事例紹介
ネットワークエッジにおける軽量なDDoS防御

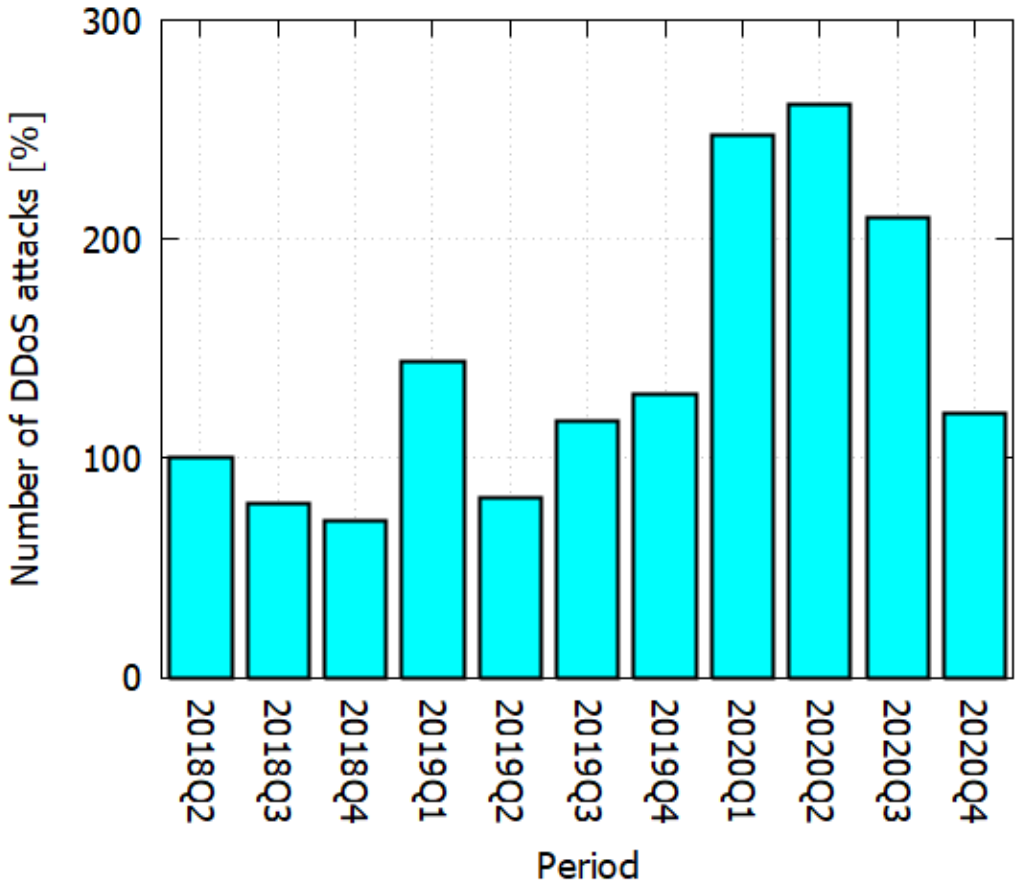
中山 悠

東京農工大学 工学研究院 准教授

2021.12.13 ユーザ連携・循環進化検討TF

研究背景｜DDoS攻撃の増加

- IoTデバイスを踏み台としたDistributed Denial Of Service (DDoS) 攻撃は回数，規模ともに増加



[1]Kaspersky’s cyberthreat research and reports Securelist <https://securelist.com/>

研究背景｜DDoS攻撃の種類

- DDoS攻撃にも様々なタイプが存在するが，本研究ではFlooding (UDP flood, HTTP floodなど) 攻撃に着目

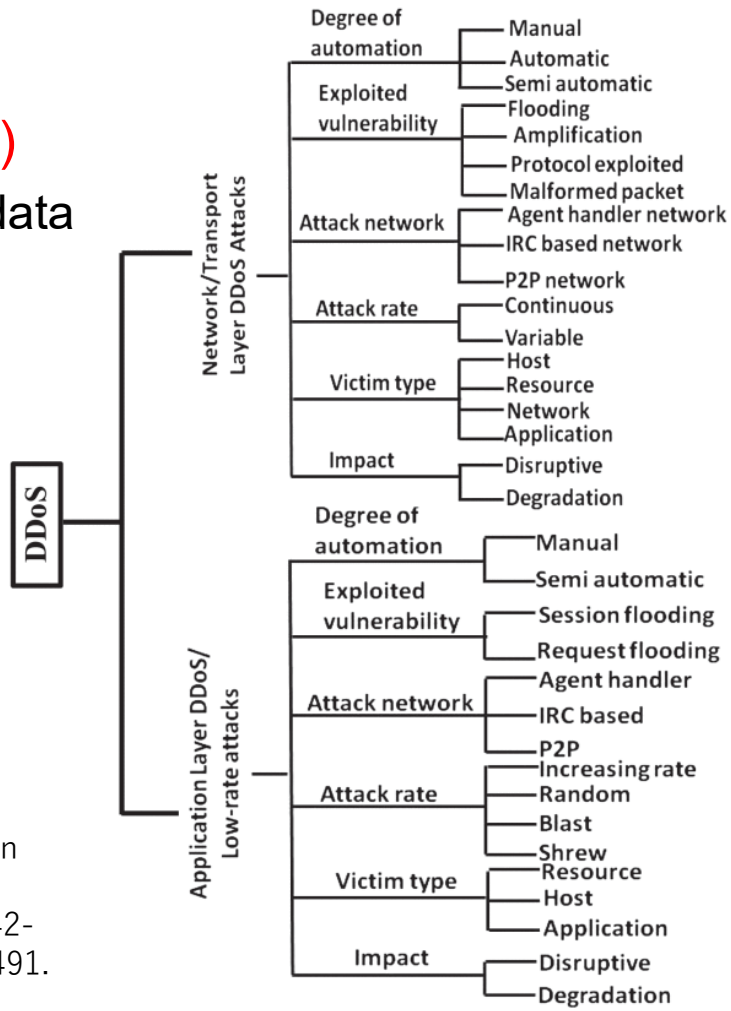
Flooding, protocol exploited, etc.

- Flooding(Target of this mitigation)

  Attack that sends a large amount of data

- Protocol exploited

  Attacks using vulnerabilities



[1]N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242-2270, Fourthquarter 2015, doi: 10.1109/COMST.2015.2457491.

研究背景｜DDoS攻撃の対策技術

- 機械学習などによる攻撃の検出・特定の研究が多く行われる
- 専用装置は高価なものが多く，導入へのハードルが存在
- 既存の安価なNW機器を用いて何らかの対策ができないか・・？

Recently proposed methods

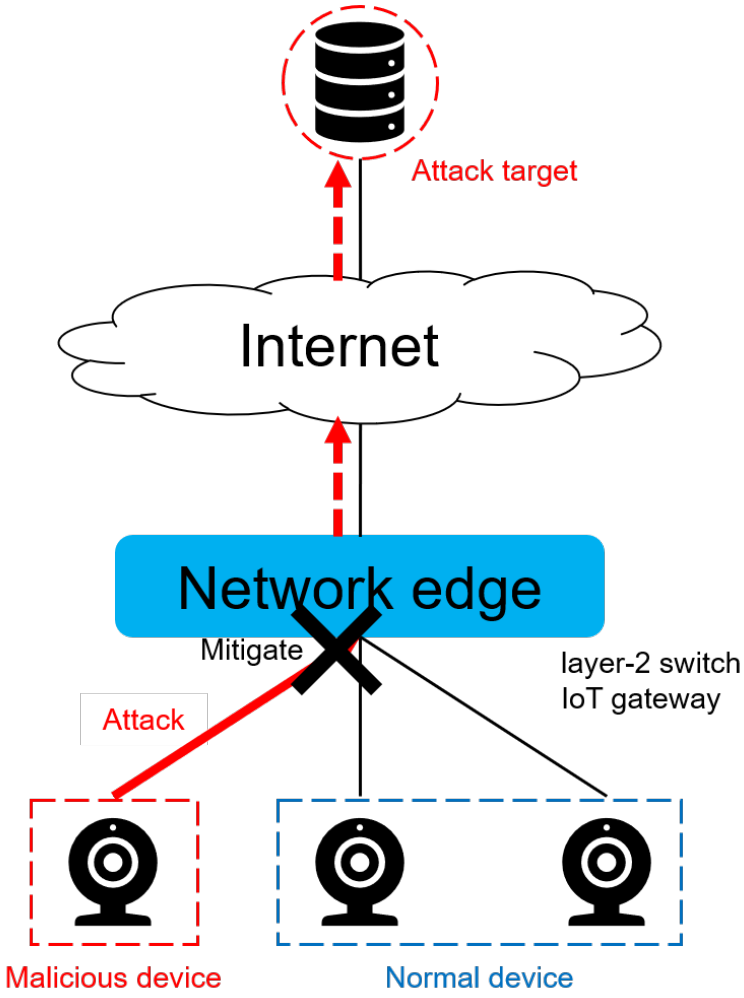
- Detection by machine learning
- Mitigation in Software Defined Networking(SDN) environment

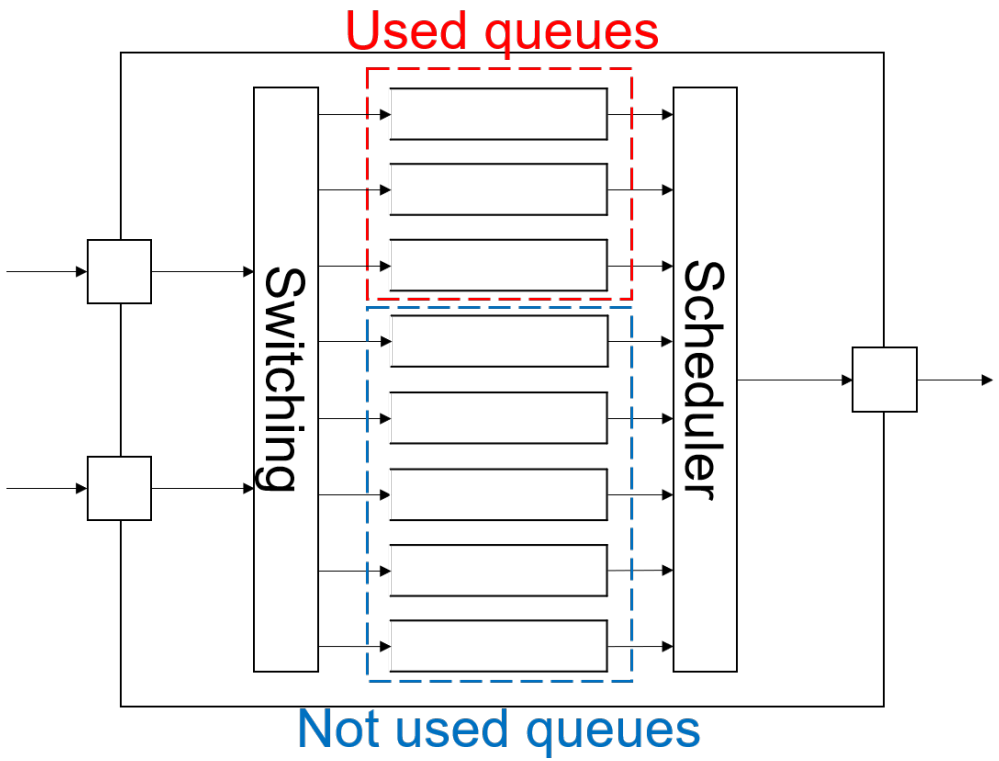
Parameters used for detection

- Source IP address, traffic increasing degree, etc.

提案手法｜概要

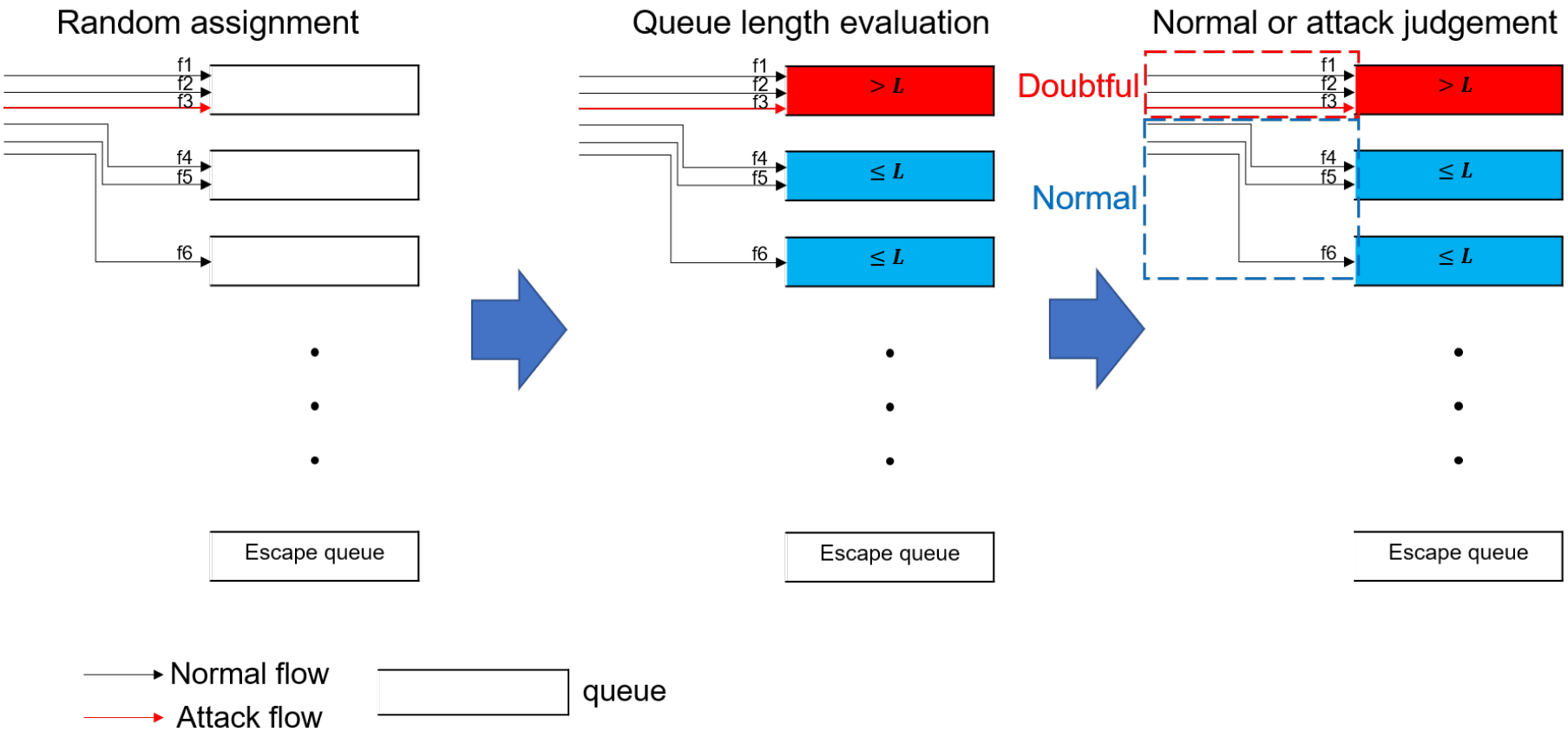
- L2SWなど既存NW機器で，未利用のQueueがあることが多い
- この未利用Queueを活用して，攻撃フローを特定し破棄する





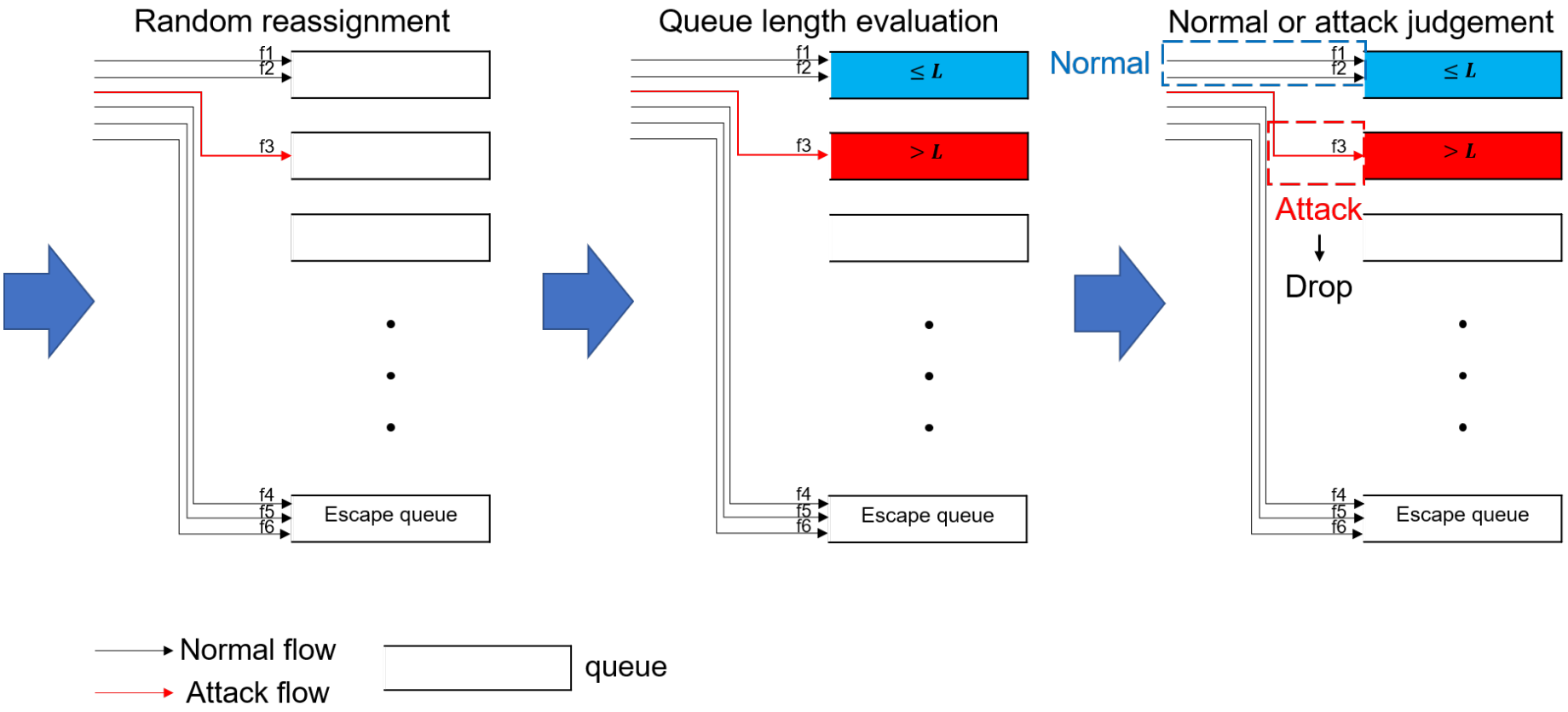
提案手法｜攻撃緩和シーケンス

- 一定時間ごとにQueue Mappingを変えながらバッファ量変動を観測
- 流量の少ないフローは“シロ”と判定



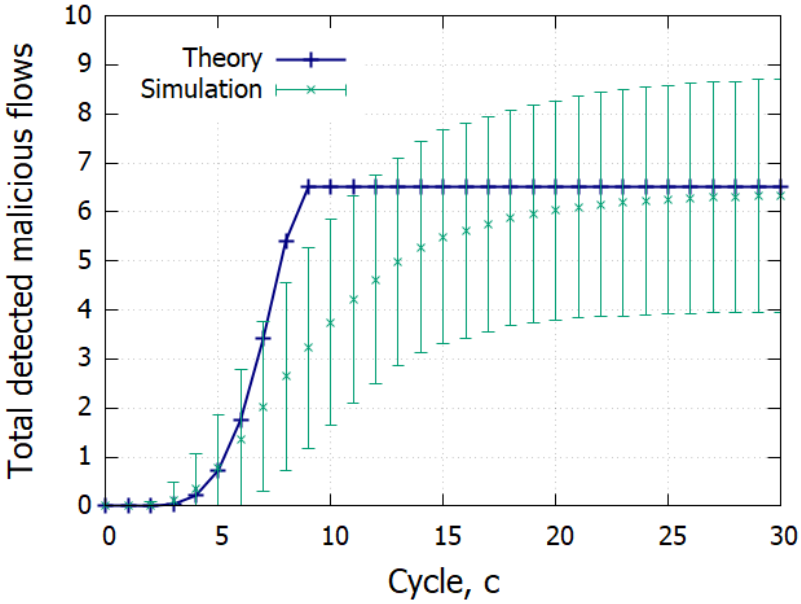
提案手法｜攻撃緩和シーケンス

- 流量の多いフロー群については，次サイクル以降にバラして挙動を観測し，攻撃フローを特定しACL等を用いて破棄

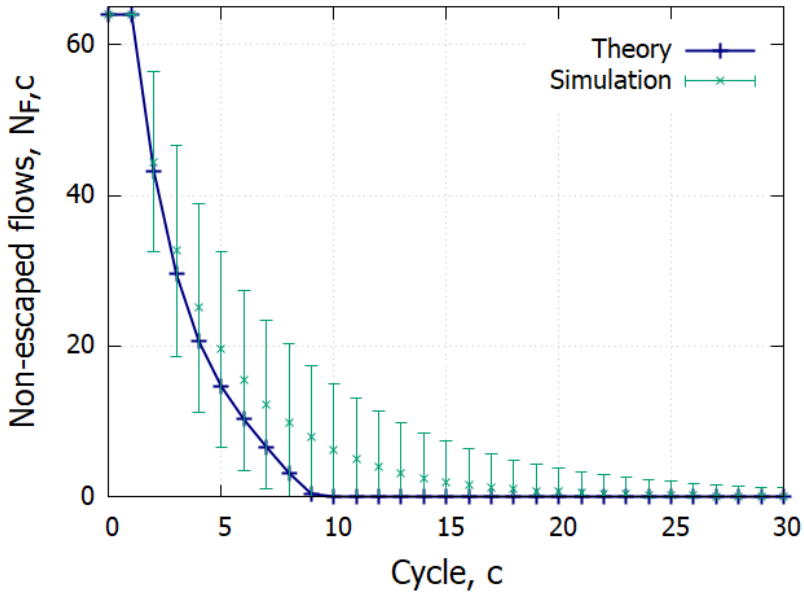


提案手法｜理論解析とシミュレーション結果

- 提案手法の検知性能については理論解析が可能 (確率の計算)
- シミュレーションにより理論値との整合と有効性を確認



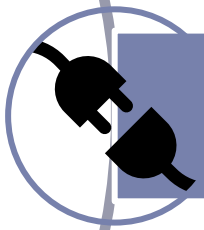
Number of detected DDoS flows, E_c



Number of non-escaped flows, $N_{F,c}$

テストベッド利用｜目的と概要

提案手法の実機検証



L2SWとNWテスタを持ち込みサーバと接続

サーバから大量のパケットを送信

テストベッド利用｜検証の手順

配線

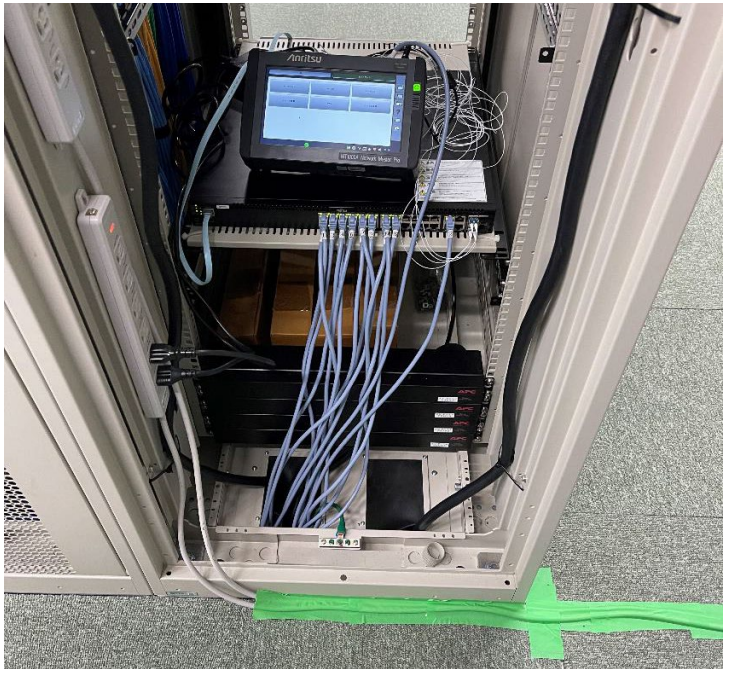
- 持ち込み機器を設置
- 実験用の1Gケーブルを差し替え

設定

- ノードにUbuntuをインストール
- ソケット通信プログラムを作成

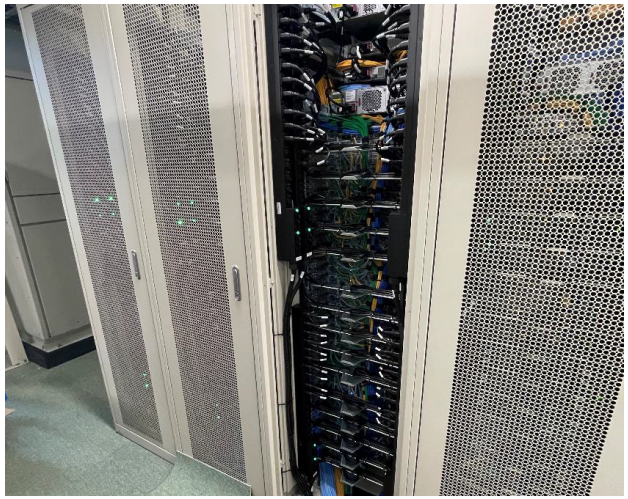
測定

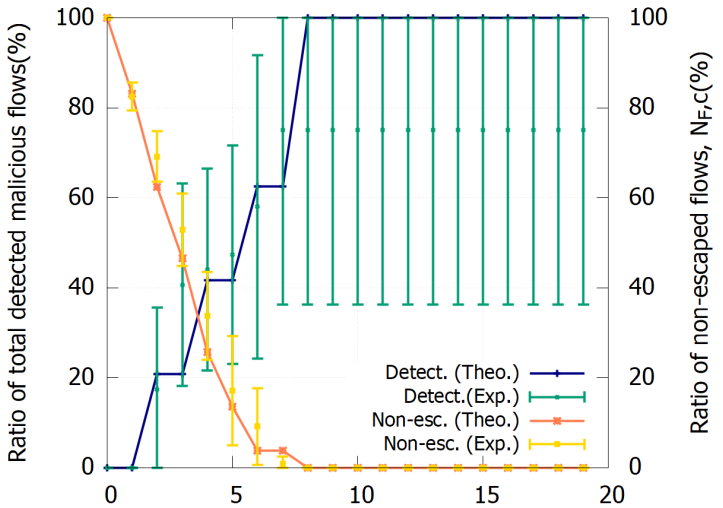
- ノード1台を制御用端末として利用しL2SWへの設定や他ノードへの情報共有
- ノード4台からパケット送信
  - 12ポート×8フロー
  - 攻撃フロー 200Mbps
  - 通常フロー 平均3Mbps

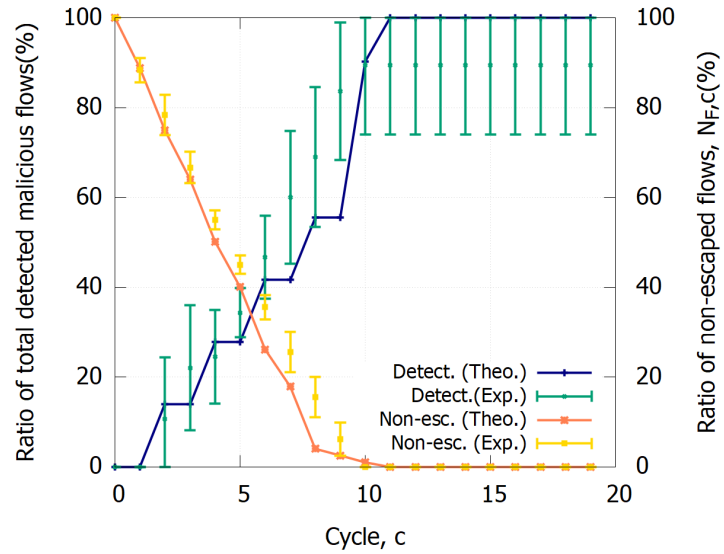


テストベッド利用｜結果

- 提案手法によるDDoS攻撃検知・緩和について実機検証が成功
- ただし，タイムロスが多く利用期間の中では十分にできなかった点もあるため，さらに追加検証を行いたい

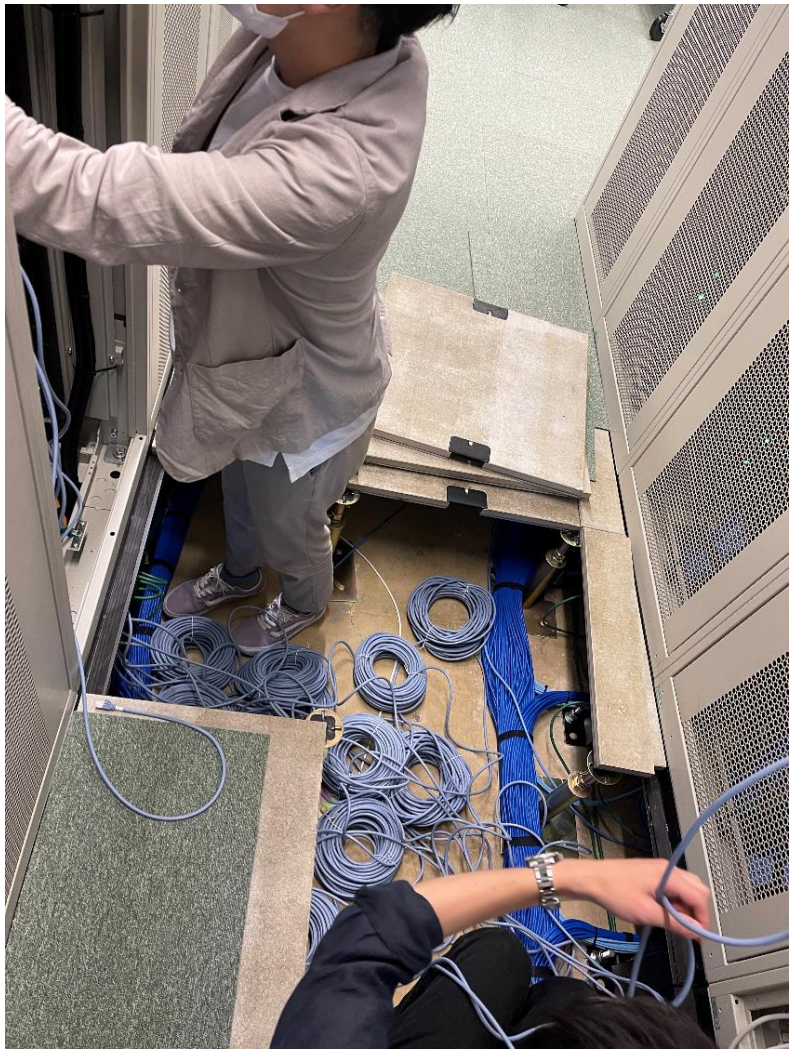






苦労した点｜床下配線

- 持ち込み機器の設置場所が限られていたため，床下配線を行う必要があり，配線作業にそれなりの稼働がかかった



まとめ

- 既存NW機器の機能を利用したDDoS攻撃の検出・緩和手法について，StarBEDの設備を利用させていただき，実機検証に成功
- 今回，VPN接続の不安定さなどのタイムロスが多く，事前に申請した1週間という期間では十分とは言えない面もあった
- スケール性の必要な検証の際には，テストベッドを利用できるのは大変ありがたく，今後も利用していきたい