BPO-2-01

Optimum Content Pollution Attack Using Genetic Algorithm in CDN

Liu Jiaqi Noriaki Kamiyama
Ritsumeikan Univ.

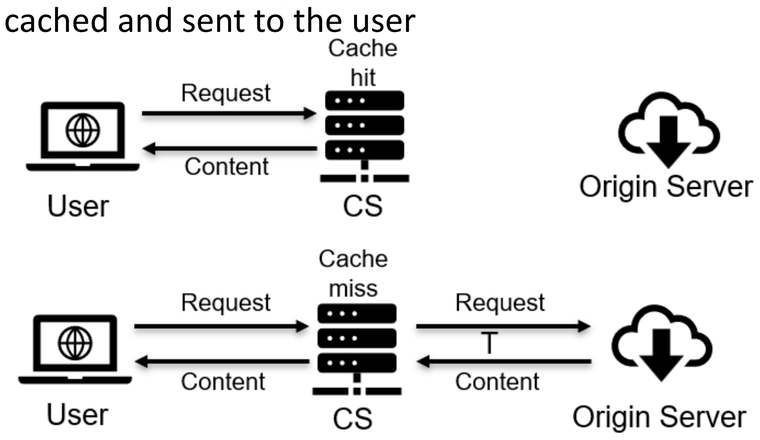
1. Introduction

- With the widespread use of CDN, attacks against CDN have attracted more and more attention
- It's rare to analyze them from the attacker's perspective

Using Genetic Algorithm to optimize the attack strategy.

2. Content Delivery Network

- The user sends the request to the cache server (CS)
  - When cache hit occurs, the CS sends the content to the user
  - When cache miss occurs, the CS sends the request to the origin server, and the origin server sends the content to the CS, which is cached and sent to the user



3. Analytical Model

- With M/M/1 queue, we use average response time W to evaluate the performance of CDN

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

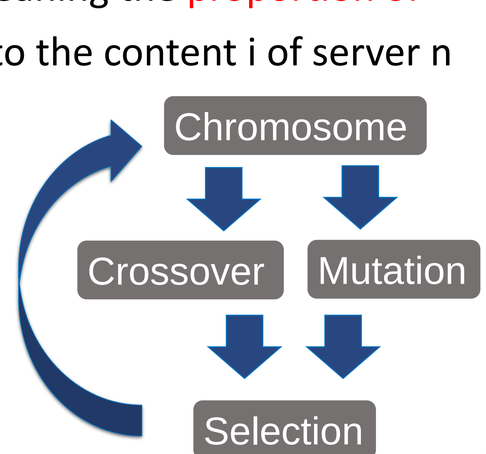
- Through che-approximation, we relate the cache hit ratio of content to its popularity.

$$h_i \approx 1 - e^{-q_i t_c}$$

$$\sum_{i=1}^{M} h_i = C$$

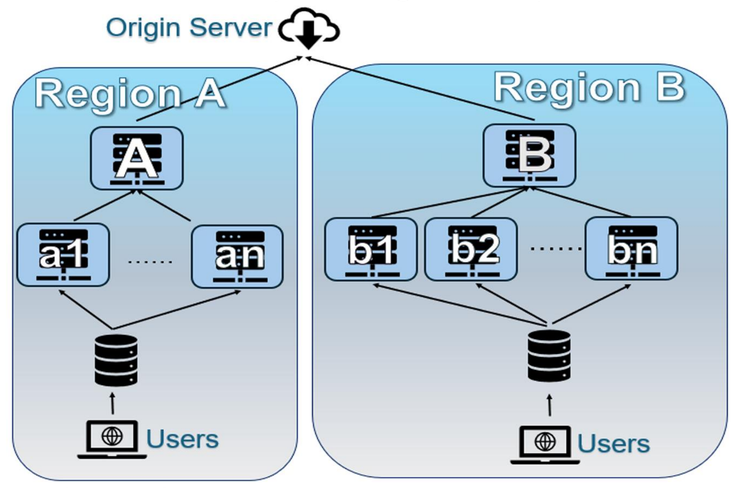
4. Genetic Algorithm

- The Genetic algorithm (GA) is commonly used to generate high-quality solutions to optimization by relying on biologically inspired operators such as mutation, crossover and selection
- We set S_n^i as the chromosome meaning the proportion of requests that the attacker sends to the content i of server n
- We use the average response time after the attack as fitness to perform selection operations



5. CDN model

- The CDN model is composed of multiple region with CSes in multiple layers.
  - The origin server provides content copies for 5 regions
  - The central server has a large cache size for storing content from the origin server and sending it to the edge servers.
  - The edge server is responsible for quickly providing popular content with a small cache size.
  - DNS server is responsible for randomly locating user requests to edge servers
  - All CSes adopt LRU



- Average response time in region A

$r_e^A = W_a$ -Cache hit in a_n

$r_c^A = W_a + W_A + T_1$ -Cache hit in A

$r_o^A = W_a + W_A + W_O + T_1 + T_2$ -Cache miss in A and a_n

- Average response time of content i in region A

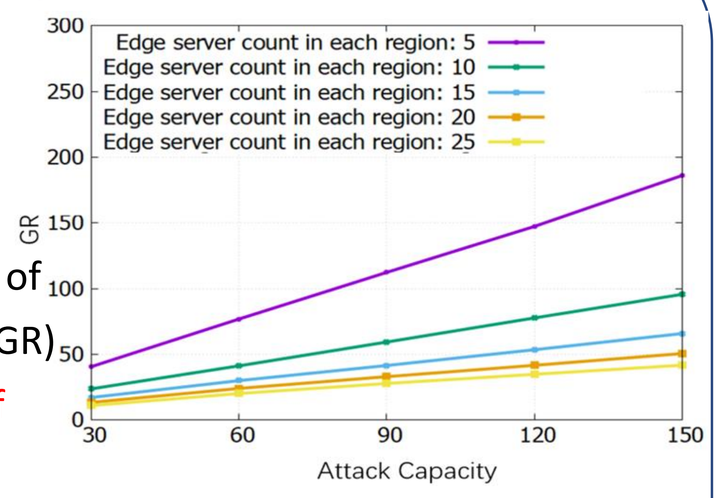
$$R_i^A = h_i^{an} r_e^A + (1 - h_i^{an}) h_i^A r_c^A + (1 - h_i^{an})(1 - h_i^A) r_o^A$$

- Average response time of all requests in region A

$$R_A = \sum_{i=1}^{M} \frac{\lambda_i^A R_i^A}{\sum_{i=1}^{M} \lambda_i^A}$$

6.Evaluation

- We set request rate to each contents based on zipf's law
- We use the growth rate of average response time(GR) to denote the change of response time



- With the same attack capacity, region with less edge server count are more vulnerable to attacks
- As the attack capacity increases, the growth rate of GR in region with lower number of edge servers increases

Paramater	Value
Number of contents provided, M	100
Edge servers' cache size	20
Central servers' cache size	50
Zipf law parameter	4
Edge server number in target area	5
Requests rate to each edge server, λ	30 /second
Av. service time of Edge servers, $1/\mu_1$	10 ms
Av. service time of Central servers, $1/\mu_2$	2 ms
Av. service time of origin server, $1/\mu_o$	1 ms
Latency, T_1	500 ms
Latency, T_2	300 ms