CDN のキャッシュサーバを騙った DDoS 攻撃の防御方式

Mitigating CDN-Pretended DDoS Attack

宮崎　椋平　　上山 憲昭

Ryohei Miyazaki　　Noriaki Kamiyama

福岡大学 工学部 電子情報工学科

Faculty of Engineering, Fukuoka University

1. はじめに

昨今のネットワークのアクセス集中やコンテンツの大容量化に伴い CDN (Content Delivery Network) でのコンテンツ配信が主流となっている．一方で近年，ネットワーク上に広く存在するボットから大量のパケットをターゲットホストに送信することで，ターゲットサーバを機能不全とする DDoS (Distributed Denial of Service) 攻撃が頻繁に発生している．しかしコンテンツ提供者 (CP) が CDN を用いている場合，ボットからの配信要求は多数のキャッシュサーバ (CS) に送付されるため，オリジンサーバ (OS) に対する脅威は低下する．またボットが OS の IP アドレス宛てに直接パケットを送信した場合も，OS に対しては本来，CS からのみ要求が届くことから，CS 以外からの配信要求をファイアウォールで棄却することで対処できる [1][2]．しかしボットが CS の IP アドレスを発アドレスとして偽り，標的オリジンサーバへパケットを送信すると，ファイアウォールでの検知ができない．ところで CS から OS への配信要求は本来，CS のキャッシュミスのときにのみ発生する．一方，DDoS 攻撃は短い時間間隔で多数の CS から連続して発生する．そこで本稿では，要求発生間隔の違いを利用した CDN を騙った DDoS 攻撃の検知方式を提案する．

2. CDN の名前解決方法

CDN を用いている場合，ユーザの配信要求時には CP の DNS サーバとの名前解決手順に加え，CDN 事業者の DNS サーバとの間で以下の手順が生じる．

1. LDNS (Local DNS) サーバの要求に対し CP の権威 DNS サーバは CNAME を LDNS サーバへ回答
2. LDNS サーバは CNAME の名前解決を CDN 事業者の権威 DNS サーバへ要求
3. CDN 事業者の権威 DNS サーバは CS を選択しその IP アドレスを LDNS サーバへ回答
4. LDNS サーバはユーザに IP アドレスを回答し，ユーザは指定された CS へアクセス
5. CS にキャッシュされていない場合は，CS は OS からコンテンツを取得してキャッシュ後，ユーザに配信

そのため CS からの正常な問い合わせ時には，CP の DNS サーバに名前解決のログが残るが， ボットからの OS の IP アドレスを直接用いた要求は DNS の名前解決を用いないため名前解決の履歴が残らない．そのため DNS のログを調べれば，CS からの正常な配信要求か，ボットからの DDoS パケットかの区別が可能である．しかし OS には大量の配信要求が到着することから，すべての配信要求に対して DNS のログを調べると OS の処理負荷の増大が懸念される．

3. 提案方式

CS から OS への問い合わせは通常，キャッシュミスした場合に生じる．しかし DDoS 攻撃の場合，ボットから短い時間間隔で膨大な量の攻撃パケットが送られてくることが想定される．そこで問い合わせ間隔に閾値 T を設け，ホストごとに要求の到着間隔を計測し，T より長い間隔の要求に対してはキャッシュミス時に生じた CS からの正常な要求と見なしてそのまま配信処理を行う．一方 T より短い間隔の要求に対してはボットからの DDoS 攻撃の可能性を考え，DNS サーバへの問い合わせ有無を確認する．そして問い合わせが有った場合は通常の CS からの要求と見做し配信処理を行う．一方，問合せが無い場合は DDoS 攻撃と判断し，アクセスを棄却する．このように DNS 検査を行う対象を限定することで，DNS のログの検索の負荷を減らすことができ，かつ正常な要求を棄却せずに DDoS 攻撃のパケットのみを規制することができる．

4. 性能評価

提案方式の有効性を計算機シミュレーションにて評価する．キャッシュ置換方式は LRU 方式とし，コンテンツ数を $N = 10,000$，キャッシュサイズを $C_S = 100$，シミュレーション時間を 1,000 秒とする．またユーザのコンテンツ選択確率はパラメタ θ の Zipf 分布に従う．

図 1(a) は Zipf 分布の θ を 0〜3 まで変化させたときの，人気順位 1，3，10 位の各コンテンツの 1 秒間あたりの平均 DNS 検査回数を示す．ただし正常な問合せのみを対象とする．高人気コンテンツほどキャッシュヒット率が上がるため， θ の増加に伴い DNS 検査数が減少すると予測できる．しかし $\theta = 1.3$ 程度までは θ の増加に伴い DNS 検査回数は増加した．これは $\theta = 1.3$ 程度までは高人気コンテンツであっても要求発生ごとにキャッシュミスが多く発生するためである．しかし $\theta = 1.3$ 程度以降は，θ の増加に伴いキャッシュヒット率が増加し，DNS 検査数が減少する．

ボットは T 未満の時間間隔で要求を OS に送ると，検知されて防御される．そのため攻撃が見逃されて成立する DDoS 攻撃の最大強度 (1 秒間にオリジンサーバに到着するパケット数の平均値) は，CS 数を C_N とすると C_N/T となる．図 1(b) に C_N の 3 つの値に対し，DDoS 攻撃の最大強度を検知閾値 T に対して示す．閾値 T が増加するほど DDoS パケットの到着回数が減少するため DDoS 攻撃強度が下がる．また CS 数が増加するほど，OS への攻撃パケットのソース IP アドレスの異なり数が増加するため DDoS 攻撃強度が増加する．

図 2(a) は T を変化させたときの人気順位 1 位のコンテンツに対する正常ユーザからの 1 秒間あたりの平均 DNS 検査回数を，Zipf パラメタ θ とキャッシュサイズ C_S のいくつかの値の組に対し各々示す．図 2(b) に人気順位 10 位のコンテンツの結果を同様に示す．$T = 1.0$ 秒あたりまでは T の増加に伴い DNS 回数が増加するが，それ以降は，ほぼ一定となるため，閾値の最大値は 1.0 がおおまかな目安となる．

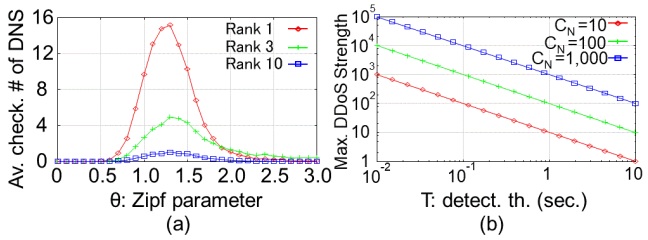

図 1: (a) 平均 DNS 検査回数，(b)DDoS 攻撃の最大強度

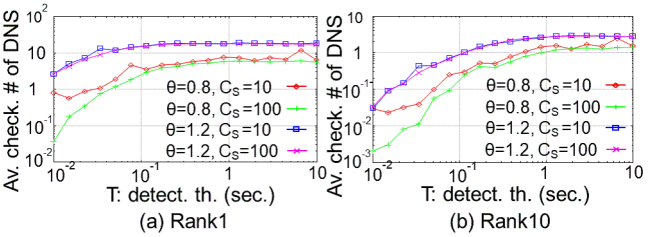

図 2: 検知閾値 T に対する平均 DNS 検査回数

謝辞　本研究成果は JSPS 科研費 18K11283 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]T. Vissers, et al., Maneuvering Around Clouds: Bypassing Cloud-based Security Providers, ACM CCS 2015

[2]D. Gillman, et al., Protecting Websites from Attack with Secure Delivery Networks, Comp. Mag., 2015