Real-time Anomaly Detection-enhanced Defense for Dynamic Memory Allocation[*]

Ga-Yeong Kim[†], Na-Eun Park and Il-Gu Lee

Sungshin Women's University, Seoul, South Korea

{20240925, iglee}@sungshin.ac.kr, nepark.cse@gmail.com

Abstract

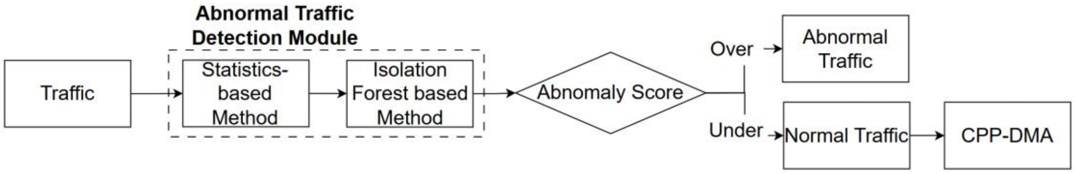
This paper analyzes the architectural vulnerabilities of content popularity prediction-based dynamic memory allocation scheme (CPP-DMA), which dynamically allocates resources according to real-time content access patterns. It proposes anomaly detection enhanced DMA, an input sanitization technique based on anomaly traffic detection, to address these weaknesses. According to the experimental results, the method achieved an 87% attack blocking rate while preserving 83% of the traffic for legitimate requests.

1 Introduction

In Edge Computing environments, dynamic resource management techniques are essential [1]. Due to this necessity, the proposed CPP-DMA dynamically allocates the popularity score, which is derived from the Autoencoder and LSTM (Long Short-Term Memory), to the Device, Edge, and Cloud layers based on a threshold. This structure achieves latency minimization and efficient resource allocation. However, since CPP-DMA relies on the incoming traffic patterns, it possesses a structural vulnerability: resource distribution becomes distorted if malicious traffic is introduced. Therefore, this study proposes an anomaly traffic sanitization model that preemptively removes anomalous requests at the input stage.

2 Anomaly Detection Enhanced-DMA

This section proposes ADE-DMA, an input sanitization technique based on anomaly traffic detection, to solve the structural vulnerabilities of CPP-DMA. The architecture of the proposed model is shown in Figure 1.



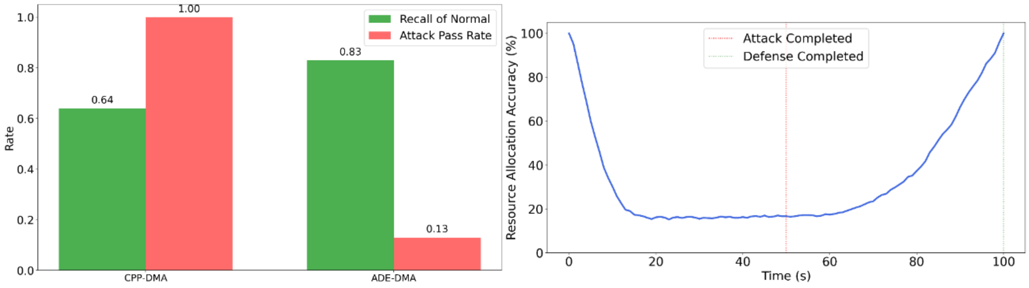
(Figure 1) Flowchart of ADE-DMA

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-13, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

[†] Corresponding author

When the request frequency traffic is input, the Anomaly Traffic Detection Module operates to block anomalous traffic. In the statistical detection method, the request frequency per content is aggregated over a fixed time unit, and requests that deviate from a threshold calculated using the mean and standard deviation are defined as anomalous traffic. The unsupervised learning-based detection technique applies Isolation Forest, which is trained on normal patterns, to remove data where the anomaly score exceeds a threshold.

To verify the performance of the proposed model, the ADE-DMA model was evaluated using a Python-based simulation. In the experiment, normal traffic was generated using a Poisson distribution, and attack traffic was designed by inserting concentrated, continuous traffic targeting a specific content, which was intended to induce the popularity-based resource allocation algorithm to assign excessive resources to that content. Figure 2 shows the results.



(a) (b)

(Figure 2) Performance of ADE-DMA (a): Legitimate Traffic Preservation Rate and Attack Success Rate of ADE-DMA, (b): Resource Allocation Accuracy)

As shown in Figure 2 (a), ADE-DMA preemptively detected and blocked anomalous requests at the input stage, thereby increasing the legitimate traffic preservation rate to 83% and reducing the attack pass-through rate to 13%. Figure 2 (b) shows the accuracy of resource allocation. CPP-DMA's memory allocation accuracy under no-attack conditions is assumed to be 100%. It can be confirmed that the accuracy gradually drops to 20% as attack traffic is injected for up to 50 seconds. After the 50-second mark, the security model is applied, and an increase in accuracy can be observed.

3 Conclusion

This paper pointed out the structural limitations of CPP-DMA and proposed ADE-DMA, an anomaly detection-based input sanitization technique, to complement them. The experimental results demonstrated that the proposed technique effectively blocked malicious requests while preserving legitimate traffic, thereby recovering the reliability of resource allocation. Future research will focus on security studies for models that rely on external traffic.