Neutrosophic Sets and Systems, {Special Issue: Advances in SuperHyperStructures and Applied Neutrosophic Theories)}, Vol. 74, 2024

University of New Mexico

A Neutrosophic Framework for Artificial Immune Systems

Antonios Paraskevas [1,*] and Florentin Smarandache [2]

[1] Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece; aparaskevas@uom.edu.gr
[2] University of New Mexico, Mathematics Department, Gallup, NM 87301, USA; smarand@unm.edu

Abstract: Artificial immune systems (AIS) draw inspiration from the mechanisms of the natural immune system. They extract ideas from the functioning of the natural immune system in order to use them to build computer models to solve real-world problems. While traditional AIS models mimic the biological immune system's capacity to distinguish between self and non-self entities, they often face challenges in environments where data may be incomplete or ambiguous. In this paper we introduce neutrosophic AIS that includes degrees of truthiness, falsehood and indeterminacy to better address ambiguity within pattern recognition tasks. Within this neutrosophic framework we discuss and redefine main AIS concepts, including self and non-self categorization, clonal selection, negative selection, and immunological memory. A numerical example, from the field of computer security, illustrates the application of the suggested approach in detecting non-self entities. With the addition of neutrosophic logic, the proposed model significantly enhances AIS's adaptability and pattern recognition capabilities, addressing uncertainties inherent in real-world applications.

Keywords: Neutrosophic logic; artificial immune system; self and non-self categorization; clonal selection; negative selection; immunological memory; pattern recognition.

1. Introduction

The human immune system is a complex system consisting of an intricate network of specialized tissues, organs, cells and chemical molecules [1]. The natural immune system recognizes, destroys and remembers an almost unlimited number of foreign particles and also protects the human body from cells that do not function normally in the body as it has the ability to distinguish (non-self or antigen) from self cells. When a pathogen (infectious foreign element) enters the body, it is detected and mobilized for elimination. The system is capable of "remembering" each infection, so that a second exposure to the same pathogen is dealt with more efficiently.

Artificial Immune System (AIS) is an area of research that bridges the disciplines of immunology, computer science and engineering [2-4]. During the last two decades, the field of AIS is progressing slowly and steadily as a branch of Computational Intelligence (CI) amongst other methods such as neural networks and evolutionary computing. Inspired by the biological immune system's ability to recognize and respond to foreign pathogens, AIS leverages these principles to develop algorithms capable of pattern recognition, anomaly detection, and adaptive learning.

The properties of the natural immune system that the artificial immune system exploits are [5]:

1. The natural immune system only needs to be aware of normal cells,
2. The natural immune system can distinguish between normal and foreign cells,
3. A foreign cell can be classified as harmful or non-harmful,
4. Lymphocytes are cloned and post-cloned in order to attach themselves to the foreign cells that the body encounters,
5. The natural immune system has a rapid response to antigens that the body has already encountered, which is due to memory cells.

Taking into account the characteristics and models of the natural immune system, several models of artificial immune systems have been developed. These models are as follows:

1. Artificial immune systems based on the classical view of the immune system are: the negative selection algorithm [6-9] and evolutionary approaches [10-14]
2. Artificial immune systems based on the clone selection theory are: dynamic clone selection [15-16] and multilayered artificial immune systems [17-18].
3. Artificial immune systems based on network theory are: artificial immune network [19], self-stabilizing artificial immune systems [20], augmented artificial immune network [21], dynamic weighted B-Cell artificial immune systems [22] and aiNet model artificial and immune network [23].
4. Artificial immune systems based on danger theory [24-27].

AIS are being used in many applications such as anomaly detection [28-29], pattern recognition [30], data mining [31], computer security [32-36], adaptive control [37] and fault detection [38-39]. These applications highlight the flexibility and robustness of AIS, positioning it as a valuable approach in environments that require adaptability, real-time response, and handling of uncertain or variable data.

In AIS related literature, it is observed that most methods utilize binary or fuzzy logic based to categorize between self and non-self entities. But in this case, the aforesaid methods are not always reliable when dealing with uncertain data or irregular conditions in real world applications, such as in cybersecurity or anomaly detection. From this point of view, we propose a new methodology that integrates neutrosophic logic in classic AIS concepts. Neutrosophic logic which is a new branch of logic is considered more flexible than other classical or fuzzy methods as it takes into account indeterminacy membership - the uncertainty and indeterminacy that frequently occur and characterize many (if not, all) real-world applications.

The main objective of current research is to present a more robust AIS framework by integrating neutrosophic logic. Rather than categorizing decisions as simply true or false, the main idea is to constitute AIS more adaptable and capable of handling uncertainty. To illustrate how this integration works, we provide a numerical example and demonstrate how our approach improves AIS performance in complex and unpredictable real-world scenarios. This research work marks a critical advancement in leveraging AIS for complex, dynamic environments, as demonstrated through its application to cybersecurity challenges.

The structure of this article is as follows: In Section 2, we define and explain the neutrosophic mathematical framework needed to formulate the proposed neutrosophic AIS (n-AIS) model. Next, in Section 3, we highlight the applicability of the suggested n-AIS model in an illustrative example from the field of cybersecurity. In Section 4, through this case study, we highlight the system's ability to assess and process various types of uncertainty, such as ambiguous threat classifications or incomplete attack vectors, leveraging the suggested n-AIS model. Lastly, the "Conclusions" section wraps up the key points of our study and proposes potential research work.

2. Materials and Methods

Definition 1 [40] Consider X to be a space of points (objects) and x to be a generic element in X. A truth membership function $\boldsymbol{T_A}$, an indeterminacy membership function $\boldsymbol{I_A}$, and a falsity membership function $\boldsymbol{F_A}$ characterize a single-valued neutrosophic set (SVNs) A in X. For each point x in X, $\boldsymbol{T_A(x)}$, $\boldsymbol{I_A(x)}$, $\boldsymbol{F_A(x)} \in [0, 1]$. Then, a simplification of the neutrosophic set A is denoted by $A = \{\langle \boldsymbol{x}, \boldsymbol{T(x)}, \boldsymbol{I(x)}, \boldsymbol{F(x)} \rangle \mid x \in \boldsymbol{X}\}$ with $0 \leq \boldsymbol{T_A(x)} + \boldsymbol{I_A(x)} + \boldsymbol{F_A(x)} \leq 3$.

In traditional binary systems, T(x) and F(x) are binary (0 or 1), but in a neutrosophic system, each value can vary continuously, allowing for nuanced classifications.

In AIS, entities are classed as "self" (belonging to the system and harmless) or "non-self" (foreign and possibly harmful). Inspired by the biological immune system, this categorization allows AIS to recognize and respond to abnormal patterns, similar to finding diseases in a biological environment.

Definition 2 Let S denote the set of self-entities and N the set of non-self entities. An entity x is categorized based on thresholds for T, I, and F as follows:

Self: if T(x) > $T_{threshold}$ and F(x) < $F_{threshold}$ (1)
Non-Self: if F(x) > $F_{threshold}$ and T(x) < $T_{threshold}$ (2)
Indeterminate if I(x) > $I_{threshold}$ (3)
representing cases where it's unclear whether x is self or non-self.

The process of cloning is most commonly known as clone selection which is the proliferation of lymphocytes that recognize antigens [5]. Learning in the immune system occurs by a process known as affinity maturation.

Definition 3 Let P(x) be the population of cloned cells associated with entity x. Each clone $\boldsymbol{c_i}$∈P(x) has a neutrosophic vector (T($\boldsymbol{c_i}$),I($\boldsymbol{c_i}$),F($\boldsymbol{c_i}$)), where mutation adjusts these values based on exposure to new information. *Mutation* can be defined as:
T′($\boldsymbol{c_i}$)=T($\boldsymbol{c_i}$)+ΔT (4)
I′($\boldsymbol{c_i}$)=I($\boldsymbol{c_i}$)+ΔI (5)
F′($\boldsymbol{c_i}$)=F($\boldsymbol{c_i}$)+ΔF (6)
where ΔT, ΔI and ΔF are changes based on mutation rates influenced by exposure to uncertain patterns.

In AIS, the fitness function is a measure used to evaluate each clone's effectiveness or "fitness" in identifying and responding to patterns or threats.

Definition 4 The *fitness function* of a clone $\boldsymbol{c_i}$ can be mathematically defined using a neutrosophic similarity measure that considers the degrees of truth (T), indeterminacy (I), and falsity (F). The fitness score Fitness($\boldsymbol{c_i}$) can be represented as:
Fitness($\boldsymbol{c_i}$)=αT($\boldsymbol{c_i}$)−βF($\boldsymbol{c_i}$)−γI($\boldsymbol{c_i}$) (7)
where α,β,γ are weighting factors that determine the relative importance of truth, falsity, and indeterminacy in evaluating fitness.

A higher fitness score indicates that the clone c_i has a closer alignment with the desired characteristics and is thus prioritized in the AIS for further replication or retention.

For over 50 years immunologists have been based their thoughts, experiments, and clinical treatments on the idea that the immune system functions by making a distinction between self (related to belonging molecules in the organism) and non-self (related to foreign molecules in the organism). AIS are based on the human immune system's ability to recognize practically any pathogenic agent. According to the Self-Nonself hypothesis, the body recognizes itself by discriminating its own cells and molecules from alien ones.

Definition 5 *Negative Selection* in a n-AIS framework involves identifying and eliminating clones that are likely to react against self-entities by measuring their similarity to known self-patterns. Define the neutrosophic distance d_{self}(x,y) between a clone x and any self-entity y as:
d_{self}(x,y) = |T(x)−T(y)|+|I(x)−I(y)|+|F(x)−F(y)| (8)
If d_{self}(x,y) < $\boldsymbol{\epsilon}$ (where $\boldsymbol{\epsilon}$ is a threshold), and T(x)≈T(y), clone x is eliminated due to high likelihood of being self-reactive.

Immunological memory could be defined as a stimulus-specific change of immune reactivity that persists in the absence of the stimulus. In neutrosophic AIS, memory cells store the neutrosophic vector (T,I,F) of each recognized non-self entity.

Definition 6 *Immunological memory* in a n-AIS model refers to the system's ability to retain information about previously identified non-self entities (patterns or threats) by storing their neutrosophic values—truth (T), indeterminacy (I), and falsity (F)—to improve future responses. Each memory cell m corresponds to a previously identified non-self entity and is represented by a neutrosophic vector:
m = (T(m), I(m), F(m)) (9)
where T(m), I(m), and F(m) denote the truth, indeterminacy, and falsity values associated with the stored pattern.

When a new non-self entity (x) is detected with neutrosophic values (T(x), I(x), F(x)), the system compares it to existing memory cells. If x matches an existing memory cell based on a neutrosophic similarity measure, the memory cell m m is updated to integrate the new values of x as follows:

$T(m)=\lambda T(m)+(1-\lambda)T(x)$ (10)

$I(m)=\lambda I(m)+(1-\lambda)I(x)$ (11)

$F(m)=\lambda F(m)+(1-\lambda)F(x)$ (12)

where $\lambda \in [0,1]$ is a decay factor that controls the weight given to past values versus the new observation.

The memory cell m is updated only if the neutrosophic distance between x and m satisfies:

$d_{memory}(x,m) < \boldsymbol{\epsilon}$ (13)

where $\boldsymbol{\epsilon}$ is a predefined similarity threshold and it determines the maximum allowable "distance" between the neutrosophic values of the new input $\boldsymbol{x}$ and the existing memory cell $\boldsymbol{m}$ for them to be considered similar enough.

The neutrosophic distance $d_{memory}(x,m)$ is defined and calculated as in equation (8). This neutrosophic immunological memory architecture enables the AIS to dynamically adapt to changing patterns by updating memory cells with new data, hence improving the system's ability to recognize and respond to non-self entities in unpredictable circumstances.

3. Results

Network security systems face continuous streams of data from diverse sources, which may vary in nature and threat level. In this section we will examine a system equipped with n-AIS that needs to evaluate incoming network traffic to determine whether it represents a "self" (normal traffic) or "non-self" (potentially malicious traffic) entity. The goal is to enhance threat detection in a dynamic environment where traffic patterns might be unpredictable or unclear.

When the n-AIS system first encounters an incoming traffic pattern x, it evaluates its characteristics against predefined rules or thresholds.

A memory cell m has previously stored a recognized malicious traffic pattern with values (Eq. 9): $m = (0.2, 0.5, 0.7)$ (14)

We set a similarity threshold $\epsilon=0.3$ for updating the memory cell based on new incoming patterns. In this way, the system stays adaptive without over-reacting to every minor fluctuation, hence boosting its resilience and flexibility in tracking new harmful tendencies.

Suppose an incoming traffic sample x has the following neutrosophic values:

$x = (0.3, 0.4, 0.6)$ (15)

By applying Eq. (8), we get:

$d_{memory}(x,m) = |T(x) - T(m)| + |I(x) - I(m)| + |F(x) - F(m)| = 0.3$ (16)

The system considers incoming traffic similar enough to the recorded pattern in memory cell, as $d_{memory}(x,m) = 0.3$, which equals threshold value ϵ. The system can update m with values from, allowing it to adapt to variations in malicious traffic patterns.

The memory cell m is updated by merging old and new values from x. A weighted average is used to determine how much weight is given to new versus old data.

Next, we need to define a value for decay factor $\lambda \in [0,1]$. The choice of λ is based on the desired memory cell sensitivity and stability. Higher λ values (0.7 or 0.8) provide more weight to previous values in memory cells, making the system less susceptible to new inputs and allowing for longer retention of old knowledge. Lower λ levels (e.g., 0.4 or 0.5) increase the system's responsiveness to new data by influencing memory cells more substantially. In this case study the decay factor is set to $\lambda = 0.7$.

Now by applying Eq. (10) – (12), the memory cell m now has: $m = (0.23, 0.47, 0.67)$ (17)

In the case study explained previously, the n-AIS framework showcases its adaptability to new but similar patterns which occur over time, highlighting a steady learning process for identifying malicious traffic. By comparing each new incoming pattern against stored patterns in its memory cells, the n-AIS refines its understanding of what constitutes "malicious" activity in network traffic. This can be achieved with the usage of appropriate neutrosophic measures (distance measure) along with the similarity threshold which allows the n-AIS to selectively update memory cells only when a

new pattern closely aligns with a previously stored one. In this way unnecessary changes are minimized and system stability is preserved.

When an incoming traffic pattern fulfils the similarity requirement, the n-AIS makes use of a proper operator (neutrosophic immunological memory operator) that controls the weight given to past values versus the new observation to update the memory cell values. The latter procedure, which is regulated by a decay factor, enables the system to respond to modest behavioral changes without significantly affecting its memory cells. Within this framework, the n-AIS stays alert to new and changing threats in network traffic but also keeps its core ability to recognize harmful patterns it's already familiar with. During the course of time the n-AIS makes small and careful advancements so that it can better adapt more precisely to changes in network traffic patterns while lowering the likelihood of false positives and missed detections.

In order to test the efficiency of proposed model we conducted the following an experimental test. The objective of the test is to compare the n-AIS model with traditional AIS methods (e.g., clonal selection algorithm) using publicly available datasets that contain various features related to network intrusion for classification tasks. To achieve this, we utilized the KDD Cup 99 dataset [41] for evaluation and tested the performance of our model against the traditional AIS model based on the following metrics: 1) accuracy, 2) false positive rate, and 3) execution time. For more technical details on the environment used for the test, please refer to Appendix B.

The results obtained are depicted in the following table:

Table 1. Summary of results between n-AIS and traditional AIS model.

Metric	*n-AIS (%)*	*AIS (%)*	*Improvement (%)*
Accuracy	96.2	93.2	+3.0
False positive rate	3.2	5.1	-1.9
Execution time (seconds)	24.3	20.1	+4.2

From the above results it is shown that the n-AIS model outperforms AIS in all metrics used for the experiment indicating a favorable trade-off for practical applications. This improvement underlines the practical advantages of integrating neutrosophic logic into AIS, enabling improved adaptability and robustness in handling uncertainty and ambiguity within real-world applications.

5. Conclusions

The field of artificial immune systems (AIS) is one of the most recent natural computing approaches to emerge from engineering, computer science and theoretical immunology. Using the immune system as inspiration has proved very useful when trying to address many computational problems. These computational techniques have many potential applications, such as in distributed and adaptive control, machine learning, pattern recognition, fault and anomaly detection, computer security, optimization, and distributed system design. By suggesting a hybrid AIS model which integrates neutrosophic logic, we achieve a flexible framework to handle uncertain data. In this light, we introduce a novel n-AIS model which redefines the main concepts and operators of AIS in order to help the system deal better with ambiguous patterns. This capacity stems from the utilization of proper neutrosophic measures and concepts that "mimic" AIS operators such as negative selection and immunological memory, ensuring enhanced efficiency in proposed model. For example, cell memory updates only when this is necessary, keeping things stable while adapting to new patterns. The case study examined demonstrates that suggested method works effectively in dynamic contexts like cybersecurity, where data is subject to change and unpredictable. It shows its capacity in detecting malicious activity without raising many false alarms.

As this research serves as an initial step towards this research direction, future work could examine the use of the n-AIS model in other fields, such as fault detection in industrial systems, financial fraud detection, or medical diagnostics, where data uncertainty is also common.

Furthermore, different neutrosophic similarity measurements might be explored to increase the model's capacity to recognize subtle patterns.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Since this paper is intended for the general public, in order for the paper to be self-contained, we provide below dictionary definitions of principal immune systems terms.

Immune system: the bodily system that protects the body from foreign substances, cells, and tissues by producing the immune response and that includes especially the thymus, spleen, lymph nodes, special deposits of lymphoid tissue (as in the gastrointestinal tract and bone marrow), macrophages, lymphocytes including the B cells and T cells, and antibodies; https://www.merriam-webster.com/dictionary/allele. Accessed 18/11/2024.

Antigen: any substance (such as an immunogen or a hapten) foreign to the body that evokes an immune response either alone or after forming a complex with a larger molecule (such as a protein) and that is capable of binding with a product (such as an antibody or T cell) of the immune response; https://www.merriam-webster.com/dictionary/allele. Accessed 18/11/2024.

Antibody: any of a large number of proteins of high molecular weight that are produced normally by specialized B cells after stimulation by an antigen and act specifically against the antigen in an immune response, that are produced abnormally by some cancer cells, and that typically consist of four subunits including two heavy chains and two light chain; https://www.merriam-webster.com/dictionary/allele. Accessed 18/11/2024.

Self and Non-Self: In immunology, "self" refers to the body's own cells and molecules, which are usually recognized and ignored by the immune system. "Non-self" refers to foreign substances (antigens) that the immune system recognizes as potentially harmful and targets for destruction;

Lymphocyte: any of the colorless weakly motile cells originating from stem cells and differentiating in lymphoid tissue (as of the thymus or bone marrow) that are the typical cellular elements of lymph, include the cellular mediators of immunity, and constitute 20 to 30 percent of the white blood cells of normal human blood; https://www.merriam-webster.com/dictionary/allele. Accessed 18/11/2024.

Clonal selection: a procedure whereby specialised immune cells (such T-cells or B-cells) that are able to identify a given antigen are chosen to proliferate, expanding the number of immune cells that are prepared to react to that antigen; https://en.wikipedia.org/wiki/Clonal_selection. Accessed 18/11/2024.

Negative Selection: the process of eliminating any *developing* T or B lymphocytes that are autoreactive, i.e. reactive to the body itself; https://en.wikipedia.org/wiki/Central_tolerance. Accessed 18/11/2024.

Immunological Memory: the ability of the immune system to quickly and specifically recognize an antigen that the body has previously encountered and initiate a corresponding immune response. https://en.wikipedia.org/wiki/Immunological_memory. Accessed 18/11/2024.

Appendix B

- Software configuration

Python Version: Python 3.8
Integrated Development Environment (IDE): Visual Studio Code (VS Code)
Package Manager: pip or conda (for package installation)
Libraries and Frameworks:
NumPy: Version 1.21.2 for numerical operations

Pandas: Version 1.3.3 for data manipulation and analysis
Scikit-learn: Version 0.24.2 for machine learning model training and evaluation

- Dataset Details

Dataset Used: KDD Cup 1999 Dataset (subset of 10% of the full dataset, used for experiment)
Number of Records: Approximately 494,000 records
Number of Features: 41 features, including categorical and continuous attributes
Target Variable: "Attack Type" (denoted as "class" in the dataset)

References

1. Brabazon, A.; O'Neill, M. (2006). *Biologically inspired algorithms for financial modelling*. Springer Science & Business Media.
2. Dasgupta, D. (1999). An overview of artificial immune systems and their applications. *Artificial immune systems and their applications*, 1, 1-21.
3. Castro, L. D.; Timmis, J. I. (2003). Artificial immune systems as a novel soft computing paradigm. *Soft computing*, 7, 526-544.
4. Timmis, J.; Hone, A.; Stibor, T.; Clark, E. (2008). Theoretical advances in artificial immune systems. *Theoretical Computer Science*, 403(1), 11-32.
5. Engelbrecht, A. P. (2007). *Computational intelligence: an introduction*. John Wiley & Sons.
6. Gupta, K. D.; Dasgupta, D. (2021). Negative selection algorithm research and applications in the last decade: A review. *IEEE Transactions on Artificial Intelligence*, 3(2), 110-128.
7. Ji, Z.; Dasgupta, D. (2007). Revisiting negative selection algorithms. *Evolutionary computation*, 15(2), 223-251.
8. Idris, I.; Selamat, A.; Nguyen, N. T.; Omatu, S.; Krejcar, O.; Kuca, K.; Penhaker, M. (2015). A combined negative selection algorithm–particle swarm optimization for an email spam detection system. *Engineering applications of artificial intelligence*, 39, 33-44.
9. Gong, M.; Zhang, J.; Ma, J.; Jiao, L. (2012). An efficient negative selection algorithm with further training for anomaly detection. *Knowledge-Based Systems*, 30, 185-191.
10. Mitchell, M.; Taylor, C. E. (1999). Evolutionary computation: an overview. *Annual Review of Ecology and Systematics*, 593-616.
11. Dasgupta, D.; Michalewicz, Z. (1997). Evolutionary algorithms—an overview. *Evolutionary algorithms in engineering applications*, 3-28.
12. Back, T.; Schwefel, H. P. (1996, May). Evolutionary computation: An overview. *In* Proceedings of IEEE International Conference on Evolutionary Computation (pp. 20-29). IEEE.
13. Vikhar, P. A. (2016, December). Evolutionary algorithms: A critical review and its future prospects. *In* 2016 International conference on global trends in signal processing, information computing and communication (ICGTSPICC) (pp. 261-265). IEEE.
14. Telikani, A.; Tahmassebi, A.; Banzhaf, W.; Gandomi, A. H. (2021). Evolutionary machine learning: A survey. *ACM Computing Surveys (CSUR),* 54(8), 1-35.
15. Haktanirlar Ulutas, B.; Kulturel-Konak, S. (2011). A review of clonal selection algorithm and its applications. *Artificial Intelligence Review*, 36, 117-138.
16. Zhang, W.; Zhang, W.; Yen, G. G.; Jing, H. (2019). A cluster-based clonal selection algorithm for optimization in dynamic environment. *Swarm and Evolutionary Computation*, 50, 100454.
17. De Castro, L. N.; Von Zuben, F. J. (2000). Artificial immune systems: Part II–A survey of applications. FEEC/Univ. Campinas, Campinas, Brazil.
18. Smith, R. E.; Timmis, J.; Stepney, S.; Neal, M. (2005). Conceptual frameworks for artificial immune systems. *International Journal of Unconventional Computing,* 1(3), 315-338.
19. Knight, T.; Timmis, J. (2001, January). AINE: An immunological approach to data mining. *In* Proceedings 2001 IEEE International Conference on Data Mining (pp. 297-304). IEEE Computer Society.
20. Saleem, O.; Mahmood-ul-Hasan, K. (2021). Hierarchical adaptive control of self-stabilizing electromechanical systems using artificial-immune self-tuning mechanism for state weighting-factors. *Journal of Mechanical Science and Technology*, 35, 1235-1250.

21. Piñas, D. F.; Morlet, C. (2008, October). AINE: An IP network emulator. *In* 2008 10th International Workshop on Signal Processing for Space Communications (pp. 1-7). IEEE.
22. Nasraoui, O.; Uribe, C. C.; Coronel, C. R.; Gonzalez, F. (2003, November). Tecno-streams: Tracking evolving clusters in noisy data streams with a scalable immune system learning model. *In* Third IEEE International Conference on Data Mining (pp. 235-242). IEEE.
23. de Castro, L. N.; Von Zuben, F. J. (2002). aiNet: an artificial immune network for data analysis. *In* Data mining: a heuristic approach (pp. 231-260). IGI Global.
24. Aickelin, U.; Cayzer, S. (2008). The danger theory and its application to artificial immune systems. *arXiv preprint arXiv*:0801.3549.
25. Cooper, E. L. (2010). Evolution of immune systems from self/not self to danger to artificial immune systems (AIS). *Physics of life reviews*, 7(1), 55-78.
26. Garrett, S. M. (2005). How do we evaluate artificial immune systems?. *Evolutionary computation*, 13(2), 145-177.
27. Laurentys, C. A.; Palhares, R. M.; Caminhas, W. M. (2010). Design of an artificial immune system based on danger model for fault detection. *Expert Systems with Applications*, 37(7), 5145-5152.
28. Dasgupta, D.; Forrest, S. (1999). An anomaly detection algorithm inspired by the immune system. *Artificial immune systems and their applications*, 262-277.
29. Dasgupta, D. (1999, October). Immunity-based intrusion detection system: A general framework. *In* Proc. of the 22nd NISSC (Vol. 1, pp. 147-160).
30. Cao, Y.; Dasgupta, D. (2003). An immunogenetic approach in chemical spectrum recognition. *In* Advances in Evolutionary Computing: Theory and Applications (pp. 897-914). Berlin, Heidelberg: Springer Berlin Heidelberg.
31. Timmis, J.; Neal, M.; Knight, T. (2002). AINE: machine learning inspired by the immune system. Published in IEEE transactions on evolutionary computation.
32. Kim, J.; Bentley, P. J. (2002, May). Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection. *In* Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600) (Vol. 2, pp. 1015-1020). IEEE.
33. Dasgupta, D. (1999, October). Immunity-based intrusion detection system: A general framework. *In* Proc. of the 22nd NISSC (Vol. 1, pp. 147-160).
34. Hofmeyr, S. A.; Forrest, S. (2000). Architecture for an artificial immune system. *Evolutionary computation*, 8(4), 443-473.
35. Balthrop, J.; Forrest, S.; Glickman, M. R. (2002, May). Revisiting lisys: Parameters and normal behavior. *In* Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600) (Vol. 2, pp. 1045-1050). IEEE.
36. Kim, J.; Wilson, W. O.; Aickelin, U.; McLeod, J. (2005). Cooperative automated worm response and detection immune algorithm (cardinal) inspired by t-cell immunity and tolerance. *In* Artificial Immune Systems: 4th International Conference, ICARIS 2005, Banff, Alberta, Canada, August 14-17, 2005. Proceedings 4 (pp. 168-181). Springer Berlin Heidelberg.
37. Krishnakumar, K.; Neidhoefer, J. (1999). Immunized adaptive critic for an autonomous aircraft control application. *Artificial Immune Systems and Their Applications,* Springer–Verlag, 242-261.
38. Bradley, D. W.; Tyrrell, A. M. (2000, April). Immunotronics: Hardware fault tolerance inspired by the immune system. *In* International Conference on Evolvable Systems (pp. 11-20). Berlin, Heidelberg: Springer Berlin Heidelberg.
39. Dasgupta, D.; KrishnaKumar, K.; Wong, D.; Berry, M. (2004). Negative selection algorithm for aircraft fault detection. *In* Artificial Immune Systems: Third International Conference, ICARIS 2004, Catania, Sicily, Italy, September 13-16, 2004. Proceedings 3 (pp. 1-13). Springer Berlin Heidelberg.
40. Smarandache, F. (1999). *A unifying field in Logics: Neutrosophic Logic. In Philosophy*, American Research Press, pp. 1–141.
41. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P. (1999). KDD Cup 1999 Data [Dataset]. UCI Machine Learning Repository. https://doi.org/10.24432/C51C7N.

Received: July 13, 2024. Accepted: September 19, 2024