JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Immune Inspired Cyber Defence-An Intrusion Detection Approach

Towards Imuune Driven Intrusion Detection

[1]Jashanpreet Kaur, [2]Daljit Singh, [3]Kuldeepak Singh

[1]Pursuing Master's Degree, [2]Assitant Professor, [3]Assitant Professor
[1]Electronics and Communciation Engineering,
[1]Guru Nanak Dev Engineering college, Ludhiana, India

Abstract : Malware is specifically designed to break into computer systems and take advantage of any weak spots in intrusion detection systems. As malicious software keeps evolving, it becomes harder for security systems to keep up. A major problem is finding new or hidden malware because attackers use tricks to hide their activities and avoid being caught. To tackle this, this paper suggests using an intrusion detection system inspired by how the human immune system works. This approach allows the system to learn from experience, spot unusual behavior, and handle new threats by using ideas like danger signals, cloning of detectors, distinguishing between normal and abnormal behavior, and removing harmful elements. Tests on standard datasets show that this immune-inspired system catches attacks more accurately and produces fewer false alarms than traditional methods. Its design, based on biological principles, helps it adjust to changing network conditions and detect threats that it hasn't seen before, making it a strong option for future cybersecurity defenses.

IndexTerms **- Cyber-security, Intrusion detection system, Artificial immune system, Artificial Immune Algorithms, Immune inspired threat protection, malware..**

I. INTRODUCTION

An **Immune-inspired Intrusion Detection System (IDS)** represents an innovative approach to cyber security, drawing on the principles of the human immune system to detect and respond to cyber threats. An Intrusion Detection System (IDS) is a security product that scans network traffic or system activity for malicious activity or policy infractions. Its main job is to identify unauthorized access attempts, abnormal usage patterns, or recognized attack patterns, and alert security staff so they can take appropriate action.Traditional IDS technologies is classified into signature-based and anomaly-based systems which often struggle with detecting new, sophisticated, or zero-day attacks. These systems typically rely on predefined patterns or statistical models, which limits their ability to recognize novel threats. In contrast, an immune-inspired IDS mimics the adaptive and self-learning processes of the biological immune system (BIS), providing a dynamic and effective means of identifying and neutralizing cyber intrusions (Dutt et al. , 2020). [6] Anyone keeping up-to-date with current affairs in computing can confirm numerous cases of attacks made on computer servers of well-known companies. These attacks range from denial-of-service attacks to extracting credit-card details and sometimes, questioning about the firewall. The fact is they often have a firewall. A firewall is a useful, often essential, but current firewall technology is insufficient to detect and block all kinds of attacks. Given these limitations, there is a need for a more robust, adaptive system that can detect both known and unknown threats while minimizing false positives alarm rates and overall systems' response time (Huang et al. , 2024). [8]

Immune-inspired IDS, with its ability to detect unknown attacks, continuously adapt to new threats, reduce false positives, and respond proactively, offers a robust solution to modern cyber-security challenges. By mimicking the self-learning, adaptive nature of the human immune system, an immune-inspired IDS provides an intelligent, dynamic, and scalable defence mechanism that can protect networks from both known and evolving cyber threats in real-time. An immune-inspired IDS provides a **proactive**

defence mechanism. In addition to detecting intrusions, the system can trigger immediate responses, such as alerting administrators, isolating affected systems, or blocking malicious traffic. Just as the immune system triggers responses like inflammation or the release of antibodies to neutralize a pathogen, the IDS can initiate countermeasures to contain and mitigate threats before they cause significant damage. This proactive defence is especially important in mitigating the risks associated with advanced persistent threats and on-going cyber-attacks that might otherwise go undetected for extended periods (Mohd et al. , 2019). [12]

II. INTRUSION DETECTION SYSTEM-

An intrusion detection system (IDS) defined as "an effective security technology, which can detect, prevent and possibly react to the computer attacks" is one of the standard components in security infrastructures. It monitors target sources of activities, such as audit and network traffic data in computer or network systems and deploys various techniques in order to provide security services. The main objective of IDS is to detect all intrusions in an efficient manner. (Kumar et al. , 2010).[10] An intrusion detection system, or IDS, is a security tool that protects computer systems and networks by monitoring them for suspicious or harmful activity. Its main purpose is to detect hackers, malware, or policy violations and alert security staff so they can respond quickly [15].An IDS can do this in two ways: by comparing current activity with known attack patterns (called signature detection) or by spotting unusual behavior that does not match what is normally expected (called anomaly detection). Some IDS solutions combine both methods to improve accuracy and reduce false alarms.

Principles on which IDS works-The main idea behind an intrusion detection system is to keep an eye on what is happening in a computer or network so that any unusual or harmful activity can be spotted quickly.First, the system gathers information, such as network traffic, user actions, or system logs. Then, it checks this information in two ways: by looking for signs of known attacks (using stored patterns) or by spotting anything that looks different from normal behavior.When something suspicious is found, the system sends out an alert so that security staff know there might be an attack. Some advanced systems can even react right away and block the threat automatically. Overall, these principles work together to help detect and respond to threats before they can do serious damage.

III. TYPES OF IDS-

An Intrusion Detection System (IDS) is a security mechanism designed to monitor and analyse network or system activities for signs of unauthorized access, malicious attacks, or other suspicious behaviors. It helps in identifying potential security breaches and notifying administrators to take necessary actions. IDS can be categorized into two main types: Network Intrusion Detection Systems (NIDS), which monitor network traffic for signs of abnormal activity, and Host-based Intrusion Detection Systems (HIDS), which monitor the activities on individual hosts or devices. IDS works by either comparing activities against known attack patterns through signature-based detection or identifying deviations from normal behavior using anomaly-based detection. Some systems combine both approaches for better accuracy. The key functions of IDS include monitoring, alerting, logging, and, in advanced systems, even initiating automatic responses to threats, making it an essential component in a multi-layered security infrastructure (Bejoy et al. , 2017). [3]

Intrusion Detection Systems (IDS) can be categorized in different ways based on how they monitor, detect, and respond to threats. Broadly, they can be divided into:

- **Host-Based IDS (HIDS):** These systems focus on protecting individual computers by monitoring activities like log files, system changes, and application behavior on that specific host.
- **Network-Based IDS (NIDS):** These monitor traffic flowing through a network to detect suspicious patterns or unauthorized access attempts across multiple devices.
- **Signature-Based IDS:** These detect intrusions by comparing activity to a database of known attack patterns. They are effective for known threats but cannot identify new, unknown attacks.
- **Anomaly-Based IDS:** These systems establish what is normal for a system or network and then look for unusual behavior that may signal an attack. This approach can catch unknown threats but may sometimes generate false alarms.
- **Hybrid IDS:** These combine signature and anomaly detection methods to increase accuracy and minimize false positives.
- **Passive vs. Active IDS:** Some IDS only detect and alert administrators (passive), while others can automatically respond to stop an attack in real-time (active or IPS — Intrusion Prevention System).[13]

IV. ARTIFICIAL IMMUNE SYSTEMS-

An Artificial Immune System (AIS) is a computational model inspired by the biological immune system, designed to detect and respond to anomalies or threats in a system. Just like the human immune system protects the body from harmful invaders, an AIS uses mechanisms such as pattern recognition, clonal selection, and affinity maturation to solve complex problems in fields like computer security, machine learning, and optimization. It involves artificial antibodies that represent potential solutions or patterns.

AISs are particularly useful for tasks like intrusion detection, anomaly detection, and data mining, where they can adapt and learn from previous experiences to enhance their performance.

Artificial immune systems (AIS) are bio-inspired paradigms that fall under the artificial intelligence category. The AIS is a computational method based on the mechanisms of the human immune system. The Artificial immune system connects the human immune system with the computational world. It connects immunology and computational modelling. Artificial immune systems (AIS) are a fascinating part of artificial intelligence, inspired by how the human immune system works. At their core, they bring together ideas from biology and computing, helping machines learn to detect problems and adapt to new challenges. Bio-inspired approaches like AIS have become especially useful in areas where flexibility and quick problem-solving are key—such as optimizing systems, spotting unusual patterns, or managing complex environments that are always changing. Among the diverse paradigms of AI, bio-inspired computation is a promising paradigm for addressing complex and dynamic challenges. The

mentioned systems have demonstrated significant potential in addressing complex challenges across optimization, anomaly detection, and adaptive system control.[1][13]

1.1 Relevance in modern AI applications, AIS stands out due to its capability to handle:

1.1.1 Anomaly Detection: By mimicking how immune cells distinguish between self and non-self-cells, AIS methods can detect unusual pattern in datasets. This makes them ideal for applications in cyber security. For e.g., intrusion detection systems, fraud detection, and fault diagnosis in industrial systems.[3]

1.1.2 Optimization: AIS algorithms search for the best or most efficient solution in a complex, high-dimensional space, much like the immune system evolves high-affinity antibodies. Applications include scheduling problems, resource allocation in cloud computing, routing optimization, and engineering design.

1.1.3 Adaptive Decision-making: This refers to the system's ability to dynamically respond to changing environments by learning from past interactions and continuously improving its decision-making process. Inspired by the biological immune system. Applications include Unmanned Aerial Systems(UAS),Fault detection in industries, and Robotics and autonomous systems.[13]

1.1.4 Data Clustering and pattern recognition: IS offers a powerful, flexible approach to unsupervised learning tasks, combining adaptability, fault tolerance, and strong generalization capabilities.

The body's natural defense against illness, infection, and toxins is the human immune system. It is a complex network of organs, tissues, and cells that work together to recognize, combat, and eliminate foreign invaders like parasites, bacteria, viruses, and fungi. The body's first line of defense is innate immunity. It responds quickly and broadly to anything it considers alien. It is made up of chemical defenses like stomach acid, physical barriers like the skin and mucous membranes, and immune cells like white blood cells that atackk the invaders. The more advanced, targeted defense is called adaptive immunity. In order for the body to react more effectively, it learns to identify and remember particular pathogens.

Artificial immune systems simulate the basic concepts of natural biological immune systems in order to solve real-world problems. Immunology is the researching of immune systems and the body’s protection against viruses, bacteria, cancer and other intruders [2].

The biological immune system (IS) is highly complicated and appears to be precisely tuned to the problem of detecting and eliminating infections. We believe that the IS provides a compelling example of a massively-parallel adaptive information-processing system, one which we can study for the purpose of designing better artificial systems. The IS is compelling because it exhibits many properties that we would like to incorporate into artificial systems: It is diverse, distributed, error tolerant, dynamic, self-monitoring (or self-aware) and adaptable. These properties give the IS certain key characteristics that most artificial systems today lack: robustness, adaptivity and autonomity [10].

The AIS simulates on the characteristics of Human immune system as listed below:

i. Immune memory: Adding responses to the memory resulting in fast response.
ii. Distributed: There is no central control and parallel processing is done.
iii. Self-Nonself Discrimination: Intruders are eliminated and self are preserved.
iv. Proliferation: The higher affinity cells that has strong attraction to antigen are proliferated.[3]

V. APLLICATIONS OF ARTIFICIAL IMMUNE SYSTESM-

Artificial Immune System (AIS) algorithms, inspired by the biological immune system, have found diverse applications in fields like machine learning, pattern recognition, and computer security. They leverage principles such as clonal selection, negative selection, and self/non-self discrimination to solve complex problems. Thus, The algorithms are separated on the basis of their applications in which they can be used.

Table 1.1 - Applications of AIS Algorithms

Applications	**Algorithms**	**NSA**	**CSA**	**DCA**	**IN**
Anomaly detection		✓		✓	
Optimization			✓		
Adaptive system & decision making		✓	✓		
Data clustering & Pattern recognition					✓

Table 1.2- Descreptive review of AIS algorithms applications

Application Area	AIS Algorithm Used	Description
Optimization	Clonal Selection Algorithm (CLONALG)	Selects best solutions, clones and mutates them to find optimal results.
Anomaly Detection	Negative Selection Algorithm (NSA)	Detects non-self patterns (anomalies) by training detectors on normal data.
Adaptive System Control	Immune Network Algorithms (e.g., aiNet)	Maintains a dynamic network of solutions that adapt to changing environments.
Clustering	Artificial Immune Network (aiNet)	Evolves antibodies to represent and discover clusters in the data automatically.

VI. COMPARISON BETWEEN ALGORITHMS

EFFICIENCY IS DESCRIBED IN FOLLOWING TERMS

- **Time Complexity** (how fast they run),
- **Memory Requirements** (how much storage they need),
- **Detection/Optimization Performance** (quality of solutions),
- **Scalability** (how well they handle large problems).

Table 1.3. Comparison on the basis of efficiency

Algorithm	Time Efficiency	Memory Efficiency	Detection/Optimization Performance	Scalability	Overall Efficiency
Negative Selection Algorithm (NSA)	Low (slow training, especially in high dimensions)	Moderate to high memory (many detectors needed)	Good for simple anomaly detection; degrades in complex spaces	Poor (curse of dimensionality)	Moderate for small datasets, poor for large
Clonal Selection Algorithm (CLONALG)	High (after initial setup)	Moderate (store best clones/memory cells)	Very good for optimization, pattern recognition	Good (depends on mutation control)	High
Immune Network Algorithm (INA)	Moderate to low (due to dynamic interactions)	High (network connections consume memory)	Good but can suffer from redundancy	Moderate (network may grow too complex)	Moderate
Dendritic Cell Algorithm (DCA)	High (signal processing is fast)	Low (only matured cells stored)	Very good for real-time anomaly detection	Good (handles large input streams)	High for anomaly detection tasks

When comparing different Artificial Immune System (AIS) algorithms, each has its strengths depending on the task. But if we're looking for the **most efficient algorithm overall**, especially for anomaly detection tasks, the **Dendritic Cell Algorithm (DCA)** comes out on top.

- **DCA is fast.** It processes signals quickly without needing long training times, unlike some other algorithms such as NSA.
- **It uses memory efficiently.** Only the relevant, matured cells are stored, which helps keep resource usage low.
- **It performs really well for real-time anomaly detection.** DCA is designed to detect unusual behavior on the fly, making it ideal for things like intrusion detection systems (IDS).
- **It scales well.** Unlike NSA, which struggles with large or complex datasets, DCA handles large streams of input data smoothly without becoming too complex or slowing down.
- **Negative Selection Algorithm (NSA)** is simple and works decently for basic anomaly detection. But it gets very slow and inefficient when dealing with large or high-dimensional data.
- **Clonal Selection Algorithm (CLONALG)** is excellent at optimization and pattern recognition. It's fast and scalable once it's up and running, but it doesn't outperform DCA in real-time detection tasks.
- **Immune Network Algorithm (INA)** can be powerful, but it tends to become too complex and memory-hungry due to the many dynamic connections it forms. That complexity can limit its efficiency in large-scale applications.[13]

VII. METHODOLOGY-

To detect intrusions, a normal behavior profile was first created based on common ports, usual user activity, and trusted resources. Then, the Negative Selection Algorithm was applied to generate detectors that identify any unusual patterns that differ from this normal behavior.

Table 1.4. Methodology of running IDS

Thus, AIS system is implemented onto IDS.

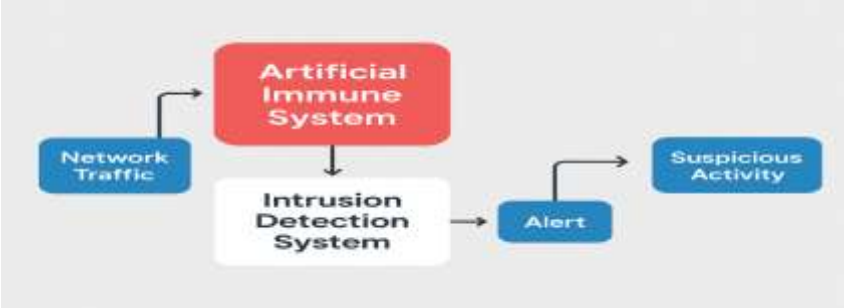

Figure- AIS Algorithm implemented on IDS

VIII. RESULTS- DETECTION PERFORMANCE EVALUATION-

The performance of the Intrusion Detection System (IDS) using only the Negative Selection Algorithm (NSA) was evaluated to establish a baseline. Similar to the enhanced system, this IDS continuously monitors the network and logs every detection outcome in log files, which serve as critical records for auditing, system tuning, and forensic analysis. The evaluation of the Intrusion Detection System (IDS) based solely on the Negative Selection Algorithm (NSA) demonstrated promising baseline performance. The system was tested on a network dataset and the detection outcomes were recorded and analyzed.

The total logs generated by the system were 17351. The confusion matrix indicates that out of all actual intrusion attempts, the IDS correctly identified 6,447 as positive (true positives) while missing 561 (false negatives). Similarly, among normal activities, 10,077 instances were correctly classified as normal (true negatives) and 827 were incorrectly flagged as intrusions (false positives).The confusion matrix below summarizes how the system classified these events:

Table 1.4. Confusion Matrix

CONFUSION MATRIX (NSA-IDS)	Predicted Positive	Predicted Negative
Actual Positive	TP=6447	FN=561
Actual Negative	FP=827	TN=10077

Table 1.5. Confusion Matrix

CONFUSION MATRIX	PREDICTED YES	PREDICTED NO
ACTUAL YES	6447	561
ACTUAL NO	827	10077

Key performance metrics calculated from the confusion matrix are as follows:

- Detection Rate (DR)/TPR/Recall = $\frac{TP}{TP+FN}$ =91.9%
- False Positive Rate = $\frac{FP}{FP+TN}$ = 7.58%
- The Detection Rate (True Positive Rate / Recall) was 91.9**%**, indicating that the IDS successfully detected most intrusion attempts
- The False Positive Rate stood at 7.58%, which is relatively low but highlights the presence of some false alarms.

These results confirm that the NSA-based IDS provides a reliable baseline capability to detect intrusions with a high detection rate and acceptable false positive level. These results indicate that the IDS using only the NSA correctly detects most intrusions while maintaining a reasonable false positive rate.

REFERENCES

[1] Aickelin, U., Dasgupta, D. and Gu, F., (2013), "*Artificial immune systems*", In Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques , Boston, Springer, pp. 187-211.

[2] Balasaraswathi, V.R., Sugumaran, M. and Hamid, Y., (2017), *"Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms"* Journal of Communications and Information Networks, vol. 2, pp.107-119.

[3] Bejoy, B. and S, J. (2017), "*Artificial Immune System based Intrusion Detection Systems- A comprehensive review*", International Journal of Computer Engineering & Technology, IJCET vol. 8, pp. 85-95

[4] Duru, C., Ladeji–Osias, J., Wandji, K., Otily, T. and Kone, R., (2022), "*A review of human immune inspired algorithms for intrusion detection systems*" In IEEE World AI IoT Congress (AIIoT), IEEE, pp. 364-371.

[5] Dutt, B. and Maitra, I. (2020), "*Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model*", IEEE Access, vol. 8, pp. 34929-34941.

[6] Dutt, I., Borah, S. and Maitra, I., (2016), "*Intrusion detection system using artificial immune system",* International Journal of Computer Applications, vol. 144, pp. 19-22.

[7] Hofmeyr, S.A. and Forrest, S., 2000. Architecture for an artificial immune system. *Evolutionary computation*, *8*(4), pp.443-473.

[8] Huang, M., Li, W., He, J., Lan, X., Li, T. and Zhang, N., (2024), "*IDG-SemiAD: An Immune Detector Generation-Based Collaborative Learning Scheme for Semi-supervised Anomaly Detection in Industrial Cyber-physical Systems*", International Journal of Computational Intelligence Systems, vol 1, pp. 1-5.

[9] Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., (2019) "*Survey of intrusion detection systems: techniques, datasets and challenges"* Cybersecurity, Springer, vol. 2, pp.1-22.

[10] Kumar, G., Kumar, K. and Sachdeva, M., (2010), *"The use of artificial intelligence based techniques for intrusion detection: a review*", Artificial Intelligence Review, vol. 34, pp.369-387.

[11] Liu, Z. and Hu, X. (2023), "*Artificial Immune Detection for Network Intrusion Data based on Quantitative Matching Method*", Computers, Materials & Continua, vol.78, pp. 2361-2389.

[12] Mohd, N., Singh, A. and Bhadauria, H.S., (2019), "*Bioinspired immune system for intrusions detection system in self configurable networks"*, International Journal of Advanced Computer Science & Applications, vol. 10, pp.159-166.

[13] Myakala, P. K., Bura, C. and Jonn, A. K. (2025), "Artificial Immune Systems- A bio inspired paradigm for computational intelligence", Journal of Artificial Intelligence and Big Data, Scientific Publications, vol. 5, pp.1-13.

[14] Otor, A. and Aderounmu, K. (2021), "*An improved bio-inspired based intrusion detection model for a cyberspace*", Cogent Engineering, vol. 8, pp. 1-23.