Intelligent decision - making support on the level of encryption of information transmitted in the UMV information exchange channels

D V Moiseev, A A Bryukhovetskiy and A V Skatkov
Sevastopol state university, 33 Universitetskaya str., Sevastopol, Russia, 299053

E-mail: dmitriymoiseev@mail.ru

Abstract. The paper considers the solution of the interdisciplinary fundamental scientific problem of ensuring the reliability and high throughput of information exchange channels (IEX) between unmanned vehicles (UMV) located in different environments and dispatch centers (DC) of the "smart city". The solution of the management problem of providing a reliable and high-bandwidth IEX between UMV and DC in different environments requires the development of an intelligent decision support system to select the level of encryption of information transmitted over open communication channels, under conditions of uncertainty.

1. Introduction

The active development of new information technologies and the concept of creation of basic elements of Autonomous artificial intelligence, as well as significant technological progress in the field of creation and active use of unmanned vehicles requires the development of new specific methods of applied mathematics and computer science: modeling and decision-making under uncertainty and risks, stochastic vector programming, methods for solving integer and nonlinear problems of mathematical programming, operations research in fuzzy formulation, use of probabilistic evaluation criteria. Based on the principles of network-centric management today, many leading countries of the world are actively developing mixed robotic groups that interact in a single information and control space, which, in turn, requires the implementation of information exchange channels (IEX) between unmanned vehicles (UMV) and dispatch centers (DC) located in different environments with high reliability and throughput [1-2].

Modern UMV can be fully attributed to the class of globally moving objects that can be located at a great distance from the DC, which requires the solution of the problem of sustainable delivery of control information on IEX with variable parameters in the conditions of destabilizing effects of natural and artificial nature.

To solve the problem of managing mobile and remote (located in remote areas) objects, such as UMV space, air, sea and land-based, radio communication is of paramount importance. However, the impact of natural and artificial nature of the aggressive environment on the radio link and control channels in different physical environments including underwater, greatly reduce the efficiency of Information exchange and control channels, so finding ways to integrated use of diverse communication channels is an important and urgent task, which requires modernization of the principles of organization, management of UMV (including being in a mixed group with a common
mission) on the global distance from DC. The development and improvement of radio communications is possible by wide use of modern achievements in the field of information technologies: concepts and algorithms "programmable radio" (SDR—Software-Defined Radio), a new paradigm of wireless communications—cognitive radio (CRS Cognitive Radio System), capable to define the best spectral position for communication, creating a minimum interference to other users; efficient modulation techniques and coding, etc. [3 – 7].

The implementation of advanced technologies requires a significant increase in computational procedures, especially for communication equipment designed to work in channels with variable parameters. This, in turn, leads to the need to modernize existing and create new highly efficient automated radio communication and radio monitoring systems with complex algorithms of functioning and information processing, which can be implemented using the apparatus of artificial neural networks (NS), expert systems (ES), fuzzy logic systems, training systems with reinforcement [8-12]. In the channels of information exchange between the UMV and DS implemented a large amount of computational procedures caused by the processing of large amounts of input, in parallel to the information received, and when partially distorted or missing data about the object, which is typical in the case of handling information on the background noise (natural and man-made interference) on the channel with variable parameters.

Special attention should be paid to the development of a set of models of classification of information situations arising in the performance of tasks of information exchange between UMV and DC. This will allow decision makers (LPR) to support decision-making on the choice of one of the alternative strategies when solving problems, in case of conflict situations in the data transmission environment, and thus maintain a reliable level of quality of IEX between UMV and DC.

Correlation signal processing is used to increase the noise immunity of the IEX, and encryption devices are introduced into the IUS to increase the crypto stability [13 – 14], which also leads to a significant complication of computational algorithms and an increase in hardware costs. Despite the rapid improvement of production technology and the element base, the development of domestic computer equipment (CE) does not yet meet the new requirements and challenges facing the IEX, especially due to the import substitution of chips and the element base in the conditions of sanctions. The present period of development of theoretical positions, methods and algorithms of synthesis devices W used in the development of advanced and improvement of existing IEX between UMV and DC, is characterized by intensive search for new principles of processing and storage of information, computational architectures and systems using modern technologies, including technology for probabilistic representation and transformation of information (PRTI) is one of the most promising. The implementation of computing devices (CD) performing arithmetic and logical operations on the probabilistic mapping (PM) leads to a multiple decrease in the hardware volume of the CD, and the PRTI itself provides noise immunity and cryptographic stability of the processed and transmitted information [15-20].

Problem statement. It is known that the use of probabilistic form of information representation allows to take advantage of not only known advantages, such as relatively small hardware volume, the ability to function in real time, increased noise immunity, but also an additional advantage expressed in the form of cryptographic protection of data represented by PM [15-20].

The principal possibility of nonlinear probabilistic transformation with a variable number of independent statistical tests of each value of the original signal, presented in analog or digital form, allows in parallel with the signal processing to carry out its cryptographic protection. Important in this case is the fact that cryptographic signal processing can be performed simultaneously with any other type of transformation. Indeed, the mathematical expectation of the probabilistic mapping is equal to the ordinate value of the integral distribution law of the auxiliary random signal $F_{X_i}(R)$ at the comparison level $X_i$: 
\[
M[Y_i(t)] = \sum_{l=1}^{2} y_{ij}P_l = P(y_{ij} = 1) = P[R_i(t) < (x_i = r_{ij})] = F_{X_i}(R). \quad (1)
\]

Since a consistent, unbiased and asymptotically effective estimate of the mathematical expectation, according to Chebyshev’s theorem, is the average value of the probabilistic map terms
\[
\{M[Y_i(t)]\}^* = \left[ F_{X_i}(R) \right]^* = \frac{1}{K}\sum_{j=1}^{K}y_{ij}, \quad (2)
\]
that for protection of information from unauthorized access it is necessary to make nonlinear unipolar probabilistic transformation of the initial information presented either in analog, or in discrete digital forms that the person who is not allowed to this information, had no data on the law of distribution of the auxiliary random signal and quantity of independent statistical tests of each transformed value of the initial information. On converted so the original signal can be performed the arithmetic and logical operations, operations, telecommunications, etc. To reverse the conversion to a digital code or to an analog signal in accordance with the expression for mathematical expectation, it is necessary to determine the estimate of the mathematical expectation of the display and by functional conversion go to the desired one.

![Figure 1](image_url). Structure of the simplest probabilistic cryptomodem.

Then the structural and functional scheme of the simplest probabilistic cryptomodem will take the form shown in Figure 1. Information that is subject to cryptographic protection, is fed to a nonlinear probabilistic transducer, the output of which is a probabilistic mapping, which in this case is a coded signal through a communication channel is served in the counter-integrator, which is added To cycles, then the estimate can be rewritten \{ \{F_{X_i}(R)\}^* \} in a functional Converter, where knowing the value of K and the distribution of the auxiliary random signal and is decoding. Interception of probabilistic display in the communication channel and search of all possible values of K with the corresponding analysis allows to decrypt the message for finite time only at the known uniform law of distribution of an auxiliary random signal \( R(t) \). With any other continuous distribution law \( R(t) \), the problem becomes practically insoluble, since the shape of the curve of the distribution law is unknown.

For the case where the auxiliary random signal \( R(t) \) obeys the normal law, using the Laplace function, one can present an expression for the integral normal distribution law as:
\[
F(R) = 0.5 \left[ 1 + \Phi \left( \frac{r - m_r}{\sigma_r} \right) \right], \quad (3)
\]
where $m_r$ and $\sigma_r$ – is the expectation and the mean square deviation of the auxiliary random function $R(t)$.

The transformation of this expression, taking into account the evaluation of the integral distribution law, will give:

$$
\Phi(\xi) = \frac{2}{K} \sum_{j=1}^{K} y_{ij} - 1,
$$

(4)

where $\xi = (x_i^* - m_r) / \sigma_r$.

In the next step, using the tables for the probability integral, is determined $\xi$, and then by functional conversion is performed decryption of the encoded signal in accordance with

$$
x_i^* = \xi \sigma_r + m_r.
$$

(5)

You can imagine a situation where the number of receipts equal numbers to the communication channel (with a certain $K$) and their correlation with the probability of occurrence of certain symbols in an arbitrary language will allow using a fairly powerful computer for the final time to determine the curve shape of the distribution law. Even in this worst case, the lack of correlation between the number of tests $K$ and the law of distribution of the auxiliary random signal $R(t)$ allows sufficiently reliable protection of information from unauthorized access. However, for a greater increase in cryptographic stability, the option of introducing another key into the protection algorithm may be considered. In a one line unipolar representation of the factors and the expression for their product in the form of probability maps can be represented as:

$$
M[Y_a(t)Y_b(t)] = F_a(R)F_b(R) \approx \frac{1}{K} \sum_{j=1}^{K} (y_{aj} \& y_{bj}).
$$

(6)

If only the symbol $a$ is subject to cryptographic protection, and the cofactor, which is not subject to cryptographic protection, is represented as a linear probability map by transformation using an auxiliary random signal having a uniform distribution law of instantaneous values:

$$
F_b(R) = \begin{cases} 
0 & \text{при } r < 0 \\
r & \text{при } 0 \leq r \leq 1 \\
1 & \text{при } r > 1 
\end{cases},
$$

(7)

then by performing simple transformations for this case we have:

$$
\Phi(\xi^*_a) = \frac{\sum_{j=1}^{K} (y_{aj} \& y_{bj}) - 0.5 \sum_{j=1}^{K} y_{bj}}{\sum_{j=1}^{K} y_{bj}}.
$$

(8)

hence, according to the already considered method, it is determined $a^*$. It is almost impossible to provide for unauthorized decryption operations in accordance with the last expression (or similar) under other laws of distribution.

Thus, the representation of information in discrete probabilistic form and the execution of arithmetic and logical operations on probabilistically represented operands can be combined with cryptographic protection of the processed information almost without additional hardware costs, and the degree of protection can vary by using different numbers of keys.
Interception of probabilistic mapping in the communication channel and search of all possible values of K with the corresponding analysis allows to decrypt messages for finite time only at the known uniform distribution law of the auxiliary random signal $R(t)$.

It becomes obvious that in order to improve the cryptographic stability of information presented in the form of PM, it is necessary to increase the number of statistical tests $T_o$, which, in turn, will lead to a significant increase in the time spent on direct and reverse probabilistic transformation of information. Currently, there are no intelligent decision support systems that allow the decision maker (LPR), depending on the activity intensity of recognition of traffic qualitative changes $\xi$, choose the appropriate value $K$ - the number of statistical tests, at the same time is an indicator of the cryptographic strength of probabilistic codes.

2. Method of solution

The purpose of this work is to study the possibilities and technical ways to create a system of intellectual decision support for the choice of the level of encryption of information transmitted over open communication channels, depending on the criticality of the IEX. The solution of the mentioned tasks on the basis of technology of intellectual processing of data, in contrast to the known, is aimed at improving the validity, reliability and efficiency of the processes of decision-making support ensures enhanced reactivity is based on the use of big data technologies that, unlike other methods of expert estimation, improves the accuracy and quality of the offered range of values $K_j$ – cryptographic strength of the probabilistic codes depending on the intensity of recognition of traffic qualitative changes $\xi_i$.

Figure 2 presents a General matrix of decision-making changes in the level of cryptographic resistance depending on the recognition of traffic qualitative changes.

| $K$ | $\xi$ | $\xi$ | $\xi$ | $\xi$ | $\xi$ | $\xi$ |
|-----|-------|-------|-------|-------|-------|-------|
| $K_{min}$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ |
| ... | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ |
| $K_j$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ |
| ... | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ |
| $K_{max}$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ | $\$i$ |

Figure 2. LPR decision Matrix on changing the level of cryptographic strength.

It becomes obvious the need to track changes in the intensity of recognition of traffic qualitative changes for a certain time period $T_{1}=\{ T_1, T_2, ..., T_n \}$.

With a fairly General formulation of the problem, we are talking about the need to compare two samples of the results of observations on the intensity of recognition of traffic qualitative changes in order to identify the significance of its qualitative change. The set of observations is a set of measurements - a set of samples [16-18]:

$$X = \{X_1, X_2, ..., X_n \},$$

where

$X_i = \{\xi_1, \xi_2, ..., \xi_V \}, \xi_i$ – the intensity of electronic warfare,

$n$ – number of samples,

$V$ is the volume of each sample.

It is proposed to use the Kulbak information measure to assess changes in the intensity of recognition of traffic qualitative changes [16-18].
The question is whether the differences observed in two of the n samples between Xp and Xq based on the evaluation of the Kulbak information measure can be considered significant or significant, or whether the differences between them should be attributed to the random dispersion of the values of the studied trait [16].

The Kulbak information measure (Kulbak distance) of the Xp distribution with respect to Xq is calculated according to rule (10) [19-20]:

$$D(X_p \parallel X_q) = \sum_{i=1}^{r} p_i \log \frac{p_i}{q_i},$$

where and probabilities of hit of values of samples Xp and Xq respectively in r-interval.

The Kulbak distance of the Xp distribution with respect to Xq can be estimated as:

$$D(X_p \parallel X_q) \leq Q \rightarrow \text{no J-effect},$$

$$D(X_p \parallel X_q) > Q \rightarrow \text{observation of J-effect},$$

Where Q – is the limit value of the distance depending on the criticality of the protected information.

The obtained results allow us to state that the application of the model on the basis of the Kulbak information measure allows to provide statistical stability [18-21] of recognition of traffic qualitative changes.

The use of the proposed method allows LPR from the complete decision matrix (see figure 2) to use only those values of the cryptographic stability parameters of probabilistic codes-Kj, which correspond of recognition of traffic qualitative changes - $\xi_i$, during monitoring T (figure 3).

| $\xi_1$ | $\xi_2$ | $\bar{\xi}$ | $\xi_{i+1}$ | n  |
|--------|--------|-------------|-------------|----|
| $K_{min}$ |        |             |             |    |
| ...    |        |             |             |    |
| $K_j$  | $(K_j, \xi_1)$ | $(K_j, \xi_2)$ | $(K_j, \bar{\xi})$ |    |
| $K_j+1$| $(K_j+1, \xi_1)$ | $(K_j+1, \xi_2)$ | $\bar{\xi}$ |    |
| ...    |        |             |             |    |
| $K_{max}$ |        |             |             |    |

**Figure 3.** Matrix of decision-making LPR about changing the level of cryptographic strength taking into account.

This, in turn, leads to a decrease in hardware and time costs for the protection of information transmitted over open/closed communication channels, presented in the form of PM (figure 4).
Figure 4. Pareto domain of solutions for hardware-time cost dependence on cryptographic stability of probabilistic codes.

From the presented figure it follows that the work of the intelligent decision support system to select the level of encryption of information transmitted over open / closed communication channels leads to a decrease in hardware and time costs.

3. Conclusions
Data streams of different structure, intensity and degree of detail, which are generated by geographically distributed sources: technical means of intelligence, intelligence data, etc. act as initial information for the formation of control actions that determine the complexity of the encryption systems used and key lengths. In this regard, there is a need to develop intelligent solutions to find a balance between cryptographic stability and hardware-time costs for encryption/decryption of information, based, inter alia, on the theory of self-organizing systems. The proposed system of intellectual decision-making support for the choice of the level of encryption of information transmitted through open communication channels, of recognition of traffic qualitative changes can significantly improve the quality and reliability of decisions taken by the LPR and use only those values of the cryptographic strength of probabilistic codes -Kj, which correspond to the recognition of traffic qualitative changes. – \( \xi \), thereby increasing the efficiency of cryptographic and steganographic protection of information transmitted over open/closed communication channels in terms of hardware and time costs. The use of PRTI allows to implement a closed communication channel and increase the cryptographic stability of the messages transmitted over it while reducing the hardware volume of the encryption and decryption device tenfold while simultaneously detecting and correcting multiple errors in the transmitted message. The use of a probabilistic format allows encryption of transmitted messages, which provides a guaranteed block unauthorized access to information that will enhance operational and technical-economic indicators IEX – reliability, strength and immunity.

Acknowledgments
This work was supported by the Russian Foundation for Basic Research (projects № 19-29-06015/19, 19-29-06023/19, 18-37-00406).

References
[1] Arzumanyan R 2008 Theory and principles of network centric wars and operations The 21st century 2 66-126
[2] Skatkov A V, Voronin D Yu and Moisseev D V 2017 Analysis of basic strategies of distribution of computational resources of the control system in "network-centric" conflicts, Actual problems of development and operation of rocket-artillery, special weapons and marine equipment (Sevastopol: PMSMU) pp 189-198
[3] Pikolashin Yu L, Miroshnikov V I, Budko P A, Zatulieeter Yu S and Semenov S S 2015 General approach to the formation of a single information and control space of the naval component of the Russian armed forces, *Russian Navy Marine Radioelectronics* 1 22-28

[4] Nikolashin Y L, Kuleshova A, Budko P A, Zholdasov E S anf Zhukov G A 2015 SDR radio devices and cognitive radio communication in the decameter frequency range, *Science-intensive technologies in space research of the Earth* 7 20-31

[5] A Deb and S Ghosh 2014 *Power Electronic Systems: Walsh Analysis with MATLAB* (Florida, USA: CRC Press)

[6] H Zepernick and A Finger 2005 *Pseudo Random Signal Processing: Theory and Application* (Chichester, United Kingdom: John Wiley & Sons)

[7] R Michael Buehrer 2006 *Code Division Multiple Access (CDMA)* (San Rafael, California, USA: Morgan & Claypool Publishers)

[8] McCulloch W S and Pitts V 1956 Logical calculus of ideas relating to nervous activity, *Automata ed. McCarthy* (Moscow: Publishing house Inostr 363-384

[9] Dreyfus H 1972 *What Computers Can’t Do* (New York: MIT Press)

[10] Wang P 2007 *The Logic of Intelligence Artificial* (Springer, Berlin, Heidelberg)

[11] T Kohonen 2001 *Self-Organizing Maps* (New York)

[12] Zhdanov A A 2012 *Autonomous artificial intelligence* (Moscow: BINOM)

[13] Ivanov M A, Kovalev A V, Matsuk N A, Mikhailov D M and Gugunkov I V 2010 *Stochastic methods and means of information protection in computer systems and networks* (Moscow: KUDITS-Press)

[14] Morelos-Zaragoza R 2006 *The Art of noise-resistant coding. Methods, algorithms, application.* (Moscow: Technosphere)

[15] Moiseev D V, Chuzhikova-Proskurnina O D and Sapozhnikov N E 2016 Application of probabilistic form of data representation in correlation-extreme systems, *Environmental control Systems* 5 47-52

[16] Moiseev D V, Chuzhikova-Proskurnina O D and Sapozhnikov N E 2016 Comparison of different forms of non-positional probabilistic display of information, *Environmental control Systems*, 4 66-73

[17] Sapozhnikov N, Polyakov A and Moiseev D 2019 Advantages of using the probabilistic form of information representation in information-control systems *2019 International Science and Technology Conference "EastConf"*

[18] Sapozhnikov N, Bryukhovetskiy A, Polyakov A and Moiseev D 2018 Modeling performing calculations over the data presented in a probabilistic form *MATEC Web of Conferences*

[19] Skatkov A V, Bryukhovetskiy A A and Moiseev D V 2016 Method of control of qualitative changes in the States of network traffic on the basis of information measures Kulbak-Leibler *Environmental control systems* 5 53-58

[20] Skatkov A V, Bryukhovetskiy A A and Moiseev D V 2017 Intelligent monitoring system for solving large-scale scientific problems in cloud computing environments *Information and control systems* 2 19-25

[21] Skatkov A V, Bryukhovetskiy A A and Moiseev D V 2017 Monitoring of structurally inhomogeneous objects in cloud computing environments *Environmental, industrial and energy security-2017* (Sevastopol: Sevsu) pp 1236-1239