Poster: Optimized Cache Pollution Attack: A DDoS Vector in Content Delivery Networks

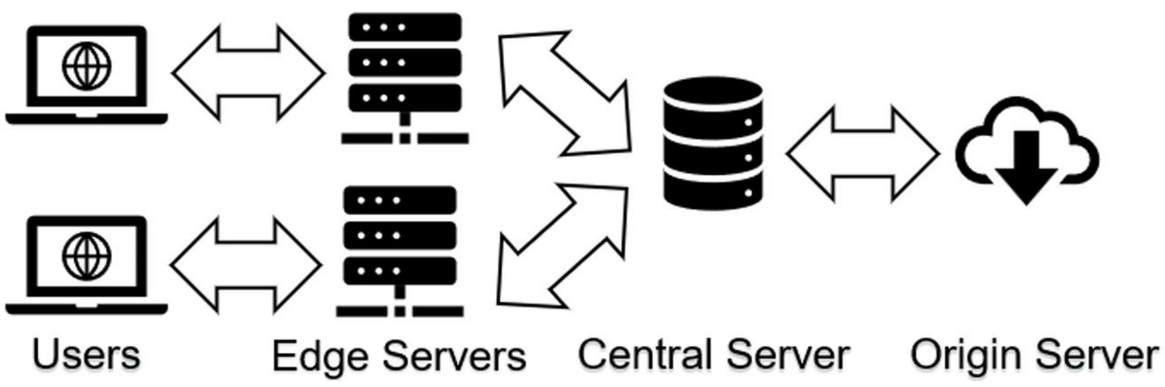
Jiaqi Liu Noriaki Kamiyama
Ritsumeikan University

1. Introduction

- Content Delivery Networks (CDNs) use edge servers to cache content, making them strong against most DDoS attacks.
- However, they are vulnerable to Cache Pollution Attacks (CPA), where an attacker floods the cache with requests for unpopular content, which can overwhelm the Origin Server.
- **Our Goal:** Investigate the optimal CPA strategy from an attacker's perspective.

2. Methodology

- We modeled a **Hierarchical Cache System**



- We used an **M/M/1 Queue Model** to calculate server response time (W) and Che Approximation for cache hit ratio (h_i)

$$W = \frac{1}{\mu - \sum_{i=1}^{M} \lambda_i^e}$$

- We use the ***Che* approximation** to estimate the cache hit ratio h_i for content i on the cache server

$$h_i \approx 1 - e^{-q_i t_c} \qquad \sum_{i=1}^{M} h_i = C$$

- We developed a **Genetic Algorithm (GA)** to find the attacker's optimal strategy
  - Fitness Goal: Maximize the Origin Server's response time (W_o).

Algorithm 1 Optimum allocation of sending rate of attack packets on each CDN edge server

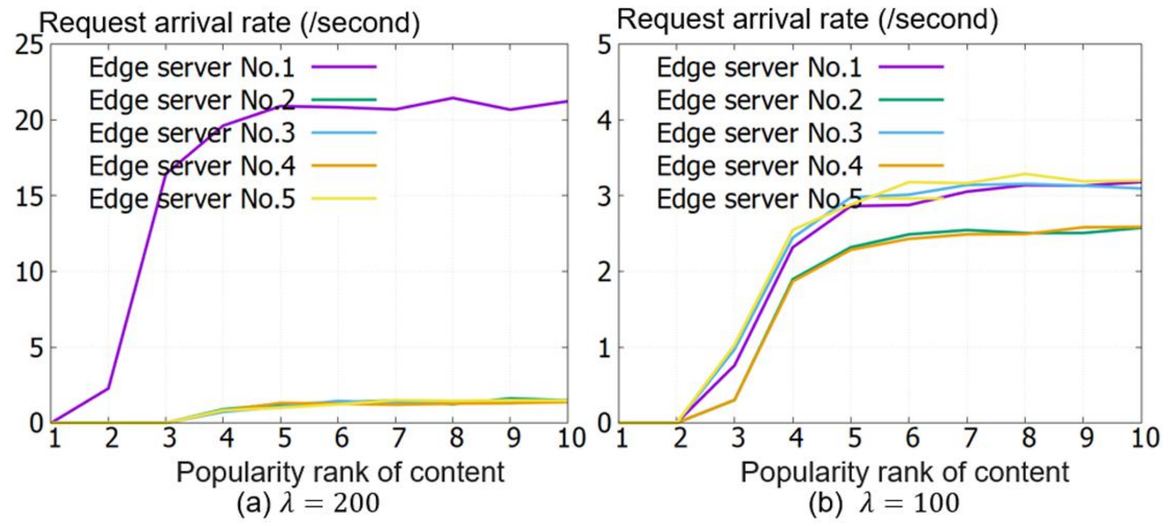
1: Randomly set s_i^n as the initialized chromosomes
2: To achieve crossover, set any two chromosomes as a group and randomly exchange of s_i^n in groups
3: To achieve mutation, randomly change two s_i^n
4: To achieve selection, add attacker's request to the normal request and calculate W_o as fitness. Then select the best chromosomes from the parents and children
5: Repeat steps 2, 3 and 4 until N generations

- Based on the obtained results, the attacker allocates attack resources.

$$\lambda_i^n = s_i^n \lambda_T$$

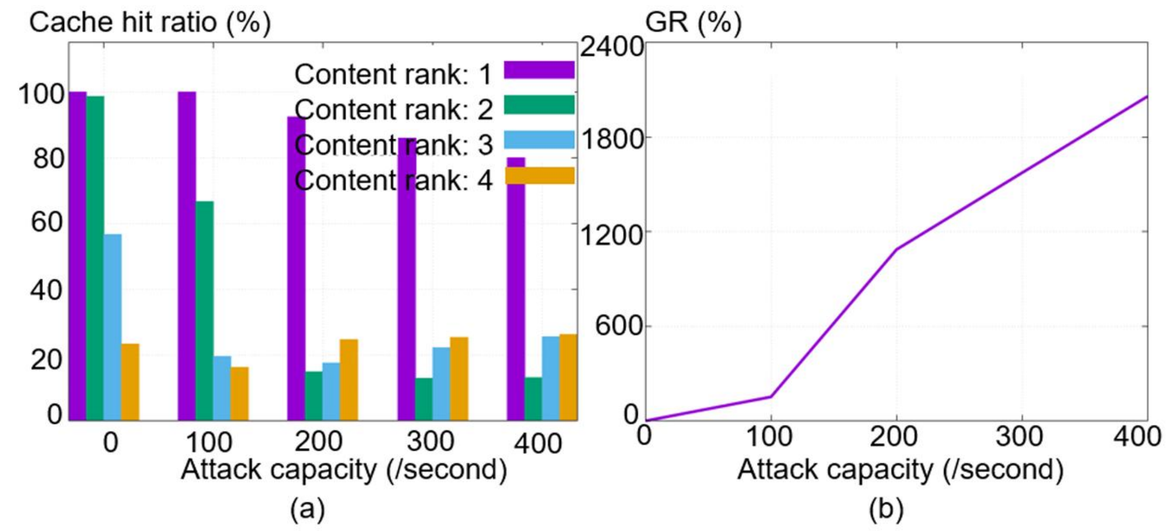
3. Key Results

- The Optimal Attack Strategy Depends on Capacity



  - Below Threshold ($\lambda_T = 100$): Optimal attack is uniform across all servers.
  - Above Threshold ($\lambda_T = 200$): Optimal attack is concentrated on specific servers.
  - Key Target: The attack always prioritizes requests for low-popularity content.

- The Attack Causes Significant Performance Degradation



  - Cache Hit Ratio (Fig. 3a): The attack significantly reduces the hit ratio for popular content (ranks 2-3).
  - Response Time (Fig. 3b): The Growth Rate (GR) of response time surges dramatically when the attack strategy shifts to "concentrated".

4. Conclusion

- Optimized CPA is a significant threat to hierarchical CDNs
  - Attackers can successfully bypass edge server isolation to launch a DDoS attack on the origin server.
  - This work highlights a pressing need for robust countermeasures against this attack vector.
  - This confirmed the feasibility for further in-depth research in the future.

This research was supported by JSPS KAKENHI Grant Numbers 25K03113 and 23K28078 and "Society for the Advancement of Science and Technology at Ritsumeikan"