ネットワーク間の協調によるDRDoS攻撃対策手法

研究駆動コース　中田有哉

背景

- DRDoS攻撃の被害は甚大であり対策が希求されている
- 現状では踏み台となる**サーバの削減**による対策や**ISPのフィルタリング**により被害を軽減する手法が運用
- ボットネットによる攻撃リソースの増加から攻撃の規模は年々増加しており**単一のISPのみによる攻撃対処は困難**

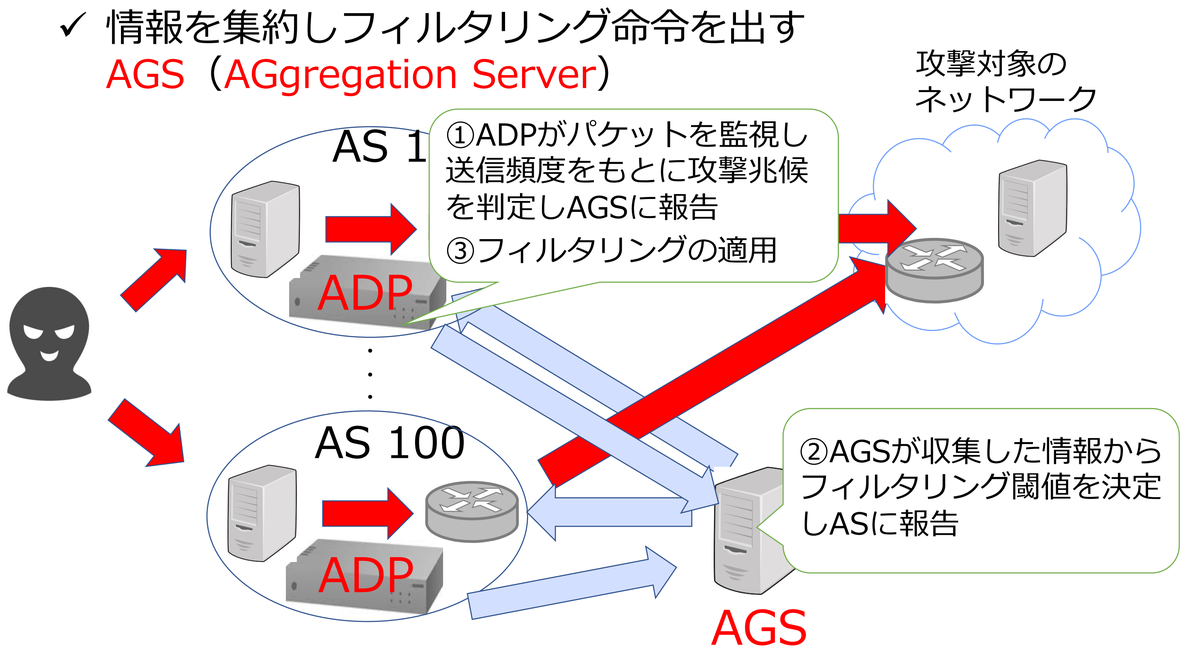
SecHack365での目標

- 攻撃の**分散対処**を可能とする手法の提案
- NICTが収集した**実際の攻撃トラフィック**を用いた提案手法の**評価**
- 学会発表や論文による**研究成果の発表**

提案手法

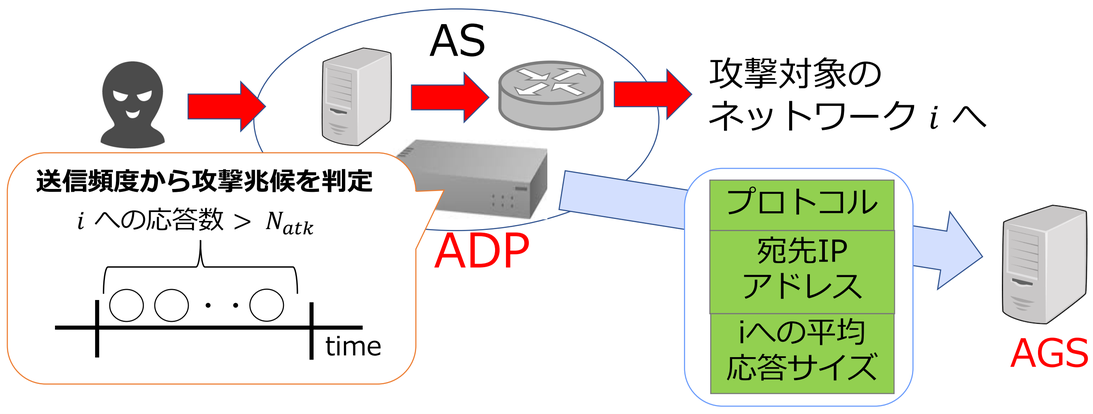
攻撃の分散対処を可能とするため複数のネットワークが**協調**し攻撃を検知、攻撃パケットをASで選択的に破棄する

- 新規に二つのサーバを設置
  - ✓ 攻撃の兆候を判定するADP（ Attack Detection Probe ）
  - ✓ 情報を集約しフィルタリング命令を出すAGS（AGgregation Server）



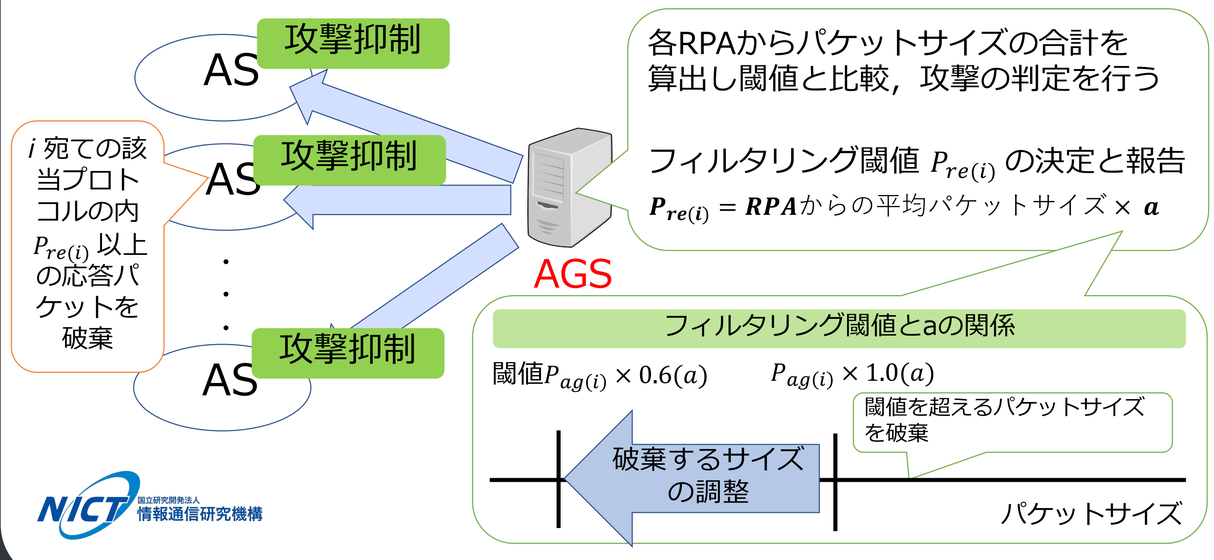
攻撃兆候の判定フェーズ

- ADPが応答パケットを監視し**送信頻度**から攻撃兆候を判定
- ADPがAGSに攻撃パケットの**平均サイズ等**を報告



攻撃抑制フェーズ

- AGSが収集した情報からフィルタリング閾値を決定しASではフィルタリングを実施



性能評価

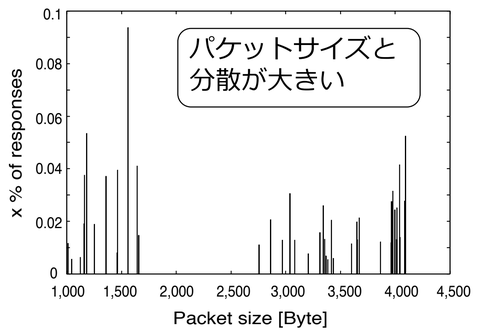
- 攻撃対象のネットワークにDRDoS攻撃が行われた際に提案手法を適用し**攻撃パケットの破棄率**と**通常ユーザのパケットの破棄率**から提案手法の有効性を評価

データセットの説明

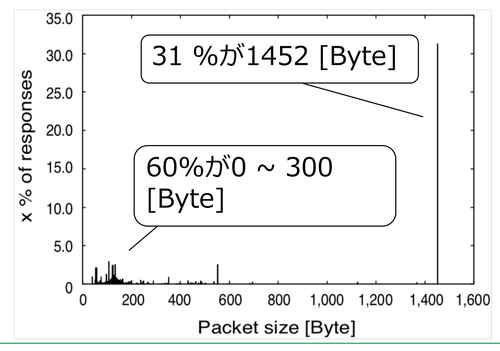
- 本評価では3つのデータセットを利用
- DNSを用いたDRDoS攻撃に限定

攻撃者

- Shumonのデータセット
  DNS ANY クエリの応答サイズの分布

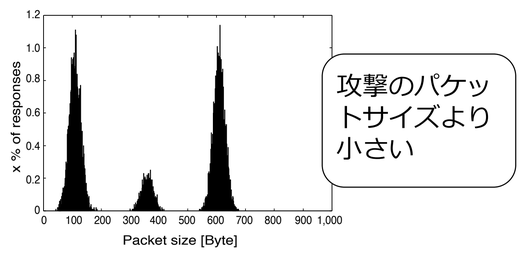


- Amppot が収集したデータセット
  実際の攻撃パケットデータ



正常ユーザ

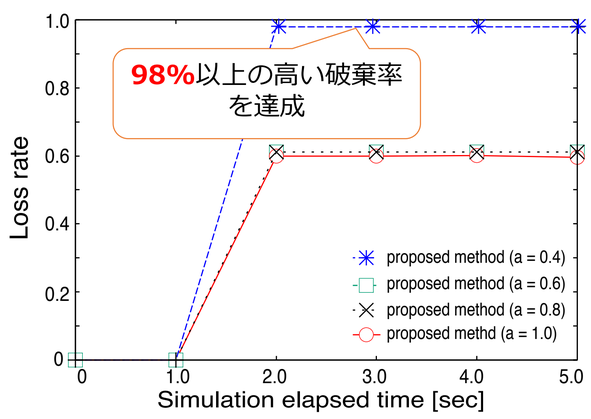
- JPDNSの資料をもとに作成したデータセット
  ユーザのクエリに対するDNS応答サイズの分布



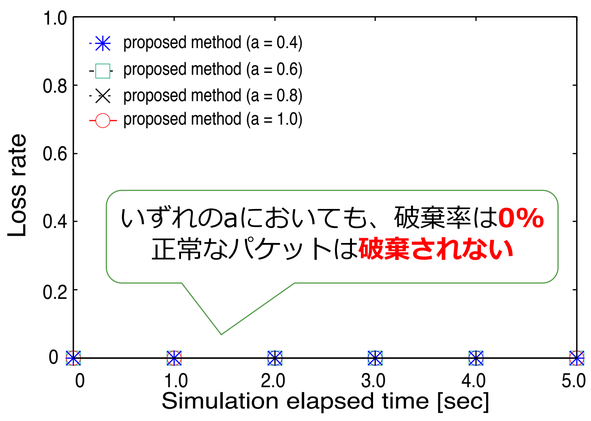
評価結果

- Shumonのデータセットを用いた評価

攻撃パケットの破棄率（**高い**ほど良い）

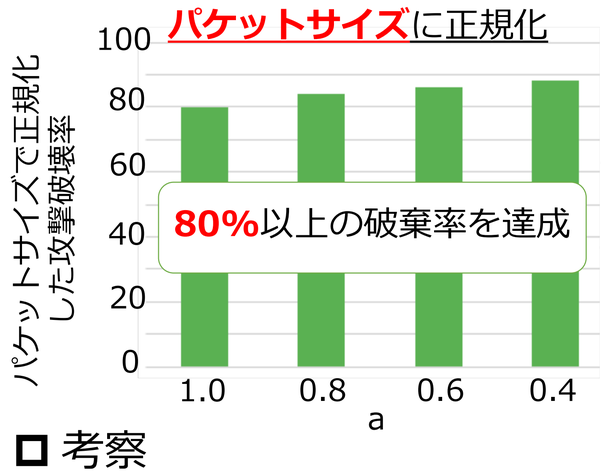


正常パケットの破棄率（**低い**ほど良い）

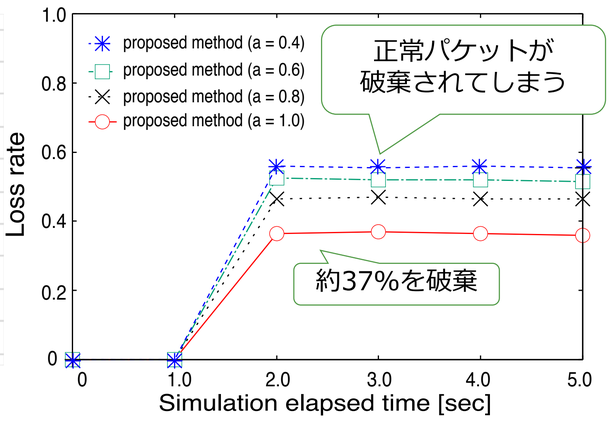


- Amppotのデータセットを用いた評価

攻撃パケットの破棄率



正常パケットの破棄率



- 考察
  - ➢応答サイズの差が大きい場合
    - ✓攻撃パケットを98%以上破棄
    - ✓正常パケットは破棄しない
  - ➢応答サイズの差が小さい場合
    - ✓大きいサイズの攻撃は破棄
    - ✓正常パケットを37%破棄

SCIS2020で発表

中田 有哉，笠間 貴弘，衛藤 将史，神薗 雅紀，猪俣 敦夫，井上 博之，“ネットワーク間の協調によるDRDoS攻撃対策手法，” 電子情報通信学会2020年暗号と情報セキュリティシンポジウム（SCIS2020），2020.

本成果は，国立研究開発法人情報通信研究機構（NICT）が実施するセキュリティイノベータ育成プログラムSecHack365における成果である．
また本研究では，横浜国立大学およびNICTが開発・運用するDRDoS攻撃観測用ハニーポットの収集データを利用した．ご指導いただいた皆様および関係者各位に深謝の意を表す