iCEST 2005 Serbia and Montenegro, Niš, June 29 - July 1, 2005

Telecommunication System with Two Kinds of Pseudo Random Sequences for Spectrum Expansion

Georgi D.Nenov, Galina P.Cherneva

Abstract – **The paper presents a method and the structure diagram of a telecommunication system where the input information spectrum expands by switching a number of pseudo random sequences. Switching is controlled by another similar sequence, the symbols of which last much longer. The system provides a high degree of protection against non-allowed access.**

Keywords – **Pseudo random sequences, spectrum expansion, protection against non-allowed access.**

I. Introduction

The protection of information is of substantial importance in different fields of modern society. It is necessary in regard to the concept of market where different economic interests oppose each other. The information protection is connected with the security of institutions and individuals.

There are different methods and means to protect information against non-allowed access. Most generally, they are based on using software and hardware resources.

The paper presents a method and a structure diagram of the telecommunication channel protection by scrambling and descrambling on two levels. On the first level this process directly concerns the primary signal, which is a carrier of information in digital kind. The second level has controlling functions in regard to the random sequences. They change in time according to a given dependency defined by a code combination.

It is known that there is a system of signal transmitting through scrambler and descrambler, which synchronize themselves each other [1]. The use of different code sequences is done by the keys K1,….Kn (Fig.1). They define the feedback in generators of random sequences, NLS (Noise like Signals).

The signal Si,, which is the information carrier, is supplied to the scrambler input. Let it consist of the lines given in Table 1. The summation by module 2 with a random sequence Ss is done in the summation device 1. The output signal Sout is obtained and it istransmitted along the line or is modulated to be transmitted along the radio line.

The dependency

$$S_{out} = S_i \oplus S_s \qquad (1)$$

where the symbol ⊕ means summation by module 2 (∑ mod 2), is valid for Sout.

Authors are with the Higher School of Transport, Geo Milev Str.158, 1584 Sofia, Bulgaria

becomes narrower in the receiver with the same kind of sequence Ss, which is synchronized as the initial signals S1, S2,…, Sn in the scrambler and the discrambler are equal, i.e. the initial conditions are S1= S2=…=Sn=1.

The fifth line in Table 1 is corresponding to output signal in the receiver S'i. If differs from Si due to noises and distortions caused with transmitting.

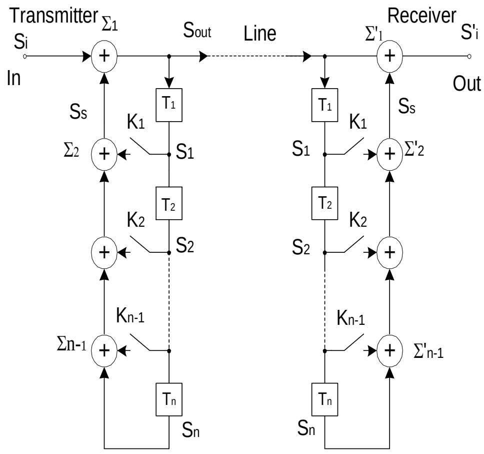

Fig.1

TABLE I

PAGE LAYOUT DESCRIPTION

1	S_i	1 1 1 1	0 0 0 0	1 1 1 1
2	S_s	1 0 1 0	1 0 1 0	0 1 1 0
3	S_{out}	0 1 0 1	1 0 1 0	1 0 0 1
4	S_s	1 0 1 0	1 0 1 0	0 1 1 0
5	S'_i	1 1 1 1	0 0 0 0	1 1 1 1
1	S_i	1 1 1 1	0 0 0 0	
2	S_s	0 1 1 1	0 1 0 1	
3	S_{out}	1 0 0 0	0 1 0 1	
4	S_s	0 1 1 1	0 1 0 1	
5	S'_i	1 1 1 1	0 0 0 0	

The summation according to module 2 of the signal along the line Sout (in that case it is an input signal for the receiver) and the elements of the sequence Ss created in the descramble is done in the summation device, i.e.

$$S'_i = S_{out} \oplus S_s \qquad (2)$$

The example shown in Table 1 is valid for a digital information signal, the symbols of which “1” and “0” are presented for clarity with a duration four times longer than the symbols of the random sequence and respectively, the same times longer than the delay T in the elements of displacing registers. The diagrams of Si and Ss from t = 0 to t = 9T are given in Fig. 2.

The protection of information against the non-allowed access is as more reliable as the pseudo-sequence Ss is longer, because it takes longer to discover it. Another disadvantage is the complex character of generators.

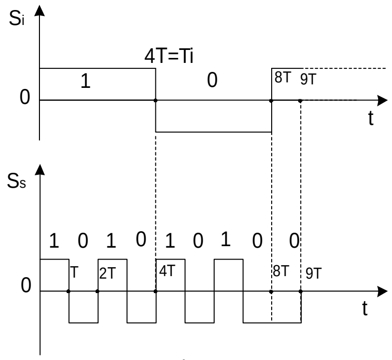

Fig.2

To improve the protectiveness, it is proposed to change the set of random sequences, which are created by switching of keys K1,…, Kn in the generators (Fig.1).

The choice of the given sequence from the set is made by a preliminary determination of correspondents.

The paper proposes to do the key control and the control on the sequences respectively using random sequence. The structure diagram of the system is given in Fig.3. The scrambler and descrambler of control are connected to the information component of the system. The interfaces are not shown to make the examination sampler. The same is made in regard to the synchronization of the two components.

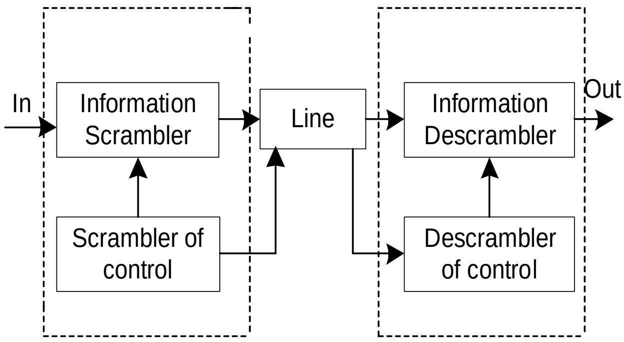

Fig.3

The initial protection of the system is provided by the information scrambler and its corresponding descrambler. Their structure is of the kind given in Fig. 1.

The controlling component contains scrambler and descrambler, the sequences of which do not need to be of full length, but symbols (elements) in them have to be of a duration many times longer than the time of switching. It means that they will change the sequences in the information component in intervals of sufficient length. It is necessary for the duration of a symbol or a code combination of the "controlling" sequence to be multiple number of times longer than the duration of a information" sequence

The prerequisites outlined can be reduced to the following quantity dependencies necessary for designing.

1. The duration T of a symbol of the random sequence Ss depends on the information transmitting and the channel flow capacity.

2. With examining the processes in real time, the duration of one symbol of the information sequence Si, i.e. Ti is of primary importance. As it is shown in Fig. 2, the condition Ti>>T should have been kept. It is quite indefinite and is kept with a ratio of Ti/T from several times to several orders, which can conditionally be expressed by the sign of multiplication (x) in the following way:

$$\frac{T_i}{T} = \times 1 \div 10^m; (m = \times 1) \qquad (3)$$

3. The other obligatory relation is between the length of the information random sequence Ss, which serves to expand the signal spectrum (carrying vibration) and the duration of the random sequence with a control function Sc. With using simple generators, they are respectively:

$$M_i = 2^i - 1 \text{ and } M_c = 2^c - 1 \qquad (4)$$

For this and other types of generators it is necessary to keep a requirement similar to (3),i.e

$$\frac{M_c}{M_i} >> 10^m; (m = \times 1) \qquad (5)$$

The satisfaction of the conditions (3) and (5) ensures system normal functioning.

The big values of *m* in (3) are favourable against the distortions of impulses in line Si. The effect towards the protection against the non-allowed access depending on *m* in (5) is reverse.

The method proposed is characterized with the following advantages in relation to the already-known methods of protection against the non-allowed access with information transmitting in the expanded spectrum systems.

1. The secret feature (protection) is ensured by two levels of random sequences, which extremely increases the degree of entropy. Hence it reduces the probability of access.

2. The main system components are well known and tested in practice.

3. There is no need of sequences with big length and using generators of more complicated structure.

The disadvantage of the system is the necessity of elements for coordinating and
synchronizing the information and control components of the system.

The method can be applied to the modern telecommunication systems of expanded spectrum with high requirements related to the protection of information against non-allowed access.

REFERENCES

[1] P. Watson, K. C. Gupta, "EM-ANN Models for Microstrip Vias and Interconnects", *IEEE Trans., Microwave Theory Tech.*,vol. 44, no. 12, pp. 2395-2503, 1996.

[2] Stallings W., *Wireless Commu-nications and Networking*, Prentice-Hall, 2002.

[3] Goiser Alois M.J., *Handbuch der Spread Spectrum Technik*, Wien – New York,1998

[4] Skler, B., *Digital Connection*, M., Williams, 2003 (in Russian)

[5] *Noise-Like signals in thesystems of transmitting infor-mation*, edited by. V.B. Pestryakov, M., Soviet Radio, 1973 (in Russian)