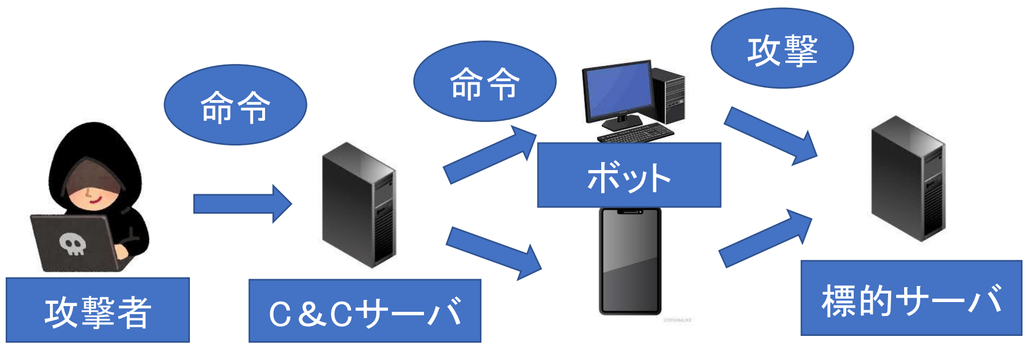
CDNのキャッシュサーバを騙った DDoS攻撃の防御方法

1. 研究背景

■ CDN（Content Delivery Network）でのコンテンツ配信が主流

■ DDoS攻撃が頻繁に発生

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ホストを機能不全にする攻撃



■ CDNを用いると、ボットからの配信要求は多数のキャッシュサーバ（CS）に送信 ⇒オリジンサーバ（OS）に対しての脅威は低下

■ ボットがOSのIPアドレス宛に直接パケットを送信した場合も、CS以外からの配信要求をOSはファイヤーウォールで棄却可能

■ 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OSへパケットを送信すると，ファイアウォールでの検知がてできない

⇒ CDNのキャッシュサーバを騙ったDDoS攻撃

■ DDoS攻撃は短い時間で多数のCSから連続して発生

■ 本研究: 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

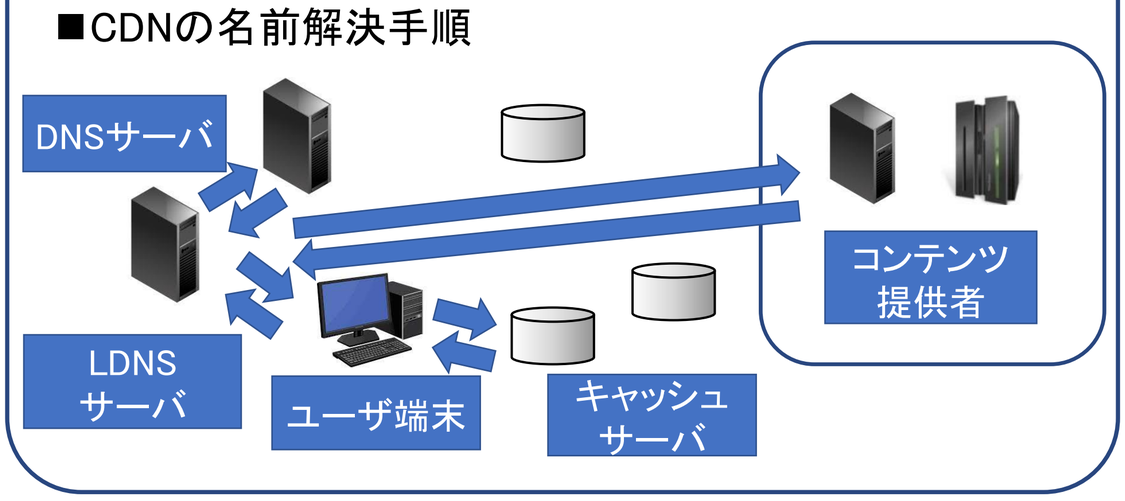
2. CDNの名前解決

■ CDNを用いている場合、CSからの正常な問い合わせ時には、Content provider (CP)のDNSサーバに名前解決のログが残る

■ 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のログを調べればボットからの要求か否かの判断が可能 ⇒ 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

■CDNの名前解決手順



3. 提案方式

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、以下の処理を実施

■ Tより長い間隔の要求

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実施

■ Tより短い間隔の要求

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

問い合わせあり

⇒通常のCSからの要求と見做し配信処理を実施

問い合わせなし

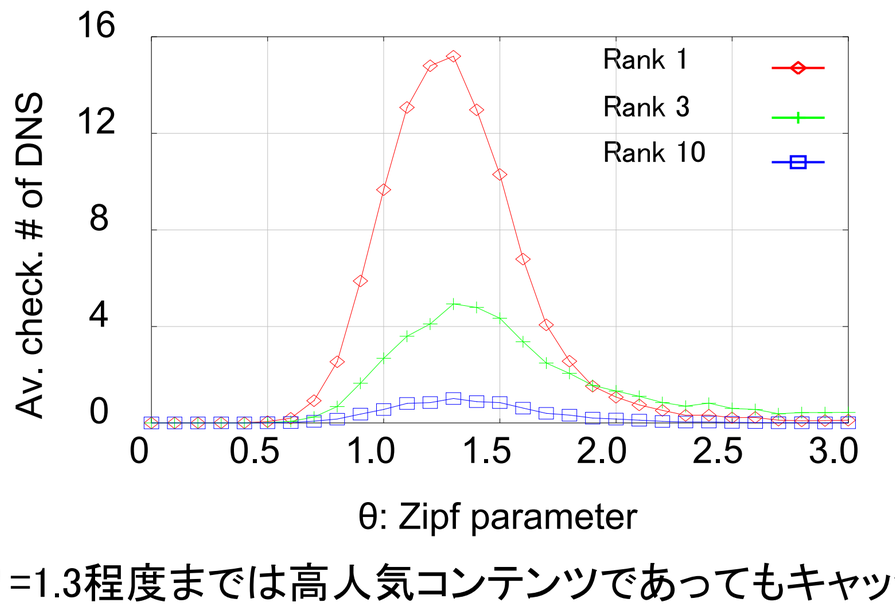
⇒ DDoS攻撃と判断しアクセスを棄却

4. 性能評価

■ キャッシュ置換方式LRU、コンテンツ数N = 10, 000、キャッシュサイズ 100

■ ユーザのコンテンツ選択確率はパラメタ θ の Zipf 分布

■ 下図: θ を変化させたときの、人気順位1、3、10位の各コンテンツに対する正常CSからOSあてに単位時間あたりに生じる要求発生数の平均値Vをプロット



■ θ =1.3程度までは高人気コンテンツであってもキャッシュミスが多く発生するため、θ の増加に伴いVは増加

■ θ が1.3程度より大きな領域では、θ の増加に伴いキャッシュヒット率が増加しVは減少

Θが小さいか大きな場合に、提案方式はOSの処理負荷の増加を抑制

5. 今後の取り組み

■OSの処理能力から定まる許容DNS検査回数の上限を満たす条件で、キャッシュサーバを騙ったDDoS攻撃の検知能力を最大化する最適閾値設定法を検討

■計算機シミュレーションにより提案方式の有効性を確認