Advances in Intelligent Systems Research, volume 166
7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019)

Qualitative Study of Some Communication Systems with Random Signals

Aleksandr Zhuk
North-Caucasus Federal University
Stavropol, Russia
alekszhuk@mail.ru

Aleksej Gavrishev
North-Caucasus Federal University
Stavropol, Russia
alexxx.2008@inbox.ru

Valerij Rachkov
North-Caucasus Federal University
Stavropol, Russia
1234567890rw6hlg@gmail.com

Irina Kuzmenko
Stavropol State Agrarian University
Stavropol, Russia
11kip11@mail.ru

***Abstract*—This article presents a qualitative analysis of common communication systems based on random signals. The analysis is given in the context of protecting transmitted data from unauthorized access: the method of chaos shift keying and the method of chaotic modulation. As a result of the qualitative analysis presented by the time diagrams of the signals transmitted in the communication channel it was established that the chaos shift keying method presented by the COOK communication system has pauses in the transmission of information by random signals. At the same time the chaotic modulation method represented by apparatus for anti-imitation protection of controlled objects does not have pauses in the transmission of information by random signals. The principle of the energy receiver functioning for the COOK communication system and apparatus for anti-imitation protection of controlled objects were shown. It is established, that communication systems based on chaotic modulation methods are more preferred for the protection of the transmitted signals from unauthorized access than the chaos shift keying method presented by the COOK communication system.**

Keywords—random signals, radio, protection

I. INTRODUCTION

The advances in the wireless communication devices, such as robotic systems, fire alarm systems and others, used in secure systems have led to the development of highly secure data encryption techniques. In these application secure and reliable monitoring are considered the most essential requirements. Actually, many encryption techniques can be used such as the traditional encryption algorithms and chaotic-based encryption systems. However, some of these traditional encryption algorithms are hard to understand, complex, not suitable for real-time application and slow encryption. On the other hand, the main advantages of using chaos lies in the observation that random signal looks like noise for the unauthorized users, has the bandwidth, the complexity structure and a strong sensitivity to the initial conditions. Therefore, chaotic-based encryption systems have highly secure and easy implemented encryption systems for secure transmission networks [1].

In these conditions, an important issue is the study of quantitative and qualitative properties of communication systems based on random signals. In this paper, two common communication systems based on chaotic modulation and the chaos shift keying method were chosen as communication systems based on random signals [2-6]. We will conduct a study of these communication systems using one of the most common methods of qualitative analysis of communication systems – time diagrams and establish which of the communication systems has greater security against unauthorized access

The purpose of this article is to compare some communication systems based on random signals to protect the transmitted data from unauthorized access.

II. RESEARCH PART

As it is known [2-6], currently one of the most common communication systems based on random signals are communication systems based on methods of chaos shift keying and chaotic modulation.

A. Communication system based on the COOK

We consider a communication system based on the method of chaos shift keying. In the simplest case, the communication system provided the chaos shift keying method is based on the use of presence or absence of the chaotic on-off keying ("the COOK"): on the time axis the positions are marked, the presence of an impulse on which means the transfer of the "1", and the absence of impulse means the transfer of the "0" [4].

Transmitter and receiver the COOK given below (Fig. 1) [4].

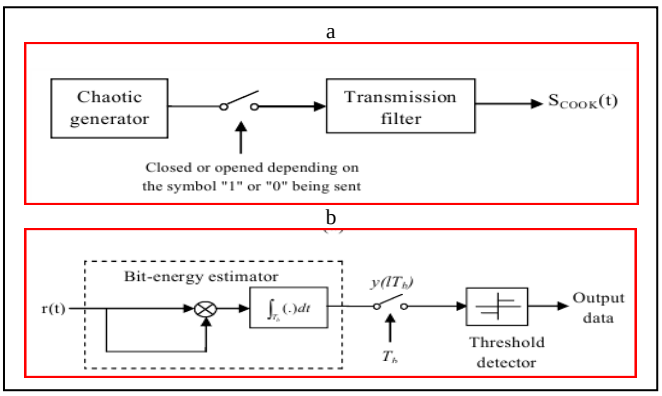

Fig. 1. The scheme of the transmitter (a) and the receiver (b) of the COOK

To analyze the COOK communication system, let us turn to the well-known sources of scientific literature. Several models of this communication system with the use of different random signal generators are known [5, 6]. One of these generators is a Chua's circuit. Fig. 2 shows the time diagram of the initial information signal and the corresponding time diagram of the signal in the communication channel, created with the help of the random signal generator presented by Chua's circuit [5].

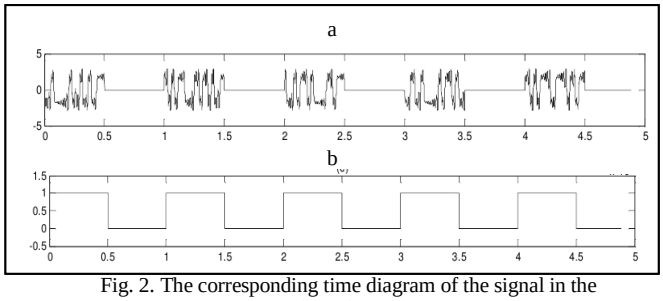

Fig. 2. The corresponding time diagram of the signal in the communication line (a), created using Chua's circuit (a) and timing diagram of the initial information signal (b)

In the source of literature [2, 6] a direct-chaotic information transfer system using the COOK communication system (Fig. 3) is given. It includes [2, 6]: 1 – ultra-bandwidth random oscillator, 2 – modulator, 3 and 7 – microwave amplifiers, 4 – source of digital control signals, 5 and 6 – transmitting and receiving ultra – bandwidth antennas, 8 – demodulator, 9 – oscilloscope. Modulation is carried out on the basis of the COOK.

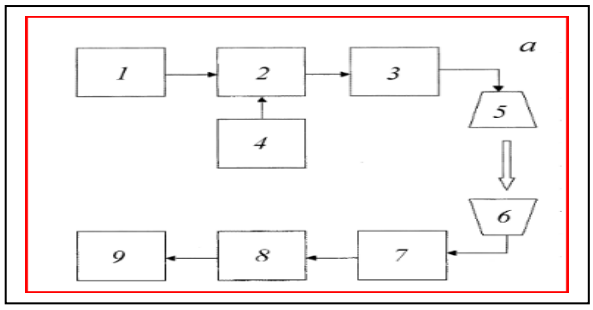

Fig. 3. Scheme of the direct-chaotic information transfer system

As a generator of random signals for a direct-chaotic information transmission system we used a specially developed generator, consisting of three bipolar microwave transistors and two frequency-selective circuits. Fig. 4 demonstrates a time diagram on which at the top is the formation of a stream of random radio impulses in the transmission of information and the initial information sequence is at the bottom [2, 6].

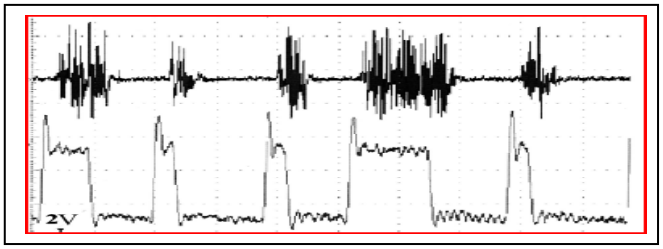

Fig. 4. Time diagram of random radio impulses in the communication channel (above) and the corresponding initial information sequence (bottom)

As it can be seen from the figures, the distinctive feature of the COOK communication system is the presence of pauses between the signals transmitted in the communication channel. However, the presence of pauses in the transmission of information by a random signal allows the conditional enemy to restore the transition times from the "1" to the "minus 1" and back, using an energy receiver consisting of a squarer and an integrator. As it is known [7, 8], the operating principle of the energy receiver is based on the signal energy allocation, which is determined by an expression of the form:

$$E_S = \int_0^T S^2(t)dt,$$

Where E_S – the energy of the received signal, T – the duration of the received signal, $S(t)$ – the time representation of the signal. In order to determine the signal energy, it is necessary to voltage the signal accepted by the receiver, square it and integrates it. For the technical realization of the squaring, one can use the quadratic characteristic of the diode, which has characteristic in the range of small signals $S^2(t)$. After $S(t)$ squaring it is necessary to integrate it. For this aim it is possible to use the integrator implemented on the RC-circuit. As a result, a diode and a series-connected integrator (RC-circuit) make it possible to calculate the signal energy. This is explained in Fig. 5 [7, 8].

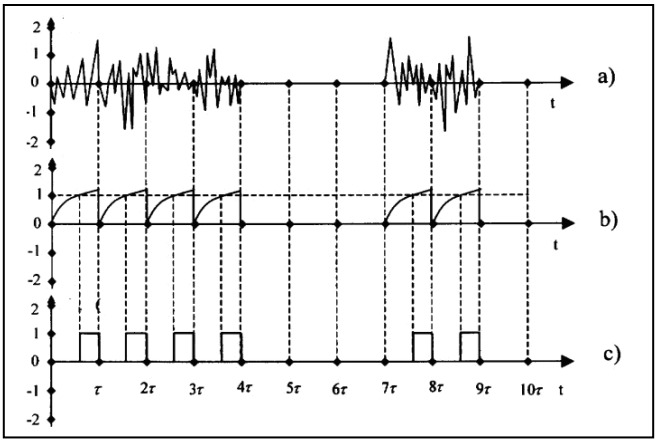

Fig. 5. The timing diagrams explaining the operation principle of the energy receiver, the input of which receives a signal generated by the COOK communication system

If the random signal used by the COOK communication system (Figure 5a) enters the input of the energy receiver (not shown), consisting of a diode and an integrator, by integrating (accumulating) the power of the received impulses within their duration, then it will be the signal on its output (Fig. 5b), which is necessary for the decision of the threshold device. Impulses are received from the output of the threshold device to the decoder input (Figure 5c) with duration equal to the duration of the excess of the integrated signal above the threshold level. From the signal received at the input of the energy receiver (Fig. 5a), useful information is extracted (Fig. 5c), while the presence of a pulse at a given position in the information stream corresponds to the transmitted "1" and to the absence of a pulse corresponds the symbol of the "minus 1" [7, 8]. Thus, the conditional enemy can restore the structure of the signal carrier, which indicates

a low structural and informational stealth of the COOK communication system [7, 8].

B. Communication system based on chaotic modulation

Let us turn to communication systems based on the chaotic modulation method. One of such communication systems based on random signals is an apparatus for anti-imitation protection of controlled objects, carrying out a secure information exchange between fire alarm sensors and the control unit [9]. This device is based on rewritable drives of random sequences [7]. Fig. 6 shows its receiving and transmitting part, which includes the following blocks: 1 – information source (control unit, sensor), 2 – random signal accumulator, 3 – modulator-transmitter, 4 – bandpass filter, 5 – amplifier, 6 – first multiplier, 7 – second multiplier, 8 – inverter, 9 – copy buffer of random signal, 10 – first integrator, 11 – second integrator, 12 – subtractor, 13 – decision device, 14 – receiver of information (control unit, sensor).

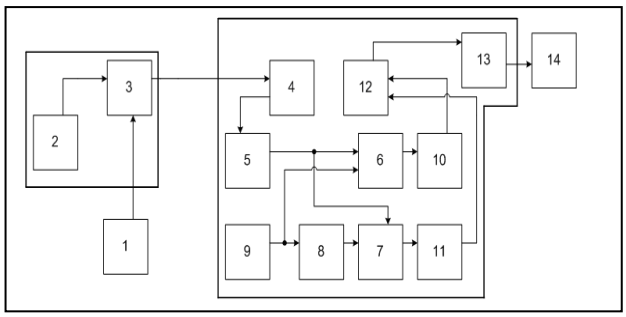

Fig. 6. Structural diagram of the receiving-transmitting part of the apparatus for anti-imitation protection of controlled objects

Let us describe mathematically [10], how the scheme shown in Fig. 7 functions. The initial data will be the following concepts [6]:

1) $S_x(t)$ – an arbitrary random signal;

2) $S_{inf}(t)$ – the initial information signal;

3) $U(t)$ – the signal transmitted in the communication channel;

4) $S_{res.inf}(t)$ – restored information signal.

The information signal $S_{inf}(t)$ can take on two data -1 and 1. In this case, the output of the modulator-transmitter is a signal $U(t)$ created by multiplying the source information signal $S_{inf}(t)$ with a random signal $S_x(t)$ in the modulator-transmitter. In the communication channel, the additive Gauss's interference acts on the transmitted signal $U(t)$, so a mixture of the transmitted signal and interference $R(t)=U(t)+N(t)$ enters the input of the receiving device [9]. After entering the synchronization mode, a signal $Y(t)=U(t)+N(t)$ is output from the bandpass filter in the receiver, which is than amplified. After that, the amplified signal $Y_{ag}(t)$ is simultaneously multiplied by a copy of the random signal $S_x(t)$, analogous to the random signal in the transmitter, and multiplied by its inverted data $-S_x(t)$. As a result, signals $S_{P1}(t)$ and $S_{P2}(t)$ are obtained and which then pass through the integrators and take the following data $G_1(t)$ and $G_2(t)$. Then the signals $G_1(t)$ and $G_2(t)$ go to the subtractor device, where their difference is calculated. From the output of the subtractor device, the difference signal $Z_{sub}(t)$ enters the decision device, where the received levels are compared to the threshold data [11]:

- $S_{res.inf}(t)=1$, herewith $Z_{sub}(t)>0$,
- $S_{res.inf}(t)=-1$, herewith $Z_{sub}(t)<0$.

After this the reconstructed information signal $S_{res.inf}(t)$ arrives at the receiver.

We shall simulate the communication scheme shown in Fig. 6, in the ScicosLab simulation environment. First, we consider the Rössler's attractor as a generator of random signals [12, 13]. Fig. 7 shows the various fragments of signals $U(t)$ transmitted in the communication channel, created using the Rössler's attractor.

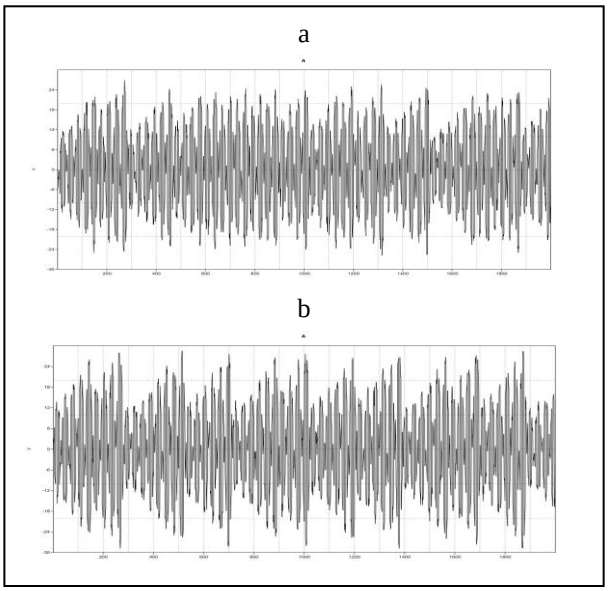

Fig. 7. Fragment of the signal $U(t)$ entering the communication channel

Further, we consider as a generator of random signals the perturbed Van der Pol's oscillator [12, 14]. Fig. 8 shows the various fragments of signals $U(t)$ transmitted in the communication channel, created using the perturbed Van der Pol's oscillator.

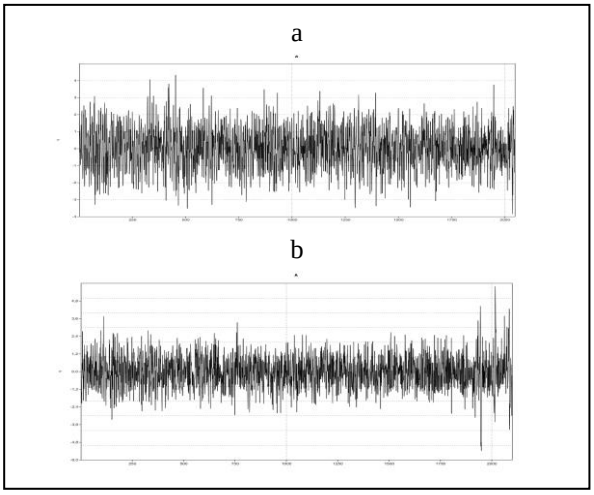

Fig. 8. Fragments of the signal $U(t)$ entering the communication channel

As it can be seen from the shown fragments of signals (Fig. 7, 8) transmitted in the communication channel, they have a continuous (without pauses) noise-like kind, and it is visually difficult to extract an information signal representing a uniform sequence of square impulses in the range [-1; 1]. An explanation for these words is Fig. 9, which shows the time diagrams explaining the operation principle of the energy receiver, the input of which receives a signal formed by the receiving-transmitting part of the apparatus for anti-imitation protection of controlled objects [6, 8].

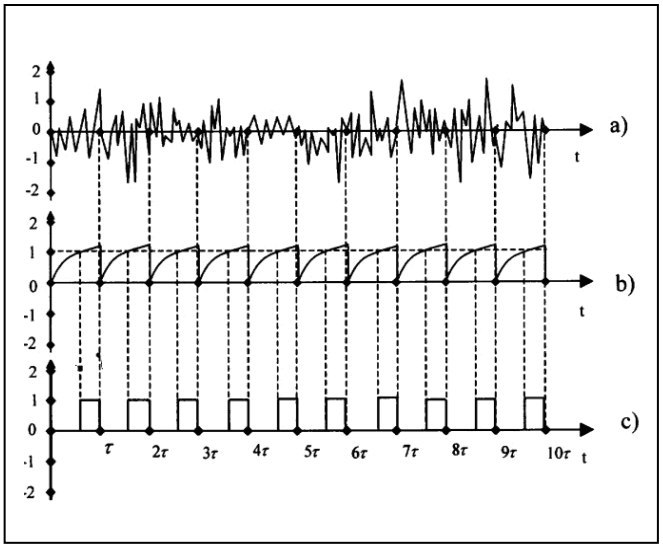

Fig. 9. Timing diagrams explaining the principle of operation of the energy receiver, the input of which receives a signal generated by the receiving and transmitting part of the apparatus for anti-imitation protection of controlled objects.

In case if the signal generated by the apparatus for anti-imitation protection of controlled objects (Figure 9a) also enters the input of the energy receiver, where by integrating (accumulating) the power of the received impulses within the duration limits, a signal necessary for making a decision by the threshold device is extracted (Figure 9b). From the output of the threshold device, impulses are input to the decoder device (Figure 9c) with a duration equal to the duration of the excess of the integrated signal above the threshold level. From the signal received at the input of the energy receiver (Fig. 9a), the information is extracted (Fig. 9c), but unlike the COOK communication system, there is no visible transition from "minus one" to "one" and back, since a copy of the information recorded on the device is unknown. It means that an energy receiver in the case of the "1" and in the case of the "minus 1" will give a decision about the "1", and it will be impossible to disrupt information secrecy without having a copy of the random carrier signal [7, 15].

Thus, the apparatus for anti-imitation protection of controlled objects has a higher structural concealment of carrier signals than the COOK communication system.

III. Conclusion

In this article a qualitative analysis of communication systems based on random signals in the context of the protection of transmitted data from unauthorized access is carried out. Two common communication systems based on random signals were considered: chaos shift keying method, represented by the use of the presence or absence of a chaotic impulse in the information position (the COOK) and the chaotic modulation method represented by apparatus for anti-imitation protection of controlled objects.

As a result of the qualitative analysis presented by timing diagrams of the signals transmitted in the communication channel, it was established that the COOK communication system has pauses in the transmission of information by random signals, while apparatus for anti-imitation protection of controlled objects does not have pauses in the transmission of information by random signals (they have a continuous, pause-free noise-like type). The principle of functioning of the energy receiver for the COOK communication system and apparatus for anti-imitation protection of controlled objects was shown. The time diagrams of the functioning of the energy receiver and the time diagrams of the signals transmitted in the channel clearly show that for the COOK communication system it is potentially possible to restore the transition times from the "1" to the "minus 1" and back (and thus restore the original information signal). But for apparatus for anti-imitation protection of controlled objects it is impossible (due to the fact that the enemy does not know the spreading random sequence) [7, 15]. In addition, the ability to rewrite random sequences in rewritable random signal stores significantly increases the security of transmitted data from unauthorized access, including from the attack method based on the use of the comparative database of known spreading sequences [16].

Thus, the communication systems based on chaotic modulation methods are more preferable for issues of protecting transmitted signals from unauthorized access than the chaos shift keying method presented by the COOK.

Acknowledgment

This work was supported by the Russian Foundation for Basic Research, project No. 18–07-01020

References

[1] S. M. Darwish, A. Elmasry and A. H. Ibrahim, "Parameter Estimation for Chaotic Systems Using the Fruit Fly Optimization Algorithm", AISC, vol. 981, pp. 80-90, 2019 [The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA 2019)].

[2] Y. V. Gulyaev, A. S. Dmitriev, V. A. Lazarev, T. I. Mokhseni and M. G. Popov, "Interaction and navigation of robots based on ultrawideband direct chaotic communication", Journal of communications technology and electronics, vol. 61, no. 8, pp. 894-900, 2016.

[3] W. Xiangjun, F. Zhengye and K. Jurgen, "A secure communication scheme based generalized function projective sunchronization of new 5D hyperchaotic system", Physica Scipra, no. 90, pp. 1-12, 2015.

[4] N. A. Hikmat and A. V. Alejandro "Efficient chaotic communication system for wireless sensing applications". IEEE Press, 5 p., 2012 [9th International Multi-Conference on Systems, Signals and Devices, 2012].

[5] I. A. Kamil and O. A. Fakolujo "Chaotic Secure Communication Schemes employing Chua's Circuit". IWSSIP Publ., 4 p., 2010 [17th International Conference on Systems, Signals and Image Processing, 2010].

[6] A. S. Dmitriev, B E. Kjarginskij, A. I. Panas, D. Ju. Puzikov and S. O. Starkov, "Sverhshirokopolosnaja prjamohaoticheskaja peredacha informacii v SVCh-diapazone [Ultra-wideband direct-chaotic information transmission in the microwave range]", Pis'ma v ZhTF, no. 29(2), pp.70-76, 2003 (In Russian).

[7] S. V. Barketov, A. P. Zhuk, V. V. Sazonov, S. I. Avdeenko., E. P. Zhuk, V. I. Lokhov and J. S Golub', "Coherent data transmission

system using random signals", Patent RF no. 2326500, pp. 6, 2008 (In Russina).

[8] A. Zhuk and A. Lysenko, "Coherent data transmission system using random signals", NCFU Publ., pp. 19-24, 2014 [Sixth international scientific and technical conference Infocommunication technologies in science, production and education, Russia, 2014].

[9] D. L. Osipov, A. P. Zhuk and A. A. Gavrishev, "Apparatus for protection against imitation of controlled objects with high structural security of carrier signals", Patent RF no. 2560824, pp. 15, 2015 (In Russian).

[10] A. A. Gavrishev and A. P. Zhuk, "Application of Methods of Nonlinear Dynamics to Study the Chaotic State of the Carrier Signals of Secure Communication Systems Based on Dynamic Chaos", Vestnik NSU. Series: Information Technologies, no. 16(1), pp. 50-60, 2018 (In Russian).

[11] K. N. Leonov, A. A. Potapov and P. A. Ushakov, "Mathematical modeling of data transition system on the base of chaotic signals with fractional dimension", Fizika volnovykh protses-sov i radiotekhnicheskie sistemy – Physics of Wave Processes and Radio Systems, no. 13 (3), pp. 47–53, 2010 (In Russian).

[12] A. Layec, "Modnum. Scilab toolbox for the communication systems. User's guide". IRCOM Group, 100 p., 2006.

[13] A. A. Gavrishev and A. P. Zhuk, "Simulation of apparatus for protection against imitation of controlled objects with high structural security of carrier signals", Prikladnaya informatika – Journal of Applied Informatics, no. 1(67), pp. 68-78, 2017 (Russian).

[14] A. A. Gavrishev and A. P. Zhuk, "Simulation of apparatus for protection against imitation of controlled objects with new set of chaotic signals", Prikladnaya informatika – Journal of Applied Informatics, no. 4(70), pp. 122-132, 2017 (In Russian).

[15] X. Nguyen, C. T. Nguyen, P. Barlet and R. Dojen, "A novel approach to security enhancement of chaotic DSSS systems", IEEE Press, pp. 471-476, 2016 [In: Sixth International Conference on Communications and Electronics, Ha Long, 2016].

[16] Jo Youngho and Wu Dapeng, "On Cracking Direct-Sequence Spread-Spectrum Systems", Wi-rel. Commun. Mob. Comput., no. 00, pp. 1–15, 2008.