Eq. (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 following form:

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

This differential equation 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 Eq. (5), while at a transmission of binary unity it is described by Eq.(6):

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

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

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.

Fig. 2 shows a block diagram of the experimental communication scheme. The delay line in the transmitter has two outputs which correspond to the delay times k and p, respectively. 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 and transmitted into a communication channel.

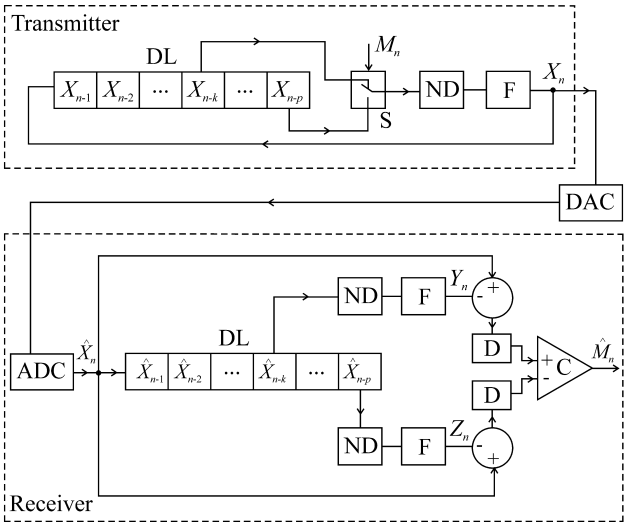

Fig. 2. Block diagram of the experimental scheme: (DL) delay lines, (ND) nonlinear devices, (F) filters, (S) commutator, (DAC) digital-to-analog converter, (ADC) analog-to-digital converter, (D) detectors, and (C) comparator.

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:

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

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

The detectors in the experimental scheme evaluate the variance of incoming difference signal using l values of this signal stored in the circular buffer array in the operative memory of microcontroller. The comparator calculates the difference R_n between the output signals of detectors and transforms R_n into a recovered information signal $\hat{M}_n$, so that the output signal is binary zero for $R_n \le 0$ and binary unity otherwise.

3. Results of the scheme operation

Let us illustrate the efficiency of the proposed communication scheme for the following values of parameters: $\tau_1 = 100$, $\tau_2 = 10$, $\tau_3 = 110$, $\lambda = 1.9$, and $f_c = 0.5$ ($\varepsilon = 2$). With these parameters, the transmitter generates a chaotic signal [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 (0 or 1) is transmitted.

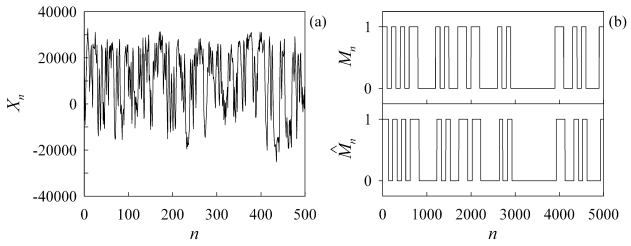

Fig. 3. The time series of chaotic signal X_n (a) and information signals M_n and $\hat{M}_n$ (b).

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

To investigate the tolerance of the experimental 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. Fig. 4(a) shows the experimental dependence of bit-error rate (BER) of the recovered message on the signal-to-noise ratio (SNR). The signal in SNR is the transmitted chaotic signal and noise is an additive zero-mean Gaussian white noise filtered in the bandwidth of the chaotic carrier. In each measuring of BER, 10^5 randomly ordered binary symbols are sent. For SNR ≥ 14 dB the signal $\hat{M}_n$ is recovered without errors. Therefore, the proposed experimental scheme is more robust against channel noise than other experimental communication systems using chaotic synchronization for the transmission of hidden information signal through analog communication channel [3].

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 the 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.

Fig. 4(b) depicts the experimental 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. For $d \le 0.1$ 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, the other schemes with chaotic switching and the schemes with nonlinear mixing fail [3].

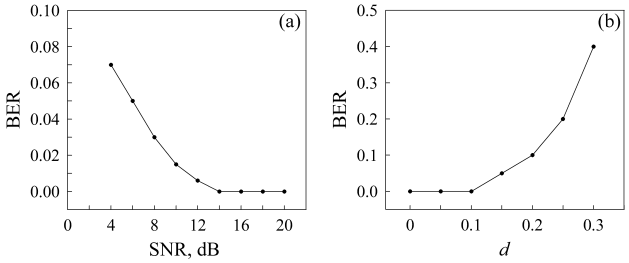

Fig. 4. The bit-error rate as a function of signal-to-noise ratio (a) and as a function of the signal attenuation in the communication channel (b).

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.

The experimental dependence of BER on the length l of the time interval during which one bit is transmitted is shown in Fig. 5 for SNR=8 dB and $d = 0$. 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.

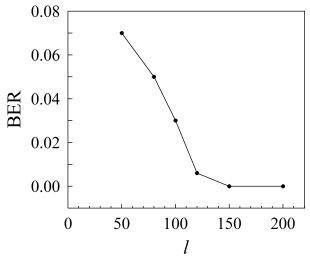

Fig. 5. The bit-error rate as a function of length of time interval during which each bit is transmitted.

It is well known that many chaotic communication schemes are not as secure as expected and can be successfully unmasked. To test the vulnerability of the proposed communication scheme against attacks we applied the method of message extraction based on the analysis of return maps [4] and the method based on the dynamical reconstruction of a chaotic transmitter from its time series [6].

It is found out that the return map method which is efficient for unmasking low-dimensional chaotic communication systems fails being applied to the proposed communication scheme based on time-delayed feedback oscillator. We have shown that the switched delay times cannot be recovered also using the method [6] based on the statistical analysis of time intervals between extrema in the time series.

4. Conclusion

We have developed the communication system with chaotic switching 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 identity of the receiver and transmitter parameters and increases the quality of hidden message extraction at the receiver output. We have illustrated the scheme efficiency for the transmission of binary information signal.

Acknowledgments

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

References

[1] U. Parlitz, L. O. Chua, L. Kocarev et al., “Transmission of digital signals by chaotic synchronization,” *Int. J. Bifurc. Chaos*, vol. 2, pp. 973–977, 1992.

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

[3] 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.

[4] G. Pérez, H. A. Cerdeira, “Extracting messages masked by chaos,” *Phys. Rev. Lett.*, vol.74, pp.1970–1973, 1995.

[5] M. D. Prokhorov, V. I. Ponomarenko, “Encryption and decryption of information in chaotic communication systems governed by delay-differential equations,” *Chaos Solitons Fractals*, vol.35, pp.871–877, 2008.

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