Synchronization system in wireless sensor networks of oil and gas complex

Dmitry Onyshko[1], *Dmitry* Fugarov[2,*], *Olga* Purchina[2], *Anna* Poluyan[2], *Nikolay* Rasteryaev[2], and *Tatyana* Skakunova[2]

[1]South-Russian State Polytechnic University (NPI) named after M.I. Platov, Novocherkassk, Russia
[2]Russian Don State Technical University, Rostov-on-Don, Russia

Abstract. The aim of this work is to study the synchronization system in wireless sensor networks of remote objects of the oil and gas complex. The objective of the study is to ensure the timely collection of reliable information about the parameters of the process. In the course of the study, methods of theoretical circuitry and mathematical modeling were used, in particular, regression and analytical models, methods of probability theory and mathematical statistics using MathCad and Matlab software packages. The conducted studies indicate a high vulnerability of the radio links of the infocommunication system for monitoring the parameters of remote objects of the oil and gas complex from attacks on the synchronization system when using deterministic synchronization signals in it. The results achieved allow us to provide the specified requirements for reliability and timeliness when deploying modern wireless sensor networks in the oil and gas industry.

1 Introduction

Recently, large oil companies have been introducing new technologies that are aimed at improving the efficiency and safety of the process while reducing overall costs. These technologies allow you to effectively manage more complex equipment in compliance with all necessary regulatory requirements. Many elements of such equipment, as well as technological processes require constant monitoring of parameters by the maintenance staff. However, such monitoring is usually very inert and inaccurate due to the degree of the human factor influence.

The most effective is the use of continuous and automated monitoring of equipment elements, which ensures a reduction in the number of errors, and also allows for the implementation, under certain conditions, of a continuous flow of information about the current state of an object. In addition, modern technologies make it possible to ensure a high transmission rate of such information, thereby increasing its efficiency. To automate the monitoring of technological processes, wireless sensor network technologies are increasingly being used on the components of the oil and gas complex infrastructure [1].

A wireless network sensor is a miniature computing and communication device, which consists of a processor, memory, digital-to-analog and analog-to-digital converter, radio

* Corresponding author: ddf_1@mail.ru

frequency transceiver, power supply and sensor. The type of sensor depends on the monitored parameter at the facility and its connection can be realized via digital or analog interfaces. The network sensor is used only for collecting, preprocessing and transmitting primary data.

The main processing of the sensor network information is performed on a node or gateway, implemented as a computer. The network sensors exchange data with each other using built-in transceivers of a certain radio range. Thus, data is transmitted from one sensor to another according to a predetermined topology, and, ultimately, sensors close to the node transmit the final data array to it. At the same time, if some of the sensors fail, then the network continues to work after its reconfiguration (fig. 1).

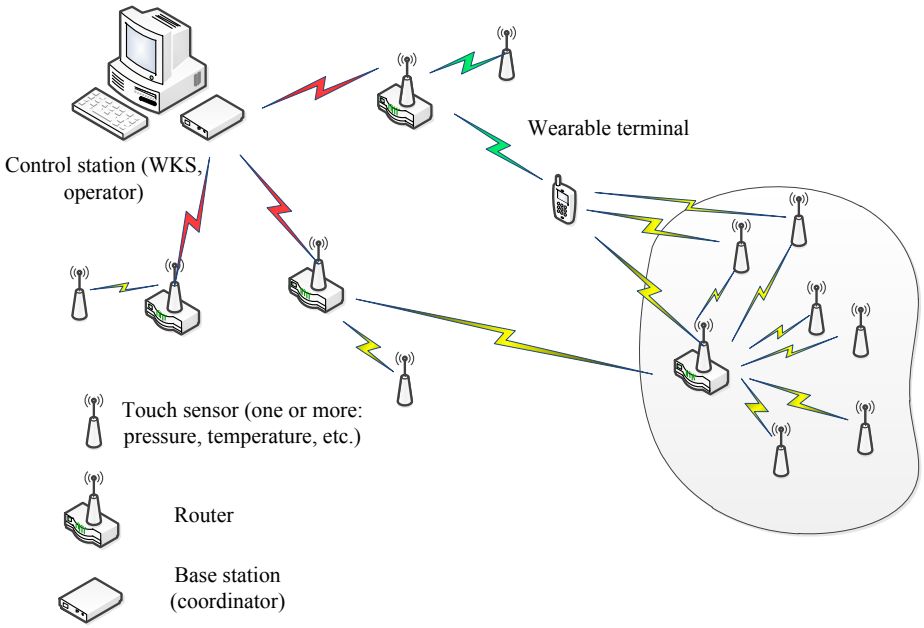

Fig. 1. General monitoring scheme.

Wireless sensor systems are built taking into account the requirements of international standards governing the protocols of physical, channel, as well as network levels of information transmission lines. At remote technological facilities, monitoring sensors with interfaces are installed, which are the “lower level” of the wireless monitoring system (fig. 2). The key elements of the top level are the WKS (workstation) and server [2].

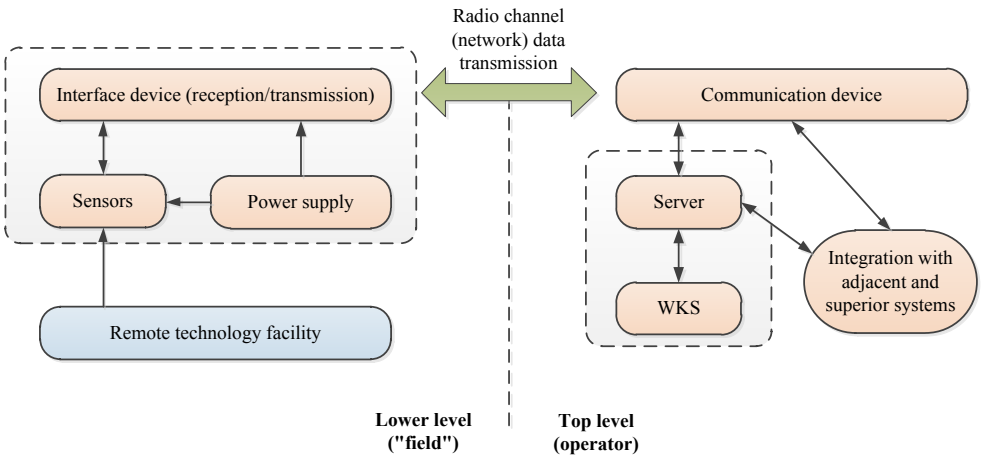

Fig. 2. General monitoring scheme.

The confidentiality of information on the network is achieved by using appropriate authentication algorithms and message encryption.

2 Materials and methods

The model for ensuring the confidentiality of information in the monitoring system is presented below, see fig. 3. Base station A transmits messages to station B.

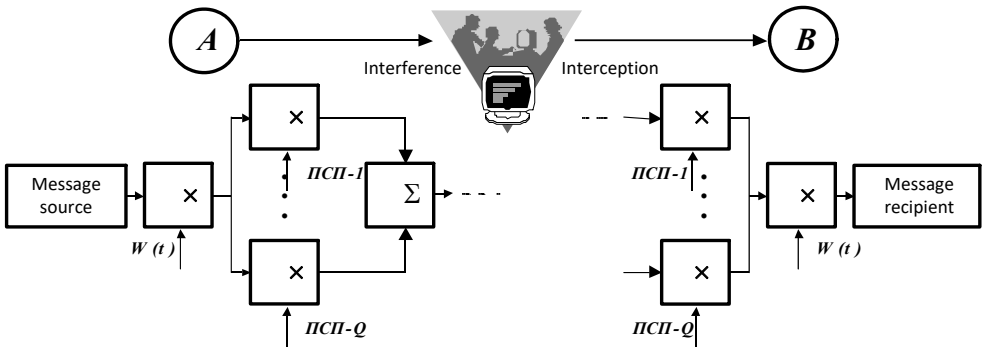

Fig. 3. Model for ensuring the confidentiality of information in the monitoring system.

The main disadvantage of sensor-based radio systems compared to wired systems is their increased vulnerability to various attacks aimed at disrupting the operation of the radio link [3-5]. This disruption of work can manifest itself in a breakdown of synchronization, or the imposition of false modes and algorithms for its operation. In addition, the purpose of the attacks may be a violation of the distribution of information flows, disruption of the implementation of services, etc.

Let us evaluate the effects of deliberate interferences on communication synchronization systems in the form of simulating false clock signals.

Consider a wireless communication system in which clock signals of known structure are used for synchronization. In this case, the jammer is able to detect the sync sequence, scout its structure and generate a similar one with a probability close to unity. As indicators of the effectiveness of functioning, we choose the following:

- probability of timely transmission of messages $h(s)$;
- average message transmission time $\bar{t}_{tr}$;

– the probability of sending messages in a time not more than specified $P(\bar{t}_n \leq T'_K)$.

To assess the impact results, we apply the method of stochastic network analysis [6–9]. Suppose there is a radio line that provides information transfer and reception of confirmations. The jammer imitates false synchronization modes in order to disrupt the exchange of information.

Consider the case when the simulation of synchronization interference by the jammer is carried out with probability P. If the jammer does not carry out an attack on the radio line, then the message is transmitted in a random time t_{tr} with the distribution function:

$$B(t) = 1 - e^{-\mu t}\,, \tag{1}$$

$$\mu = \frac{1}{\bar{t}_{tr}}\,, \tag{2}$$

where $\bar{t}_{tr} = \frac{\bar{V}}{R_{op}}$ - average transmission time in the absence of interference; $\bar{V}$ - average volume of transmitted messages; R_{op} - operational transmission rate.

Otherwise, the communication line is recovered in a random time t_{rec} and by the distribution function $\Delta(t)$:

$$\Delta(t) = 1 - e^{-dt}\,, \tag{3}$$

where $d = \frac{1}{t_{rec}}$; $\bar{t}_{rec}$ - the average recovery time of the communication line.

If attacks in the form of a simulation of a false sync sequence are active in a radio communication line, the stochastic network of the process of its functioning will have the form shown in Figure 4. The indicated network consists of vertices that mean logical operations and directed branches. The vertex in the stochastic model consists of input and output functions. An input such as an exclusive "OR" ⋈ means that any branch that leads to a given vertex can be implemented, but one and only one of the branches can be implemented at a given time. A probabilistic exit ▷ means that after the vertex is implemented, only one branch is selected [6].

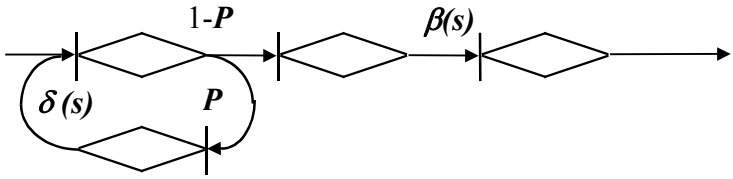

Fig. 4. A stochastic network of the process of a communication line functioning in conditions of simulation of false sync sequences.

For the considered radio link, the equivalent function of the stochastic network has the form [9-12]:

$$h(s) = \frac{1-P}{1-P\delta(s)}\beta(s)\,, \tag{4}$$

where $\beta(s) = \int_0^\infty e^{-st}\, d[B(t)] = \mu/(\mu + s)$ – Laplace-Stieltjes transform of the distribution function of the information transmission time; $\delta(s) = \int_0^\infty e^{-st}\, d[\Delta(t)] = d/(d + s)$ – Laplace-Stieltjes transform of the distribution function of the recovery time.

Omitting the intermediate transformations, we obtain the formula for the probability of timely transmission of messages:

$$h(s) = \frac{(1-P)(1+\bar{t}_{rec}s)}{(1+s\bar{t}_{rec}-P)(1+s\bar{t}_{tr})} = \frac{\bar{t}_{ag}(\bar{t}_{ag}+\bar{t}_{rec})(1-P)}{(\bar{t}_{ag}+\bar{t}_{rec}-P\bar{t}_{ag}+\bar{t}_{tr})}, \quad (5)$$

where $s = 1/\bar{t}_{ag}$; $\bar{t}_{ag}$ - average aging time of information; P - the probability of entering false information, defined as the product of the probability of a radio link availability to entering false information P_{en} and the probability of temporary contact P_{tc}.

3 Results

The dependences of the probability of timely information transmission on the probability of simulating a false sync sequence for various $A = \bar{t}_{tr}/\bar{t}_{ag}$ are shown in figure 5.

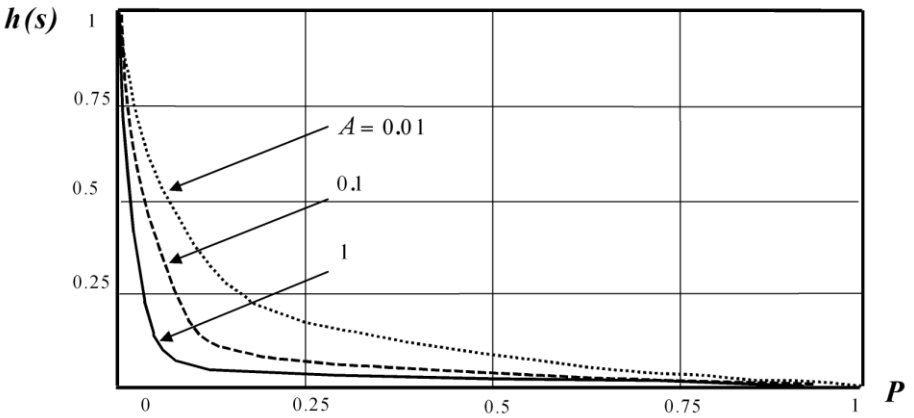

Fig. 5. Graphs of the probability of timely message transmission on the probability of simulating a false sync sequence.

The average transmission time is the first-order moment from $h(s)$. Having made the necessary transformations, we obtain the formula:

$$\bar{t}_n = \bar{t}_{tr} + \bar{t}_{rec}\frac{P}{1-P}. \quad (6)$$

The probability of transmission messages in a time not more than specified is determined by the formula:

$$\left(\bar{t}_n < T'_{sp}\right) = \begin{cases} \frac{(\bar{t}_{tr}+\bar{t}_{rec})(1-P)}{\bar{t}_{tr}(1-P)-\bar{t}_{rec}}\left[1 - exp\left\{-T'_{sp}/\bar{t}_{tr}\right\}\right] - \\ \frac{\bar{t}_{tr}P}{\bar{t}_{tr}(1-P)-\bar{t}_{rec}}\left[1 - exp\left\{-\frac{1-P}{\bar{t}_{rec}}T'_{sp}\right\}\right] \\ if\ \bar{t}_{tr}(1-P) - \bar{t}_{rec} > 0 \\ 0, if\ \ \bar{t}_{tr}(1-P) - \bar{t}_{rec} \le 0 \end{cases} \quad (7)$$

4 Discussion

The graphs of the dependence of the transmitting information probability at a specified time for various probabilities of simulating a false sync sequence, constructed in accordance with the above formula, are presented in figure 6.

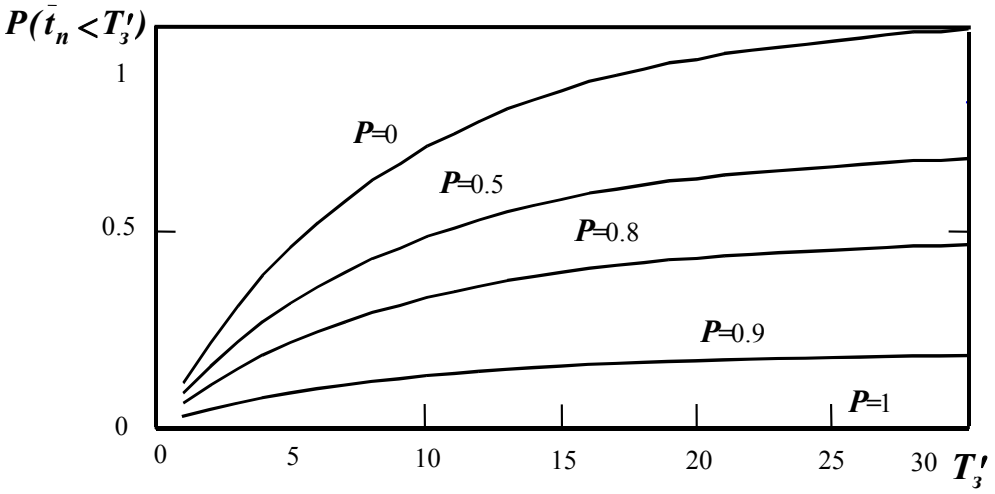

Fig. 6. Graphs of the dependence of the transmitting information probability at a specified time for different probabilities of simulating a false sync sequence.

As a result of the analysis of the dependencies shown in figures 5 and 6, we can draw the following conclusions:

– the use of well-known sync sequences structure in radio lines makes it much easier for the jammer to detect them and generate a false sync sequence with high probability. This leads to a significant reduction in the noise immunity of the radio link;

– the simulating a false sync sequence leads to a significant reduction in the probability of timely transmission. So, if the simulation probability is not lower than 0.5, the probability of timely transmission does not exceed 0.1 for A = 0.01, which practically disrupts the process of transmitting information in a radio link;

– the effect of deliberate interference at high probabilities of simulating a false sync sequence leads to a significant increase in the average transmission time of information, since the radio link goes into the continuous reception and analysis of false sync sequences;

– the possibility of simulating a false sync sequence with high probability leads to a significant decrease in the probability of transmitting information at a specified time. So, if the simulation probability is not lower than 0.8, the probability of transmitting information at a specified time does not exceed 0.5;

– the analysis indicates a high vulnerability of the radio links of the infocommunication system for monitoring the parameters of remote objects of the oil and gas complex from attacks on the synchronization system when deterministic synchronization signals are used in it. Providing the specified probabilistic - temporal characteristics of information transfer under attacks on the synchronization system requires additional measures aimed at significantly reducing the probability of simulating false clock signals, for example, using pseudo-random structure signals for synchronization [6,7].

Recently, methods based on pseudo-random sequences have been actively used for synchronization systems. The most effective in the conditions of attacks on the synchronization system are pseudo-random M-sequences (pseudo-random sequences of the maximum period), which are built on the basis of digital shift registers with feedbacks [13-16]. To form the M-sequence, the following recurrence formula is used:

$$a_0 \cdot d_j = a_n \cdot d_{j-n} \oplus a_{n-1} \cdot d_{j-(n-1)} \oplus \dots a_2 \cdot d_{j-2} \oplus a_1 \cdot d_{j-1}\,, \qquad (8)$$

where d_j - the j-th element of the M-sequence, which is obtained by using the exclusive "OR", connected to the elements of the register, for which the coefficients are 1.

It is known that a linear recursive register forms a sequence of maximum period in the case of an irreducible primitive polynomial. In this case, the period of the pseudo-random sequence (M-sequence) equals

$$L = 2^n - 1\,, \tag{9}$$

where L — sequence period: n — order of the generating polynomial.

5 Conclusion

Improved synchronization of remote monitoring systems of oil and gas facilities based on M-sequences is characterized by the following features and advantages:

— there is no preliminary quantization of the signal, which leads to the loss of some part of the data array;

— there is analog-to-digital signal processing;

— the next element is predicted based on the recursive properties of the pseudo-random sequence;

— the calculation of the estimated values of the pseudo-random sequence elements is carried out both within the clock intervals and at their borders.

These properties lead to an increase in the probability of the correct reception of a pseudo-random sequence element and thereby reduce the time of entering synchronism.

References

1. D.D. Fugarov, Y.Y. Gerasimenko, J. Phys. Conf. Ser **1118**, 012055 (2018). DOI:10.1088/1742-6596/1118/1/012055
2. A.V. Sedov, D.A. Onyshko, *Proceedings of 2017 IEEE East-West Design and Test Symposium, EWDTS 2017*, 8110141 (2017). DOI: 10.1109/EWDTS.2017.8110141
3. Y.O. Chernyshev, Journal of Theoretical and Applied Information Technology **80(1)**, 13-20 (2015)
4. D.D. Fugarov, J. Phys. Conf. Ser **1333**, 062020 (2019). DOI:10.1088/1742-6596/1333/6/062020
5. A.Y. Poluyan, J. Phys. Conf. Ser. **1015**, 022013 (2018). DOI:10.1088/1742-6596/1015/2/022013.
6. A.V. Sedov, D.A. Onyshko, S.M. Lipkin, *2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016 - Proceedings*, 7911481 (2019). DOI: 10.1109/ICIEAM.2016.7911481
7. K.Y. Solomentsev, J. Phys. Conf. Ser **1015**, 032179 (2018). DOI :10.1088/1742-6596/1015/3/032179
8. A.Y. Poluyan, J. Phys. Conf. Ser **1333**, 032056 (2019). DOI:10.1088/1742-6596/1333/3/032056
9. A.V. Sedov, M.S. Lipkin, S.M. Lipkin, D.A. Onyshko, N.A. Lytkin, N.V. Rarova, *AIP Conference Proceedings* **1623**, 551-554 (2014). DOI: 10.1063/1.4901498
10. V.I. Lachin, K.I. Solomentcev, Q.U. Nguyen, A.L. Yufanova, I.G. Balaban, *International Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings*, 7147120 (2015). DOI:10.1109/SIBCON.2015.7147120

11. V.S. Elsukov, V.I. Lachin, O.Y. Demidov, *International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2019*, 8743032 (2019). DOI:10.1109/ICIEAM.2019.8743032
12. A.Y. Poluyan, J. Phys. Conf. Ser **1333**, 032057 (2019). DOI:10.1088/1742-6596/1333/3/032057
13. Y.O. Chernyshev, Journal of Theoretical and Applied Information Technology **81(3)**, 466-473 (2015)
14. D.A. Plotnikov, V.I. Lachin, K.Y. Solomentsev, *IOP Conference Series: Materials Science and Engineering* **463(3)**, 032060 (2018). DOI:10.1088/1757-899X/463/3/032060
15. A.I. Klimenko, V.I. Lachin, Y.A. Kolosov, S.V. Gvetadze, Middle-East Journal of Scientific Research **20(12)**, 2090-2093 (2014). DOI:10.5829/idosi.mejsr.2014.20.12.21092
16. K.D. Savvina, V.A. Kucherov, S.G. Yanvarev, K.Y. Solomentsev, D.D. Savvin, *International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2019*, 8934874 (2019). DOI: 10.1109/FarEastCon.2019.8934874