CDNのキャッシュサーバを騙った DDoS攻撃の防御法

1. はじめに

■ 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によりで機能不全にする攻撃

■ 攻撃者が標的サーバのIPアドレスを特定した場合

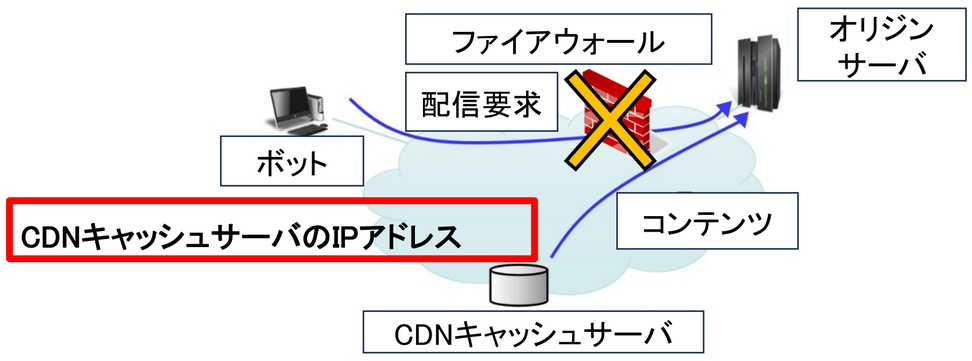
DNS (Domain Name System)を用いずに，特定したIPアドレス宛に直接パケットを送信

→ CDNキャッシュサーバ以外からのパケットファイアウォールで遮断

■ CDNのキャッシュサーバを騙ったDDoS攻撃

ボットがキャッシュサーバ(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

→ ファイアウォールでの検知不可



■ 要求発生間隔の違いを利用した動的な検知方式

→ Zスコア法を用いた検知方法を提案

2. 先行研究について

■ 先行研究: DDoS攻撃の二段階検知法

DNSの名前解決ログにより，攻撃を検知

■ DNSの名前解決ログによるパケットの判別法

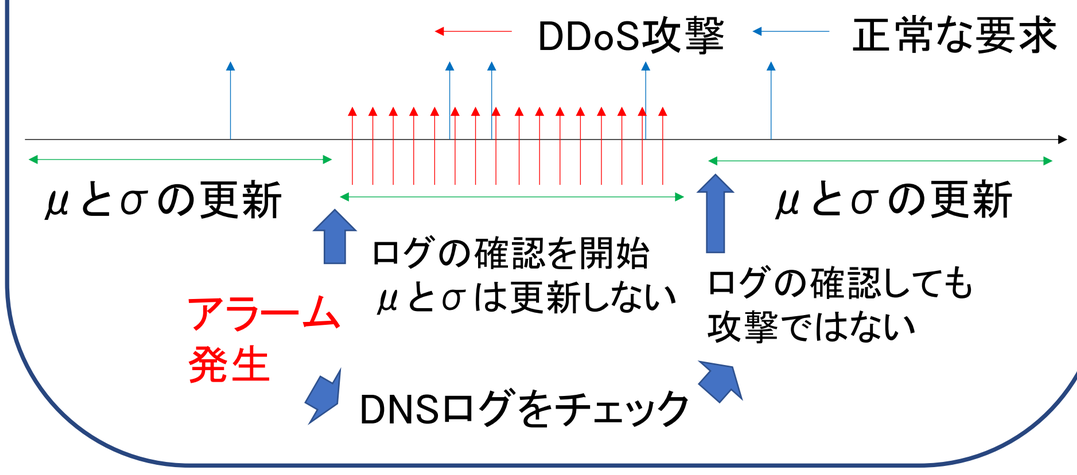
- 問い合わせあり: 配信処理を実施
- 問い合わせなし: DDoS攻撃と判断し，アクセス棄却

→ 全要求に対しDNSのログを確認するとOSの負荷増大

→ Zスコア法を用いたパケットレート判定により危険性のある要求を判別

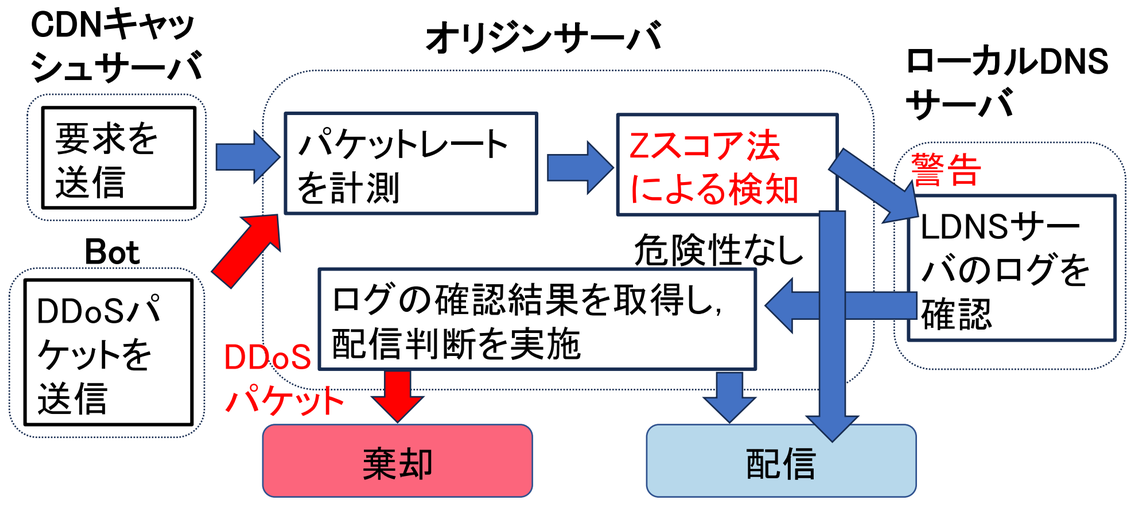
■ 問題点

権威DNSでのログ確認では，LDNSサーバでキャッシュヒットした場合に，ログが欠損しており正常な判定が困難



3. 提案方式

■ アルゴリズム



■ 提案方式

1. リクエストの到着間隔を計測
2. 逆数をデータとしてZスコア法に使用
3. LDNSでログデータを確認
   - キャッシュヒットログの欠損リスクを回避
4. OSでLDNSからのログ確認結果を取得し，判断

■ 変更に伴う遅延時間 T の算出式

$$T = 5 \times 10^{-6} d + T_m \quad (1)$$

$$T_m = \left(\frac{2}{n \cdot T_r} - \frac{c}{T_s} \right)^{-1} \quad (2)$$

4. 性能評価

■ 遅延時間の評価

- LDNSサーバでのログ確認処理に伝搬遅延とメモリアクセスの遅延が発生
- メモリアクセスの遅延時間は数 μ 秒程度

← 1kmあたり5 μ 秒必要とする伝搬遅延と比較し，非常に小さい

■ 検知精度の評価

- 提案方式を使用しない場合と比較すると，OSの負荷が減少
- 攻撃レートが増加するほど，攻撃数に対するOSの負荷を軽減
- 攻撃数の増加に伴い，LDNSの負荷も増加