CDNのキャッシュサーバを騙ったDDoS攻撃の防御方法

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

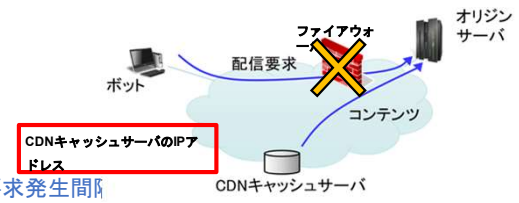
DNS(Domain Name System)を用いずに，特定したIPアドレス宛に直接パケットを送信

→ 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)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，アクセスを棄却

→ 全要求に対しDNSのログを確認するとOSの負荷増大

→ 固定閾値で危険性のある要求を判別

■ 先行研究の特徴

- 単一閾値を用いる検知法
- 要求発生パターンの違いを利用

■ 問題点

単一閾値を用いているため，見逃し誤検知が多い

3. 提案方式

■ アルゴリズム

1. 到着間隔の逆数をデータとして利用
2. Zスコア法で危険性のある要求に対し，信号が発生
3. DNSのログにより，検知した要求が攻撃であるかを判断
4. 攻撃であった場合，検知を開始
5. DNSのログを確認，正常である要求が継続
6. 検知終了

■ 提案方式のメリット

■ 到着間隔の逆数をデータとしてZスコア法に使用

→ 到着間隔の違いよりDDoSパケットが発生したことを判別

■ 攻撃発生中の誤ったデータを平均に反映しない

→ 正常な要求のみが起こっている時とは異なった到着間隔のパターンを検知

■ Zスコア法のメカニズム

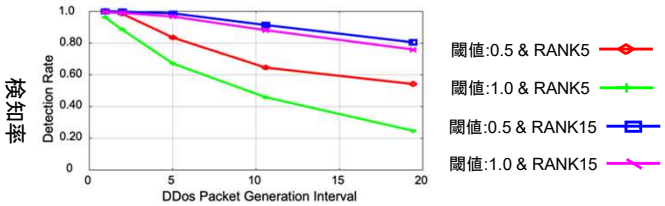
- 過去のデータより平均を算出
- 平均から外れ値を検知
- 外れ値を平均に基づいて編集しデータとして記録

4. 性能評価

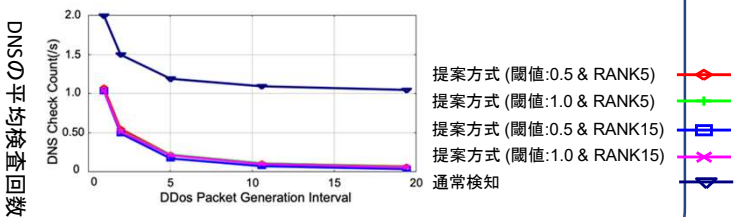
■ シュミレーションで有効性を評価

■ 攻撃パケットの検知率で評価

- 検知率は90パーセント以上を検知
- 提案方式は処理負荷を軽減



単位時間当たり平均DDoSパケット発生回数



単位時間当たり平均DDoSパケット発生回数