CDNのキャッシュを対象とした最適攻撃法

Optimal Attack Method Targeting CDN Caches

劉 甲奇　　上山 憲昭
Liu Jiaqi　　Noriaki Kamiyama
立命館大学 情報理工学部 情報理工学科
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

近年，インターネットでのコンテンツ配信のトラフィック量増加しており，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 Content Delivery Network (CDN) が，インターネットの基幹技術として利用が拡大している．CDN を効果的するには，CDN のキャッシュサーバを対象とした Distributed Denial of Service (DDoS) 攻撃や，Cache Pollution Attack (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．しかしこれまでに DDoS 攻撃の検知/防御技術や，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．そこで本稿では攻撃をより効果的に防御するために，攻撃者がターゲットキャッシュサーバ (TCS) に対し，CPA と DDoS により攻撃を行う場合の最適攻撃法を提案する．

2. 提案方式

M/M/1 モデルを用いて，CDN のキャッシュサーバに対するユーザの要求の平均滞在時間 W を導出する．DDoS 攻撃や CPA によってコンテンツの要求率が増加するため，攻撃が発生した後の平均滞在時間の変化を観察して最適攻撃対象を選択する．

ユーザの要求がレート λ のポアソン過程に従い到着し，キャッシュサーバの処理時間は平均が μ の指数分布に従うことを想定する．M/M/1 の公式により W は次式で得られる．

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

コンテンツの集合 $\boldsymbol{M}$ に対して，各要求は独立に各コンテンツ m $(m \in M)$ を確率 q_m で選択するとき，各コンテンツ m の要求はレート $\lambda_m(=q_m\lambda)$ のポアソン過程に従う．h_m をコンテンツ m のキャッシュヒット率，キャッシュサーバの処理レートを μ_a とすると，キャッシュサーバに到着した要求がキャッシュミス時にオリジンサーバにコンテンツを要求するレートを $\tilde{\lambda}$ 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．

$$W_a = \frac{1}{\mu_a - \sum_{m=1}^{M} \lambda_m} \tag{2}$$

$$\tilde{\lambda} = \sum_{i=1}^{M} \lambda_i (1 - h_i) \tag{3}$$

また，オリジンサーバの処理レートを μ_b で，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のレートを λ_b とすると，オリジンサーバの平均滞在時間 W_b は次式で得られる．

$$W_b = \frac{1}{\mu_b - (\tilde{\lambda} + \lambda_b)} \tag{4}$$

各コンテンツ i の平均滞在時間 W_i は，キャッシュヒット時のキャッシュサーバの平均滞在時間 W_a と，キャッシュミス時の平均滞在時間 $W_a + W_b$ から，次式で得られる．

$$W_i = h_i W_a + (1 - h_i)(W_a + W_b) \tag{5}$$

各コンテンツの要求確率が異なることを考慮して，コンテンツ全体の平均滞在時間 W_M は次式で得られる．

$$W_M = \sum_{i=1}^{M} \frac{\lambda_i W_i}{\lambda} \tag{6}$$

次にコンテンツ m のキャッシュヒット率 h_m の近似式 [1] を次式で得る．

$$h_m \approx 1 - e^{-q_m t_c} \tag{7}$$

ただし t_c は，キャッシュサーバのキャッシュ容量 C を用いて，$\sum_{i=1}^{M} h_m = C$ で得られる [1].

3. 性能評価

キャッシュサーバの要求が平均 1 秒間隔でポアソン到着して (λ_a = 1 個/秒)，処理時間は平均 0.4 秒の指数分布に従う (μ_a = 2.5 個/秒)．オリジンサーバの他の要求が平均 2 秒間隔でポアソン到着して (λ_b = 1 個/秒)，オリジンサーバの処理時間は平均 0.5 秒の指数分布に従う (μ_b = 2.5 個/秒)．コンテンツ集合 M は 6 コンテンツとし，正常ユーザが各コンテンツ m を要求する確率は $q_m = 0.35, 0.25, 0.2, 0.12, 0.07, 0.01$ とする．またキャッシュサーバのキャシュ容量を ($C = 3$) とする．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 増加する．

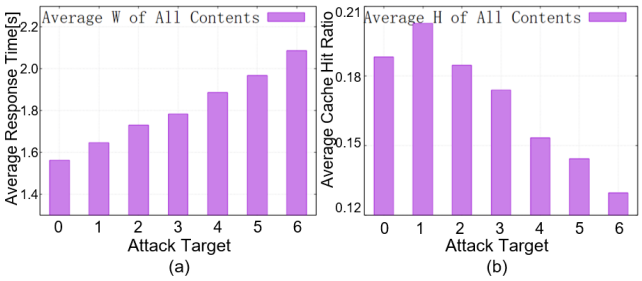

図 1: Average response time and Average cache hit ratio of all legitimate requests

図 1 に，攻撃者が攻撃対象として選択したコンテンツごとに，正常ユーザの全コンテンツに対する平均レスポンス時間と平均ヒット率をプロットする．ただし攻撃ターゲット 0 は攻撃が発生しない場合である．図 1(a) 示すように，攻撃が発生すると平均レスポンス時間が増加し，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．また図 1(b) に示すように，低人気コンテンツを対象に DDoS や 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．そのため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．

4. まとめ

本稿では M/M/1 モデルとキャッシュヒット率近似式 [1] を用いて，CDN キャッシュサーバに対する 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合を導出し，CDN キャッシュサーバをターゲットとした攻撃の影響を分析した．今後は，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．また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する．

謝辞

本研究成果は JSPS 科研費 21H03437 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[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