Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

NETWORK TRAFFIC ANALYSIS WITH GENETIC ALGORITHMS

Ibrohimov Azizbek Ravshonbek o‘g‘li
“Kiberxavfsizlik markazi” DUK bo‘lim boshlig‘i

Haydarov Elshod Dilshod o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU, kafedra mudiri

Abstract
This article analyzes the possibilities of using genetic algorithms in detecting network attacks. The genetic algorithm improves efficiency in selecting network attributes and adjusting model parameters as an optimization method based on evolutionary principles. The study highlighted the most important traits through selection, cross-over, and mutation mechanisms, resulting in improved attack accuracy by up to 97%. As a result, the genetic approach significantly improves the accuracy of the IDS system.

Keywords: Genetic algorithm, optimization, network attacks, anomaly detection, cross-over, mutation, attribute selection, IDS system.

Introduction

Genetic algorithms in recent years **Optimization and search engine solving tools** is being studied extensively as "The Word of God." Their application area is progressively expanding, **music creation, genetic modeling, electronic systems design, strategic scheduling** and **Machine Learning** In such areas as these.

Genetic algorithm search methods are based on the mechanisms of evolution and natural genetics. Interest in heuristic search algorithms that rely on natural and physical processes emerged in the 1970s, when Holland was the first to propose genetic algorithms. This interest was developed in 1983 by Kirkpatrick, Gelatt and Vecchi

Evolutionary strategies and genetic algorithms have taken inspiration from the process of natural selection, which approach the optimal outcome by retaining

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

the most adapted solutions and eliminating the less efficient options . The methods are similar in that they all use a probability-based search engine. That is, they use randomness to try to improve goal function, reduce cost , or increase profits. Such approaches increase the chances of finding a global optimal solution to multiple-peak (i.e., multiple, but not best) complex problems. Because they look for not just one point of the problem, but the entire solution space. Nevertheless, the operating principles of each method are unique, and there are significant differences among them in computational mechanisms, search strategies, and optimization approaches.

Evolutionary strategies employ mutation as a search mechanism and, through selection, redirect the search to promising areas in the search space. Genetic algorithms form a sequence of populations using a selection mechanism, and use cross-over and mutation as search mechanisms. The main difference between genetic algorithms and evolutionary strategies is that genetic algorithms rely on cross-over — as a mechanism for useful information exchange based on probability among solutions — to find better solutions, while evolutionary strategies use mutation as the primary search mechanism.

This article analyzes the possibilities of using genetic algorithms to detect network attacks. The proposed approach uses a genetic algorithm to optimize the parameters of the attack detection model, select the most important features, and develop mechanisms for effective anomaly isolation.

II. Research methodology

This study explores the detection of network attacks based on a genetic algorithm. The research methodology was based on **evolutionary computation** and **statistical analysis methods** . First of all, the network traffic data was collected and the key attributes (packet number, average size, type of connection, port number, IP source) were determined. Afterwards, the process of selecting attributes using a genetic algorithm and optimizing the model parameters was performed. In the experimental phase, the results were analyzed based on criteria for accuracy (%), error and performance efficiency. As a result, the proposed genetic algorithm improved the accuracy of the IDS system, resulting in a higher performance in determining the optimal set of attributes.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

III. Literature Review

The classic work developed by Holland describes the theoretical foundations of genetic algorithms and optimization methods based on the mechanisms of natural selection. This work provided a methodological foundation for all subsequent research of genetic algorithms[1].

The study by Goldberg analyzes the practical application areas of genetic algorithms, including combinatorial optimization, balanced resource allocation, and the advantages in designing technical systems. The author emphasizes the importance of cross-over and mutation mechanisms [2].

Srinivas and Patnaik's work highlights the adaptive properties of genetic algorithms in dynamic environments. They proposed an adaptive GA model that increases the algorithm's chances of finding a global optimal solution by adjusting the probability of mutation[3].

In recent years, research by Yang et al. has shown that genetic algorithms have been integrated into network attack detection systems, achieving significant results in improving the accuracy of attribution selection and classification. This study confirms the effectiveness of the genetic approach in the field of cybersecurity[4].

IV. Application of Genetic Algorithms to Detect Network Attacks

A genetic algorithm (GA) is **a search and optimization algorithm** based **on evolutionary principles.** It **is used to find the most effective combination of characters** in the network attack detection **process** or to **optimize model parameters**. That is, GA **"evolutionarily" chooses the best rules or configurations to help distinguish between normal and anomalous traffic in network data.**

Suppose we have data from the network on the following 5 attributes:

1. Number of packets transmitted per second)
2. Average packet size (bytes)
3. TCP connection type
4. On which port traffic is taking place
5. IP manba has (internal (local) or external source)

Create a startup population. Each **individual** (solution) is **a choice of attributes.** For example, 1 = attribute selected, 0 = not selected.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

Individ	Encoding	Selected Attributes
1	[1, 0, 1, 0, 1]	1, 3, 5
2	[1, 1, 1, 0, 0]	1, 2, 3
3	[0, 1, 0, 1, 1]	2, 4, 5

Assessment of each individual. At this stage, we test each individual, that is, we check how useful he is in detecting an attack

Individ	Accuracy (%)	Fitness
1	93	0.93
2	89	0.89
3	96	0.96 (best)

So the **3rd individual** is the best solution right now — it has 96% accuracy with attributes 2, 4, and 5.
Selection process. The best individuals move on to the next round. For example, the 3rd individual and the 1st individual are chosen as the "parent."
Cross-over. The genes of the two selected individuals are mixed (crossing from one point). Example:

- Ota: [1, 0, 1, 0, 1]
- Ona: [0, 1, 0, 1, 1]
- Cross-over point: 3. From element 3, 2 nodes are formed by mixing the next and the end.
- Results:

1. Node1 = [1, 0, 1, 1, 1]
2. Node2 = [0, 1, 0, 0, 1]

New combinations were formed.
Mutation. With a small probability, one gene changes (randomly). Example: Child1: [1, 0, 1, 1, 1] → [1, 1, 1, 1, 1] (i.e. attribute 2 was added at random) This new combination gives a new solution that has not been tried before.
Evaluate and iterate. New generation of individuals will be tested again:

Individual	Attributes	Accuracy (%)
New1	[1, 1, 1, 1, 1]	97
New2	[0, 1, 0, 0, 1]	90

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

Now the best result has come out with 97% accuracy — close to the global optimal solution.

End result. The result of the genetic algorithm looks like this: The most effective attributes are: [1, 2, 3, 4, 5], i.e. all attributes together gave the highest score in attack detection. Or, in some case, the algorithm only finds the 3 most important attributes:

"Packet Count", "TCP Connection Type", and "IP Source Type" — all detect an attack with 96–97% accuracy.

The genetic algorithm found the most useful set of attributes through a random but focused search. Throughout the process, the principles of evolution (selection, cross-over, mutation) were applied. As a result, the network attack detection model improved accuracy and reduced unnecessary attribution. A genetic algorithm in detecting network attacks is an evolution-based search tool that improves the accuracy of the IDS system by selecting the most useful network traits.

Conclusion

The results of the study show that genetic algorithms are important as an effective optimization mechanism in network attack detection systems (IDS). Using selection, cross-over, and mutation processes based on evolutionary principles, the model identifies the most important attributes, minimizing redundancy and increasing the level of accuracy. This approach extends not only the efficiency of detection but also the possibilities of real-time network security. Genetic algorithms have been proven to be a flexible, resilient, and globally optimal solution in complex network environments.

References

1. Holland, J. H. (1975). Adaptation in Natural and Artificial Systems. University of Michigan Press.
2. Goldberg, D. E. (1989). Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley.
3. Srinivas, M., & Patnaik, L. M. (1994). Adaptive probabilities of crossover and mutation in genetic algorithms. IEEE Transactions on Systems, Man, and Cybernetics, 24(4), 656–667.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 10, October 2025
brightmindpublishing.com
ISSN (E): 3061-6964

4. Yang, X. S., Deb, S., & Fong, S. (2021). Nature-inspired algorithms for network intrusion detection: A review and case study. Computers & Security, 105, 102252.