CDN のキャッシュを対象とした最適攻撃法

劉甲奇　上山 憲昭

立命館大学 情報理工学部

2023.09.15

研究背景

- Content Delivery Network (CDN)
  - CDNはインターネット上でコンテンツを効率的に配信する技術として広く普及

- CDNのキャッシュサーバを対象としたサイバー攻撃
  - DDoS(Distributed Denial of Service) とは, ターゲットサーバに大量のパケットを送りつけることで, ターゲットサーバの処理負荷を増加させサービス不能とする攻撃

  - CPA(Cache Pollution Attack)とは,低人気のコンテンツに意図的に大量の要求を出すことでキャッシュの性能を低下させる攻撃

  - CDN を効果的するには, DDoS攻撃や, CPAの攻撃方法を解明し, それらを効果的に防ぐ必要がある.

研究目的

- DDoS とCPA の検知/防御技術の研究は多く見られるが，攻撃側の戦術に関する研究は少数である.

- 攻撃者がターゲットキャッシュサーバに対し，CPAとDDoSにより攻撃を行う場合の最適法を検討ため、攻撃効果の評価方法を提案

提案方式 (1)

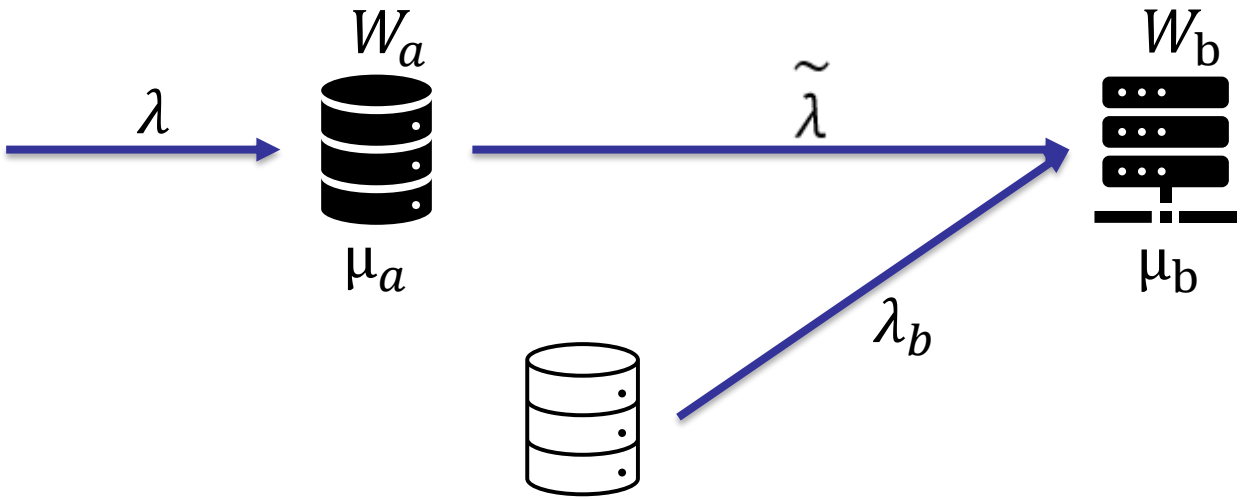
- M/M/1 モデル
  - ユーザの要求がレート λ のポアソン過程に従い到着
  - キャッシュサーバの処理時間は μ の指数分布に従う
  - M/M/1 の公式により 平均滞在時間W は次式で得られる

$$W = \frac{1}{\mu - \lambda}$$

  - コンテンツの集合 M に対して，各要求は独立に各コンテンツ m (m ∈ M) を確率 q_m で選択
  - 各コンテンツ m の要求はレートλ_m (= $q_m\lambda$) のポアソン過程に従い到着.

提案方式 (2)

- M/M/1 モデル
  - h_m: コンテンツ m のキャシュヒット率
  - λ_a: キャッシュサーバに到着する要求レート
  - μ_a: キャッシュサーバの処理レート
  - $\tilde{\lambda}$: キャシュミス時にオリジンサーバにコンテンツを要求レート
  - μ_b: オリジンサーバの処理レート
  - λ_b: オリジンサーバに他のキャッシュサーバから到着する要求レート



提案方式 (3)

- $\tilde{\lambda}$ とキャッシュサーバの平均滞在時間W_aは次式で得られる

$$W_a = \frac{1}{\mu_a - \sum_{m=1}^{M} \lambda_m}$$

$$\tilde{\lambda} = \sum_{i=1}^{M} \lambda_i (1 - h_i)$$

- オリジンサーバの平均滞在時間 W_b は次式で得られる

$$W_b = \frac{1}{\mu_b - (\tilde{\lambda} + \lambda_b)}$$

- 各コンテンツ i の平均滞在時間 W_iは次式で得られる

$$W_i = h_i W_a + (1 - h_i)(W_a + W_b)$$

- コンテンツ全体の平均滞在時間W_Mは次式で得られる

$$W_M = \sum_{i=1}^{M} \frac{\lambda_i W_i}{\lambda}$$

提案方式 (4)

- キャッシュヒット率
  - コンテンツmのヒット率h(m) はCheの近似式で付与[1]

$$h_m \approx 1 - e^{-q_m t_c}$$

  - t_cは，キャッシュサーバのキャッシュ容量 C を用いて次式で得られる[1]

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

[1] H. Che, et al.,“Hierarchical Web Caching Systems: Modeling, Design and Experimental Results,” IEEE J. Selected Areas of Commun., vol.20, no.7, Sep. 2002

性能評価

- 評価条件
  - キャッシュサーバの$\lambda_a = 1, \mu_a = 2.5,\ C = 3$
  - オリジンサーバの$\lambda_b = 0.5, \mu_b = 2$
  - q_mは次表のように設定

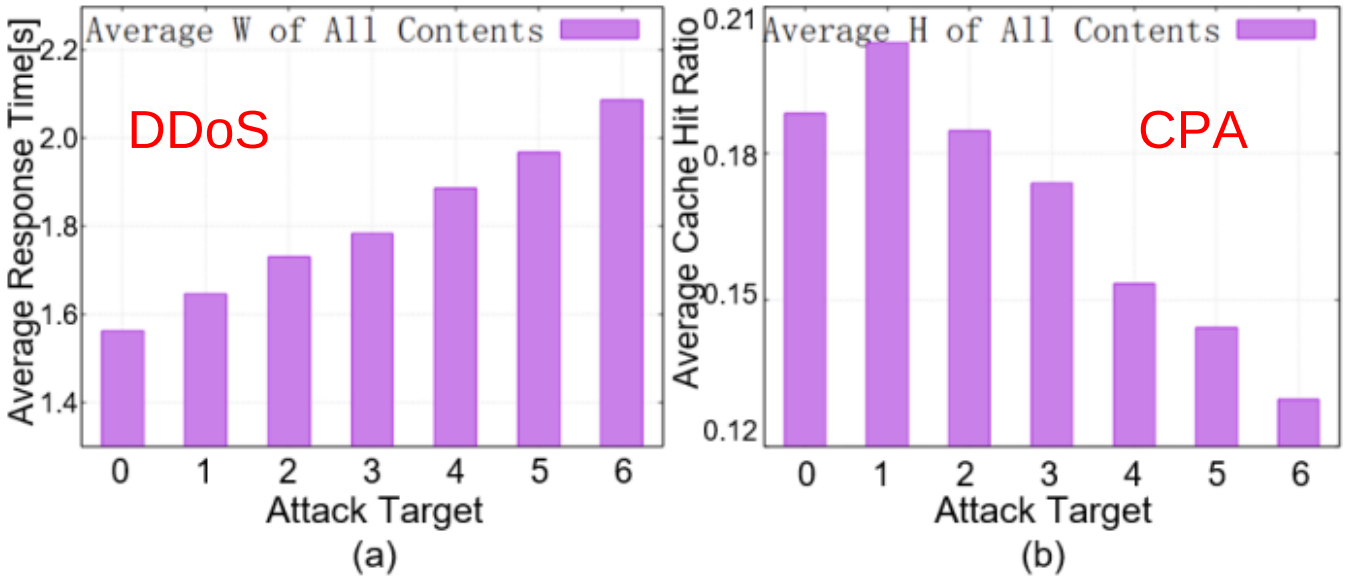
q_1	q_2	q_3	q_4	q_5	q_6
0.35	0.25	0.2	0.12	0.07	0.01

  - 攻撃者がコンテンツ m を攻撃対象として選択すると，要求レート λ m が 0.5 増加

評価結果

(a) Average Response Time[s]：コンテンツ全体の平均滞在時間

(b) Average Cache Hit Ratio：コンテンツ全体の平均ヒット率



攻撃ターゲット0は攻撃が発生しない場合

- DDoS攻撃が発生すると平均滞在時間が増加し，特に人気の低いコンテンツへの攻撃ほど，応答時間の増加が大きい．
- 低人気コンテンツを対象に CPA を行うことで，すべてのコンテンツに対する正常ユーザの平均ヒット率が低下し，攻撃の効果が高い．

- 人気の低いコンテンツに対する攻撃ほど，全体的に攻撃の効果が高い．

まとめ

- 本稿では DDoS 攻撃や CPA が発生したときの，正常ユーザの応答時間やキャッシュヒット率の低下度を導出し，攻撃の影響を分析

- 今後の取り組み
  - 異なるコンテンツへの攻撃のヒット率と平均滞留時間の変化を評価し，最適な攻撃方法を明らかにする
  - マルチエッジサーバのCDN のキャッシュを対象とした最適攻撃法を検討