UDC 519.25
DOI: 10.15587/2706-5448.2022.251918
Article type «Reports on Research Projects»

**Andrii Shyshatskyi,
Volodymyr Ovchynnyk,
Andrii Momotov,
Nadiia Protas,
Andriy Solomakha**

DEVELOPMENT OF A MATHEMATICAL MODEL OF RADIO RESOURCE MANAGEMENT OF SPECIAL PURPOSE RADIO COMMUNICATION SYSTEMS BASED ON AN EVOLUTIONARY APPROACH

The object of research is a special-purpose radio communication system. A special purpose radio communication system is affected by many different destructive influences. The main ones are deliberate interference and cybernetic impact of various purposes. The above causes the search for new scientific approaches to identify and identify the destructive impact on special-purpose radio communications in order to increase the operational efficiency of special-purpose radio communications systems. In this work, the problems of developing a mathematical model for managing the radio resource of special-purpose radio communication systems based on the evolutionary approach are solved.

In the course of the research, the authors of the work used the main provisions of the theory of artificial intelligence, the theory of automation, the theory of complex technical systems, as well as general scientific methods of cognition, namely analysis and synthesis. The proposed methodological approach was developed taking into account the practical experience of the authors of this work during military conflicts of the last decade.

The research results will be useful for:

– development of new radio resource management algorithms;

– substantiation of recommendations for improving the efficiency of radio resource operational management;

– analysis of the radio-electronic situation during the conduct of hostilities (operations);

– when creating promising technologies for increasing the efficiency of radio resource operational management;

– assessment of the adequacy, reliability, sensitivity of the scientific and methodological apparatus for the operational management of the radio resource;

– development of new and improvement of existing radio resource management models.

Directions for further research will be aimed at developing a methodology for intelligent control of the radio resource of special-purpose radio communication systems.

Keywords: *radio communication systems, electronic jamming, data transmission systems, radio resource management, operational management.*

Received date: 17.11.2021
Accepted date: 24.12.2021
Published date: 30.12.2021

How to cite
Shyshatskyi, A., Ovchynnyk, V., Momotov, A., Protas, N., Solomakha, A. (2022). Development of a mathematical model of radio resource management of special purpose radio communication systems based on an evolutionary approach. Technology Audit and Production Reserves, 1 (2 (63)), 31–36. doi: http://doi.org/10.15587/2706-5448.2022.251918

1. Introduction

As evidenced by the experience of local wars and armed conflicts of recent decades, in the course of conducting operations (combat actions), as a rule, radio communication facilities (RCF) form the basis of any communication system for groupings of troops (forces). This is due to the high dynamism of operations (combat actions), the long range of the RCF and the RCF ability to work on the move [1, 2]. Given the great importance of the RCF in the command and control system of a grouping of troops (forces), there is a need to find new ways to improve the efficiency of their functioning.

One of the main features of the special-purpose RCF is that a rather limited frequency resource has been allocated for the needs of special users, in which a large number of radio-emitting devices operate [3, 4].

In the specified frequency range, there is a large number of intentional and natural interference, as well as various types of signal fading. Recently, a large list of cyber attacks has been added to the list of possible deliberate destructive influences on radio communication systems (RCS).

ISSN 2664-9969

It should also be specially noted that radio-emitting means also affect each other during the transmission of information, which in turn complicates the electromagnetic compatibility in the grouping of troops (forces) [5].

The analysis of studies [3, 5] indicates that the key features of the latest means of electronic suppression are:

– possibility of effective suppression of the entire operating frequency range of the RCF;

– intellectual suppression of RCS of groupings of troops (forces), taking into account the peculiarities of information transfer between command posts, that is, a unique obstacle is created for each type of RCF;

– simultaneous (quasi-simultaneous) suppression of several radio directions, and in case of group suppression – of the entire RCS;

– the possibility of imposing false modes of operation of the RCF and the transfer of false information to the RCS.

It is impossible to reliably foresee all possible variants of the destructive impact on the RCS of groupings of troops (forces) at the stage of communication planning and at the stage of RCS deployment. Therefore, the most preferred method of radio resource management is operational management [5].

The existing RCFs that are in operation do not allow counteracting intelligent electronic jamming and require the participation of the operator to control the operating modes and parameters. This significantly limits the RCF ability to effectively counteract deliberate and natural interference. In a number of studies, it is proposed to use adaptive and intelligent radio resource management systems for RCS. The adaptive paradigm combines control methods that are effective in the absence of a priori information about the dynamic characteristics of the RCS, and when using these control methods, a posteriori information about the dynamics of the RCS is collected during the functioning of the adaptive system [6, 7].

The control methods included in the intellectual paradigm are based on the theory of artificial intelligence. However, it would be wrong to assert the clear advantages of any one paradigm over the others. Each of them, along with a large number of positive features, has its drawbacks. However, the ability of intelligent systems to conduct self-learning determines their advantage, which is expressed in a higher efficiency of decision-making, which is the main factor in the conditions of electronic conflict [7].

Under the criterion of the effectiveness of the RCS operation in conditions of electronic suppression, let's consider the noise immunity of the transmission of a particular type of information with a given data rate.

Taking into account the existing capabilities of electronic jamming and the prospects for further development, it is proposed to apply the intelligent control of the radio resource of special-purpose radio communication systems.

The object of research is a special-purpose radio communication system. *The aim of this research* should be considered to be an increase in the efficiency of the functioning of a special-purpose radio communication system by developing a mathematical model of radio resource management based on an evolutionary approach.

2. Research methodology

Currently, machine learning is actively used in many areas: optical character recognition, spam detection, identification of biometric indicators, building recommender services, etc. But at the same time, when using machine learning, a number of difficulties arise with the identification of the destructive impact on RCS [8, 9].

In this study, under the intentional destructive impact on RCS, let's mean:

– intentional obstacles – noise and imitation;

– cyber-attacks.

Determination of the detection of a destructive impact on RCS includes not only identification by patterns, but also the detection of a previously unseen impact. At the same time, machine learning methods in the context of setting such a problem are aimed only at searching for relationships and patterns of RCS operation, finding activity similar to that previously encountered in the training sample [10, 11].

The use of ready-made machine learning tools to the task of identifying the destructive impact on RCS leads to a large number of unidentified influences and disorganization of the RCS itself. First of all, this is due to the dynamism of the radio exchange and the heterogeneous traffic circulating in the network. In addition, it is difficult to track the cyclicity or seasonality of such an exchange [12, 13].

Therefore, the following approach is proposed for training intelligent systems for managing the RCS radio resource:

– the maximum possible description of the set of all controlled parameters of the RCS;

– application of correlation analysis methods to eliminate components, and sometimes their linear combinations, with dispersion close to zero;

– the remaining feature set is used to train and validate the machine learning model.

To this end, it is proposed to develop an artificial immune system to detect and identify the destructive impact on RCS.

This study proposes an evolutionary-based artificial immune system model for identifying destructive effects on RCS, which is described as:

$$AISEA = \langle D_\tau, D_M, S_A, S_N, G, R, \Psi \rangle, \quad (1)$$

where $D_\tau \subset D$ – set of temporary immune detectors; D_M – set of immune memory detectors; $S_A \subset S$ – training sample consisting of anomalous instances (a set of known variants of RCS suppression); $S_N \subset S$ – test set consisting of normal instances (multiplicity of the RCF grouping parameters); $D = D_\tau \bigcup D_M$ – set of immune detectors; $G = \{G_1, ..., G_K\}$ – strategies for genetic optimization of immune detectors; $R: D \times 2^{S_A} \times 2^{S_N} \times G \to D$ – rule of teaching immune detectors; S – set of possible input objects; $\Psi: D \times S \to \mathbb{R}_+$ – function for calculating the affinity (correspondence rule) between the immune detector $d \in D$ and the test object, $s \in S$, where $\mathbb{R}_+ = \mathbb{R} \bigcap [0, +\infty)$.

Each immune detector $d \in D$ is described as a tuple of the following form:

$$d = \langle representation, threshold, life\_time, state \rangle, \quad (2)$$

where

$$representation \in \begin{Bmatrix} BitString, RealVector, \\ NeuralNetwork, PetrNet..., \end{Bmatrix}$$

– internal representation (internal structure) of the immune detector d, which can be specified as a binary string with the r-continuous bits rule (BitString), a real vector (RealVector),

an artificial neural network (NeuralNetwork), a Petri net (PetriNet), etc.; $threshold \in \mathbb{R}_+$ – activation threshold of the immune detector d; $life\_time \in \mathbb{R}_+$ – duration of the immune detector d;

$$state \in \{immature, semimature, mature, memory\}$$

– current state of the immune detector (1), which may be an immature, semi-mature, mature state, or a state corresponding to the memory detector $\mathbb{R}_+^* = \mathbb{R}_+ \bigcup \{+\infty\}$.

The general preparatory process for constructing artificial immune system parameters for identifying destructive effects on RCS can be described as follows:

1. Determination of the corrective coefficient for the degree of awareness of the force and means of the destructive impact on RCS. The degree of awareness can be: complete uncertainty, partial uncertainty, complete awareness.

2. Choice of the internal structure of each detector $d \in D$: *representation*.

3. Formation of the training data set S_A, containing pre-selected «foreign» objects.

4. Formation of a test data set S_N containing pre-selected «own» objects.

5. Choice of strategy for genetic optimization of immune sensors.

6. The choice of the training method R for immune sensors D depending on their internal representation [6].

7. Choice of the matching rule between the immune detector and the input object.

The proposed model of the artificial immune system is a set of immune detectors presented in the form of temporal and memory detectors with a given learning algorithm, as well as a genetic optimization strategy.

Moreover, the data set is intended for the first preliminary adjustment of immune detectors, and the role of the S_N data set is to filter the trained detectors. Strategies for genetic optimization of immune detectors include a set of genetic operators (crossover, mutation, inversion) and their combinations to change the parameters of an immune detector after its cloning. The immune detector learning rule is a two-step procedure. In the first step, immune detectors learn exclusively from the elements of the S_A dataset and undergo clonal selection, during which the created copies of immune detectors are mutated according to the chosen strategy $G' \in G$. This phase is repeated several times to form semi-mature sensors. In the second phase of training, these detectors are checked for compliance with their objects: those that are erroneously activated are destroyed, re-initialized and learned. Within this model, each immune detector undergoes several stages of differentiation. At the beginning of its development, each detector is initialized in an arbitrary way in accordance with its internal representation. During the functioning of the artificial immune system, temporary detectors record the parameters of the destructive effect on RCS in the updated S_{A^*} database in case of detection.

All immune detectors except memory detectors have a finite lifespan. If during a given lifetime they have not shown any destructive effect on RCS, they are retrained on an expanded data set containing S_A and S_{A^*} elements.

At the same time, if the immune sensor recognizes a destructive effect on RCS, its lifespan increases. Unlike them, memory detectors have an infinite lifetime and do not participate in filling the updated set of destructive effects.

To detect each class of destructive effect $c \in C$, several immune detectors are allocated, which are combined into a class of detectors $\left(\bigcup_{c \in C} D_{\varsigma(C)} = D\right)$. Each of the detectors $d \in D_{\varsigma(C)}$ uses deep learning proposed in [6] on various random subsamples of the sets S_A and $S_N - S_A^{(d)}$, and $S_{A^*}^{(d)}$, which may contain some duplicate and reordered objects from the original sets. This achieves a variety of immune detectors inside $D_{\varsigma(C)}$.

Accordingly, the q-th group of detectors is understood as a set of detectors $D_{\varsigma(C)}\left(\bigcup_{q=1}^{m} D^{(q)} = D\right)$, m – the number of classes of destructive impact on RCS that completely cover the given set of attack classes. If detector d responds to any element $s' \in S_N^{(d)}$, that is, if $\exists s' \in S_N^{(d)} \Psi(d, s') > \min\limits_{s \in S_A^{(d)}} \Psi(d, s)$, then detector d undergoes apoptosis and is replaced by a new randomly generated detector. For each class of destructive impact $c \in C$, exactly one memory detector is determined $d_m^{(C)}$ – a detector that satisfies the requirement of maximum fitness for object recognition $S_A^{\left(d_m^{(C)}\right)} \bigcap C$. Thus, the set of immune memory detectors can be defined as follows:

$$D_M = \bigcup_{c \in C} \left\{ \arg\max_{d \in D_{\varsigma(C)}} \left(\frac{\sum\limits_{s \in S_A^{(d)} \bigcap C} \Psi(d,s)}{\#\left(S_A^{(d)} \bigcap C\right)} \right) \right\}. \quad (3)$$

The set of temporary immune detectors is defined as follows:

$$D_\tau = \frac{D}{D_M}. \quad (4)$$

The activation threshold of the immune detector $d \in D$ trained on sets $S_A^{(d)}$ and $S_N^{(d)}$ is calculated as follows:

$$threshold = \frac{\overbrace{\min\limits_{s \in S_A^{(d)}} \Psi(d,s)}^{h_{\bar{d}}^-} + \overbrace{\min\limits_{s \in S_N^{(d)}} \Psi(d,s)}^{h_d^+}}{2}. \quad (5)$$

This formula is used to calculate the activation threshold of only those detectors d that, after training on a set of anomalous data $S_A^{(d)}$, do not have erroneous responses on a set of normal data $S_A^{(d)}$, i. e. $\forall s' \in S_N^{(d)} \Psi(d, s') < h_{\bar{d}}^-$. If such a condition is met, then an additional gap appears, equal to the value $h_d = h_{\bar{d}}^- - h_d^+ > 0$, and thus it becomes possible to «shift» the limiting value $h_{\bar{d}}^-$ that ensures the response of the detector d to any «foreign» object $s \in S_A^{(d)}$ by a value $\frac{h_{\bar{d}}^- - h_d^+}{2}$ to the side h_d^+ $threshold = h_{\bar{d}}^- - \frac{h_{\bar{d}}^- - h_d^+}{2} = \frac{h_{\bar{d}}^- - h_d^+}{2}$.

Identification of the destructive impact on RCS using the considered model is carried out as follows:

1. Determination of the corrective coefficient for the degree of awareness of the force and means of the destructive impact on RCS.

2. Calculation of the value of its activation:

$$a_d = \Psi(d,s) - threshold$$

for each immune detector $d \in D$. It is assumed that if $a_d \geq 0$, then the detector d is activated, otherwise the corresponding detector does not respond to the incoming object.

ISSN 2664-9969

3. Majority voting within each class of detectors:

$$\underbrace{\sum_{d\in D_{\varsigma(C)}}[a_d\geq 0]}_{A_c} > \underbrace{\sum_{d\in D_{\varsigma(C)}}[a_d<0]}_{B_c=\#D_{\varsigma(C)}-A_c}$$

is recognized as a «foreign» object. If $A_C=B_C$, then s is recognized as «own» object. In case of conflicts, i. e. $A_C=B_C$ is classified as a «foreign» object if $a_{d_m^{(C)}}\geq 0$, and s is classified as a «own» object if $a_{d_m^{(C)}}<0$, where $d_m^{(C)}\in D_M\bigcap D_{\varsigma(C)}$, $d_m^{(C)}$ – memory detector trained to recognize a «own» object and a «foreign» object of class C.

4. Formation of a set of classes of immune detectors $\{D_{\varsigma(C')}\}_{C'\in c}$ that were activated by those recognizing the input object s as a «foreign» object, where:

$$C^*=\left\{C'\middle|C'\in c\wedge\left(A_{C'}>B_{C'}\vee\left(A_{C'}=B_{C'}\wedge a_{d_m^{(C')}}\geq 0\right)\right)\right\}\subset c.$$

5. Determination of the object class s. If $C^*=\varnothing$, then the object s belongs to the class of «own» objects. If $E_{c^*}\rightleftharpoons\max_{C'\in c^*}A_{C'}$ is reached at one single point, then the class of object is $\arg E_{C'}$, otherwise the class of object s is:

$$\arg\max_{C'\in\left\{\arg E_{c^*}\right\}}\sum_{d\in D_\varsigma(C')}\times[a_d\geq 0].$$

This algorithm is based on comparing the affinity value of immune detectors with their individually adjusted activation thresholds and taking into account the same votes received from most of the detectors. If there are conflicts in distinguishing between normal and abnormal class (step 3), the deciding vote is given to the memory detector. If after that a conflict persists at the level of a group of detectors, then the sum of the affinity values that are activated in response to a given stimulus (input object) of immune detectors is taken into account (step 5).

The input object is «own» if and only if $\forall C\in c$:

$$A_C<B_C\vee\left(A_C=B_C\wedge a_{d_m^{(C)}}<0\right).$$

The following were used as the basis for this model:

1) model with a life cycle (M_1) proposed in [12];

2) model with a library of genes (M_2) [13], proposed in [14];

3) AISEA(M_3) [15] model;

4) model (M_4), which was supplemented by a number of improvements, namely:

– taking into account the type of uncertainty about the radio-electronic situation (RES);

– improved algorithm for learning immune detectors;

– a mechanism for automatic selection of their activation threshold, as well as a procedure for resolving conflict cases of classifying one object using immune memory detectors.

A comparison of these four models is given in Table 1. The «+» sign indicates the characteristics inherent in the corresponding model, the «–» sign means the lack of support for this feature of the model.

The results of the comparative analysis are given in Table 1 allow to conclude about the advantage of the indicated model in comparison with the known ones.

3. Research results and discussion

This approach is proposed to be used in the course of resolving military conflicts. This will improve the efficiency of data processing and transmission.

The developed M_4 model is universal in relation to the internal representation of immune detectors, while the M_1 model is focused on using bit strings as immune detectors, and the M_2 model is focused on cluster discretization of fields (genes) of immune detectors. The M_1 model lacks the possibility of clonal selection of detectors, and also does not provide genetic mutation operators. In all of the presented models, in the context of detecting a destructive effect on RCS, a dynamically updated population of immune detectors is used, which allows the artificial immune system to adapt to the changing radio-electronic environment in the mode of its operation. However, here an additional restriction is introduced for the M_1 model: after the activation of the detector, as a result of the accumulation of a sufficient number of matches with antigens, a signal from the administrator external to the system (costimulation signal) must be generated. Such a signal will allow the activated detector to get a chance to enter the pool of memory detectors and possible further continuous analysis of the electronic situation. The M_2 model is characterized by a distributed mechanism for generating detectors: detectors that are beneficial in terms of anomaly recognition can be propagated to other network nodes to increase the overall performance of the system; this property is absent in models M_1 and M_3.

Table 1

A selection of immune models for the detection of a destructive influx on radio communication systems

Immune model	Independence from the internal structure of the immune sensor	Availability of clonal selection and genetic optimization	Presence of negative selection	Accounting for the type of RES uncertainty	Automatic selection of the immune sensor activation threshold	Availability of learning mechanisms	Presence of memory detectors	Presence of a life cycle of lymphocytes	Dynamic retraining	Training of detectors on new data during operation	Distribution of immune detectors	Support for multiclass detection of destructive impact on RCS	Autonomy of the immune system (work without operator intervention)	Availability of a set of procedures for processing heterogeneous data
M_1	–	–	+	–	–	–	+	+	+	+	–	–	–	–
M_2	–	+	+	–	–	–	+	–	+	+	+	–	–	–
M_3	+	+	+	–	+	+	+	+	+	+	–	–	+	–
M_4	+	+	+	+	+	+	+	+	+	+	+	+	+	+

However, in the developed model M_4 additionally:
– take into account the type of uncertainty about the available capabilities of electronic warfare, means of cybernetic influence on the RCS;
– an improved set of procedures for processing heterogeneous data is used;
– an improved training procedure is used;
– a mechanism for resolving conflict cases of classification is used;
– the procedure of automatic calculation of the activation threshold of immune detectors is used, as well as the universality of the presentation structure;
– there is a constant renewal of immune detectors during different stages of maturation (life cycle) and their retraining using an expanding set of destructive effects on RCS.
The limitations of this research should be considered:
– taking into account time restrictions on the transmission of a specific type of message (formalized report);
– the presence of a primary base of the radio-electronic situation in the region;
– the need for complete and reliable information on the number of RCF and their technical characteristics;
– limitation of the quality of data transmission channels.

4. Conclusions

In this research, the development of a mathematical model for managing the radio resource of special-purpose radio communication systems based on an evolutionary approach was carried out.

The mathematical model of radio resource management of special-purpose radio communication systems, unlike the existing models of radio resource management of special-purpose radio communication systems, is an artificial immune system.

Also additional elements of scientific novelty are:
– taking into account the type of uncertainty about the available capabilities of electronic warfare, means of cybernetic influence on the RCS;
– an improved set of procedures for processing heterogeneous data is used;
– an improved training procedure is used;
– mechanism for resolving conflict cases of classification is used;
– procedure of automatic calculation of the threshold of activation of immune detectors is used, as well as the universality of the structure of their representation;
– there is a constant renewal of immune detectors during different stages of maturation (life cycle) and their retraining using an expanding set of destructive effects on RCS.
The research results will be useful for:
– development of new radio resource management algorithms;
– substantiation of recommendations for improving the efficiency of radio resource operational management;
– analysis of the radio-electronic situation during the conduct of hostilities (operations);
– when creating promising technologies for increasing the efficiency of radio resource operational management;
– assessment of the adequacy, reliability, sensitivity of the scientific and methodological apparatus for the operational management of the radio resource;
– development of new and improvement of existing radio resource management models.

Directions for further research will be aimed at developing a methodology for intelligent control of the radio resource of special-purpose radio communication systems.

References

1. Shyshatskyi, A. V., Bashkyrov, O. M., Kostyna, O. M. (2015). Rozvytok intehrovanykh system zviazku ta peredachi danykh dlia potreb Zbroinykh Syl. *Ozbroiennia ta viiskova tekhnika, 1 (5),* 35–39.
2. Tymchuk, S. (2017). Methods of Complex Data Processing from Technical Means of Monitoring. *Path of Science, 3 (3),* 4.1–4.9. doi: http://doi.org/10.22178/pos.20-4
3. Romanenko, I. O., Shyshatskyi, A. V., Zhyvotovskyi, R. M., Petruk, S. M. (2017). The concept of the organization of interaction of elements of military radio communication systems. *Science and Technology of the Air Force of the Armed Forces of Ukraine, 1,* 97–100.
4. Shevchenko, D. (2020). The set of indicators of the cyber security system in information and telecommunication networks of the Armed Forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defence, 38 (2),* 57–62. doi: http://doi.org/10.33099/2311-7249/2020-38-2-57-62
5. Makarenko, S. I. (2017). Prospects and Problems of Development of Communication Networks of Special Purpose. *Systems of Control, Communication and Security, 2,* 18–68. Available at: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf
6. Dudnyk, V., Sinenko, Y., Matsyk, M., Demchenko, Y., Zhyvotovskyi, R., Repilo, I. et. al. (2020). Development of a method for training artificial neural networks for intelligent decision support systems. *Eastern-European Journal of Enterprise Technologies, 3 (2 (105)),* 37–47. doi: http://doi.org/10.15587/1729-4061.2020.203301
7. Brownlee, J. (2011). *Clever algorithms: nature-inspired programming recipes.* LuLu, 441.
8. Gorokhovatsky, V., Stiahlyk, N., Tsarevska, V. (2021). Combination method of accelerated metric data search in image classification problems. *Advanced Information Systems, 5 (3),* 5–12. doi: http://doi.org/10.20998/2522-9052.2021.3.01
9. Meleshko, Y., Drieiev, O., Drieieva, H. (2020). Method of identification bot profiles based on neural networks in recommendation systems. *Advanced Information Systems, 4 (2),* 24–28. doi: http://doi.org/10.20998/2522-9052.2020.2.05
10. Dasgupta, D., Nino, F. (2008). *Immunological computation: theory and applications.* CRC press, 277. doi: http://doi.org/10.1201/9781420065466
11. Celada, F., Seiden, P. E. (1992). A computer model of cellular interactions in the immune system. *Immunology Today, 13 (2),* 56–62. doi: http://doi.org/10.1016/0167-5699(92)90135-t
12. Chan-Tin, E., Heorhiadi, V., Hopper, N., Kim, Y. (2011). The frog-boiling attack: Limitations of secure network coordinate systems. *ACM Transactions on Information and System Security, 14 (3),* 1–23. doi: http://doi.org/10.1145/2043621.2043627
13. Hofmeyr, S. A., Forrest, S. (2000). Architecture for an Artificial Immune System. *Evolutionary Computation, 8 (4),* 443–473. doi: http://doi.org/10.1162/106365600568257
14. Kim, S. S., Reddy, A. L. N. (2008). Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data. *IEEE/ACM Transactions on Networking, 16 (3),* 562–575. doi: http://doi.org/10.1109/tnet.2007.902685
15. Barford, P., Kline, J., Plonka, D., Ron, A. (2002). A signal analysis of network traffic anomalies. *Proceedings of the Second ACM SIGCOMM Workshop on Internet Measurment – IMW'02,* 71–82. doi: http://doi.org/10.1145/637201.637210

ISSN 2664-9969

✉***Andrii Shyshatskyi,*** *PhD, Senior Researcher, Research Department of Electronic Warfare Development, Central Scientific Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine, e-mail: ierikon13@gmail.com, ORCID: https://orcid.org/0000-0001-6731-6390*

Volodymyr Ovchynnyk, *Lecturer, Department of Armored Vehicles, Odessa Military Academy, Odesa, Ukraine, ORCID: https://orcid.org/0000-0001-7653-7136*

Andrii Momotov, *Department of Construction and Road-Building Machinery, Kharkiv National Automobile and Highway University, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0001-5997-4561*

Nadiia Protas, *PhD, Associate Professor, Department of Information Systems and Technologies, Poltava State Agrarian University, Poltava, Ukraine, ORCID: https://orcid.org/0000-0003-0943-0587*

Andriy Solomakha, *Senior Lecturer, Department of Military Training, The Bohdan Khmelnytsky National University of Cherkasy, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0001-7390-4156*

✉*Corresponding author*

UDC 629.7.615.3
DOI: 10.15587/2706-5448.2022.252712
Article type «Reports on Research Projects»

Natalja Ashhepkova

ANALYSIS OF THE INERTIA TENSOR OF AUTONOMOUS MOBILE ROBOT

The object of research is the inertia tensor of an autonomous mobile robot (AMR) with a manipulator with different configurations of their mutual position. As an example of the AMR design of a changing configuration, an all-wheel drive four-wheeled platform with a manipulator is considered, consisting of a docking disk rotating around a vertical axis and rod links of the arm connected by rotational kinematic pairs of the fifth class. The mass of moving structural elements, i. e., a manipulator with a load, is 10–20 % of the mass of the robot platform. Let's consider that the links of the manipulator and the platform are absolutely rigid and homogeneous bodies with a constant density; let's neglect the mass of kinematic pairs. The next step in the analysis of the AMR inertia tensor of a changing configuration can be a study taking into account the elastic properties of the manipulator links, the uneven distribution of the masses of the platform, and the characteristics of the kinematic pairs.

The dependence of the values of the elements of the AMR inertia tensor of a changing configuration on the values of the generalized coordinates of the moving elements of the structure and the ratio of the mass of the platform and the mass of the moving elements of the structure has been studied. The analysis of the inertia tensor of the AMR with a manipulator at different configurations of their mutual position showed that the values of the centrifugal moments of inertia of the system during the relative motion of the manipulator are commensurate with the value of the axial moments of inertia of the system, even if the mass of the moving structural elements is less than 10 % of the mass of the platform. In most existing AMRs, the mass of moving structural elements is up to 20 % of the platform mass, therefore, in the general case, the inertia tensor of such a system should be taken as off-diagonal and non-stationary. In the future, this will make it possible to refine the equation of dynamics, take into account the relationship of control channels, simulate the movement of AMR of a changing configuration, and optimize energy costs.

Since AMR with the manipulator is an example of the «changing AMR» object class, the results obtained can be applied to all objects of this class.

Keywords: *autonomous mobile robot, manipulator, moment of inertia, off-diagonal and non-stationary inertia tensor.*

Received date: 01.11.2021
Accepted date: 08.12.2021
Published date: 15.02.2022

How to cite
Ashhepkova, N. (2022). Analysis of the inertia tensor of autonomous mobile robot. Technology Audit and Production Reserves, 1 (2 (63)), 36–40. doi: http://doi.org/10.15587/2706-5448.2022.252712

1. Introduction

In robotics, there is a tendency to increase the autonomy of mobile robotic systems (RS). The works [1, 2] emphasize the importance of using the modular principle of assembling the structures of autonomous mobile robots (AMRs). The introduction of the modular principle leads to the creation of flexible functional reconfigured complexes with the possibility of further modernization. Replacing modules in AMR designs allows to timely send the RS to solve a new problem when the operational environment or working space conditions change, quickly carry out current repairs and extend the service life. The expansion of the scope and complication of tasks for modern AMR determines