ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies

Patryk Widuliński | Faculty of Electronics and Computer Science, Koszalin University of Technology, Poland, ORCID: 0000-0001-7258-3522

Received: 24.10.2023

Accepted: 30.11.2023

Published: 07.12.2023

Cite this article as:
P. Widuliński "Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies," ACIG, vol. 2, no. 1, 2023. doi: 10.60097/ACIG/162896.

Corresponding author:
Patryk Widuliński, Faculty of Electronics and Computer Science, Koszalin University of Technology, Poland; ORCID: 0000-0001-7258-3522; E-MAIL: patryk.widulinski@tu.koszalin.pl

Abstract

In this paper, an overview of artificial immune systems (AIS) used in intrusion detection systems (IDS) is provided, along with a review of recent efforts in this field of cybersecurity. In particular, the focus is on the negative selection algorithm (NSA), a popular, prominent algorithm of the AIS domain based on the human immune system. IDS offer intrusion detection capabilities, both locally and in a network environment. The paper offers a review of recent solutions employing AIS in IDS, capable of detecting anomalous network traffic/breaches and operating system file infections caused by malware. A discussion regarding the reviewed research is presented with an analysis and suggestions for further research, and then the work is concluded.

Keywords

artificial immune systems, cybersecurity, intrusion detection, negative selection, malware

1. Introduction

In the contemporary digital era, computer systems enjoy immense popularity. However, this widespread use has not come without drawbacks, as it has attracted actors with various

motivations, many of whom frequently seek unauthorised access to user data. The threat to computer systems doesn't just stem from individuals desiring to remotely control compromised workstations but is also posed by malicious software, commonly known as malware.

In response to these escalating threats, there has been significant development in intrusion detection systems (IDS) over the past few decades. These systems are dedicated to identifying and combatting both network and local infections, representing a crucial and rapidly evolving category of software within the cybersecurity domain. IDS employ a range of strategies for threat mitigation, which may include, for instance, the filtering of network packets based on predefined rules, or utilising a database of antivirus software signatures.

However, these traditional methods often fall short in detecting novel or previously unidentified threats. This limitation initiated the development of the first IDS inspired by artificial immune systems (AIS), conceptualised to overcome the constraints of their predecessors. IDS that incorporate AIS typically rely on algorithms, such as the negative selection algorithm (NSA) [1], positive selection [2], or clonal selection [3], all of which draw inspiration from biological immune systems. The need to study AIS in intrusion detection for cybersecurity arises from their adaptability and learning capabilities, which are crucial for countering evolving cyber threats. Unlike traditional systems that rely on known threat patterns, AIS can identify and adapt to new/unknown threats in a similar way to biological immune responses. These capabilities are especially vital in tackling zero-day attacks and advanced cyber threats that evade conventional detection methods. Also, the self-organising nature of AIS enables autonomous operation which may be essential in large-scale networking environments where manual monitoring is impractical. The ability of AIS to reduce false positives and their resilience against advanced evasion methods further highlights their suitability for modern applied cybersecurity.

Of the aforementioned algorithms, the NSA approach in particular has garnered substantial attention from the global scientific community. This algorithm functions by generating a collection of receptors, serving as the cyber equivalent of antibodies and T lymphocytes in a biological immune framework. The concept hinges on the principle that these digital "receptors" can identify and flag non-self elements, akin to how a living organism's immune system detects and responds to pathogens. This innovation marks a significant stride forward in ensuring cybersecurity by mimicking the resilience and adaptability of biological immune responses.

The generation of these receptors within the system can be accomplished through various methodologies: some may be randomly created [4], others might be pattern-based [5], among other techniques. Furthermore, these receptors operate based on a parameter known as the activation threshold. Depending on the specific implementation, this threshold may be fixed [6] or varying [7]. However, the application of these solutions has frequently encountered limitations, such as constraints related to the size of the processed files or the presence of vulnerabilities that result in a high percentage of undetectable infections.

To overcome these limitations, the past decade or so has witnessed the emergence of numerous modifications to the NSA, which incorporate various enhanced learning methods for training the receptor set. These methods include the use of real-values [8], Voronoi diagrams [9], two-stage training [10], hierarchical clustering [11], genetic algorithms [12], and mechanisms of adaptive immunoregulation [13]. These solutions are geared towards finding the most effective ways to train receptors, with a prevailing emphasis on approaches that employ variable activation thresholds. The result is an increasingly sophisticated system capable of processing large files and mitigating vulnerabilities.

The aim of this paper is to provide an overview of artificial immune systems used in intrusion detection systems, particularly the negative selection algorithm, and to provide a review of efforts in this field with regard to local and network applied cybersecurity.

2. Background

The fundamental concept that necessitates definition is the security of a computer system. But first, we need to describe what we mean by a computer system. A computer system is defined as an integrated set of hardware and software components that work together to enable users to perform specific computational tasks [14]. An individual instance of a computer system, which might be a personal computer or a high-performance setup for more demanding tasks, is often referred to as a computing device or simply a computer.

The components of a computer system are divided into physical and logical categories [14]. The physical category encompasses computer hardware like the motherboard, RAM, processor, and hard drive [15]. In contrast, the logical category involves various types of data and

software: this includes the configuration of physical components (such as UEFI/BIOS settings), system firmware, the operating system that manages the computer's functions, and user data stored on the hard drive [14, 15].

Computer system security denotes the system's resilience to various threats and unauthorised access [16]. The process of securing a system is a comprehensive effort directed towards the safeguarding of both the hardware components and the data contained within the computing device [16]. Thus, when we discuss computer system security, this encompasses the safety protocols for both physical hardware and the data processed and stored by the system.

Physical security is typically ensured by protecting the computing device from unauthorised physical access by third parties. Data security, however, is a multifaceted challenge. It is not solely dictated by the configuration of UEFI/BIOS, firmware, and the operating system. Instead, it includes a broader suite of protective measures. These can span data encryption, establishment of stringent access controls, network security measures, secure communication protocols, regular software updates, and the implementation of secure data storage and transmission practices.

Several fundamental aspects comprise computer system security [5]:

- **Availability** – a computer system should ideally provide uninterrupted access to its resources and data for authorised users,
- **Data confidentiality** – the system should ensure the confidentiality of user data, preventing access by unauthorised individuals,
- **Integrity** – data within the system should be protected against unwanted alterations, whether it is deletion, overwriting, or corruption,
- **Accurate threat classification** – security software should strive to minimise instances of false positive detections,
- **Accountability** – the computer system should have a built-in logging mechanism so that in the event of a security breach, it is possible to detect the incident and identify potential culprits.

Depending on certain factors, it might be essential to focus on specific aspects of security mentioned above. For instance, if a workstation is used for data archiving, it might be crucial to concentrate on the

integrity aspect of the system's data. A computer system's security policy is determined by the security aspects the system administrator focuses on [17].

An intrusion, or breach, refers to the act of unauthorised individuals accessing a computer system's data. It is important to note that "access" doesn't just refer to data viewing but also includes modifying or deleting them. In such instances, there is a violation of availability, data confidentiality, and system integrity principles. Intrusions can be committed directly by human actors (like hackers) or automated threats (using malware-type software). Breaches carried out by malicious software often serve as preliminary intrusions, paving the way for human actors to access data unauthorisedly [18].

The implementation of a chosen computer system security policy relies on selecting appropriate methods to address specific issues. To protect a workstation from intrusions, an administrator might employ software specialised to prevent such activities. For instance, securing the system against network intrusion attempts can begin with the installation of firewall software, allowing the administrator to block selected system network ports, among other things. This kind of blockade significantly hinders attacks on the ports specified by the administrator. A critical step in securing the system is installing software that detects malicious programs and network traffic. An IDS can constitute such software.

2.1. Intrusion detection systems

In recent years, tools known as intrusion detection systems (IDS) have gained significant traction within the scientific community. These tools are designed to differentiate between desirable and undesirable events through specific operational methods. In general, IDS are primarily employed for identifying unwanted network activities, but they can also serve to detect local threats [19].

IDS essentially utilise two basic primary techniques: rule-based detection and profile-based detection [20]. The former involves matching a sequence of samples against known patterns, which are identified as harmful, termed as "signatures". The latter, on the other hand, relies on system behaviour analysis to detect activities that deviate from the "normal" operational patterns of the environment. However, these fundamental IDS techniques do not incorporate dynamic learning or adaptation based on mitigated intrusions, limiting their capacity for advanced detection of unknown threats.

Consequently, researchers have been motivated to explore contemporary solutions that align with IDS themes. One such solution, derived from nature itself, is the biological immune system (BIS). This system consists of biological structures and processes within an organism that protect against diseases. For effective operation, the immune system must possess the capability to detect a wide array of harmful agents, such as viruses, bacteria and parasites, and distinguish them from the organism's healthy tissues [5].

The immune system is fundamentally composed of two subsystems: the innate system and the adaptive system. The innate system, present in nearly all living organisms, provides what is known as innate (or nonspecific) immunity. Its response to an invading pathogen is immediate; however, it does not retain memory of the exposure and, therefore, does not construct immunological memory [5]. In contrast, the adaptive system allows an organism to build immunological memory, providing specific immunity. Cells involved in this process include T lymphocytes and B lymphocytes, among others. T lymphocytes are responsible for cellular response, eliminating infected or mutated cells, while B lymphocytes are tasked with producing proteins called antibodies. These antibodies bind to antigens on the surfaces of harmful cells, effectively "marking" them for destruction, thereby initiating the humoral response [5]. This intricate biological framework provides an inspiration for cybersecurity measures, propelling the exploration and implementation of advanced and adaptive IDS strategies. One such strategy is artificial immune systems (AIS).

2.2. Artificial immune systems

The innovative field of artificial immune systems has emerged from the parallels between the functionalities of intrusion detection systems and biological immune systems. AIS encompass a suite of computational methods that draw inspiration from biological immunity, appealing due to their inherent capabilities for learning and adaptation within a given environment [21]. A pivotal feature of IDS strategies based on AIS algorithms is their proficiency in distinguishing "self" from "non-self" cells. Notably, algorithms widely applied in AIS-related matters include the negative selection algorithm [19], positive selection algorithm [22], and clonal selection algorithm [3]. These AIS algorithms share certain similarities with neural networks, as they incorporate system training based on a specified dataset.

The negative selection algorithm (NSA), inspired by the adaptive mechanisms of biological immune systems, operates by generating binary strings that can match foreign strings while never aligning with self strings [23]. If a generated binary string matches a self string, it is discarded, mirroring the adaptive system's production of antibodies that bind only with harmful antigens and T lymphocytes that recognise only foreign cells [24].

Conversely, the positive selection algorithm (PSA) functions similarly to the NSA, but instead of matching foreign strings, the strings it produces align solely with self strings [2].

The clonal selection algorithm (CSA) is inspired by the biological immune response that triggers the proliferation of antibodies identifying a specific antigen. The activation of B lymphocytes (for particular antibodies) prompts their cloning, followed by intensive genetic mutation of the antibodies to enhance their antigen compatibility [25]. Similarly, the algorithm identifies the best-matching binary strings and clones them for further mutation, improving the compatibility of the mutated strings [25]. It is employed as a supplementary algorithm to the NSA and PSA.

Both the NSA and PSA present unique advantages and disadvantages. Research indicated in [22] suggests that detection efficiency is superior when using the positive selection algorithm. However, if the number of strings generated by the NSA is fewer than the number of self strings, the negative selection algorithm may prove more effective [7].

2.3. Negative selection algorithm

The primary objective of the negative selection algorithm (NSA) is to establish a collection of strings proficient in intrusion detection [6]. These strings, generated by the algorithm, are usually referred to as "receptors" or "detectors", but the term "antibodies" also occurs. Each receptor possesses a definitive length denoted as *l* [4]. *E*very prospective receptor undergoes scrutiny for its compatibility with any "self" string, wherein a "self" string signifies a sequence that should never be flagged as an anomaly. For this purpose, the NSA employs a parameter, *m,* representing the receptor's activation threshold [26]. A receptor is deemed activated if it matches another binary string. Depending on the rule used for matching, the matching process usually involves the occurrence of *m* identical, consecutive bits at the same position *k* in both the receptor and the binary string under examination [5].

If a generated string matches with at least one "self" string, it cannot become a receptor and is consequently dismissed. Traditionally, the NSA assumes the existence of a single receptor set **R**, encompassing all generated receptors [4].

The methodology behind receptor generation is not predefined – many methods of generation exist – but for the sake of simplicity, the random generation method will be outlined [4]. Random generation involves a parameter R_{max}, which dictates the maximum count of receptors to be generated. Given a defined parameter *l*, R_{max} candidates for receptors are generated. Each receptor candidate is subjected to the aforementioned verification before being included in the resultant set **R**. Typically, receptors generated via NSA do not facilitate a 100% anomaly detection rate. Zones not covered by receptors are referred to as holes [27].

The negative selection algorithm can be adapted as the foundational mechanism for infection detection in IDS. When the NSA is employed for infection detection, the input from the receptor generator is substituted with a stream of strings for IDS examination. The set of "self" strings is replaced by the receptor set **R**. Compatibility is assessed using the same parameters *l* and *m* as in the case of receptor generation. If at least one "self" string matches, the algorithm ceases operation, signalling an infection detection, which is a divergence from the receptor-generation stage (where the algorithm would have rejected the receptor candidate instead).

Key performance indicators for the IDS and the algorithms applied within it, including the negative selection algorithm, are:

- TP (True Positives) – the count of accurately identified infections,
- TN (True Negatives) – the count of correctly unidentified infections,
- FP (False Positives) – the count of inaccurately identified infections,
- FN (False Negatives) – the count of inaccurately unidentified infections.

Additional indicators may be:

- the duration required for receptor generation,

- the quantity of receptors retained in memory following generation,
- memory usage by primary receptors,
- memory usage by all receptors,
- memory occupied by the original program.

3. Review of the use of artificial immune systems

Algorithms of artificial immune systems are eagerly employed, explored, and refined within the scientific community.

González, Dasgupta and Kozma [28] applied a data representation using a two-dimensional plane and real numbers for the space of self and non-self strings in their examination of the algorithm (RNSA – real-valued negative selection algorithm). Research was also conducted using binary numbers represented in Grey code. A crucial conclusion drawn by the researchers was the emphasis on the importance of appropriately tailoring the matching rule of the negative selection algorithm in accordance with the intended use of the IDS. They highlighted that for applications where the entire space of self strings is known (such as, for instance, scanning for data integrity verification), the generalisation of self-data is not as critical. Ji and Dasgupta [29] discussed the challenges encountered when implementing the NSA grounded in real number values. They posited that the majority of the problems reported are often the result of incorrect application of the technique or challenges that aren't exclusively related to negative selection algorithms. They argued that, in contrast, tests using artificial and established real-world data demonstrate that NSAs possess significant adaptability in maintaining a balance between effectiveness and robustness, as well as in incorporating elements tailored to specific fields within the approach, such as different types of distance calculations.

Ji and Dasgupta [7] enhanced the NSA through the introduction of variable-length detectors (V-detectors). These detectors, thanks to their variable length, more efficiently "plug" the holes that arise during generation. Studies demonstrated that the algorithm's performance improved without a significant increase in its complexity. Lu, Zhang, Wang, and Gong [30] proposed an NSA method using V-detectors for ransomware detection. In work [11], a fast negative selection algorithm based on the hierarchical structure of the

self-string set was presented. Zhu, Chen, Yang, Li, Yang, and Zhang [31] utilised Voronoi diagrams to enhance the NSA. Their proposed VorNSA algorithm constructs a Voronoi diagram based on a test set, subsequently generating two types of receptors based on this diagram, reducing the receptor-generation time. The testing (detection) phase was also redesigned – data are divided into smaller intervals, mapped, and sorted during the reduction stage. Another approach using Voronoi diagrams is described in [9].

González, Dasgupta, and Niño [32] introduced a version of the negative selection algorithm, which was expanded to estimate the optimal number of receptors needed to cover the space of non-self strings (RRNSA – randomised real-value negative selection algorithm). In addition to expanding the algorithm itself, the authors conducted an in-depth theoretical analysis forming the basis for performance analysis of their improved version. They inferred that the RRNS variant operates faster than RNS but noted that in certain cases, heuristic algorithms are even more efficient, although other algorithms may have a better theoretical foundation.

Marciniak, Wawryn and Widuliński [33] demonstrated the use of the negative selection algorithm for controlling a heating boiler. In [10], a version of the algorithm trained multiple times for a different number of self strings to enhance performance was described. The approach proposed in [13] takes into account the use of an adaptive immune regulation mechanism to calculate the radius on the plane of self strings. Saurabh and Verma [34] proposed an NSA version with a tuning function called NIIAD. Balicki [35] introduced NSA to overcome the limitations of a multi-criteria evolutionary algorithm. Study [36] indicated that AIS could be applied to threat detection in mobile operating systems.

In [37], a system called MILA (multilevel immune learning algorithm) was proposed, which considers not only the application of NSA but also receptor expansion using the clonal method and a dynamic receptor-generation method in one solution. Fakhari and Moghadam [38] introduced an NSA version named NSSAC, which is capable of adapting to data sets. Gao, Ovaska, and Wang [12] proposed a receptor-generation method based on a genetic algorithm in their work. Paper [39] describes an IDS system based on an evolutionary algorithm for anomaly detection in distributed computer systems. In [40], information about estimating the range of receptors in NSA was provided.

Kamal and Bhusry [41] presented negative selection algorithms optimised by artificial bee colonies (ABC algorithm). Nunes de Castro and von Zuben [42] described the aiNet system based on AIS algorithms for data analysis. Prathyusha and Kannayaram [43] introduced a novel mechanism based on AIS for mitigating DDoS network attacks in the cloud.

3.1. Use of artificial immune systems in intrusion detection

The use of artificial immune systems in intrusion detection systems is a popular notion among researchers.

In [44], the authors introduced an implementation of a clonal-based artificial immune system as the central mechanism for a network intrusion detection system.

The research was structured around two main stages: training and testing. The initial step in the training phase involved creating a series of "antibodies". These antibodies are essentially pieces of information that were derived from six specific types of network attacks: Smurf, Land, Satan, Neptune, Ipsweep, and Portsweep. Each antibody possesses eight unique features that allow it to effectively differentiate between these various forms of attacks: the duration, type of protocol, type of service, flag, source bytes, number of access files, number of outbound commands and service difference host rate.

In the testing phase, the researchers examined the effectiveness of their AIS-based IDS against the six types of attacks mentioned. The aim was to evaluate how well the system could detect these intrusions in practice, reflecting real-world applications where an IDS needs to reliably identify any attempt to breach network security.

The researchers used a dataset known as the KDD Cup, containing 284,948 connection data, of which 10% (28,494 connections) were randomly chosen for testing, while the rest were used for training. Initially, a probability value of 0.2 was employed, indicating a 20% chance of each attack connection being chosen for testing. The AIS algorithm correctly identified 27,552 out of 28,494 attack connections, a true-positive rate of roughly 97%.

Further experiments were conducted with different probability values (0.3, 0.4, and 0.5) to discern their effect on the study. The findings revealed that the AIS algorithm recognised more attack connections

as the probability value increased. A 0.3 probability yielded a 97% true-positive rate, 0.4 resulted in 98%, and 0.5 demonstrated the highest rate at 99.86%, with only 39 attack connections not correctly identified.

The authors observed that using a high probability value for selection might skew the testing dataset towards connections from the early part of the dataset, possibly consisting of many similar data connections, since the same attack data are grouped together in the raw dataset. This could reduce the effectiveness of testing the algorithm's performance in network intrusion detection. Hence, a smaller probability value is recommended to ensure a more even distribution of attack patterns in the testing dataset. Regarding the training process, the primary aim was to generate antibodies with high fitness values that are considered crucial for recognising attack data during testing. The fitness value in this context ranges between -1 and 1, with values close to 1 indicating high-quality antibodies. The AIS algorithm, after running 100 iterations, produced the best-quality antibody with a fitness value of 0.46 using a 0.2 selection probability. Other probabilities yielded slightly lower fitness values, with the 0.5 probability producing the lowest-quality antibody with a fitness value of just 0.41.

The authors concluded that the cloning and mutation processes are crucial for the suggested algorithm to produce effective solutions during training. The positive results shown by AIS demonstrated its capability to address the issue, matching the performance of other methods in existing scientific research.

Study [45] introduces an Internet of Things (IoT) anomaly intrusion detection system specifically for smart homes, employing a hybrid model that combines artificial immune system and extreme learning machine (ELM) methodologies, referred to as the AIS-ELM IDS framework. This system is integrated into a smart home environment through a Mozilla gateway installed on a Raspberry Pi, which connects all smart devices via a router using the REST API for streamlined monitoring and control.

The AIS component of the IDS uses the clonal selection method to enhance the system's detection capabilities through receptor maturation. The process begins with an initialisation stage where input data is assessed to determine the optimal inputs with the highest affinity and lowest negative selection. This is followed by the clonal selection stage, encompassing clonal, mutation, and substitution phases.

The ELM algorithm assigns arbitrary input weights and biases, calculates a hidden layer output matrix, and determines the output weight. The integration of AIS and ELM processes in the IDS helps in the accurate detection of normal and abnormal patterns in network traffic, flagging them as "1" for normal and "0" for anomalies.

The system enhances home security by initiating an immediate response when an anomaly is detected. It employs a custom-designed alarm system to alert the homeowner, prompting them to act – either by disconnecting the internet in the event of an external threat or by isolating the compromised segment within the smart home for internal threats. If the system doesn't detect any user action within two minutes, it autonomously disconnects the internet, adding an extra layer of security. This approach not only optimises intrusion detection but also provides an automated, rapid response mechanism.

Brown, Anwar and Dozier [46] proposed the modified artificial immune system (mAIS) model. In mAIS, two usual sets of detectors are developed: the self detector set and the non-self detector set. Following generation of the detector sets, in the "Proportion Based Classification" phase, these detector sets work in tandem to classify unknown traffic instances. An instance is labelled as non-self or abnormal if a larger fraction of non-self detectors identify it compared to self detectors, and vice versa. Given the potentially more severe consequences of false negatives compared to false positives, any instance equally identified by both detector types is classified as non-self to minimise risk.

An "Interval Matching Rule" is employed, involving each detector's 41 intervals, each corresponding to a specific dataset feature. A match between a detector and an instance is determined by selecting an "r-value". If the number of features within a detector's intervals meets or exceeds this r-value, the detector is considered to match the instance.

The dataset used for this work was the UNB ISCX Intrusion Detection Evaluation Dataset, selected for its recentness and relevance to contemporary network scenarios. It comprises 148,517 instances of network traffic, with 77,054 normal and 71,463 anomalous instances. Each instance has 41 different features. The testing method involved dividing the dataset into training, tuning, and test sets. Initially, all instances were in the training set, from which 50,000 instances were moved into the test set and another 50,000 into the tuning set, leaving 48,517 in the training set. This process was repeated 30 times for each of the 6 folds. Detectors were evaluated and those

not matching any instance were promoted to mature detectors. The best-performing detectors were retained for testing. After each fold, data sets were rotated and the process repeated, resulting in 180 total runs.

The study opted for 1,000 initial immature detectors to reduce computational demands, with a fixed width of 1.0 for the detectors. While general detectors cover more hypothesis space, they can increase false positives.

Experiments ran for approximately 10 hours on a test computer. As per the results, the standard AIS marginally surpassed the mAIS in detection rate and accuracy, whereas the mAIS performed slightly better in terms of the true negative rate and false positive rate. The standard AIS covered more hypothesis space due to less internal competition between detectors. The authors concluded that both standard AIS and mAIS demonstrated similar performance levels on the dataset utilised. The varied nature of normal and abnormal network instances might contribute to this outcome, potentially restricting the efficiency of mAIS. The authors suggested that employing a larger and more diverse set of initial detectors could enhance the performance of both systems.

Tosin and Gbenga [47] enhanced their proposed network intrusion detection system by integrating the NSA with a feature selection mechanism. Due to the NSA's non-prior knowledge requirement and nature as a one-class classifier, NSA faces scalability issues due to the large number of detectors needed and high false positives. To address the scalability issues, the research introduces a feature selection process, utilising an artificial neural network (ANN) to reduce the dimensionality of the input data, thereby tackling NSALG's scalability issue. This process involves passing each feature (data column) through the ANN to evaluate its relevance based on classification accuracy, with those exceeding 80% accuracy being retained. The methodology encompasses three stages: data preprocessing for normalisation and feature selection, the NSA stage for detector generation and anomaly detection, and finally, an alert generation phase.

Utilising the NSL-KDD dataset, the model's performance was evaluated using a confusion matrix approach. The experiments were conducted in two scenarios: with and without the feature selection mechanism. Improvements were observed when the feature selection was employed. Specifically, there were significant increases in true-positive rate (TPR), true negative rate (TNR), and overall accuracy (ACC), alongside reductions in the false positive rate (FPR) and false

negative rate (FNR). TPR saw an 11.65% increase, TNR improved by 213.91%, and ACC increased by 26.54%. FPR and FNR decreased by 70.62% and 19.75%, respectively, indicating fewer false alarms and missed detections.

In the work's conclusion, the authors state that the integration of feature selection with NSA substantially enhanced IDS performance by mitigating scalability issues.

Local-based intrusion detection systems utilising AIS also exist. In strona 24, Widuliński and Wawryn explored the possibility of employing an AIS-based IDS locally to scan for infections on a computer. They discuss an advanced system for detecting unauthorised changes to files within an operating system. The IDS works by constantly monitoring a designated area within the operating system, which the user sets up first. Its primary job is to scan files in this area to detect any unexpected or suspicious alterations that are indicative of potential security threats or malware intrusions. The IDS's functionality is managed by a central component called the control unit (CU). The CU oversees the operations of two critical parts of the system: the receptor-generation unit (RGU) and the anomaly detection unit (ADU). When the system starts, the RGU runs first. Its role is to create the set(s) of receptors which will be used to identify whether the system's files have been tampered with.

In the case of this IDS, these receptors are binary strings, sequences of bits: ones and zeros, with a specific length. They're designed to detect "non-self" data – essentially, infections or modifications – within the monitored program files. Each file under surveillance gets its own unique set of receptors, which are stored separately, either in memory (RAM) or as a file on non-volatile storage such as a hard drive or flash drive, to ensure they're secure and intact. The system is designed with a special interface to allow the IDS to be adaptable and functional across different platforms.

Once the receptors are generated, the CU instructs the ADU block to start operation. The ADU scans the safeguarded files, comparing their contents with the receptors. This comparison is done using a formula (or rule) that checks for matching bit patterns between the receptors and each 32-bit segment of the monitored program's bytes. When a match is found, it flags that part of the program as potentially compromised.

In instances where the ADU identifies an intrusion, it logs the issue. Afterwards, it informs the user precisely where the problem is and

what parts of the data have been altered – likely due to malicious software (malware). The system doesn't stop after one scan; it continues to check the files repeatedly until the user decides to halt operation. However, legitimate updates to files, such as when a software update occurs, necessitate the creation of new receptors. If there is a valid change, the system doesn't mistake it for an intrusion; the CU simply instructs the RGU to start the receptor-generation process anew. In strona 24, a modification of the NSA was proposed to mitigate false negatives when anomalies (or infections) occurred between 32-bit program memory cells. The modification, called intercellular receptors (ICR), offers an additional, smaller receptor set to assist with detection of infections that might occur between memory cells.

4. Discussion

The reviewed research highlights the versatility of artificial immune systems, particularly when used with intrusion detection systems, which is a domain of cybersecurity. The adaptive and self-learning characteristics of AIS algorithms have shown considerable promise in identifying and responding to network intrusions, underlining their adaptability and efficiency in real-world applications.

Research by González, Dasgupta, and others highlights the importance of tailoring the matching rule in negative selection algorithms for specific applications, affirming that the flexibility of AIS can be optimal when the algorithms are adapted for their intended purposes. The introduction of variable-length detectors, as discussed by Ji and Dasgupta, and the use of V-detectors in the algorithms, show an evolutionary leap, enhancing detection efficiency without substantially increasing system complexity.

The effectiveness of AIS in IDS, as evidenced in studies [44] and [45], is particularly noteworthy. The high true-positive rates reported confirm the system's robustness and ability to identify network intrusions. However, the studies also caution about potential biases in the testing dataset and the importance of a balanced and diverse set of data for training, highlighting that the reliability of AIS is significantly influenced by the quality of the input it receives. This is a critical insight, reflecting the principle that the output is only as good as the input.

Moreover, the integration of AIS with other methodologies, such as the extreme learning machine (ELM) in [45] and artificial neural

networks (ANN) in [47], points towards a growing trend of hybrid models. These models aim to combine the strengths of various systems to achieve higher efficiency and reliability, while also addressing inherent challenges such as scalability issues and high false positives in NSA.

Despite these advances, studies such as those carried out by Brown, Anwar, and Dozier [46] suggest that there is still room for improvement, especially concerning the reduction of false positives and enhancement of detection accuracy. This indicates that while AIS solutions are a powerful tool, their efficacy can be further optimised, potentially through the integration of more diverse detectors, refinement of algorithms, or hybridisation with other effective techniques.

The IDS proposed by Widuliński and Wawryn introduces a localised solution for detecting unauthorised alterations within an operating system. This approach represents an application of AIS in cybersecurity, marking a departure from more generic, network-focused IDS. The system's capacity to continually generate and update receptors allows for an adaptability and sensitivity to changes within the system's files. The operation of the IDS seems to face some unique challenges, particularly concerning the differentiation between legitimate alterations, like software updates, and unauthorised changes. The system's reliance on user-initiated receptor regeneration following legitimate updates could potentially introduce vulnerabilities, particularly if the user is unaware of the necessity of this action following updates. The introduction of intercellular receptors (ICR) addresses a critical gap in traditional locally utilised NSA methodologies by targeting the detection of anomalies occurring between 32-bit memory cells, and improves the true-positive rates by about 15% while slightly increasing the memory usage.

Reviewing the recent advances in local and network AIS-based cybersecurity, a distinct lack of IDS solutions combining both local and network anomaly detection can be observed. A novel hybrid AIS-based IDS that integrates both local and network detection capabilities would represent a significant advancement in cybersecurity. Such a system could combine the strengths of both approaches to provide a more comprehensive defence mechanism against a variety of cyber threats. Some of the potential benefits of such a system could include:

- **Dynamic receptor generation** – the system could continuously update its defence mechanisms based on new potential threats detected across the network and local machines. This would

be especially beneficial in combatting zero-day exploits, where traditional signature-based methods are inadequate,

- **Context-aware detection** – by analysing data from both the local environment and network traffic, the hybrid IDS could employ machine learning algorithms to better understand the context, enhancing its ability to distinguish between normal changes and potential threats,

- **Real-time cross-verification** – when an anomaly is detected locally, the system could cross-verify it with network data to confirm if the anomaly is an isolated incident or part of a broader network intrusion,

- **Adaptive learning** – over time, the hybrid system could learn from the traffic patterns and typical file changes within the network and local systems, improving its detection rates further.

Nonetheless, the development of such a hybrid system would also pose some challenges, such as the complexity of integrating local and network IDS functionalities, potential privacy concerns, and the increased system resources required.

The overview presented in this paper contributes to the recent state of research in the field of cybersecurity by offering a focused analysis of the NSA within AIS for IDS. A detailed exploration of the NSA's theoretical and practical applications, highlighting recent advancements, has been provided. The interdisciplinary approach – drawing insights from biological systems – also highlights the connection between biology and cybersecurity, encouraging innovative ideas in IDS research.

While a comprehensive overview of the application of AIS in IDS has been provided, it is also important to acknowledge certain limitations inherent in this focused approach. The primary limitation is the concentrated emphasis on NSA. While NSA is a significant and influential algorithm within AIS, the focus on this single algorithm potentially overlooks the diverse range of other algorithms within the AIS domain, such as the positive selection algorithm (PSA) or the clonal selection algorithm (CSA). This narrow scope may limit the comprehensiveness of the review in capturing the full spectrum of AIS capabilities. Another limitation of the work is the lack of a comparative analysis with non-AIS-based IDS approaches, which would be adequate for providing a balanced view of where NSA stands in relation to other methodologies.

5. Conclusions

An overview of artificial immune systems, intrusion detection systems and a review of efforts in the field have been presented. The reviewed research shows significant potential of AIS in enhancing intrusion detection systems. The adaptability, versatility, and self-regulatory aspects of AIS make it a formidable approach to securing local computers and networks against a variety of intrusions.

In conclusion:

- Tailoring algorithms to specific applications enhances the effectiveness of AIS. This customisation, particularly in negative selection algorithms, is crucial for optimising performance in different environments.
- The introduction of innovative methods, such as variable-length detectors and the use of Voronoi diagrams, improves the efficiency of intrusion detection without overly complicating the systems.
- Hybrid models, combining AIS with other techniques like ELM or ANN, have emerged as highly effective in improving accuracy and reducing false positives, indicating a promising direction for future research and application.
- Despite the demonstrated efficacy of AIS in IDS, there remains a need for further refinement to reduce false positives and improve detection accuracy.
- The success of AIS significantly hinges on the quality of data used for training, stressing the importance of proper datasets that reflect real-world scenarios.

All in all, AIS hold substantial promise in the realm of IDS, providing a robust, adaptable, and intelligent approach to local and network cybersecurity. Continued research and development in this field are to be encouraged, focusing on customised solutions, algorithmic advancements, and hybrid models, to fully realise the potential of AIS in safeguarding digital environments. Research on hybrid solutions combining local and network approaches in particular appears to be a reasonable avenue to explore in the future.

References

[1] P. Helman and S. Forrest, *An efficient algorithm for generating random antibody strings*, Technical Report CS-94-07, The University of New Mexico, 1994.

[2] H. Alrubayyi, G. Goteng, M. Jaber, and J. Kelly, "A Novel Negative and Positive Selection Algorithm to Detect Unknown Malware in the IoT," *IEEE INFOCOM 202*1 – *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–6, 2021. doi:10.1109/infocomwkshps51825.2021.9484483.

[3] A. S. Perelson and G. F. Oster, "Theoretical studies of clonal selection: Minimal antibody repertoire size and reliability of self-non-self discrimination," *Journal of Theoretical Biology*, vol. 81, no. 4, pp. 645–670, 1979. doi:10.1016/0022-5193(79)90275-3.

[4] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," *Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 202–212, 1994. doi:10.1109/risp.1994.296580.

[5] S. Hofmeyr, "An Immunological Model of Distributed Detection and Its Application to Computer Security," doctoral dissertation, University of Witwatersrand, Johannesburg, South Africa, 1999.

[6] D. Li, S. Liu, and H. Zhang, "Negative selection algorithm with constant detectors for anomaly detection, "*Applied Soft Computing*, vol. 36, pp. 618–632, 2015. doi:10.1016/j.asoc.2015.08.011.

[7] Z. Ji and D. Dasgupta, "Estimating the detector coverage in a negative selection algorithm," *Proceedings of the 2005 conference on Genetic and evolutionary computation – GECCO '05*, pp. 281–288, 2005. doi:10.1145/1068009.1068056.

[8] S. E. Dixon, "Studies on Real-Valued Negative Selection Algorithms for Self-Nonself Discrimination," M. Sc. thesis, California Polytechnic State University, San Luis Obispo, USA, 2010.

[9] G. Zhao et al., "Voronoi-Based Continuous k Nearest Neighbor Search in Mobile Navigation," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 6, pp. 2247–2257, 2011. doi:10.1109/tie.2009.2026372.

[10] M. Gong, J. Zhang, J. Ma, and L. Jiao, "An efficient negative selection algorithm with further training for anomaly detection," *Knowledge-Based Systems*, vol. 30, pp. 185–191, 2012. doi:10.1016/j.knosys.2012.01.004.

[11] W. Chen, T. Li, X. Liu, and B. Zhang, "A negative selection algorithm based on hierarchical clustering of self set," *Science China Information Sciences*, vol. 56, no. 8, pp. 1–13, 2011. doi:10.1007/s11432-011-4323-7.

[12] X. Gao, S. Ovaska, and X. Wang, "Genetic Algorithms-based Detector Generation in Negative Selection Algorithm," *2006 IEEE Mountain Workshop on Adaptive and Learning Systems*, pp. 133–137, 2006. doi:10.1109/smcals.2006.250704.

[13] H. Deng and T. Yang, "A negative selection algorithm based on adaptive immunoregulation," *2020 5th International Conference on Computational Intelligence and Applications (ICCIA)*, pp. 177–182, 2020. doi:10.1109/iccia49625.2020.00041.

[14] A. Elahi, C*omputer Systems: Digital Design, Fundamentals of Computer Architecture and Assembly Language*, 1st ed. Cham: Springer, 2018.

[15] N. Nisan and S. Schocken, *The Elements of Computing Systems: Building a Modern Computer from First Principles*, 1st ed. Cambridge, MA: The MIT Press, 2005.

[16] L. F. Reese, "Challenges faced today by computer security practitioners," *[1989 Proceedings] Fifth Annual Computer Security Applications Conference*, 1989. doi:10.1109/csac.1989.81044.

[17] L. Mixia, Y. Dongmei, Z. Qiuyu, and Z. Honglei, "Network Security Risk Assessment and Situation Analysis," *2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID)*, 2007. doi:10.1109/iwasid.2007.373676.

[18] A. Datta, S. Jha, N. Li, D. Melski, and T. Reps, "Analysis Techniques for Information Security," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 2, no. 1, pp. 1–164, 2010. doi:10.2200/s00260ed1v01y201003spt002.

[19] C. J. Delona, P. V. Haripriya, and J. S. Anju, "Negative Selection Algorithm: A Survey," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 6, no. 4, pp. 711–715, 2017.

[20] L. Reznik, "Intrusion Detection Systems," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security*, 1st ed. Hoboken, NJ: Wiley-IEEE Press, 2022, pp. 109–176.

[21] J. D. Farmer, N. H. Packard, and A. S. Perelson, "The immune system, adaptation, and machine learning," *Physica D: Nonlinear Phenomena*, vol. 22, no. 1–3, pp. 187–204, 1986. doi:10.1016/0167-2789(86)90240-x.

[22] F. Zhang and Y. Ma, "Integrated Negative Selection Algorithm and Positive Selection Algorithm for malware detection," *2016 International Conference on*

Progress in Informatics and Computing (PIC), pp. 605–609, 2016. doi:10.1109/pic.2016.7949572.

[23] M. Ayara, J. Timmis, R. de Lemos, L. N. de Castro, and R. Duncan, "Negative selection: How to generate detectors," *Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS)*, pp. 182–196, 2002.

[24] R. J. De Boer and A. S. Perelson, "How diverse should the immune system be?," *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 252, no. 1335, pp. 171–175, 1993. doi:10.1098/rspb.1993.0062.

[25] L. N. de Castro and F. J. Von Zuben, "Learning and optimization using the clonal selection principle," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 239–251, 2002. doi:10.1109/tevc.2002.1011539.

[26] F. González, D. Dasgupta, and J. Gómez, "The Effect of Binary Matching Rules in Negative Selection," *Genetic and Evolutionary Computation – GECCO 2003*, pp. 195–206, 2003. doi:10.1007/3-540-45105-6_25.

[27] P. D'haeseleer, S. Forrest, and P. Helman, "An immunological approach to change detection: algorithms, analysis and implications," *Proceedings 1996 IEEE Symposium on Security and Privacy*, 1996. doi:10.1109/secpri.1996.502674.

[28] F. Gonzalez, D. Dasgupta, and R. Kozma, "Combining negative selection and classification techniques for anomaly detection," *Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No.02TH8600)*, pp. 705–710, 2002. doi:10.1109/cec.2002.1007012.

[29] Z. Ji, "Negative selection algorithms: From the thymus to V-detector," PhD dissertation, Department of Computer Science, The University of Memphis, Memphis, Tennessee, USA, 2006.

[30] T. Lu, L. Zhang, S. Wang, and Q. Gong, "Ransomware detection based on V-detector negative selection algorithm," *2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, pp. 531–536, 2017. doi:10.1109/spac.2017.8304335.

[31] F. Zhu, W. Chen, H. Yang, T. Li, T. Yang et al., "A Quick Negative Selection Algorithm for One-Class Classification in Big Data Era," *Mathematical Problems in Engineering*, vol. 2017, pp. 1–7, 2017. doi:10.1155/2017/3956415.

[32] F. González, D. Dasgupta, and L. F. Niño, "A Randomized Real-Valued Negative Selection Algorithm," *Lecture Notes in Computer Science*, vol. 2787, pp. 261–272, 2003. doi:10.1007/978-3-540-45192-1_25.

[33] J. Marciniak, K. Wawryn, and P. Widulinski, "An artificial immune negative selection algorithm to control water temperature in the outlet of the chamber," *2018 International Conference on Signals and Electronic Systems (ICSES)*, pp. 236–241, 2018. doi:10.1109/ICSES.2018.8507293.

[34] P. Saurabh and B. Verma, "A Novel Immunity inspired approach for Anomaly Detection," *International Journal of Computer Applications*, vol. 94, no. 15, pp. 14–19, 2014. doi:10.5120/16418-6034.

[35] J. Balicki, "Negative Selection with Ranking Procedure in Tabu-Based Multi-criterion Evolutionary Algorithm for Task Assignment," *Computational Science – ICCS 2006*, pp. 863–870, 2006. doi:10.1007/11758532_112.

[36] J. Brown, M. Anwar, and G. Dozier, "Detection of Mobile Malware: An Artificial Immunity Approach," *2016 IEEE Security and Privacy Workshops (SPW)*, pp. 74–80, 2016. doi:10.1109/spw.2016.32.

[37] D. Dasgupta, "Immunity-based Intrusion Detection System: A General Framework," *Proceedings of 22nd National Information Systems Security Conference*, pp. 147–160, 1999.

[38] S. N. S. Fakhari and A. M. E. Moghadam, "NSSAC: Negative selection-based self adaptive classifier," *2011 International Symposium on Innovations in Intelligent Systems and Applications*, pp. 29–33, 2011. doi:10.1109/inista.2011.5946064.

[39] C. R. Haag, G. B. Lamont, P. D. Williams, and G. L. Peterson, "An artificial immune system-inspired multiobjective evolutionary algorithm with application to the detection of distributed computer network intrusions," *Proceedings of the 2007 GECCO conference companion on Genetic and evolutionary computation – GECCO '07*, pp. 420–435, 2007. doi:10.1145/1274000.1274035.

[40] Z. Ji, D. Dasgupta, "Real-Valued Negative Selection Algorithm with Variable-Sized Detectors," *Genetic and Evolutionary Computation – GECCO 2004*, pp. 287–298, 2004. doi:10.1007/978-3-540-24854-5_30.

[41] P. Kamal and M. Bhusry, "Artificial Bee Colony Optimization based Negative Selection Algorithms to Classify Iris Plant Dataset," *International Journal of Computer Applications*, vol. 133, no. 10, pp. 40–43, 2016. doi:10.5120/ijca2016908072.

[42] L. Nunes de Castro and F. J. Von Zuben, "aiNet: An Artificial Immune Network for Data Analysis," *Data Mining: A Heuristic Approach*, pp. 231–260, 2002. doi:10.4018/978-1-930708-25-9.ch012.

[43] D. J. Prathyusha and G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment," *Evolutionary Intelligence*, vol. 14, no. 2, pp. 607–618, 2020. doi:10.1007/s12065-019-00340-4.

[44] S. I. Suliman, M. S. Abd Shukor, M. Kassim, R. Mohamad, and S. Shahbudin, "Network Intrusion Detection System Using Artificial Immune System (AIS)," *2018 3rd International Conference on Computer and Communication Systems (ICCCS*), pp. 178–182, 2018. doi:10.1109/CCOMS.2018.8463274.

[45] E. D. Alalade, "Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach," *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–2, 2020. doi:10.1109/WF-IoT48130.2020.9221151.

[46] J. Brown, M. Anwar and G. Dozier, "Intrusion Detection Using a Multiple-Detector Set Artificial Immune System," *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, pp. 283–286, 2016. doi:10.1109/IRI.2016.45.

[47] S.-I. T. Tosin and J. R. Gbenga, "Negative selection algorithm based intrusion detection model," *2020 IEEE 20th Mediterranean Electrotechnical Conference (MELECON)*, pp. 202–206, 2020.

[48] P. Widulinski and K. Wawryn, "A human immunity inspired intrusion detection system to search for infections in an operating system," *2020 27th International Conference on Mixed Design of Integrated Circuits and Systems (MIXDES)*, pp. 187–191, 2020. doi:10.23919/MIXDES49814.2020.9155771.