クラウドサーバへの攻撃から守るセキュリティ手法

前田　香織 †　　高野　知佐 †

† 広島市立大学大学院　情報科学研究科

概要

日常生活にクラウドサービスが浸透するとともに、クラウド上のサーバへの攻撃は増加し、巧妙になってきている。
本研究ではクラウドサーバの安定的な運用を支援するための２つのセキュリティ技術の提案と実装について紹介する。
1つは**移動透過通信を用いてサーバの攻撃コストを大きくするためのMoving Target Defense**で、もう1つは**拡散型フロー制御を用いて自律分散でDDoS攻撃を緩和する技術**である。

サーバの攻撃コストを大きくするための Moving Target Defense

背景と課題：
- サイバー攻撃の高度化・多重化による防御コストの増大
- クラウド（インターネット上）のサーバは静的にIPアドレスを持つことから、容易に特定され攻撃対象 (標的)となる

→ サイバー攻撃の標的となるリスクの低減が求められる

標的（サーバ）のネットワーク的位置を動的かつ予測困難な値に移動

Moving Target Decense（MTD）システム

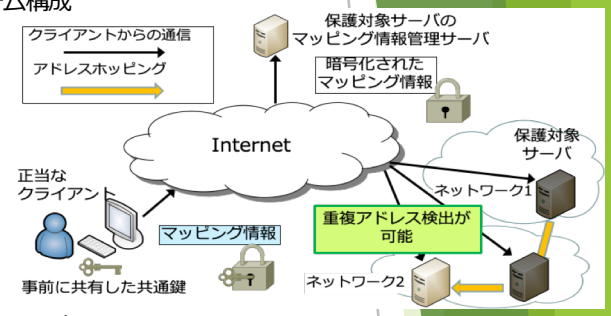
1.目的：攻撃者の攻撃コストを増大することにより、攻撃対象のリスクを低減しつつ、正規通信の通信品質を維持する

2. 設計方針
- サーバのIPアドレスを予測困難な値に動的に変更する（IPアドレスホッピング）
  → 攻撃対象の特定が困難となる＝攻撃コスト増大
- アクセスを許可したクライアントからのみサーバのIPアドレスを解決できる　→　正規通信の通信品質確保

緩和のキーアイデア

3. IPモビリティ技術 MAT によるMAT MTDシステムの実現
- IP モビリティ技術：通信相手がネットワークを移動（ハンドオーバ）によりIPアドレスが変更しても通信を継続できる技術
  - 移動ノードと通信相手ノードがアプリケーションでアドレス（ホームアドレス）と実際に通信で使うアドレス（モバイルアドレス）を分離し、ホームアドレスとモバイルアドレスの対応づけを通信過程に組み込む
- MAT (IP Mobility Architecture and Technology)　：独自開発
  - MAT対応ノード自身でホームアドレスとモバイルアドレスの変換機構をもつ
- MATをサーバのIPアドレスホッピングに使用

4. システム構成



5. システム評価
- システム利用により攻撃コストの増大を評価するために、ネットワークスキャンやワーム伝搬に対する耐性を評価
  ・対象アドレス空間に応じてネットワークスキャン成功確率を低減
  ・ワームの伝搬速度を大幅に低減
- IPアドレスホッピングによる通信品質への影響を調べるため、TCPやUDPストリームの伝送60秒間のスループットを評価
  ・ホッピング間隔5秒においてMAT MTD使用時はTCPは0.1%低下，UDPは1.4%低下
  ・パケットロス率は0%。既存研究(SWIFT) におけるTCPの39.8%低下を大きく改善

DDoS攻撃を緩和する技術の提案と実装

背景と課題：
- クラウドサービス増加により、インフラストラクチャレイヤーへのDDoS攻撃の頻度高、機規大
- DDos攻撃の検知から対策開始までは正規通信の被害対応が必要

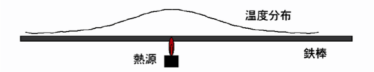
DDoS攻撃緩和システム

1. 目的：DDoS攻撃検知後の正規通信の被害低減
2. 設計方針：
- DDoS攻撃のトラヒックは攻撃対象に近づくにつれ合流するため、攻撃対象から離れたところで緩和開始。水際対策をする。
- 複数の攻撃元からのDDoS攻撃に対応
- 対策開始まで全パケットを損失しない

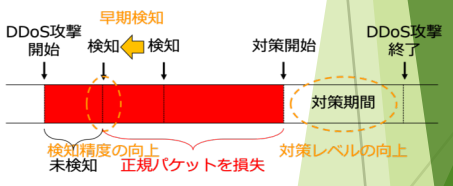
緩和のキーアイデア

3. 拡散型フロー制御の利用：
- 拡散現象のメカニズムをネットワークのトラヒック制御に適用

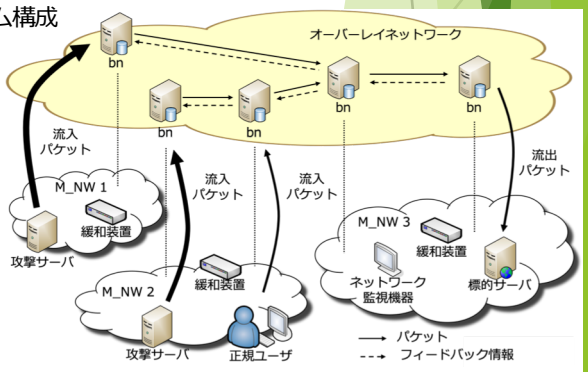
ex.拡散現象例： 冷やした鉄棒の一ヶ所を熱すると，温度分布は正規分布となり，拡散



- ノードの自律的な動作ルールを，うまく作りこむことにより，ネットワーク全体を間接的に制御
- ボトルネックリンク手前のルータが転送レートとバッファ量をフィードバック情報として上流ノードに通知
- 上流ノードはその情報を基に転送レートを決定するため、各ノードにバッファが拡散
- 利点
  ① パケットロスが起きない
  ② スループットが激減しない
  ③ 自律分散で制御可能



4. システム構成



5. システム評価

評価方法：
- シミュレーション実験により、提案システムが緩和対策まで、どの程度パケット損失を防ぐことが可能かをトラヒック制御パケット損失発生時刻により評価

結果と考察
- 伝搬遅延時間が大きいほどパケット損失発生時刻が早い
- ネットワークトポロジによりパケット損失発生時刻に差がある
- 途中ノードのバッファ容量が大きいほどバッファを効率的に使用可能