Artificial Intelligence

CS351-E

Semester Project Report

"Optimizing Cyber Security Techniques for Large Infrastructures using Genetic Algorithm"

Submitted by:

M. Bilal Aslam - 2022361

Syed Ahmed Haseeb - 2022557

Abstract

The project addresses the optimization of cybersecurity rules using Genetic Algorithms. The algorithm evaluates and evolves hexadecimal chromosomes representing cybersecurity rules strategies against simulated attacks. Diverse initialization, selection techniques, crossover, and mutation were employed to iteratively enhance the fitness of solutions, culminating in a robust defense mechanism.

Problem Statement

Cybersecurity defense mechanisms must evolve to counteract ever-advancing attack strategies. Optimizing these mechanisms is a complex problem due to the diverse and dynamic nature of cyber threats. Hence, we have tackled this problem by implementing it in Genetic Algorithm, which aims to optimize cybersecurity rules to converge to a best solution that is effective against the everchanging landscape of cybersecurity attacks.

Proposed Solution

A Genetic Algorithm (GA) was developed to optimize cybersecurity rules represented as hexadecimal chromosomes. Each chromosome represents a security configuration: the first four digits represent the detection rate, the next four digits represent the resilience of the system against attacks, and the remaining two digits representing the response time.

Methodology

The algorithm begins with a diverse population of chromosomes to prevent premature convergence. Then, it employs a fitness function to the chromosomes to see which ones are the best performing ones. We implemented a hybrid approach in our selection function, from generations one to ten, it uses a Roulette Wheel Selection to choose the chromosomes for crossover, and then Rank-Based Selection after the tenth generation as that is when convergence starts to appear. Hence, when fitness values are similar to each other, using a rank-based selection was the appropriate choice. The algorithm incorporates crossover to generate offspring by blending traits from superior parents, promoting variability. To further ensure genetic diversity, mutations are applied at specified rates, introducing new potential solutions and avoiding local optima. Iterative evaluations and enhancements over successive generations refine the solutions, culminating in optimized defence strategies against evolving threats.

The Genetic Algorithm was implemented with the following parameters:

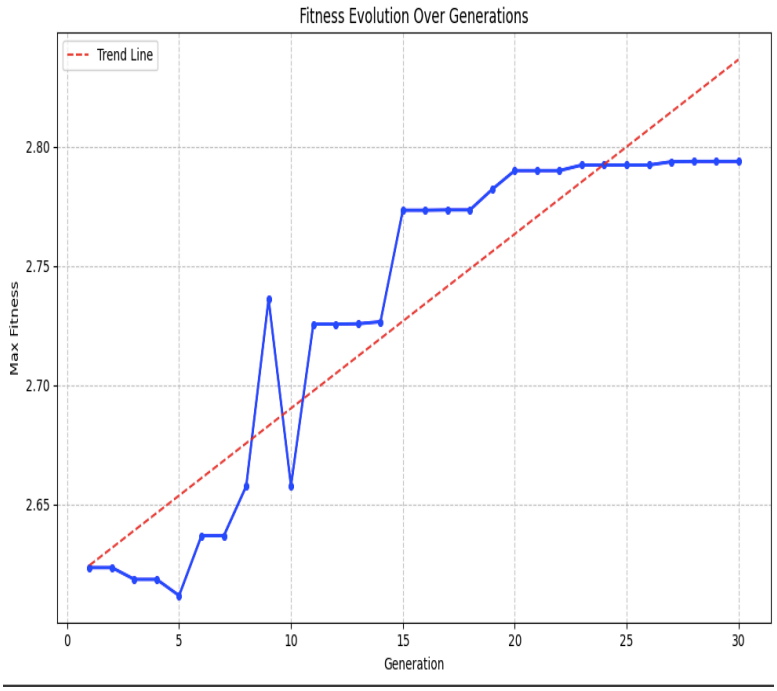
- Population Size: 50
- Chromosome Length: 10 (hexadecimal)
- Generations: 30
- Crossover Rate: 8%
- Mutation Rate: 5%

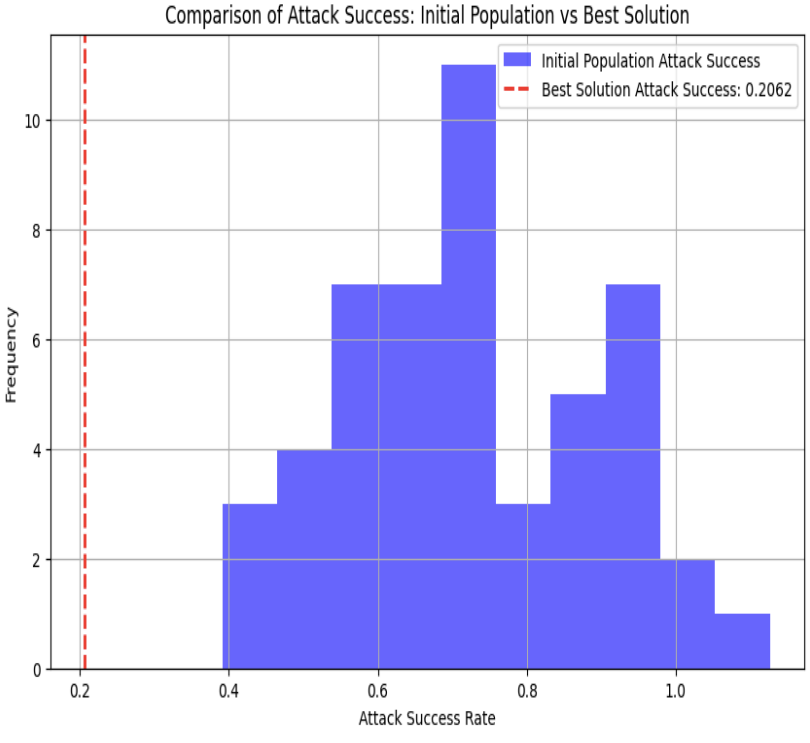
Key steps include:

1. Initialization of population.
2. Fitness evaluation using a weighted formula based on detection rate, system resilience, and response time.
3. Roulette Wheel and Rank-Based Selection.
4. Single-point crossover and mutation for diversity.
5. Iterative evolution over 30 generations.
6. Attack success rate calculated based on the inverse of the effectiveness of the defense system.

Results

- The fitness of solutions improved over generations, converging to an optimal fitness value.
- The algorithm identified security rule configurations with increased defense effectiveness and reduced attack success rates.
- Graphs detailing the fitness evolution and attack success comparisons were generated to validate findings.





Conclusion & Future work

The project demonstrated that Genetic Algorithms are a viable approach to optimizing cybersecurity mechanisms. By iteratively evolving strategies, the algorithm improved defense effectiveness, as evidenced by fitness scores and reduced attack success rates. Future work could include extending the algorithm to incorporate real-time adaptive mechanisms and scaling it for more complex threat landscapes.

Real-Time Adaptation: Modifying the algorithm to react dynamically to real-time data inputs, such as emerging attack patterns or changes in system vulnerabilities.

Scalability for Complex Threats: Extending the algorithm to optimize defense mechanisms for complex threats such as in enterprise networks or cloud environments, where multi-layered defense strategies are required.

By embracing these directions, the applicability and effectiveness of Genetic Algorithms in cybersecurity can be further enhanced, driving innovation in automated defense mechanisms.