A Genetic Algorithm Approach to Attack Path Optimization Using Attack Graphs*

Jong-Eun Lee[1] and Dong-Wook Kim[2†]
[1] Department of AI · Software, Graduate School, Gachon University
jjoki1258@gmail.com
2 Department of AI·Software, Postdoctoral Researcher, Gachon University,
kog73006@gachon.ac.kr

Abstract

An attack graph structurally represents vulnerabilities and privilege-escalation relationships within a network to support attack path analysis and prioritization of defenses. This paper proposes a framework that uses a genetic algorithm (GA) to search for realistic and executable optimal attack paths on such attack graphs. We convert raw network traffic data into an attack-graph representation and feed it into the GA to derive the optimal attack paths. Through this process, we demonstrate that our method can discover better routes than existing attack techniques.

1 Introduction

Modern cyberattacks have evolved beyond simple exploits of single vulnerabilities, advancing toward multi-stage and correlated attacks. Recently, attackers have increasingly tended to exploit weaknesses in external services to gain limited privileges, then move laterally within internal networks by compromising vulnerable hosts, gradually escalating their privileges, and ultimately targeting critical assets or performing system cracking. To defend against such threats, the attack graph concept was introduced as a quantitative and structural representation of the sequential attack process, and research on attack graph–based modeling has been actively conducted [1].

In this paper, we propose a method that employs a genetic algorithm to identify the optimal attack path within an attack graph. The proposed method introduces a modified fitness function that simultaneously increases the attack success probability while reducing the detectability (stealthiness) of the route, thereby enhancing the attack's sophistication. This evolutionary search process is well-suited for handling the nonlinear combinatorial nature and uncertainty of attack-path exploration, efficiently discovering optimal or near-optimal paths that heuristic searches often fail to reach.

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-49, December 16-18, 2025, Sapporo, Japan.
† Corresponding author

2 Motivation

Recent studies have increasingly applied genetic algorithms to attack graphs. [2] applied a GA to identify attack routes defined as the Most Likely Attack Path (MLAP). [3] proposed an evolutionary-search framework that represents multiple paths or scenarios as individuals and evolves them through the GA process. [4] used a GA to mass-produce potential attack paths, linking path generation with security decision-making that takes risk and cost into account.

3 Proposed Method

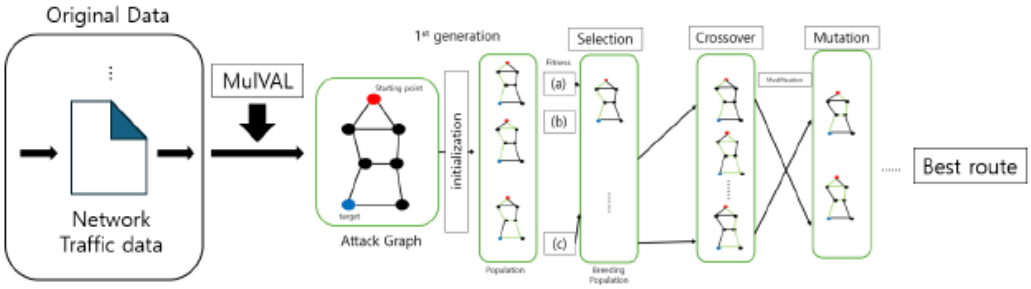

Figure 1: A framework using genetic algorithms to find optimal attack routes in attack graphs

As explained in Section 1, this paper explores how to find the optimal attack path within an attack graph using a genetic algorithm (GA). As the experimental dataset, CIC-IDS2017 network traffic data was used, and this was converted into an attack graph format through MulVAL. Since the goal is to search for the optimal path, each chromosome in GA was defined as one attack path to form a population. In order to simultaneously improve the stealth and the probability of success of an attack, the fitness function integrated three elements: success probability, detection risk, and cost. stealth was modeled through path length and cumulative threat. After the fitness evaluation, an excellent parent entity was selected and a new path was created through crossover. Since a disconnected path may occur in the process of recombining the graph path, a repair step was added to restore connectivity by inserting a shortest-path segment. Over several generations, GA evolved to yield an optimal route. As a result of the experiments, the proposed method converges efficiently within approximately 40 to 50 generations, generating a path with a higher attack success probability and lower detection risk compared to existing heuristic techniques.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (RS-2023-00211871).

References

[1] Jianping Zeng et.al.. (2019, December). Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing. Security and Communication Networks. Volume 2019, Issue 1. 2031063

[2] Mohammed Alhomidi and Martin Reed. (2013 September). A Genetic Algorithm Approach for the Most Likely Attack Path Problem. ARES '13: Proceedings of the 2013 International Conference on Availability, Reliability and Security. Pages 360 - 366
[3] Mohammed Alhomidi and Martin Reed. (2014 March). Attack Graph-Based Risk Assessment and Optimization Approach. Journal of Internet Technology and Secured Transactions (JITST), Volume 3, Issue 1
[4] Mohammad Ryiad Al-Eiadeh and Mustafa Abdallah. (2024 September). GeniGraph: A genetic-based novel security defense resource allocation method for interdependent systems modeled by attack graphs. Computers & Security. Volume 144. 103927