Detection and Defense Method against Distributed SYN Flood Attacks

大阪大学　大学院情報科学研究科
博士前期課程　村田研究室
大下 裕一
E-mail: y-ohsita@ist.osaka-u.ac.jp

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する
- 近年攻撃の大規模化が問題となっている
- 攻撃のほとんどが SYN flood 攻撃
  - 大量の接続要求を送ることによりサーバの資源を浪費する攻撃

SYN flood 攻撃対策の問題点

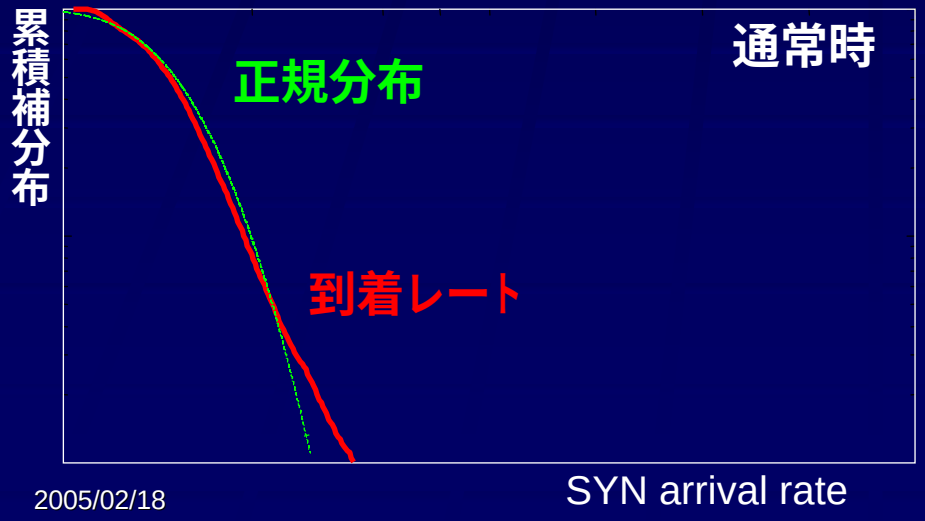
- 検出が難しい
  - SYN flood 攻撃に用いられるパケットは通常の接続要求との違いがない
    - 通常トラヒックの負荷が高いときとの区別が難しい
  - 既存の方式はトラヒックの時間的性質を考慮していない
    - 検出に時間がかかる
- 対策にスケーラビリティが必要
  - 分散した多数の攻撃者からのパケットを一箇所の防御機構で対応することは難しい
- 攻撃者の近くで攻撃検出・遮断を行うのは難しい

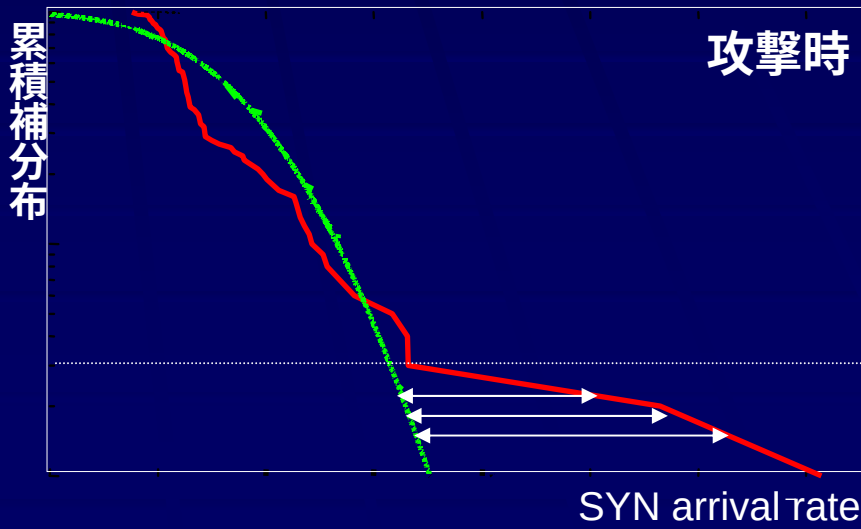
研究の目的

- 大規模な攻撃にも耐えることができる SYN flood 防御機構の開発
  - 攻撃の検出
    - トラヒックの時間による変化を考慮した検出手法
  - スケーラビリティの確保
    - 分散箇所で防御
      - 検出は被害者側で、防御は攻撃者側

攻撃検出手法

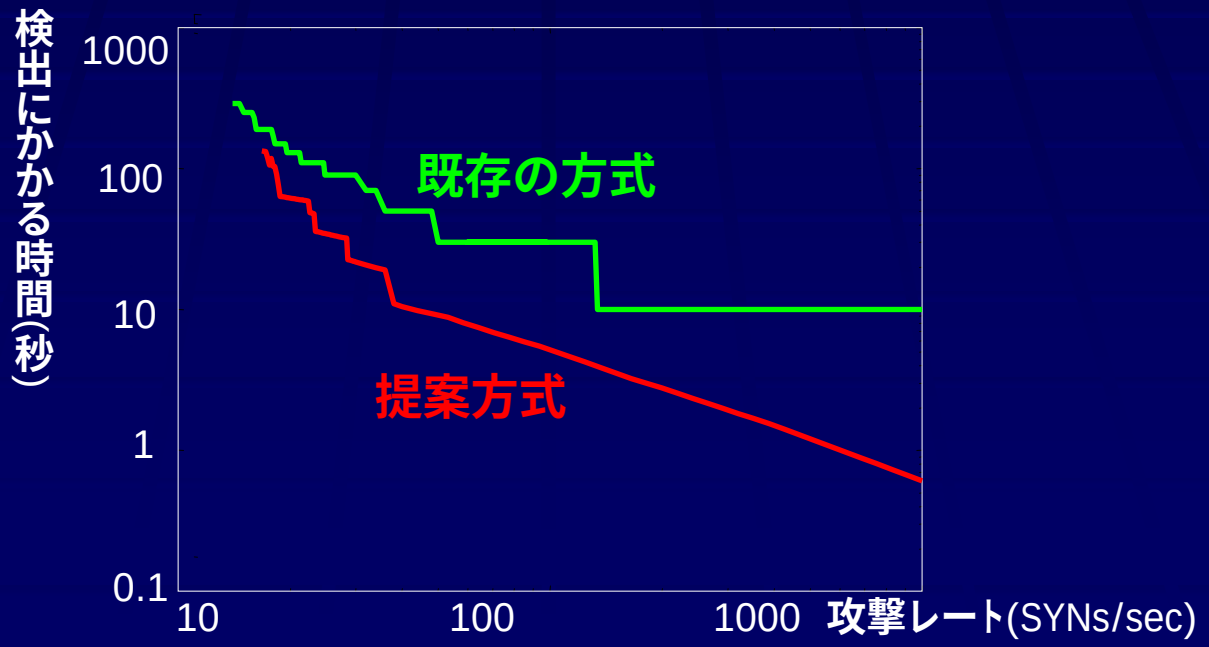
- 観測した到着レートと統計モデルを比較
  - 大阪大学のゲートウェイで SYN パケットを観測、統計情報を取得･解析
    - 正常パケットの到着レートは時間帯によらず正規分布でモデル化
    - 攻撃が開始されると到着レート分布のテイルが長くなる



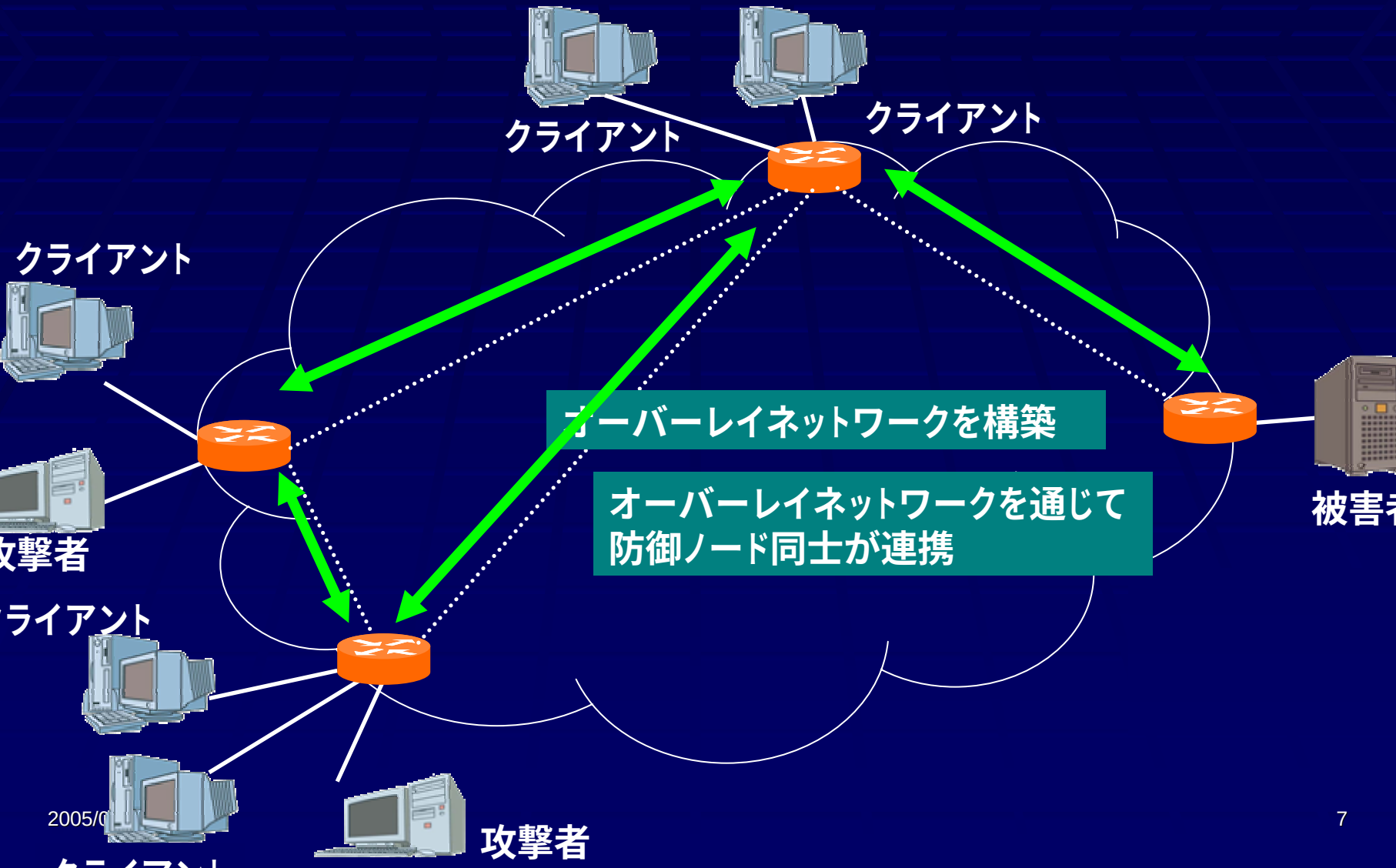


攻撃検出性能の評価

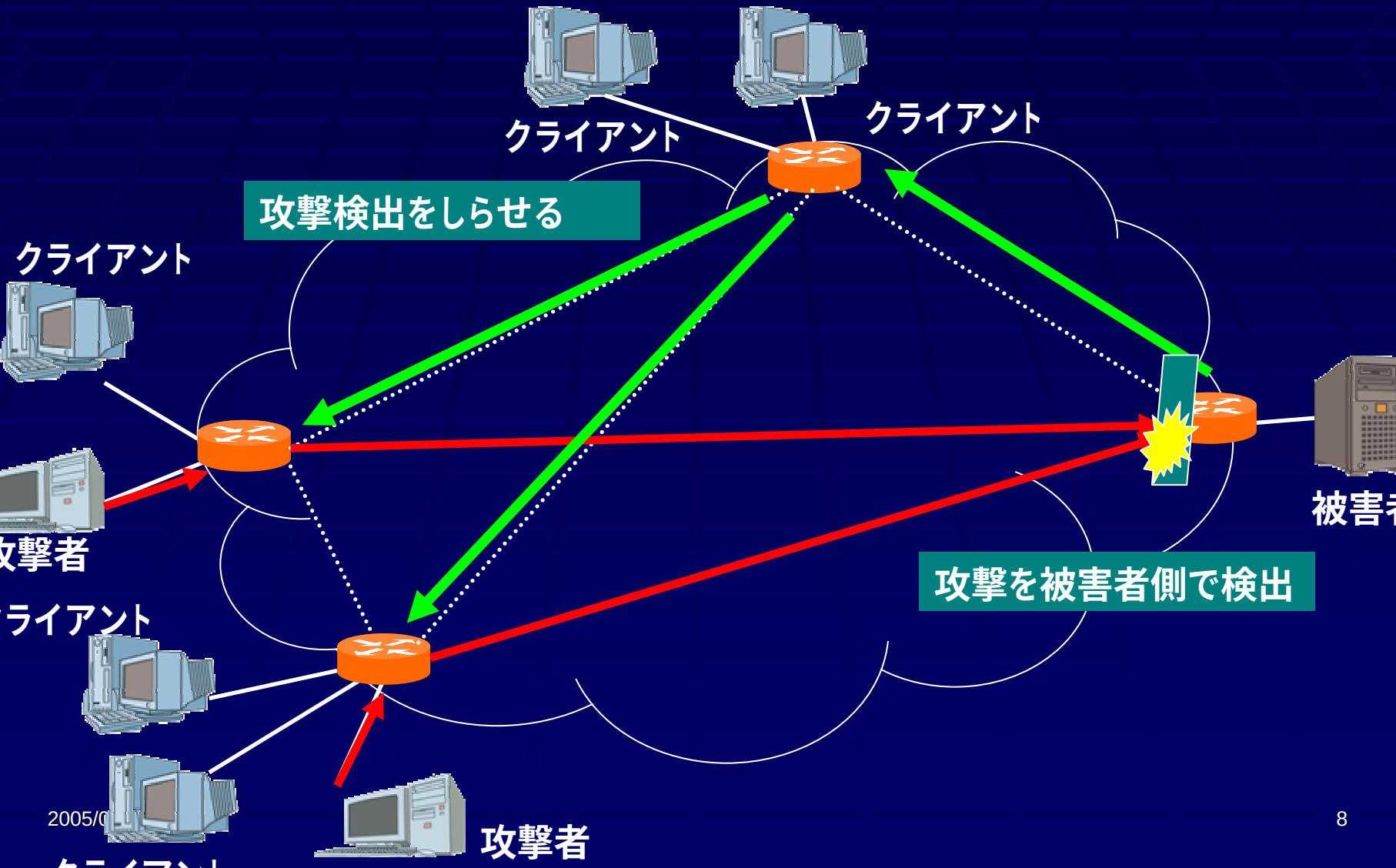
- 大阪大学で観測したトラヒックに擬似的な攻撃トラヒックを混ぜ、検出性能を評価
- 提案方式はより早く検出可能
  - 到着レートの時間変化を考慮に入れているため



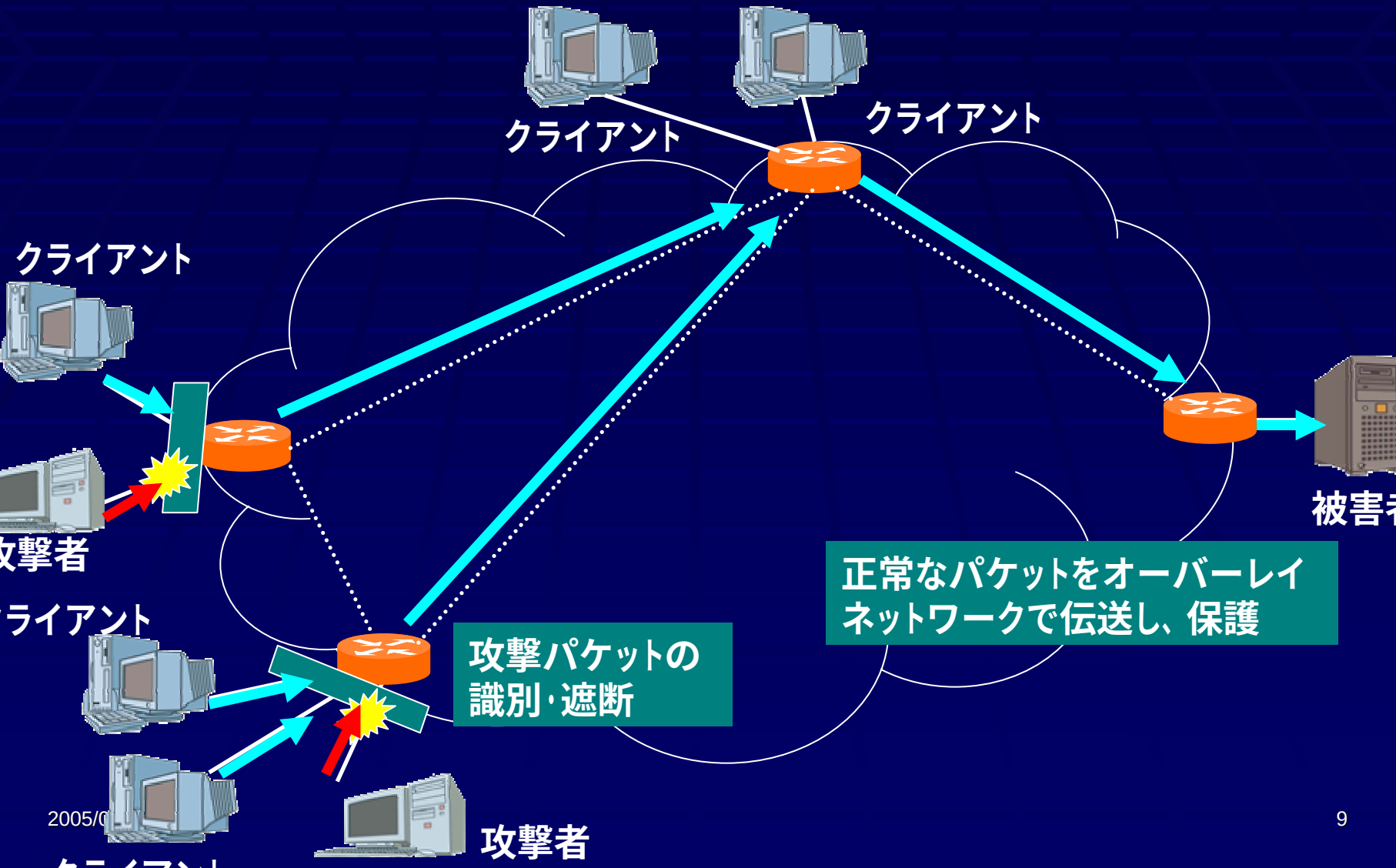
分散防御


クライアント
クライアント
クライアント
オーバーレイネットワークを構築
オーバーレイネットワークを通じて
防御ノード同士が連携
攻撃者
攻撃者

分散防御

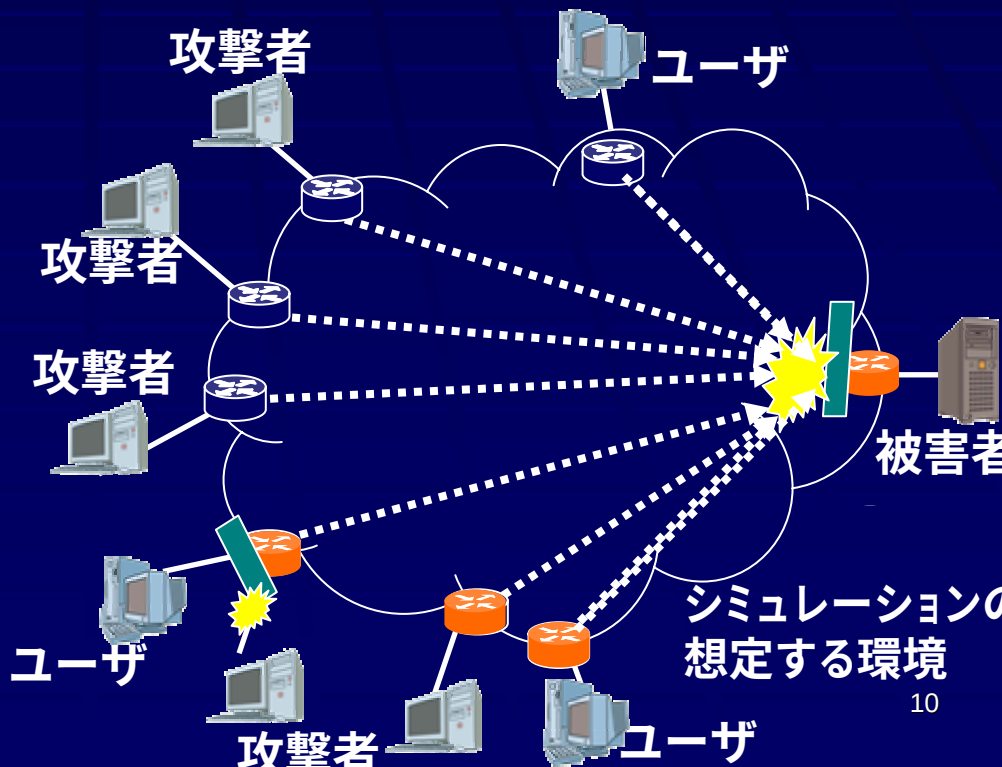

クライアント
クライアント
攻撃検出をしらせる
クライアント
攻撃者
ライアント
攻撃を被害者側で検出
被害者
攻撃者

分散防御


クライアント
クライアント
クライアント
攻撃者
ライアント
攻撃パケットの
識別･遮断
正常なパケットをオーバーレイ
ネットワークで伝送し、保護
被害者
攻撃者

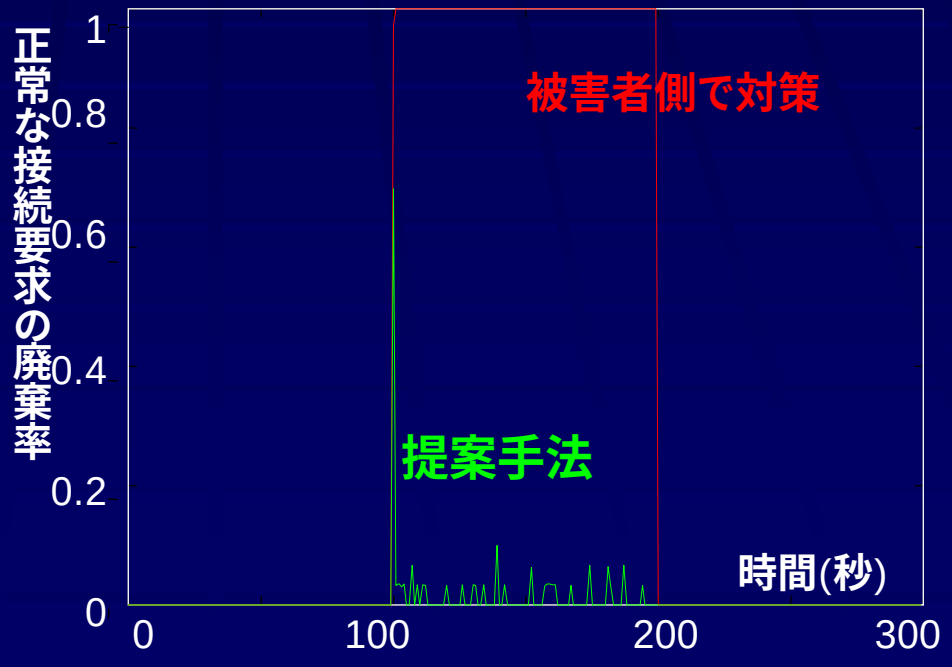
分散防御の評価

- シミュレーションによる評価
  - 各攻撃者は20万SYNs/secの攻撃パケットを送信
  - 被害者側で対策した場合との比較



正常パケットの廃棄率

- 被害者側での対策では、攻撃レートが高く、正常なパケットの保護ができない
- 提案方式では検出後、迅速に連携をとり、正常なパケットを保護



まとめ

- 分散 SYN flood 攻撃に対する対策を提案
  - 時間変動を考慮した攻撃検出手法
    - 大阪大学での観測結果をもとに SYN パケットの到着レートをモデル化
  - 分散防御手法
    - オーバーレイネットワークを用いて、分散箇所で連携
    - 被害者側で検出、攻撃者側で攻撃を遮断

今後の研究計画

- 帯域浪費型の DDoS 攻撃に対する対策
  - 効率的なトレースバック手法の提案
    - ネットワークに負荷をかけず、瞬時に攻撃者方向を絞り込む機構の提案
  - トレースバック手法を考慮した効率的フィルタリング手法の提案
    - トレースバックと連動し、攻撃パケットを遮断し、正常パケットを保護する機構
  - シミュレーション・実装評価