CDNのキャッシュサーバを騙った DDoS攻撃のZスコア法を用いた防御法

立命館大学　情報理工学部　情報理工学科
谷口 和也　上山 憲昭

CDNの普及

■ CDN(Content Delivery Network)とは

サーバにキャッシュしたコンテンツを効率的に配信するサービス

⇒配信の遅延時間を短縮、トラフィックを削減

■ CDNのトラフィック量は年々増加傾向

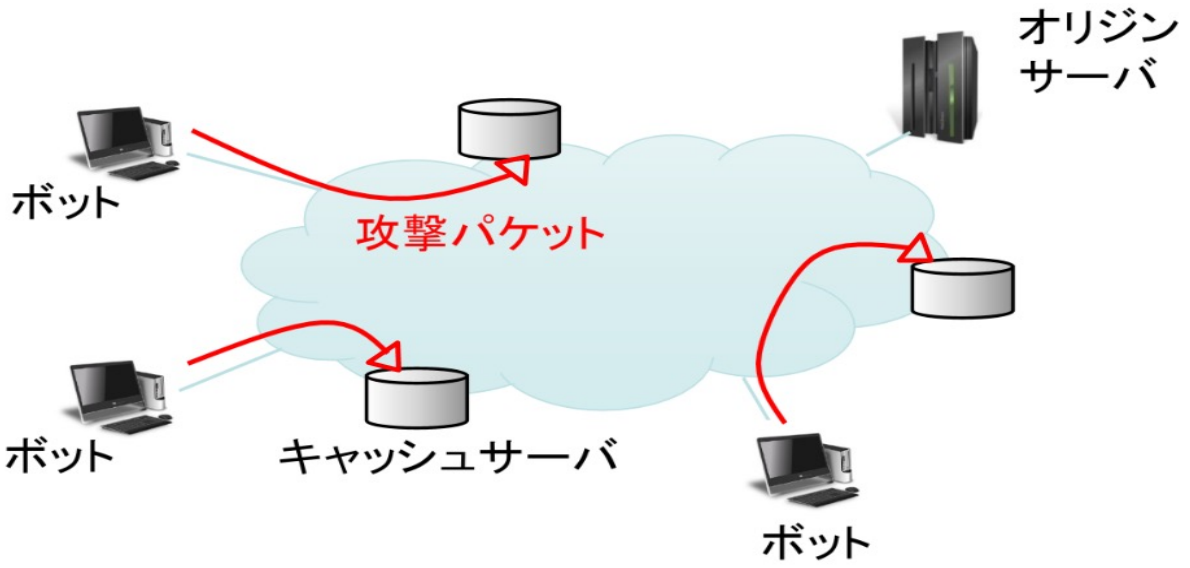
⇒2020年には約50%以上のトラフィックがCDNを利用

データ引用: Cisco Visual Networking Index:Forecast and Methodology, 2015-2020

CDNによるDDoS攻撃への有効性

- DDoS攻撃（Distributed Denial of Service attack）が頻繁化
- CDNを用いた配信により，DDoS攻撃を緩和
- 攻撃者がCDN利用者を標的にした場合
  - 接続先として分散してCDNキャッシュサーバへ

  ⇒大量のパケットを軽減

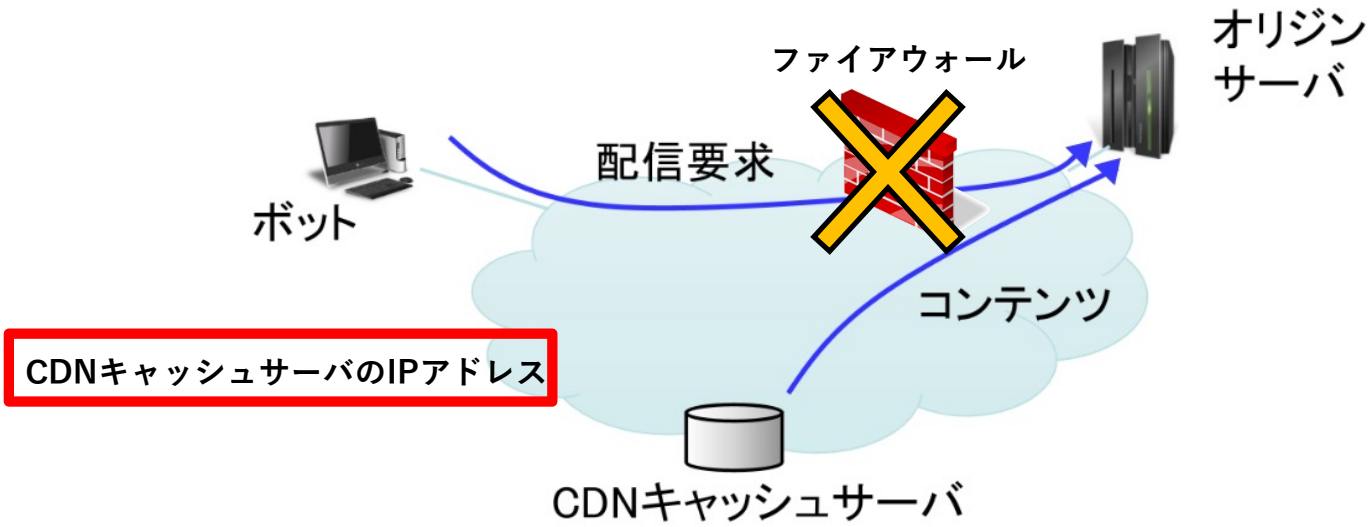


CDNのDDoS攻撃に対する課題

- 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

  ⇒DDoS攻撃が成立
  - CDNキャッシュサーバ以外から到着したパケットはファイアウォールで遮断
- 攻撃者がCDNキャッシュサーバのIPアドレスを発アドレスとして偽った場合

⇒DDoSパケットを送るとファイアウォールで検知不可



先行研究：DDoS攻撃の二段階検知法

- DNSの名前解決処理のログにより，攻撃を検知
  - 問い合わせが有り: 配信処理を実施
  - 問い合わせが無し: DDoS攻撃と判断し,アクセスを棄却

⇒全ての要求に対し，DNSのログを確認するとオリジンサーバの負荷が増大

- 著者らの先行研究[1]
  - 単一閾値を用いる検知法
  - 正常な配信要求: キャッシュミス時に発生
  - DDoS攻撃: 短い時間間隔で膨大な数が連続して発生

⇒要求発生パターンの違いから攻撃を検知

問題点: 単一閾値を用いているため見逃し，誤検知が多い

[1] 宮崎椋平, 上山憲昭, CDNのキャッシュサーバを騙ったDDoS攻撃の防御方式, 信学会2021年総合大会, B-11-10

研究の目的

- CDNキャッシュサーバを騙った攻撃パケットをDNSのログを用いて検知
  - 全要求のログを確認

  ⇒オリジンサーバの負荷増大
  - 正常なコンテンツ配信要求と攻撃パケットには要求発生パターンの違いが存在

- オリジンサーバの負荷を軽減する方法を検討

⇒要求発生パターンの違いからZスコア法を使用

Zスコア法

- データの外れ値を検知するアルゴリズム
- 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
- 3つのパラメタ
  - ラグ(L): 平均値を作成する過去のデータの個数
  - 閾値(η): 信号を検知する際の感度
  - 影響(α): 値を更新する際の過去のデータの影響度

$$S_i = \begin{cases} 1, & \text{if } E_c - \mu_{i-1} > \eta\sigma_{i-1} \\ -1, & \text{if } E_c - \mu_{i-1} < -\eta\sigma_{i-1} \\ 0, & \text{otherwise} \end{cases}$$

$$E_i = \begin{cases} E_c, & \text{if } S_i = 0 \\ \alpha \times E_c + (1-\alpha) \times E_{i-1}, & \text{otherwise} \end{cases}$$

$$\mu_i = mean(E_{i-L+1}, E_{i-L+2}, ..., E_i)$$

$$\sigma_i = std(E_{i-L+1}, E_{i-L+2}, ..., E_i)$$

Zスコア法を通常使用した際の問題点

- Zスコア法でデータを到着間隔として活用
- 問題点: 正方向の正常パケットを誤検知
  - 正方向の変化量: 正常パケット 大 ⇄ DDoSパケット 小

  ⇒正方向の正常パケットを誤検知

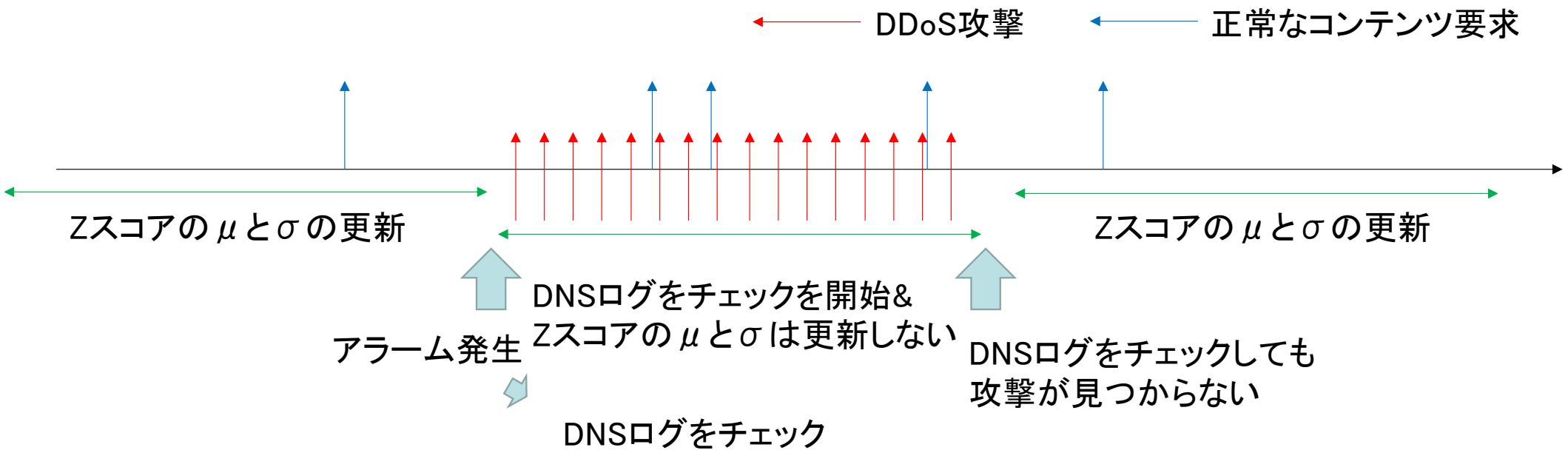
⇒提案方式: データの逆数を使用

- Zスコア法を攻撃発生中，平均値や標準偏差を更新
- 問題点: 誤った到着間隔パターンを学習
  - 攻撃パケットを含めた到着間隔のパターンを学習

  ⇒攻撃パケットを見逃し，棄却

⇒提案方式: 検知時点の平均値や標準偏差を継続して使用

提案方式: Zスコア法を用いたDDoS攻撃の検知法



- 提案方式の二つの解決法
  - 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

シミュレーション条件

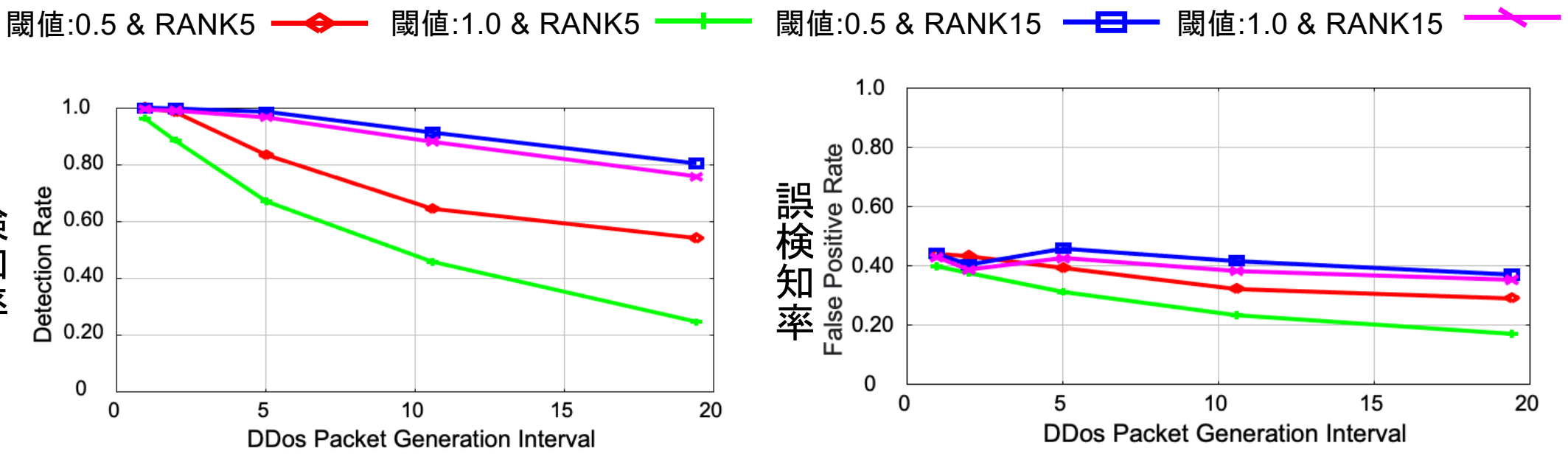
- データはRANK5(Zipf分布に基づいた人気度)のコンテンツ要求の到着間隔の逆数
- Zスコアのパラメタ: ラグ(L): 5, 閾値(η): 1.0, 影響(α): 0.5
- コンテンツ要求のシミュレータの設定

項目	設定した値
シミュレーション時間	100秒
コンテンツの種類	100個
キャッシュ容量	10個
要求の平均発生回数	100回
DDoS攻撃の平均発生間隔	約1/100, 1/50, 1/20, 1/10, 1/5秒
攻撃を受ける期間	30～60秒の間

- 評価項目
  - DDoSパケットを検知できた割合(検知率)
  - 正常パケットを誤ってDDoSの可能性ありと検知した割合(誤検知率)
  - DNSの単位時間あたりの平均検査回数

シミュレーション結果（1）

- コンテンツを変更（低人気コンテンツに変更）した場合
  - 検知率が高く，誤検知率が高く
- 閾値が小さく（感度が高く）変更した場合
  - 検知率が高く，誤検知率が高く

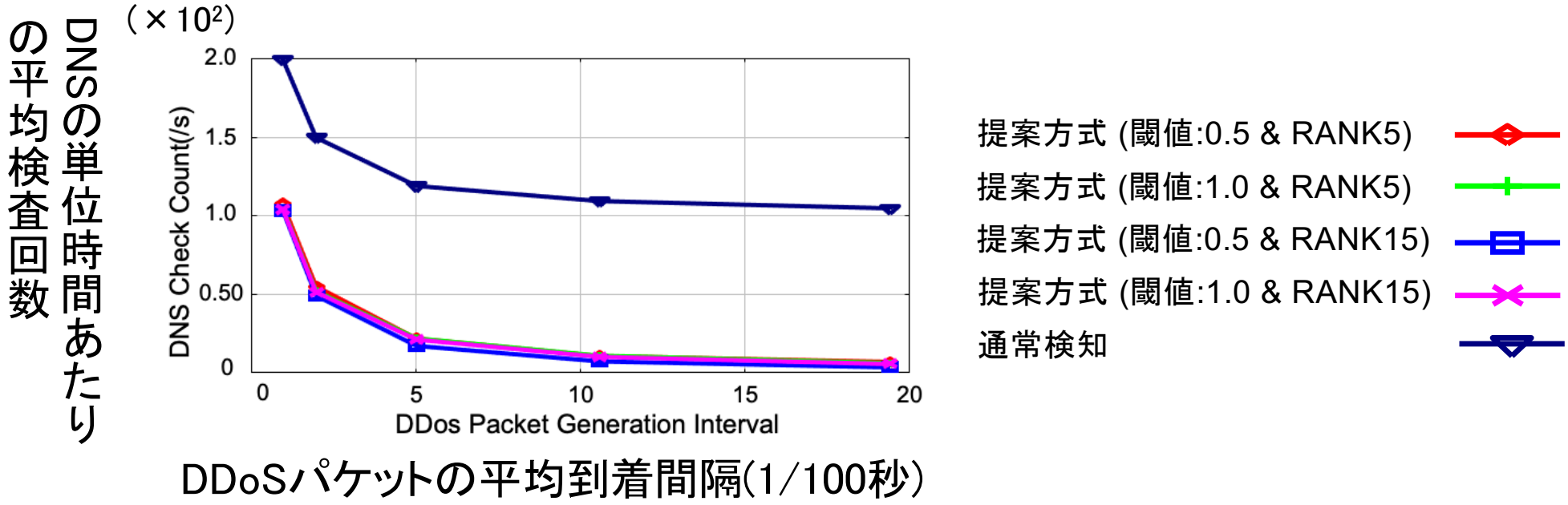


DDoSパケットの平均到着間隔(1/100秒)　　DDoSパケットの平均到着間隔(1/100秒)

シミュレーション結果 (2)

- 提案方式を利用
  - 平均検査回数　減少

⇒提案方式によりオリジンサーバの負荷を大幅に軽減



DDoSパケットの平均到着間隔(1/100秒)

まとめ

- Zスコア法を用いた危険性のある要求を到着間隔から検知する方式を提案

⇒DNSの負荷から提案方式の有効性を示した

- 攻撃者がCDNのIPアドレスを発アドレスとして偽った場合を想定
- 正常なコンテンツ要求とDDoS攻撃の要求発生パターンの違いを検知に利用
  - 攻撃発生時にZスコア法の平均・標準偏差を更新しない

  ⇒正常なコンテンツのみが発生している場合のデータを学習

  ⇒攻撃が発生した際の到着間隔パターンの変化を検知

- 今後の方針
  - 到着間隔のデータのより良い活用法を検討
  - ChangeFinderを用いた検知法を検討
    - 時系列データから外れ値や変化点を検知