Analysis of the Use of Artificial Immune Systems

R M Mikherskii¹, M R Mikherskii¹

¹V.I. Vernadsky Crimean Federal University, Simferopol, Prospekt Vernadskogo, 4, 295007, Russia

E-mail mrm03@mail.ru

Abstract. Artificial immune systems are systems of artificial intelligence at the basis of work, which are based on the principles of the functioning of the biological immune system. These systems are of great interest from researchers developing models and algorithms in the field of machine learning for solving complex computational and engineering problems. In the presented work, a review of modern methods for the implementation of artificial immune systems is carried out, taking into account the results obtained recently.

Keywords: Artificial intelligence; Machine learning

1. Introduction
Recently, machine learning systems are increasingly used in the study of a wide range of problems, the solution of which until recently was available only to humans. The most used machine algorithms are now algorithms of convolutional neural networks [1-10].

This popularity is due to two factors. First, convolutional neural networks currently demonstrate the best quality of pattern recognition and data classification among all existing methods. Secondly, a large number of software libraries have been implemented that allow a wide range of users to use convolutional neural networks.

However, it should be noted that convolutional neural networks also have a number of disadvantages, the main one of which, perhaps, is the long training time of such networks. In some tasks, this time can be tens of hours [11]. In addition, if such a network is trained to classify data according to a certain set of classes, then adding a new class requires a complete retraining of the network.

The artificial immune systems studied in this work do not have the disadvantages described above. Artificial immune systems are computing systems based on the principles of the biological immune system [12-17].

2. Review
The field of application of artificial immune systems is quite extensive. Currently, these networks are used for processing data without a structure [18], searching for anomalous data [19], control [20], solving problems of classification and optimization [21, 22, 23], information compression [24], security computer systems [25], machine learning [26, 27].

In the article [28], an implementation of an artificial immune system is presented, which makes it possible to recognize from 77.55% to 99.78% of the images of human faces presented to this system for identification.
The use of artificial immune systems for recognition of visual images is investigated in works [29,30]. In these works, a new algorithm for an artificial immune system is presented, which makes it possible to recognize such images in real time using a webcam. As a result of the experiment, it was determined that this artificial immune system can be successfully used not only to recognize the faces of people, but also any other objects. These works also investigate the possibility of using artificial immune systems in parallel computing systems. The developed artificial immune system can be trained in a new image at any time of its operation. It should also be noted that this system learns new images rather quickly. The advantages described above allow you to create artificial intelligence systems that learn in real time.

The article [31] presents a new set of multiple artificial immune system detectors for detecting malicious programs on mobile devices running the Android operating system. An artificial immune system with multiple detectors differs from the commonly used artificial immune system in that several sets of detectors are developed simultaneously through negative selection. The first set of detectors includes detectors associated with protected applications, the second set - related to malicious applications. An artificial immune system with multiple detectors also includes, along with the negative selection method, feature selection, known as the detector separation technique. The approach presented in this work allowed achieving recognition accuracy of 93.33%.

It should be noted that artificial immune systems are also used in desktop computers to protect against malicious attacks over the Internet. The article [32] investigated security systems based on an artificial immune system used in such computers. In works [33, 34], a fairly successful attempt was made to use an artificial immune system to solve the problem of identification and authentication of users using biometric data. For this purpose, iris recognition was used.

The works [35,36] consider the use of an artificial immune system in e-mail to solve the problem of detecting messages containing spam. To solve this problem, the authors proposed to use two classes of antibodies. The first class included antibodies that multiply when interacting with email messages in which spam is absent. The second class is those that multiply when interacting with mail messages that contain spam.

In [37], a detailed analysis of algorithms used in pattern recognition and intelligent analysis is made. An overview of the use of artificial immune systems in problems of authentication and identification of people using their biometric data is carried out. It is shown that these systems have advantages in use in comparison with "fuzzy extractors" and artificial neural networks. Possible solutions to the problem of secure storage of biometric data using an artificial immune system were also considered.

In [38], it was proposed to use an artificial immune system to detect information security incidents in intrusion detection systems. In this system, a modification of the clonal selection algorithm is considered, in which an external optimization structure is used, the principle of which is based on the use of the strategy of evolutionary algorithms.

In article [39], it is proposed to use an artificial immune system to identify the author of a Russian handwritten text based on his handwriting sample. When implementing this system, methods of negative selection, Erne idiotypic networks and risk theory were used.

The paper [40] presents a method for analyzing handwritten text, which is based on the principle of functioning of an artificial immune system. To solve this problem, a negative selection algorithm was used. The initial data for this system are the coordinates of the pen taken from the output of the digitizer, as well as the value of the pen pressure. This method allows for a text-independent analysis of the manuscript. According to the authors, it potentially has a higher analysis accuracy and, accordingly, expands the scope of online manuscript analysis systems.

The paper [41] considers the possible use of an artificial immune system to create a search system for design solutions in the electronic archive of design documentation. An immune multimodal algorithm was used as a search method. The descriptions of software implementation tools are given.

In article [42], a model of an intrusion detection system based on an artificial immune system is proposed. This model examines the abnormal behavior of packets in network traffic during transmission.
It combines machine learning rules and negative selection theory to improve the performance of an intrusion detection system. The article tested the proposed model on the DARPA1999 dataset.

In [43], a hybrid approach to predicting the temporal change in the parameters of an on-board automated control system is considered. To solve this problem, a modified immune clonal selection algorithm was proposed. The theoretical results obtained in this work can be used in the development of intelligent decision support systems for monitoring the state of complex technical objects of the rocket and space industry. Application of the proposed approach makes it possible to increase the operational efficiency and reliability of the operation of these objects.

In [44], an algorithm for an artificial immune system is proposed that allows solving problems of controlling autonomous systems, symbolic regression, and recognition of single characters. Based on the presented algorithm in the C# programming language, a software system has been developed that has shown its efficiency in solving the assigned tasks. Computational experiments were carried out for each considered problem. The accuracy of the results obtained was compared with that for such methods as: linear classifier (1st level neural network); k-nearest neighbors method; principal component analysis and quadratic classifier; support vector machine (Gaussian kernel); two-layer, three-layer and six-layer neural networks. In general, compared with these methods, the artificial immune system showed good results.

In [45], the theoretical foundations of the three main types of algorithms for the artificial immune system, such as the clonal selection algorithm, the negative selection algorithm, and the immune network algorithm, are studied in detail. The paper also discusses the possible benefits of artificial immune systems for understanding how real biological immune systems work.

To solve the problem of resource allocation when using an artificial immune system, an optimal approach based on control was proposed in [46].

In [47], studies were carried out on the use of dendritic cells to detect abnormal or dangerous events in the data stream.

In [48], a type of data space representation was proposed that can evolve and adapt over time, providing a link between the data and the immune algorithm itself.

In [49], it was proposed to use a model of an artificial immune system for early diagnosis of breast cancer. This model is called the artificial immune system for associative classification.

The goal of [50] was to develop a decentralized adaptive system capable of studying the model of incoming problems and being able to choose the best from a given set of solutions. The system presented in this work is based on the integration of three main theories in immunology: the theory of the immune network, the theory of danger and the theory of clonal selection. The efficiency of the proposed mechanism in real scenarios was tested experimentally on a physical network of real robots.

The application of the principles of artificial immune systems to control mobile robots is discussed in [51]. In this article, an algorithm for an artificial immune system was proposed by combining two models: clonal selection and the immune network. This hybrid mechanism has been tested on a real robot located in an unknown environment including obstacles. The main goal of the robot was to detect safe areas in the environment. The results obtained in various test cases indicate that the proposed model is viable and able to cope with different environmental conditions.

The article [52] presents a model of an artificial immune system using the CNN algorithm. The model is based on the bone marrow and thymus model. The results obtained and the time measurement carried out at the same time show that the model presented in this work can be implemented in applications in real time.

3. Conclusion
The literature review presented in this article is, of course, incomplete. This is due to the fact that artificial immune systems are a rapidly developing and promising direction in the development of machine learning and the scope of their application is extremely wide. Nevertheless, we very much hope
that this work will be useful both for specialists in the field of artificial intelligence and machine learning, and for scientists working in related fields of knowledge.

4. Acknowledgment
The authors would like to express their gratitude to Marina Vsevolodovna Glumova, Director of the Physico-technical Institute of the V. I. Vernadsky Crimean Federal University, and Viktor Milyukov, head of the Department of computer engineering and modeling of the Physico-technical Institute of the V. I. Vernadsky Crimean Federal University, for their comprehensive assistance in organizing research work.

References
[1] Bulat A and Tzimiropoulos G 2020 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 42 no 02 pp 343-356
[2] Farrugia and Guillemot C 2020 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 42 no 05 pp 1162-1175
[3] Rocco I, Arandjelovic R and Sivic J 2019 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 41 no 11 pp 2553-2567
[4] Lian C, Liu M, Zhang J and Shen D 2020 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 42 no 04 pp 880-893
[5] Kalayeh M and Shah M 2020 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 42 no 06 pp 1483-1500
[6] Lin S, Ji R, Chen C, Tao D and Luo J 2019 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 41 no 12 pp 2889-2905
[7] Sindagi V A and Patel V M 2017 Pattern Recognit. Lett. vol 107 pp 3–16
[8] Zhou Z, Shin J, Zhang L, Gurudu S, Gotway M and Liang J 2017 Proc. IEEE Conf. Comput. Vis. Pattern Recognit. pp 7340–7349
[9] Li Y, Zhang X and Chen D 2018 Proc. IEEE Conf. Comput. Vis. Pattern Recognit. pp 1091–1100
[10] He K, Gkioxari G, Dollar P and Girshick R 2020 IEEE Transactions on Pattern Analysis & Machine Intelligence vol 42 no 02 pp 386-397
[11] Nemkov R M 2015 Development of neural network algorithms for invariant pattern recognition (The thesis for the Candidate’s degree in Technical Sciences, Stavropol)
[12] Dasgupta D 1999 Artificial Immune Systems and Their Applications (Springer, Berlin Heidelberg) pp 3–21
[13] Dasgupta D and Gonzalez F 2002 IEEE Trans Evol Comput vol 6 no 3 pp 281–291
[14] Timmis J, Knight T, LN de Castro and Hart E 2004 An overview of artificial immune systems, in Computation in Cells and Tissues: Perspectives and Tools for Thought ed. by R Paton, H Bolouri, M Holcombe, JH Parish, R Tateson. Natural Computation Series
[15] Hofmeyr S 1999 An Immunological Model of Distributed Detection and Its Application to Computer Security (Ph.D. Dissertation, Department of Computer Science, The University of New Mexico, Albuquerque)
[16] Hofmeyr S and Forrest S 1999 The Proceedings of the 1999 Genetic and Evolutionary Computation Conference (GECCO-1999) (Morgan-Kaufmann, San Francisco)
[17] Al-Enezi J R, Abbod M F and Alsharhan S 2010 International Journal of Research and Reviews in Applied Sciences vol 3 no 2 pp 118 – 131
[18] Knight T and Timmis J 2001 IEEE Intern. Conf. on Data Mining pp 297– 304
[19] Garrett S M 2005 Evolutionary Computation vol 13 pp 145–178
[20] Krishna K K and Neidhoefer J 1999 Immunized adaptive critic for an autonomous aircraft control application ed. by Dasgupta D (Springer-Verlag Inc.) vol 20 pp 221–240
[21] Bryukhovetskiy A A and Skatkov A V 2010 Optimization of viral processes vol 7 pp 119–122
[22] Gao X Z, Ovaska S J, Wang X and Chow M Y 2009 Neural Computing and Applications vol
18 no. 7 pp 719–729
[23] Bardachev Yu N and Didyk A A 2007 Automation, automation, electrical complexes and system vol 2 pp 107-111
[24] Stankevich L A and Kazansky A B 2006 Actual problems of protection and security: tr. 9th All-Russia. scientific-practical conf. vol 5 pp 145-152
[25] Kim J and Bentley P 2002 In Proc. Congress on Evolutionary Computation (Honolulu, HI, USA) pp 1244–1252
[26] Hunt J E and Cooke D E 1996 Journ. of Network Computing Applications vol 19 pp 189–212
[27] Dasgupta D, Yu S and Nino F 2011 Applied Soft Computing vol 11 no 2 pp 1574-1587
[28] Luh G 2014 Immune Computation vol 2 no 1 pp 21-34
[29] Mikherskii R 2018 Computer Optics vol 42 no 1 pp 113 – 117
[30] Mikherskii R 2017 Information technologies and nanotechnologies (ITNT-2017): III international Conf. and youth school (Samara) pp 518-521
[31] Brown J, Anwar M and Dozier G 2017 EURASIP J. on Info. Security 2017 7
[32] Ramakrishnan S and Srinivasan S 2009 Artif Intell Rev vol 32(1-4) pp 13–43
[33] Hou H and Dozier G 2005 Proceedings of the ACM Symposium on Applied Computing pp 952–956
[34] Hou H 2006 GENERTIA: A System for Vulnerability Analysis, Design and Redesign of Immunity-Based Anomaly Detection Systems (Ph.D. Dissertation, Computer Science & Software Engineering Department, Auburn University, Auburn)
[35] Idris I and Abdulhamid SM 2014 An Improved AIS Based E-mail Classification Technique for Spam Detection arXiv preprint arXiv:1402.1242
[36] Idris I 2012 International Journal of Artificial Intelligence & Applications (IJAIA) vol 3 no 1 pp 83–94
[37] Sulavko A E, , Shalina E V, Stadnìlov D G and Choban A G 2019 Information security issues vol 1 no 124 pp 38 - 46
[38] Zhukov V G and Salamatova T A 2014 Vestnik SibGAU vol 4(56) pp 41–47
[39] Eremenko Yu I and Shatalov 2013 A A Scientific Bulletin of the Belgorod state University. Series: Economics. Informatics vol 28 no 22-1 (165) pp 218-224
[40] Bryukhomitsky Yu 2015 A Proceedings of the southern Federal University. Technical Sciences no 5 (166) pp 174-183
[41] Eremenko Yu I, Melnikova I V and Shatalov A A 2011 Bulletin of the Voronezh state technical University vol 7 no 7 pp 115-121
[42] Burlakov M E and Ivkin A N 2019 Bulletin of Perm national research Polytechnic University. Electrical engineering, information technology, control systems no 29 pp 209-224
[43] Smirnov V A and Smirnov D V 2018 Science-intensive technologies in earth space research vol 10, no 1 pp 66-78
[44] Astachova I R, Zolotukhin A E, Kurklinskaya E Yu and Belyaeva N V 2019 J. Phys.: Conf. Ser. 1203 012036
[45] Timmisa J, Honec A, Stibord T and Clarka E 2008 Theoretical Computer Science 403, pp 11–32
[46] Hone A and Van den Berg H 2007 Silico Immunology (Springer) pp 351–374
[47] Greensmith J, Aickelin U and Twycross J 2006 Proceedings of the 5th International Conference on Artificial Immune Systems, vol 4163 pp 404–417
[48] Bentley P J, Greensmith J and Ujjin S 2005 Proc. of the 4th International Conference on Artificial Immune Systems, ICARIS, in: Lecture Notes in Computer Science (Springer) vol 3627 pp 139–152
[49] González-Patiño D, Villuendas-Rey Y, Argüelles-Cruz A J, Camacho-Nieto O and Yañez-Márquez C 2020 Appl. Sci. vol 10 515
[50] Semwal T and Nair S B 2020 Applied Soft Computing vol 86 105920
[51] Shrivastava K, Jha S S and Nair S B 2013 Proceedings of Conference on Advances in Robotics,
ACM pp 1-7

[52] Csereny G, Falus A, Porod W and Roska T 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No.04CH37512) (Vancouver, BC) pp III-17