Measurement, Analysis and Control to Changes of Network Traffic

大下　裕一
大阪大学　大学院経済学研究科
y-ohsita@econ.osaka-u.ac.jp

背景

- ネットワークは、想定したトラヒックを効率よく転送できるように設計される
  - 輻輳、大きな遅延等を生じないように
- 想定外のトラヒックが流入した場合は、ネットワークの性能が劣化してしまう
  - 輻輳の発生
  - 遅延の増大
  - パケットロス

想定外のトラヒックが発生する原因

- 攻撃トラヒックの流入
  - 攻撃トラヒックを遮断することが望ましい
- 通常のトラヒックの増加
  - 現在のトラヒックに適するようにネットワークの設定を変更することによって対応する必要がある

ネットワークの性能劣化を防ぐには
- トラヒック変化の原因を切り分け、適切な制御が必要

研究の目的

- 想定外のトラヒックが発生した場合に
  - 想定外のトラヒックが発生した原因を切り分け、
  - ネットワークの品質低下を防ぐ制御を行う手法の確立
- 論文の構成

Chapter 1　Introduction
Chapter 2　Detection, Identification and Defense against Denial-of-Service Attacks
Chapter 3　Measurement, Estimation and Control to Changes of Traffic
Chapter 4　Conclusion

Chapter 2
Detection, Identification and Defense against Denial-of-Service Attacks

攻撃対策手法

攻撃への対策

- 攻撃トラヒックから正常なトラヒックを保護する手法
  - 早急な**攻撃検出・攻撃元特定**
  - 攻撃パケットの**遮断**と正常なパケットの**保護**
- Chapter 2の構成

Section 3　Detection of Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically
- 被害者側での攻撃の検出手法

Section 4　Identification of Attack Nodes from Traffic Matrix Estimation
- 攻撃者が接続しているルータの特定手法

Section 5　Overlay Network Against Distributed SYN Flood Attacks
- 攻撃パケットを遮断し、正常なパケットを保護する手法

Section 3
Detection of Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically

攻撃の検出

攻撃検出の問題点

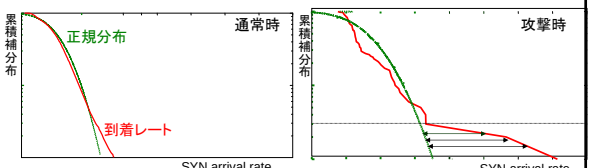
- 通常の通信と**同種類のパケット**が攻撃に用いられる
  - 通常トラヒックの負荷が高いときとの区別が難しい
- 従来手法では、検出に時間がかかる

⇩

- より迅速、正確な攻撃検出手法が必要

提案する攻撃検出手法の概要

- 観測した到着レートと**正規分布**と比較
  →差が閾値を超えると、攻撃の検出を行う
  - 正常パケットの到着レートは時間帯によらず正規分布に近い分布
  - 攻撃が開始されると到着レート分布のテイルが長くなり、**正規分布から逸脱**

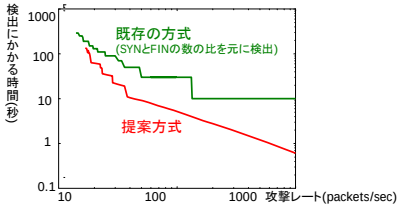


攻撃検出性能の評価

- 提案方式はより早く検出可能
  - 30 packets/secの攻撃ならば10秒で検出可能
  - 攻撃トラヒックが流入し、到着レートがモデルから外れた時点で、攻撃検出を行うことが可能であるため

評価環境

大阪大学のGWで観測されたトラヒックに擬似的に攻撃トラヒックを混入



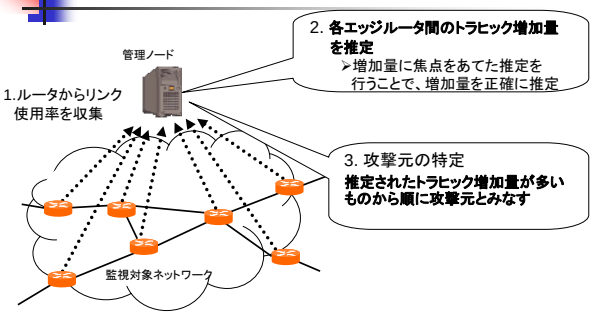
Section 4
Identification of Attack Nodes from Traffic Matrix Estimation

攻撃元の特定

攻撃元特定の問題点と提案手法

- 問題点
  - 攻撃パケットの送信元が偽装されているため、攻撃元の特定が難しい
  - 従来手法では、ルータの置き換えが必要
- 提案手法
  - ルータで観測しているリンク使用率を元に、被害者宛のトラヒックを増加させている攻撃元を特定
    - トラヒック増加量を元にしているため、パケットの送信元の偽装の影響を受けない
    - リンク使用率を用いているので、既存のルータに適用可

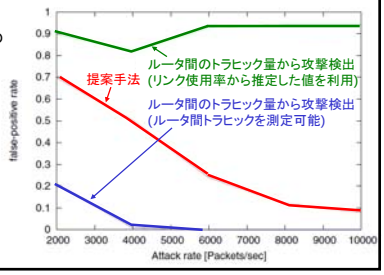
攻撃元特定の手順



評価結果

- 提案手法は、リンク使用率のみを用いても、正確に攻撃元を検出可能
  - 推定時から増加量に焦点をあてているため

比較環境
トポロジ:
Abileneのバックボーン
(11ノード、14リンク)
攻撃元数:5
各手法のパラメータ:
未検出率が0.1以下となるように設定



Section 5
Overlay Network against Distributed SYN Flood Attacks

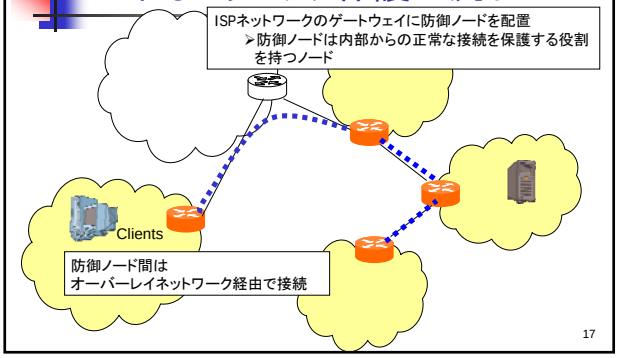
正常なトラヒックの保護

既存の防御手法の問題点と提案手法

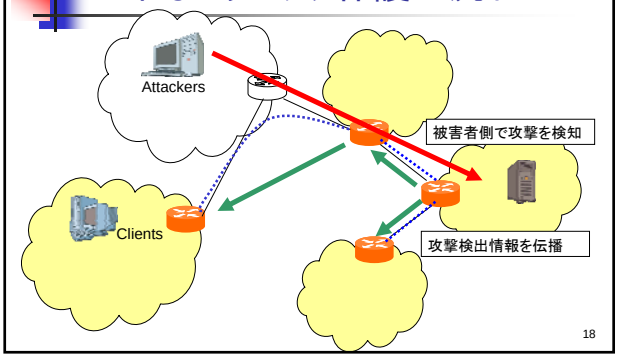
- 攻撃パケットの遮断が主目的
  - 正常なパケットの保護が考えられていない
    - 正常なパケットもサーバに到達できない可能性もある
- 透過的な動作をしない
  - 正常なトラヒックであると確認する際に、クライアント側に認証用ソフトウェアの導入が必要

- 正常なトラヒックの保護を主眼に置いた手法の提案
  - クライアントの置き換えの必要なく動作可能な手法

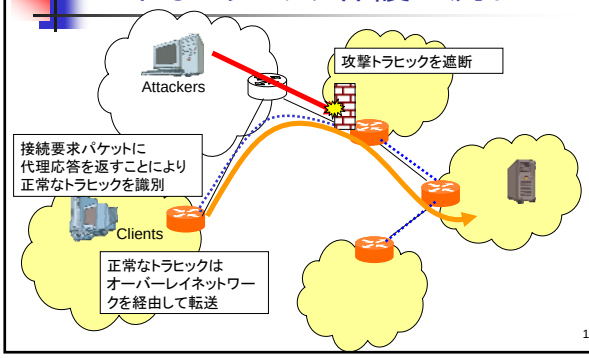
正常なトラヒック保護の流れ



正常なトラヒック保護の流れ



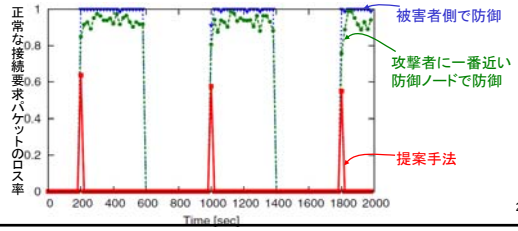
正常なトラヒック保護の流れ



評価結果

評価環境
・攻撃レート: 6,000,000 packets/sec
・クライアント・サーバ間のパケットは、防御ノードを配置していないISPネットワークを経由

- 被害者側・攻撃者側の手法はいずれもパケットロス率が高い
  - 正常なパケットと攻撃パケットが途中の経路で混ざってしまうため
- 提案手法では、パケットロス率を著しく低下させることが可能
  - 攻撃パケットと混入せず、区別して転送できるため

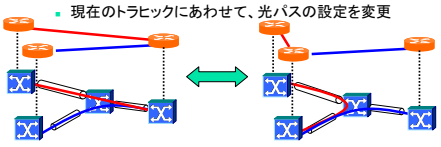


Chapter 3
Measurement, Estimation and Control to Changes of Traffic

正常なトラヒックの変動への対応

正常なトラヒックの変化への対応

- 現在のトラヒックに合致するようにネットワークの構成を変更する
  - Optical layer Traffic Engineering (TE)
    - 想定している環境:
      - 物理ネットワーク上に光パスを構築
      - 光パスで構成されるネットワークがIPネットワークに論理トポロジを提供
    - 動作:
      - 論理トポロジの再構成
        - 現在のトラヒックにあわせて、光パスの設定を変更



Optical layer TEの入力

- 各エッジノード間のトラヒック量
  （トラヒックマトリクス）
  - **直接観測することは困難**
  - 推定手法が提案されているものの、**推定誤差がOptical layer TEに影響を与える**

⇩

- 推定したトラヒックマトリクスで適切にTEを行う必要がある

提案する手法

- トラヒックマトリクスの推定精度を向上させながら、適切なネットワーク構成へ移行する手法の提案

- Chapter 3の構成
  - Section 6 Gradual Reconfiguration of Virtual Network Topology
    - ネットワークを短い間隔で徐々に変更を行いつつ、トラヒックマトリクス推定にフィードバックを行う手法
  - Section 7 Estimation of Current Traffic Matrices from Long-term Traffic Variations
    - トラヒック変動を考慮したトラヒックマトリクス推定をおこなう手法

Section 6
Gradual Reconfiguration of Virtual Network Topology

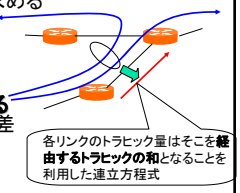
論理トポロジの段階的再構成

トラヒックマトリクスの推定誤差

- 一般的なトラヒックマトリクス推定手法：
  - 各リンクのトラヒック量を元に以下の連立方程式をたて、その条件にあうトラヒックマトリクスを求める

$$X = AT$$

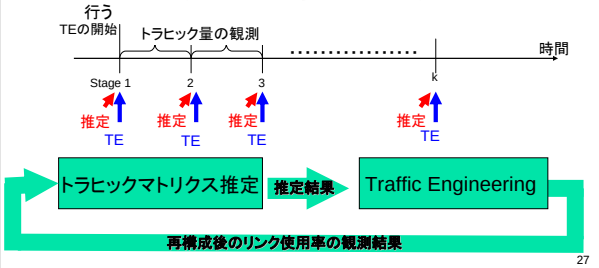
    - X:各リンクのトラヒック量
    - A:ルーティングを表す行列
    - T:トラヒックマトリクス
  - **トラヒックマトリクス推定に用いている連立方程式の数が少ない**ために誤差が生じる



- 提案手法：
  - TEの前後の観測結果を推定に用いる方程式に追加することにより、**推定に用いる条件を増やす**

段階的再構成の概要

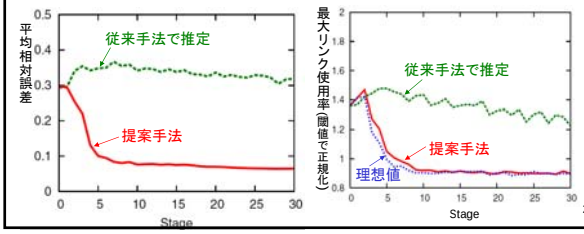
- TEを数分程度のステージに分けて段階的に行う
  - 各ステージで**観測されたリンク使用率を連立方程式に追加**しながらTEを行う



評価結果

評価環境
物理トポロジ：EON
(19ノード・37リンク)
TEの目標： 最大リンク使用率を
閾値以下にする
トラヒック： ランダムに生成

- 提案手法では、ステージが経過するにつれ、推定誤差を削減可能
  - 各ステージでの観測結果を推定に用いる情報として追加するため
- 最大リンク使用率も目標値まで削減可能



Section 6
Estimation of Current Traffic Matrices from Long-term Traffic Variations

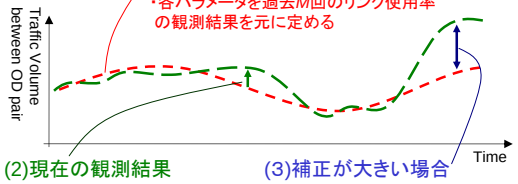
トラヒック変動を考慮した推定手法

段階的再構成中にトラヒックが変動した場合

- 過去のステージの観測結果を推定に用いることができない
  - 過去のステージの観測結果が現在のトラヒックと合致していないため
- 対処方法
  - トラヒック変動を考慮にいれた推定方法

トラヒック変動を考慮にいれた推定手順

(1)長期変動の推定
- **周期変動をモデル化**
- 各パラメータを過去*M*回のリンク使用率の観測結果を元に定める



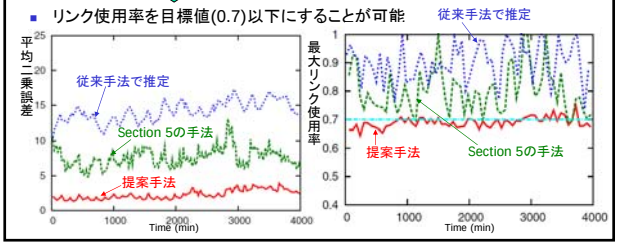
(2)現在の観測結果にあわせて**補正**

(3)補正が大きい場合
- **長期変動の変化を検出**
- 補正の大きいトラヒックに関する**過去の情報を除外して再推定**

評価結果

評価環境
物理トポロジ：EON (19ノード・37リンク)
TEの間隔：**1時間に一回**
TEの目標：最大リンク使用率を0.7以下
トラヒック：位相・振幅がランダムで与えた周期変動にランダムな短期変動を加えて生成

- 提案手法は精度よく推定できている
  - トラヒックの時間変動を考慮に入れつつ、多くの観測結果を用いることができるため
- リンク使用率を目標値(0.7)以下にすることが可能



まとめ

- トラヒックの観測を元にトラヒック変動に対応する手法を提案
  - 攻撃に対する手法 (*Chapter2*)
    - 観測結果と統計モデルを比較することによる攻撃検出
      - 20 packets/sec以下の攻撃であっても瞬時に検出
    - リンク使用率の観測結果から攻撃元を特定する手法
      - リンク使用率のみを用いても正確に攻撃元を特定可能
    - 攻撃検出後に、正常なトラヒックを保護して転送する手法
      - 正常なトラヒックのロス率を0.1以下に抑えることが可能
  - 正常なトラヒックの変動に対する手法 (*Chapter 3*)
    - トラヒックマトリクスの推定精度を向上させつつ、精度が向上したトラヒックマトリクスを用いてネットワークの再構成を行う手法
      - 相対誤差を0.1以下に抑えつつ、適切にネットワークの再構成を行うことが可能
- 今後の課題
  - 帯域を浪費させる攻撃等、異なる種類の攻撃への対処
  - 推定誤差を考慮したネットワークの再構成手法