TIME UNIT SYNCHRONIZATION RESTORATION AT THE RECEIVER OF SECURE COMMUNICATION SYSTEM WITH CHAOTIC SIGNALS

M.V.Larionova, A. J. Tomashevsky

fks@srv-vmss.mpei.ac.ru

Moscow Power Engineering Institute (Technical University)
Dept. of Generation of Oscillations and Signals

ABSTRACT

Two methods of time unit synchronization restoration, using the received chaotic sequence are considered in this work. They are based on *Fisher criterion* and *synchronous chaotic response*. The comparison between their from the viewpoint of function quality is conducted under conditions of presence of noise in the communication channel.

1. INTRODUCTION

Last decade, the questions of application of complex chaotic oscillations generated by nonlinear dynamical systems with continuous and discrete time for problems of data secure communication have been actively researching in the literature - Ref.1. Amongst offered principles of such systems design, the most perspective from standpoints of noise-immunity is the *chaotic shift keying*, for which the digital data transmission is possible when changing of the initial conditions or one of the dynamical system control parameters - Ref.2. Herewith, the data recovering from the received signal and noise mix in the absence a priori information about the oscillation construction method at the transmitter is the highly difficult problem, but in some cases it's practically impossible.

In previous our papers (for instance, - Ref.2) the functioning of communication network with discrete time chaotic signals was demonstrated, in the case of known full kit of elementary signals at the receiver, corresponding to each symbol of data transmitted and at presence of the external source of tact and symbol synchronization of transmitter and receiver. The block-diagram of such communication network with chaotic carrier is shown in the Fig.1 Algorithms of parameter and initial conditions reconstruction of the underlying map were offered in - Ref.3, connected with the inverse problem chaotic dynamics, in the case of the information absence about it at the receiver. However, for satisfactory functioning of the whole communication network, it is also required the information about time moments of switching between nearby symbols of message or, in other words, time unit synchronization.

We consider two methods of time unit synchronization restoration, using the received chaotic sequence in this work. They are *Fisher criterion* and *synchronous chaotic response*.

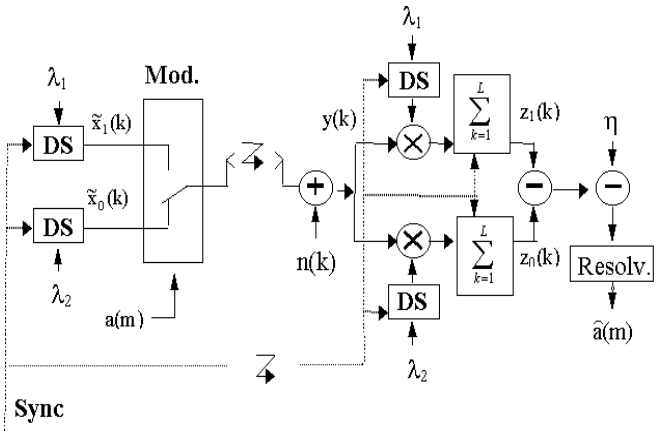

Fig.1. The block-diagram of communication network with chaotic carrier.

2. PROBLEM STATEMENT

Let's suppose for consideration a information communication system is digital. Let's choose a simplest dynamical system (DS) with a discrete time as a source chaotic carrier, that is described of one-dimensional map by the form of $x(k+1)=F[\lambda, x(k)]$, where F - nonlinear function, λ - map parameter, k = 0, 1, 2,... - discrete time. As an example we would like to consider the logistic map

$$x(k+1)=\lambda\, x(k)(1 -x(k))= F [\lambda, x(k)], \qquad (1)$$

with initial condition of $x(k=0)=x(0)$. For $0<\lambda<4$ expression (1) describes the map of unit interval points $0<x(k)<1$ to itself - Ref.3.

Discrete binary modulation method, named by *chaotic shift keying* - Ref.2, is corresponded the use for zero and unit transmission of two chaotic sequences, distinguishing by types of nonlinear functions F, map parameter λ or initial conditions x(0). Let for the example the modulation is realized by shift keying of parameter $\lambda(t)$ in (1) between two slightly distinguishing values (λ_1, λ_2), corresponding to DS chaotic modes.

Then, as it's shown in - Ref.4 and is presented in the Fig. 2 a,b, even in the absence of the noise it is practically impossible to distinguish visually the transmitted message in received chaotic signal. The measurement of statistical parameters of chaotic signal prohibits to find a fact of information transmission The mean value, dispersion and other parameters stays practically constant.

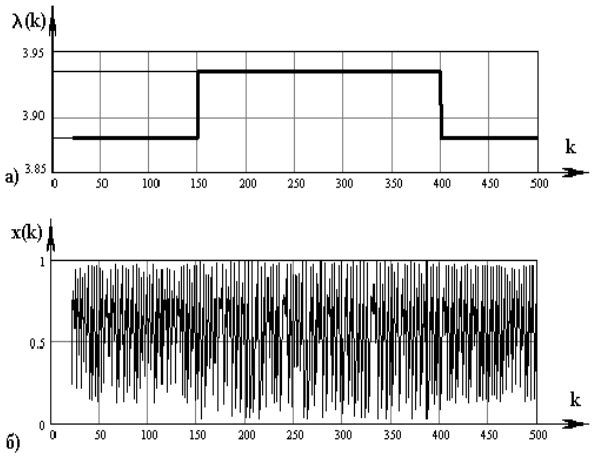

Fig. 2. Transmitted data (a) and chaotic signal (b).

However, under completely knowing information about the type and parameters of transmitter DS at the receiver, it is possible to demodulate the transmitted binary message - Ref.2. Herewith, the correlation receiver possesses the best noise-immunity. For functioning of which time unit synchronization of transmitter and receiver must be realized. Suppose that for transmission information security increasing a communication network with chaotic carrier is prevented from special synchro-channel. Then the receiver of communication network must provide a restoration of time unit synchronization. For instance, it can contains a special system of restoration of time unit synchronization (SS) presenting itself a receiver scheme, at output of which only information about time moments of the possible symbol keying instead of completely demodulated information message is presented.

In the literature, for instance in - Refs.5,6, different methods of SS designing for communications networks with harmonic carrier are described. However, many described methods such as active or passive filtration of received signal, had failed for communication networks with chaotic carrier, as far as spectrum of chaotic signal usually has complex, non-smooth form and it has not a brightly denominated spectral component at the symbol synchronization frequency. But in literature, for instance in - Refs.2,4,6, a lots of receiver designing methods for communication networks with chaotic carrier are described.

The aim of given work is a problem of time unit synchronization restoration method choice for the communication network with chaotic carrier that operates in the presence of additive noise.

3. PROBLEM SOLUTION

The Fisher's criterion use for a DS transmitter parameter perturbation detection for the first time was offered by authors of work - Ref.4.

This method idea consists of the comparison of statistical characteristics in receiver of difference of received chaotic signal and noise mix y(k) = x(k) + n(k) (were n(k) is a discrete Gaussian white noise) and its step-by-step prediction z(k):

$$z(k) = F(\widetilde{\lambda}, y(k-1)), \qquad (2)$$

in neighboring intervals ("windows") with fixed lengths N at each discrete time moment k. Here $\widetilde{\lambda}$ is a non-perturbed estimation of receiver DS parameter corresponded to λ_1 or λ_2.

A difference

$$d(k)=x(k) - y(k) \qquad (3)$$

is called as linear discriminant function - Ref.5.

If now we have calculate mean values and dispersions of signal and noise mix y(k) and its step-by-step prediction z(k) (2) difference in windows 1 and 2

$$\begin{cases} M_1(k) = \dfrac{1}{N}\displaystyle\sum_{i=k-2N+1}^{k-N} d(i) \\ M_2(k) = \dfrac{1}{N}\displaystyle\sum_{i=k-N+1}^{k} d(i) \end{cases}, \qquad (4)$$

$$\begin{cases} S_1^2(k) = \dfrac{1}{N}\displaystyle\sum_{i=k-2N+1}^{k-N} [d(i) - M_1(k)]^2 \\ S_2^2(k) = \dfrac{1}{N}\displaystyle\sum_{i=k-N+1}^{k} [d(i) - M_2(k)]^2 \end{cases}, \qquad (5)$$

then after the function

$$H(k) = \frac{(M_1(k) - M_2(k))^2}{S_1^2(k) + S_2^2(k)}, \qquad (6)$$

achieves the certain threshold (so-called "Fisher's criterion" - Ref.4) it is possible to judge about time moments of uneven parameter λ shift keying at the transmitter, that allows us to determine time moments of symbol switching. In the simplest case the half of height of maximum peaks of value H(k) can be chosen as the threshold value. At Fisher's criterion does not give information nor about the value of jump (λ_2-λ_1), nor about λ_2 and λ_1 values itself.

Disadvantage of SS, constructed on the base of Fisher's criterion, is high sensitivity of this method to the influence of noises in communication channel. So large enough errors in time unit synchronization reconstruction are

observed already at signal/noise ratio equaled to 0,0004. Procedure of time unit synchronization restoration with the help of the Fisher's criterion in presence of noise is demonstrated in Fig. 3.

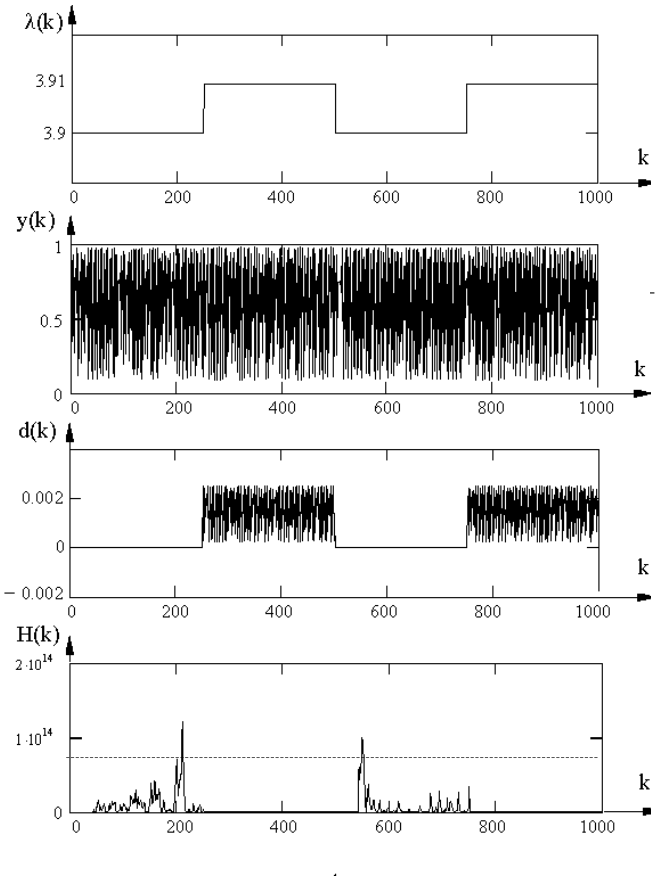

Fig. 3. The transmitted message (a), chaotic signal and noise mix (b), discriminant function d(k) realization (c), Fisher's criterion response (d).

Another method of time unit synchronization restoration can be based on the phenomenon of synchronous chaotic response - Ref.6. This algorithm is also based on the calculation of linear discriminant function d(k)=x(k) - y(k). When using this algorithm for time unit synchronization reconstruction it is necessary to conduct an averaging of data obtained and fixation of time moments of uneven changing of value d(k), as this is demonstrated in the Fig. 4. More simple algorithm of synchronous chaotic response in contrast with the Fisher's criterion greatly decreases the number of operations when processing the received signal in SS and allows to increase the noise-immunity of time unit synchronization restoration method.

For the quantitative comparison of noise-immunity of two described algorithms in the Fig. 5 there is a dependency of bit error ratio (BER) of time unit synchronization reconstruction on the signal/noise ratio σ_x/σ_n, where σ_x and σ_n accordingly standard deviations for processes x(k) and n(k), obtained by computer simulation. It's noticeably the advantage of method of synchronous chaotic response in noise-immunity.

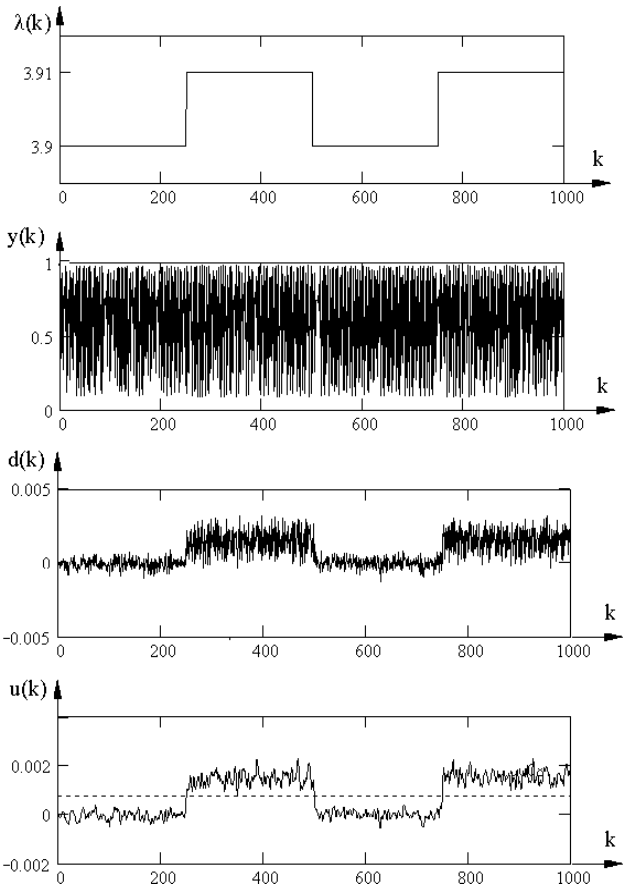

Fig. 4. The transmitted message (a), chaotic signal and noise mix (b), discriminant function d(k) realization (c), result of d(k) average(d).

4. CONCLUSIONS

Thus, the conducted study has shown better usefulness of synchronous chaotic response method in contrast with the Fisher's criterion for the construction of time unit synchronization restoration system of the receiver in communication network with chaotic carrier. As far as the signal at the output of SS possesses a denominated spectral component at the symbol synchronization frequency, for additional perfecting of SS noise-immunity a combination of synchronous chaotic response scheme with the active filter, that is based, for instance, on the phase-locked loop - Ref.7 can be used.

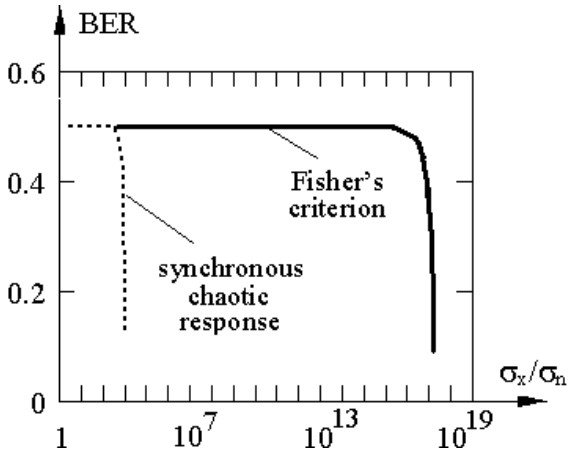

Fig. 5. The dependency of bit error ratio (BER) of time unit synchronization reconstruction on the signal/noise ratio σ_x/σ_n.

REFERENCES

1. A. S. Dmitriev, A. I. Panas, S. O. Starkov. “Dynamical chaos as paradigm of modern communication systems”. *Foreign Radio Electronics. Successes of Modern Radio Electronics*, no. 10, pp. 4-26, 1997.
2. M. V. Kapranov, V. N. Kuleshov, M. V. Larionova, A. G. Morozov, N. N. Udalov. “Features of communication systems with manipulation of parameters and initial conditions of chaotic oscillator”. *Foreign Radio Electronics. Successes of Modern Radio Electronics*, no. 11, pp. 48-62, 2000.
3. F. C. Moon. “Chaotic vibrations”. Cornell Univ., Ithaca, New York, 1990.
4. O.L.Anosov, O.Ya.Butkovskii, Yu.A.Kravtsov, et.al. “Exposure of non-stationarity of random-like signals of dynamical nature”. *Radio Engineering and Electronics.* 1995, vol. 40, no. 2, pp. 255-260.
5. M. S. Nemirovsky. “Digital information transmission in communications”. Moscow, Sviaz Publ. House, 1980.
6. Pecora L. M., Carroll T. L. “Synchronization in Chaotic Systems”. – *Phys. Rev. Letters*. 1990, vol. 64, no. 8, pp. 821-824.
7. W. S. Lindsey. “Synchronization systems in communication and control”. Prentice-Hall. Inc., Englewood Cliffs, New Jersey, 1972.