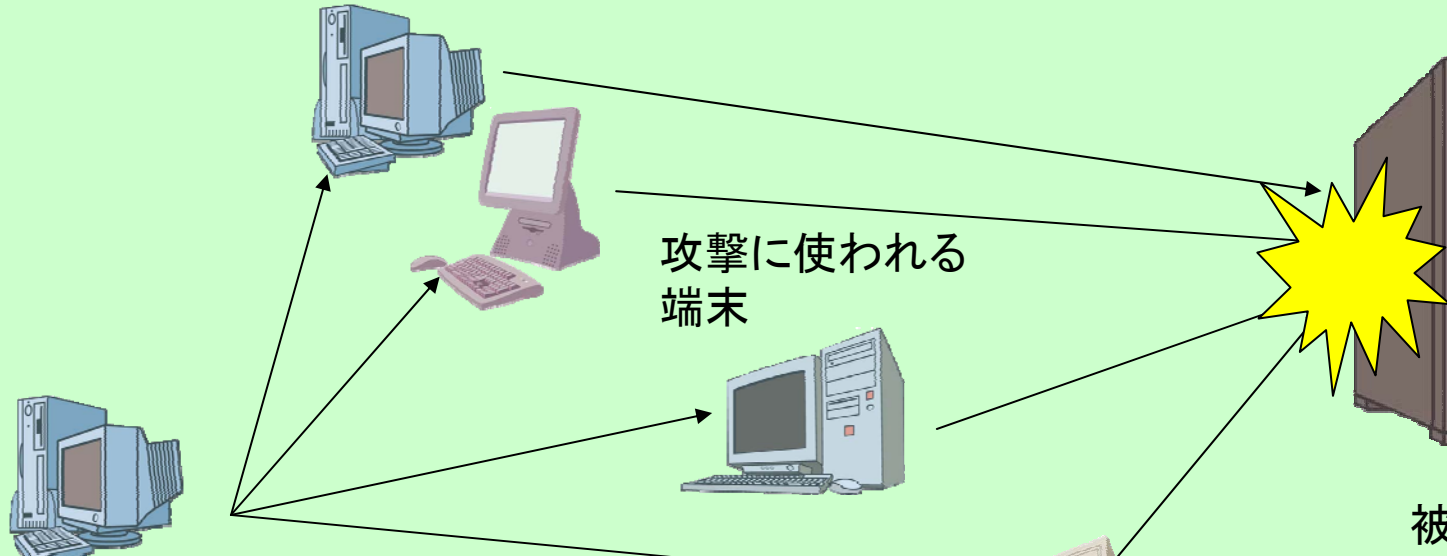
攻撃元特定手法

大下裕一(1)　阿多信吾(2)　村田正幸(1)
(1)大阪大学 大学院 情報科学研究科
(2)大阪市立大学 大学院　工学研究科

背景～DDoS 攻撃とは～

–攻撃者は複数の端末に攻撃プログラムを仕掛け大量のパケットを攻撃対象に送信し、対象の通信を阻害する

–**攻撃元を特定し、攻撃元で攻撃を遮断することが有効**



- ルータがパケット転送時に自信の識別情報を宛先に送る
- ルータにおいて転送したパケットのハッシュ値を保存
- 問題点
  - ルータの置き換えが必要
  - 攻撃元と通常のパケットの送信元が分からない

研究目標

送信元・宛先間のトラヒック増加量を推定することによる攻撃元特定手法の構築

- **既存のルータで実現可能**
  - SNMP で収集可能なリンクのトラヒック量から送信元・宛先のトラヒック増加量を推定
- **攻撃元・通常のクライアントの区別可能**
  - 増加量をもとに特定するため、トラヒックを急増させない通常のクライアントを誤検出しない

概要

トラヒック情報の収集

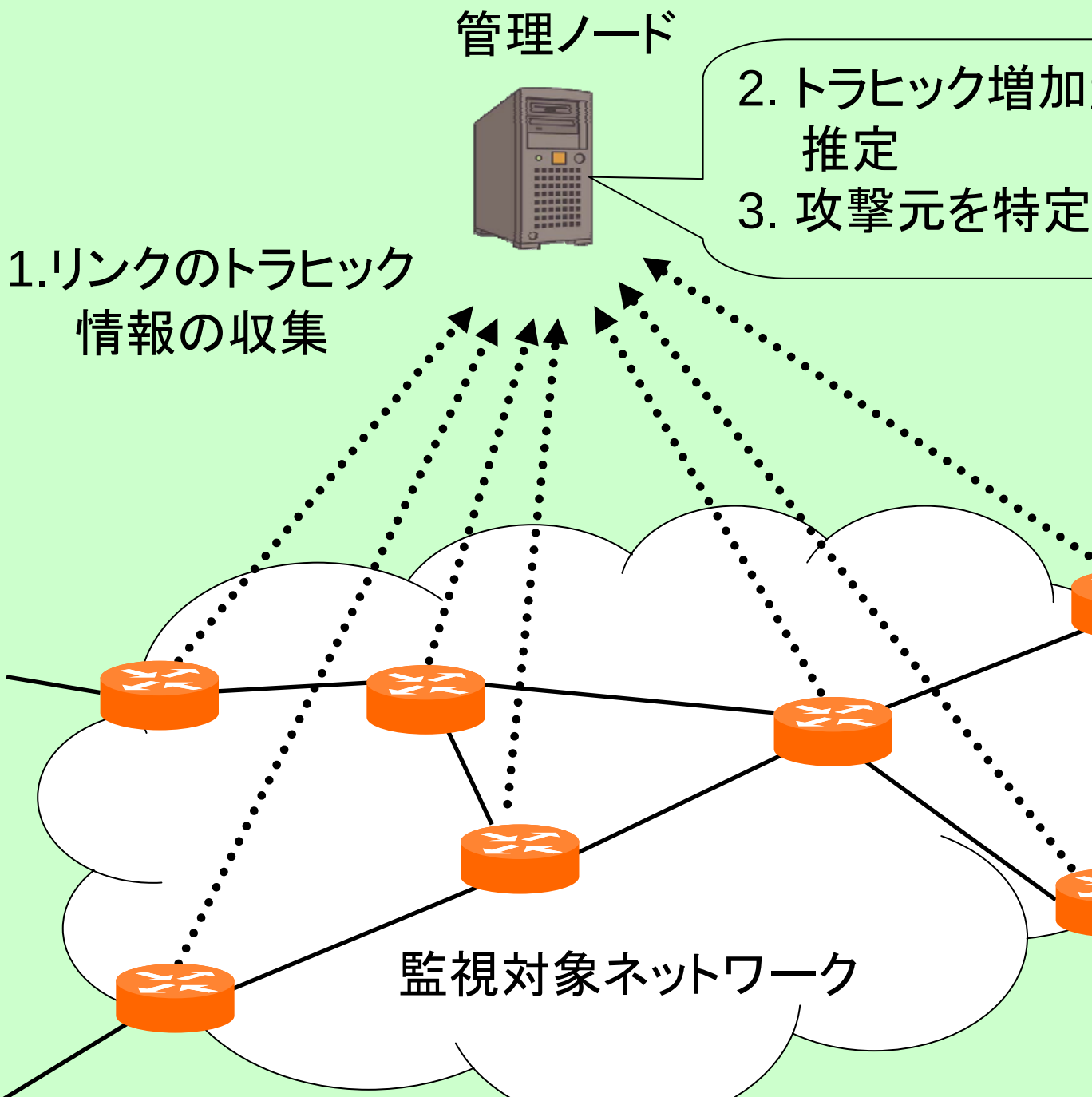
- SNMP 等を用いて観測対象ネットワークのルータから収集

増加量の推定

- 既存のトラヒックマトリクス推定を元にした提案手法を用いて推定

攻撃元の特定

- 推定されたトラヒック増加量をもとに攻撃元を特定



(Gravity modelを用いた手法)

- i から j へのトラヒック量は i を通るトラヒック量、j を通る
  ラヒック量に比例するとして推定
- 問題点
  - 攻撃によるトラヒックの増加が、正常なトラヒックの分布
    従って分配されてしまう

提案する推定手法

- 各リンクのトラヒックの増加量をもとに推定
  - 正常なトラヒックの影響を除外可能
  - トラヒックが急増した送信元からのトラヒックほど増加量
    が大きいと判断可能

ラヒック増加量推定の手順

各リンクごとに現在のトラヒック量の、正常なトラヒック量の平均との差を求める

$$G_n = X_n - \overline{X_n}$$

- X_n はすべてのリンクの時刻 n でのトラヒック量をあらわす行列
- $\overline{X_n}$ は各リンクの時刻n以前の正常なトラヒック量の平均を表す行
- G_n は現在のトラヒック量と正常なトラヒック量の平均の差を表す

各リンクの正常なトラヒック量との差を入力とし、Gravity model を用いて推定を行う

途中の経路のトラヒック量の情報を反映させる

推定結果をもとに $\overline{X_{n+1}}$ を定める

経路のリンクの反映とヒラ

リンクの観測結果とトラヒック増加量の関係

各リンクのトラヒック量はそこを経由するトラヒックの和となる

$$G = AF$$

- F は送信元・宛先間のトラヒック増加量を要素とするベクトル
- G はリンクで観測されたトラヒック増加量を要素とするベクトル
- A は要素 $a_{(i,j),k}$ が i から j へのトラヒックがリンク k を経由する場合は1
  それ以外は0

反映方法

$G = AF$ がなりたつようにGravity modelの結果を補正

- 以下の計算を行い F を最終的な推定結果とする

$$F = F' + A^{-1}(G - AF')$$

  - F' はGravity Modelでの推定結果
  - A^{-1} はルーティング行列 A の擬似逆関数

正常なトラヒック量の定め方

正常なトラヒック量の定め方に必要な条件

- トラヒックの急増の影響を受けない
- リンク間で整合性のある値に定める

正常なトラヒック量を定める手順

- 推定されたトラヒック量から、急増していない箇所のみを抜き出す
  - 急増していない箇所を抜き出した行列 $\hat{F}_n$ の要素を次のように定義
    - トラヒックが急増したフローに対する要素は0
    - それ以外の要素は F_n と等しい
- すべてのリンクに反映

$$\overline{X}_{n+1} = \alpha(\overline{X}_n + A\hat{F}_n) + (1-\alpha)\overline{X}_{n+1} \quad (0 < \alpha < 1)$$

撃元である条件

- 被害者宛のトラヒックのうちトラヒックを急増させているもの
- すべての攻撃元からの攻撃レートを足し合わせると被害者側での攻撃レー
  なる

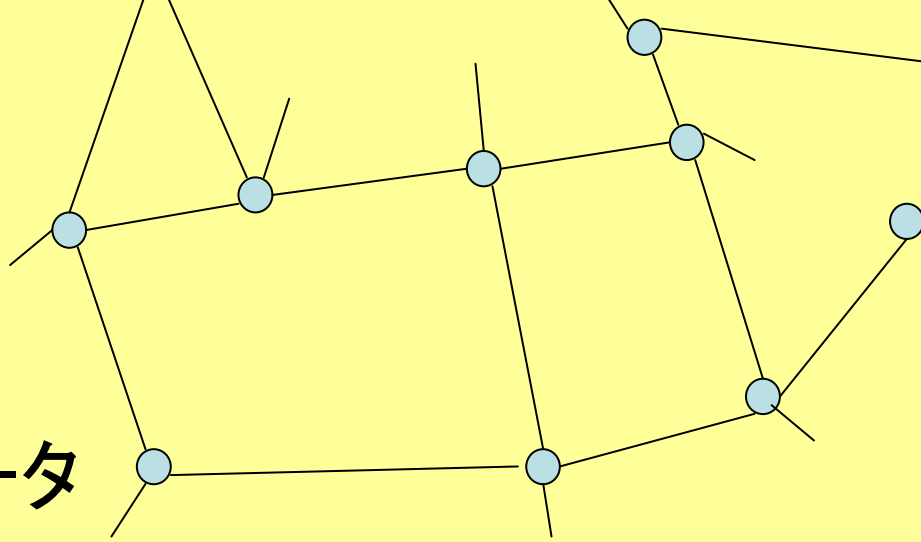
定方法

- **被害者側のトラヒック増加量から検出する攻撃の合計の
  レート $\tilde{g}^{\text{out}}$ を定める**

$$\tilde{g}^{\text{out}} = g^{\text{out}} - \mu^{\text{out}} - \gamma$$

  - g^{out} は被害者側でのトラヒック増加量
  - μ^{out} は被害者側のトラヒック増加量の最近J個の平均
  - γ　は正常なトラヒックの変動を吸収するためのパラメータ
- **推定されたトラヒック増加量が多いものから順に攻撃元と
  なす**

– トポロジ
  - Abileneのバックボーントポロジ
– トラヒックデータ
  - 大阪大学のゲートウェイでの観測されたデータをもとにしたデータ



評価指標

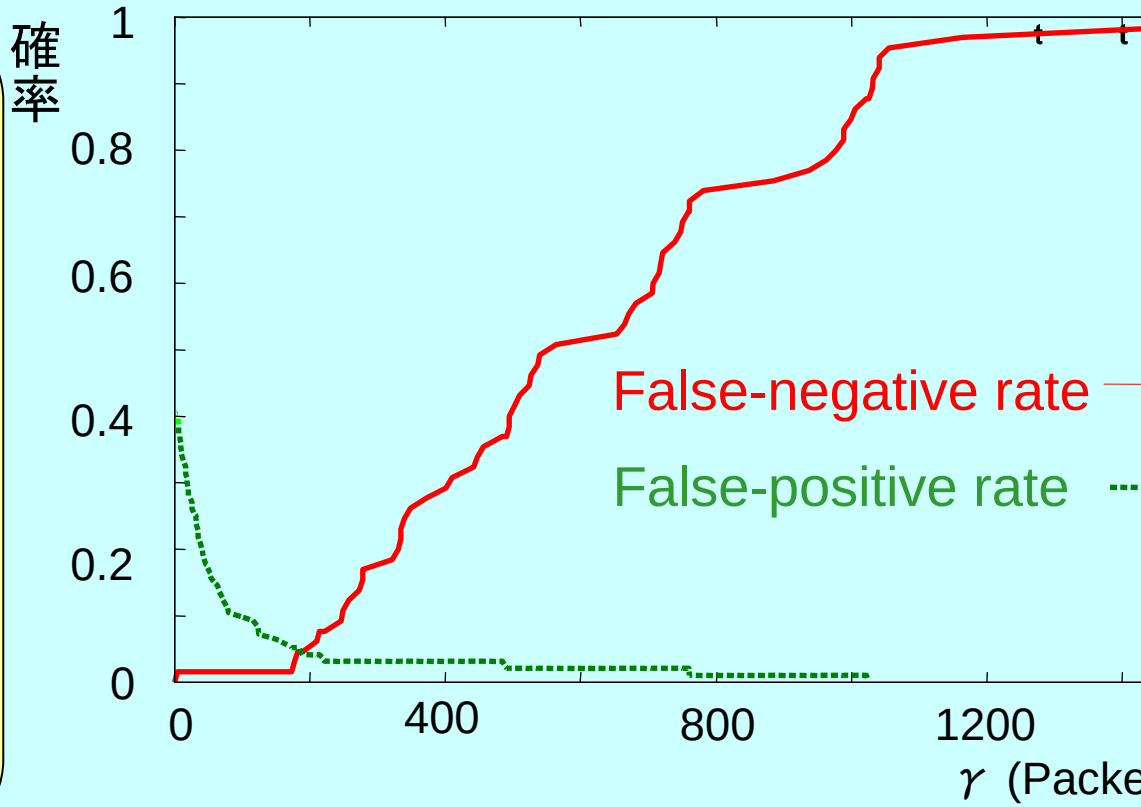
– False-positive
  - 攻撃元ではないのに攻撃元であるとみなされた箇所
– False-negative
  - 攻撃元であるのに検出されなかった箇所
– False-positive rate $\frac{\text{false - positve の数}}{\text{攻撃以外の送信元の　数}}$
– False-negative rate $\frac{\text{false - negative の数}}{}$

攻撃元の数にかかわらず攻撃元を特定可能

γを大きな値に設定するとfalse-negativeが増え、小さな値に設定するとfalse-positive が増える

γと未検出の攻撃元には密接な関係があり、影響がない攻撃レートを決めることによりγを定めることが可能

(攻撃レートの合計 1000Packets/sec、攻撃元の数



元の数と検出結果

ートの合計 1000Packets/sec、γ=200 Packets/sec)

元	False-positiveの数 (false-positive rate)	False-negativeの数 (false-negative rate)
	0 (0.00)	2 (0.01)
	0 (0.00)	0 (0.00)
	0 (0.00)	3 (0.02)
	3 (0.04)	4 (0.04)
	12 (0.15)	4 (0.05)

γと未検出の攻撃元からの攻撃レー