# Evaluation and Analysis of Two Types of Attacks CPA and DDoS Targeting CDN caches

Jiaqi Liu  Noriaki Kamiyama

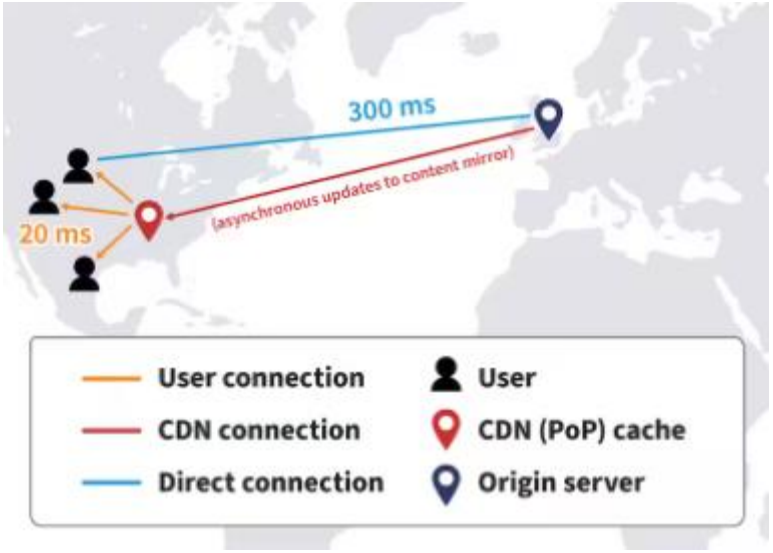
Ritsumeikan Univ

2024.03.01

# Content Delivery Network

- Content Delivery Network (CDN)
  - Origin servers: Provide the original version of the content
  - Cache servers: Cache the copy of contents, and they are responsible for delivering that content to nearby users.
  - DNS servers: Respond user's request with the name of a cache server from which the content can be served faster.

- The feature of CDN
  - Serves a large portion of the Internet content
  - Provides a faster and high-performance experience
  - Reduce bandwidth costs



# Attacks targeting CDN

- Distributed denial-of-service (DDoS)
  - Disrupt the normal traffic of the targeted server, service or network by overwhelming the target with a flood of Internet traffic.

- Cache pollution attack（CPA）
  - Pollute the cache with low-popularity content to degrade the performance of the cache

# Existing research

- There are many methods to prevent DDoS or CPA but there are no existing research investigating on DDoS and CPA on cache server.

- Knowing the attacker how to optimize the attack, CDN provider can better defend the attack

# Purpose of research

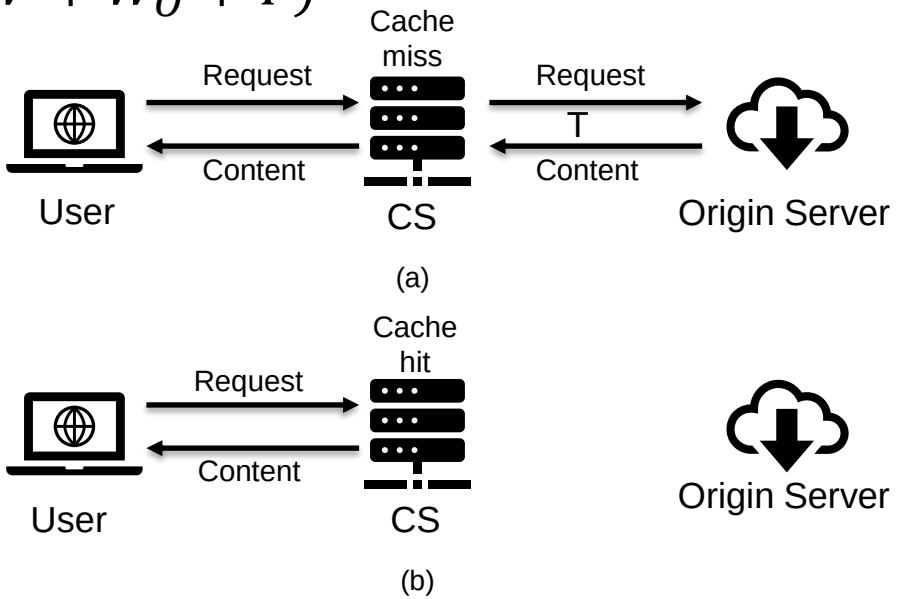
- Propose the analytical model to evaluate the impact of DDoS or CPA.
- Analyzes the impact of specific scenarios on DDoS and CPA
- Analyzes the influence of different factors on the attack
  - CDN providers can control factors to reduce the impact of attacks

# Analytical Model

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

| Parameter | Definition |
|---|---|
| W | Average response time |
| 1/μ | Average service time |
| M | Number of contents |
| $\lambda_i$ | Poisson arrival rate of request for content i |
| $h_i$ | Cache hit ratio of content i |

- Cache Server (CS)
  - The latency time T is spent when cache misses
  - $R(i) = h_i W + (1 - h_i)(W + W_O + T)$



# Analytical Model

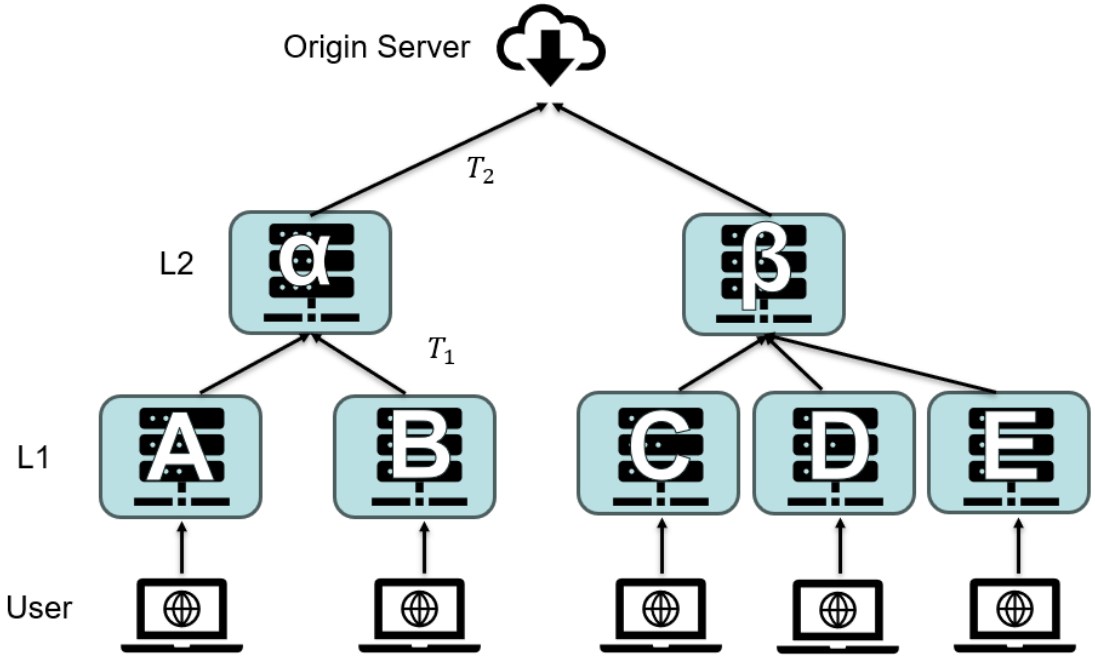
- Che-Approximation
  - $h_i \approx 1 - e^{-q_i t_c}$
  - $\sum_{i=1}^{M} h_i = C$

| Parameter | Definition |
|---|---|
| $q_i$ | Request ratio of content i |
| $C$ | Capacity of cache |
| $t_c$ | Characteristic time |

- The factor that affects average response time
  - Average service time（1/μ）
  - Arrival rate of request（λ）
  - Latency time (T)
  - Capacity of cache (C)

# Multilayer CDN Model

- Multiple layer
  - Origin server provide the original version of the content
  - L2 CSes caches content from the origin server and connect to L1 CSes
  - L1 CSes caches content from L2 CSes and accommodate the user's request
  - All CSes adopt LRU



# Multilayer CDN Model

- Average response time in CS A
  - $r_A = W_A$ -Cache hit in A
  - $r_\alpha = W_A + W_\alpha + T_1$ -Cache hit in $\alpha$
  - $r_O = W_A + W_\alpha + W_O + T_1 + T_2$ -Cache miss in A and $\alpha$
- Average response time of content i when request arrives at CS A
  - $R_A(i) = h_i^A r_A + (1 - h_i^A) h_i^\alpha r_\alpha + (1 - h_i^A)(1 - h_i^\alpha) r_O$
- Average response time of all requests in CS A
  - $R_A = \frac{\sum_{i=1}^{M} R_A(i)}{M}$

# Evaluation: Simulation parameter

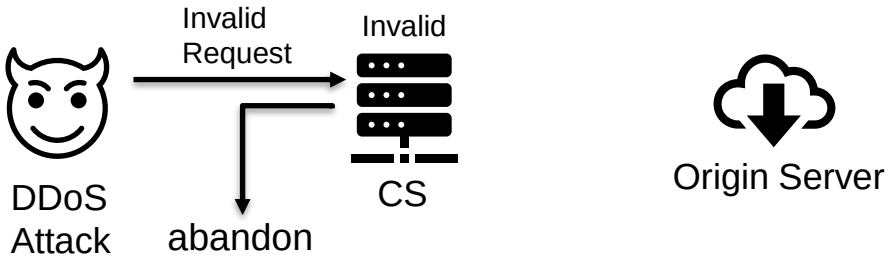
- Simulation parameter settings
  - Every CS has the same cache capacity (C)
  - Following the zip's law,

    $\lambda_i$ = 80, 9, 6, 4, 1 in L1 CSes
  - The offered load of each CS is 50% without attack

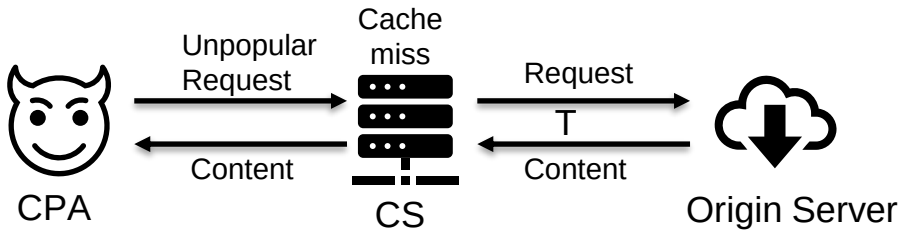
| Parameter | Value |
|---|---|
| M | 5 |
| C | 3 |
| $\sum_{i=1}^{M} \lambda_i$ | 100 /s |
| 1/μ of L1 CS | 5ms |
| 1/μ of CS α | 5ms |
| 1/μ of CS β | 3.3ms |
| 1/μ of origin server | 3.3ms |
| $T_1$ | 50ms |
| $T_2$ | 30ms |

# Evaluation: Attack definition

- DDoS
  - Sends request packets to invalid contents that will increase the processing load of CSes and invalid contents are not stored in the CS

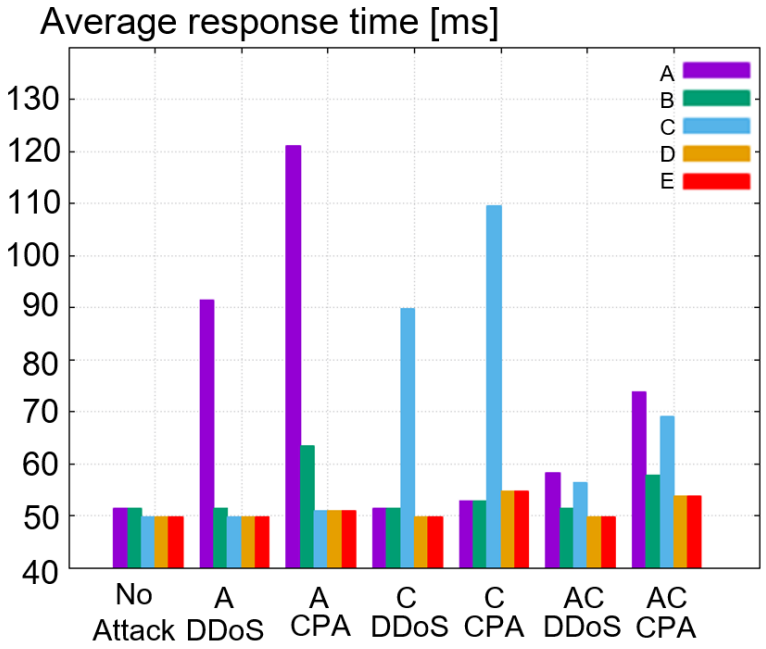


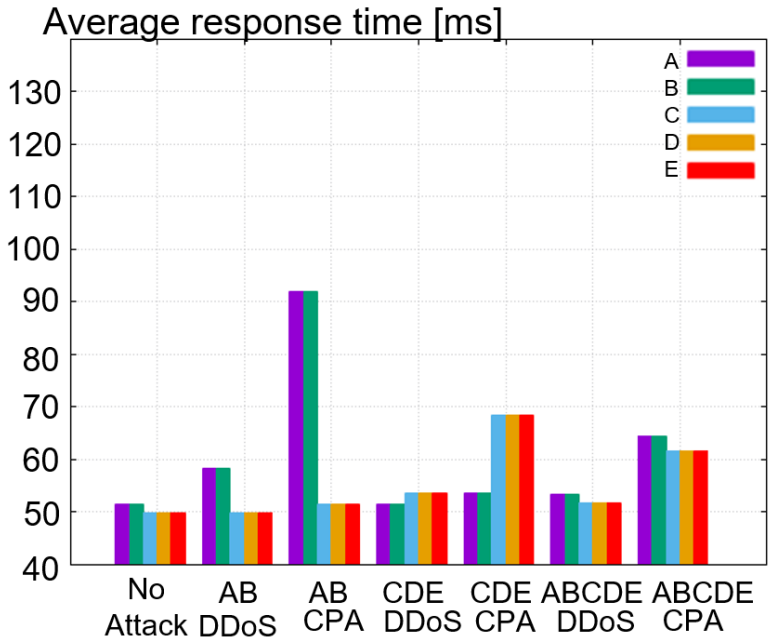

- CPA
  - Sends request packets to unpopular contents to decrease popular contents' cache hit ratio and increase the processing load



# Evaluation: Attack with limited resources

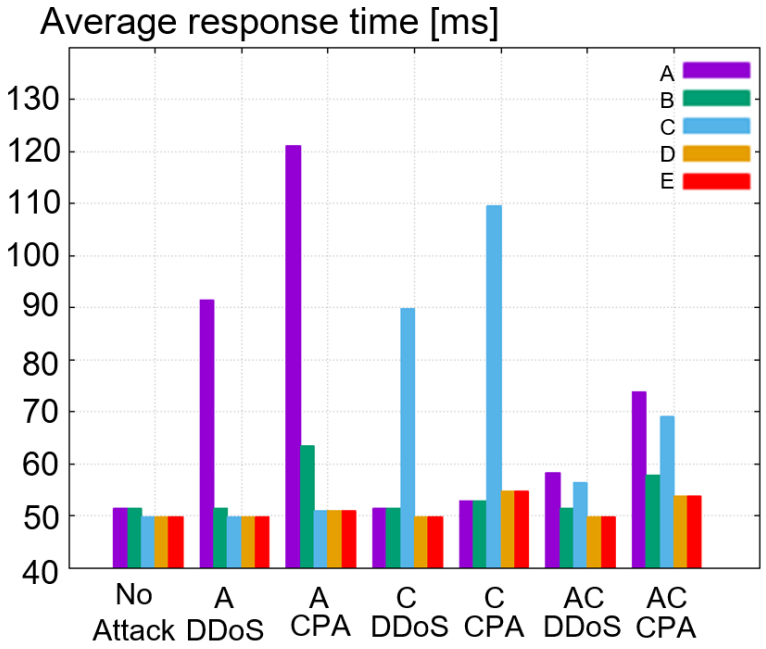
- Attack with limited resources
  - Assume that the attacker has limited resources to attack and set attacker's request rate 80/s
  - The attacker will assign requests to different CS
  - When the attacker send request packets to multiple CSes, it equally sends packets among the CSes

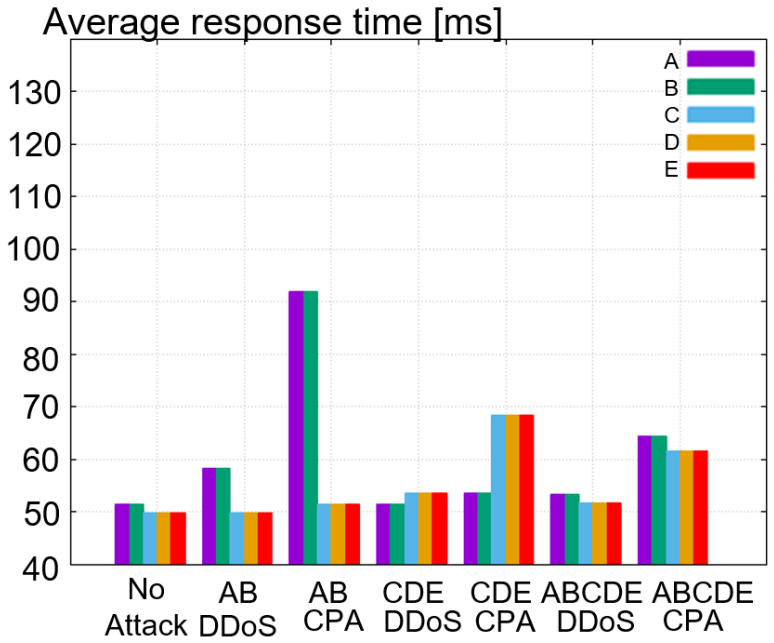


# Evaluation: Attack with limited resources

- Evaluation
  - CPA largely increased the response time of CSes
  - CPA also increased the response time of other CSes
  - CPA is still effective when multiple CSes are attacked
    but DDoS attack has little effect because the resources are dispersed



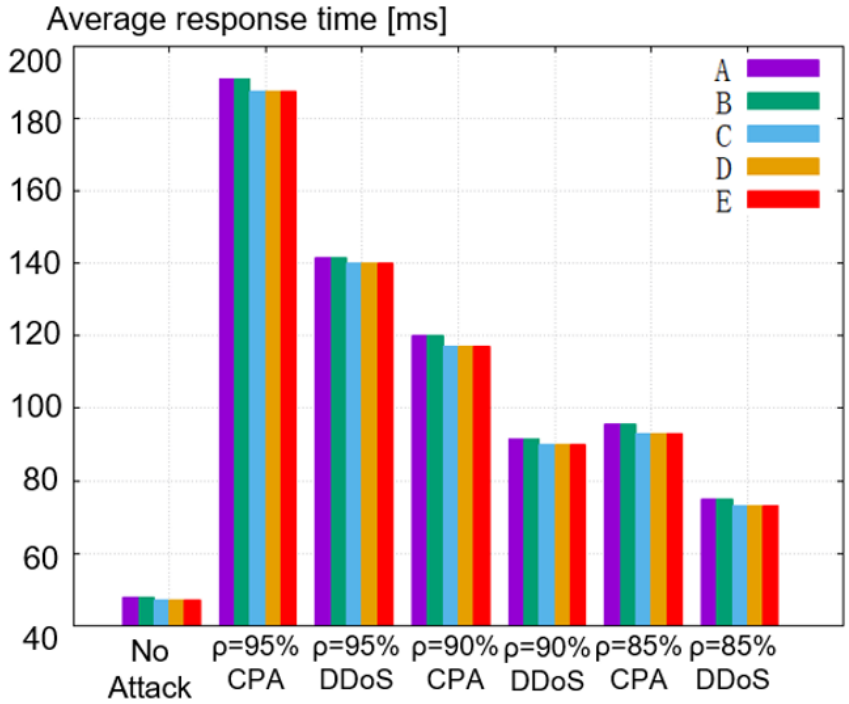
# Evaluation: Attack under protection

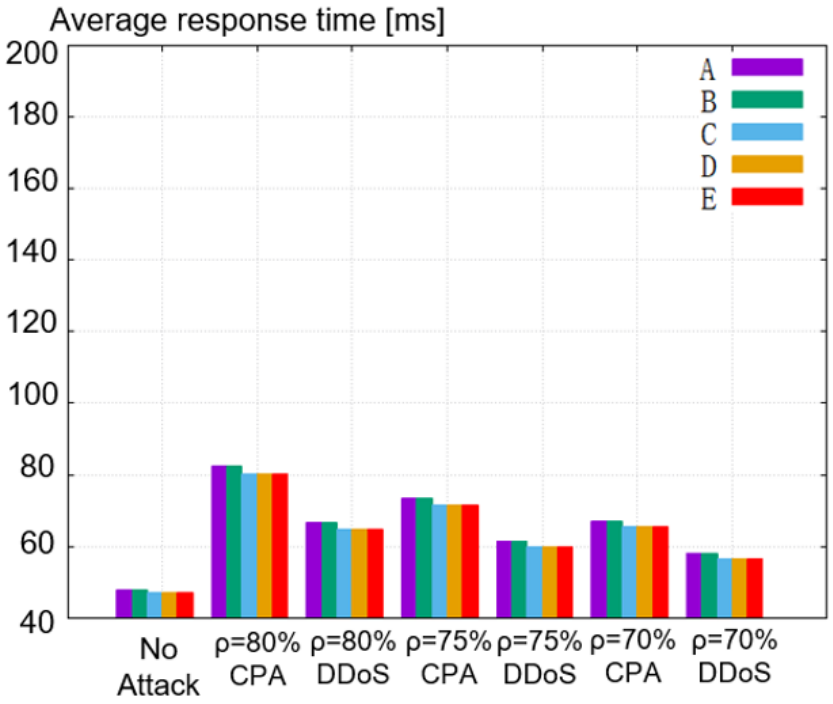
- Attack under protection mechanism
  - Assume CSes can bound the offered load of CSes below the threshold ρ even when DDoS or CPA occurs
  - Attacker will attack all CSes as much as possible
  - Reset the average service time in some CSes

| Parameter | Value |
|---|---|
| 1/μ of CS α | 3.3ms |
| 1/μ of CS β | 2.2ms |
| 1/μ of origin server | 2.2ms |

# Evaluation: Attack under protection

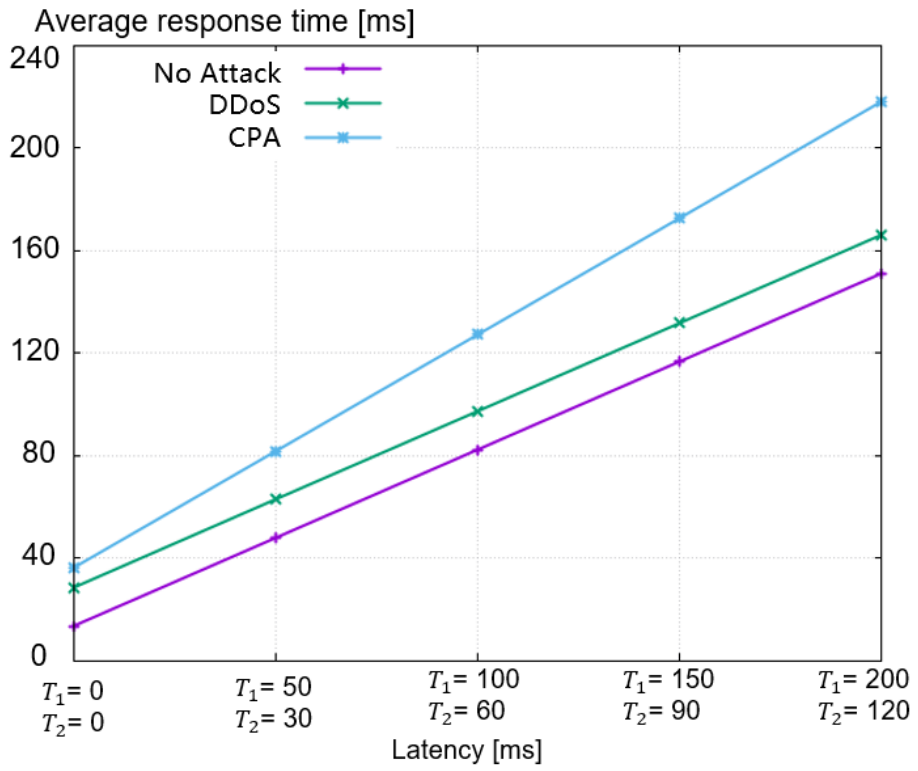
- Evaluation
  - Compared with case of DDoS attack, the CPA apparently increased the response time of CSes with the same ρ
  - When ρ becomes low, the effect of both attacks become weak, and the advantage of CPA also become weak.



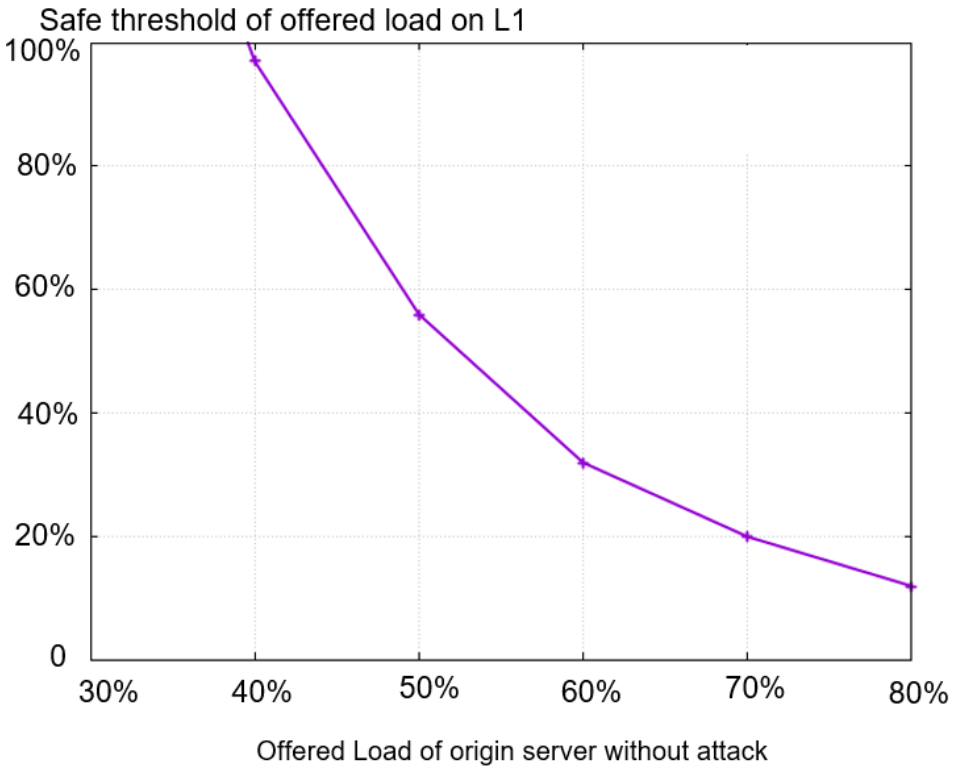
# Evaluation: Factors

- Latency
  - We obtained the average response time for different latency based on the attacks under protection
  - As the latency increased, the gap between CPA and DDoS attack became larger, indicating that CPA was sensitive to latency.



# Evaluation: Factors

- Offered load
  - Safe threshold
    - The maximum offered load under the normal serve of the origin service
  - When the origin server load is less than 39%, safe threshold exceed 100%
  - As the offered load of origin server increases, the security threshold decreases sharply.



# Conclusion

- We used the M/M/1 queue model to derive the response time for CSes in CDN
- We build a multi-layer CDN model according to the actual CDN, and compared the response time under different attacks
- We investigated factors, and we revealed the potential threats in the multi-layer CDN model.

- OVERLEAP
- CACHE HIT RATIO CHART
- MORE SERVER ON L2.
- LRU LFU