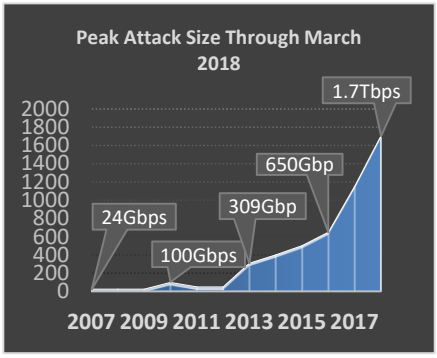
# DDoSミティゲーションを可能にするネットワークルーティングアルゴリズム

## Network routing algorithms for DDoS mitigation

増田 絢斗・ネットワーク分科会・中央大学

DDoS attacks are increasing in size and number due to the appearance of DDoS attack services and attacks using IoT devices. The scale of DDoS attacks will be larger in future, and countermeasures become more important. DDoS mitigation is one of the countermeasures for DDoS attacks. It reroutes abnormal network traffic to the mitigation device, and DDoS trafic is weeded out while clean trafic is passed on. In the conventional method, DDoS mitigation uses virtual circuits. In this research, we propose a method to enable DDoS mitigation by routing control without using virtual circuits.

## 背景




DDoS攻撃とは？

・企業のサーバ等に大量のリクエストを送り，機能停止に追い込む攻撃

・攻撃者が大量のコンピュータを踏み台にして攻撃を行う

・攻撃規模が大きく，攻撃元の特定が困難

**2017年のDDoS攻撃件数（9月30日 時点）**

**・攻撃の件数：610万件**
**・1日あたり：22,426件**

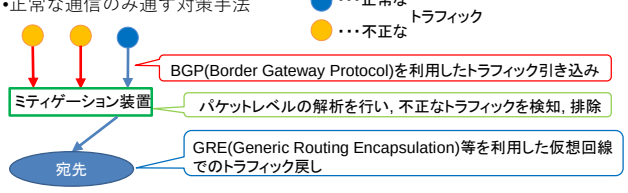
| 日時 | 継続時間 | 攻撃対象 | 影響内容 |
|---|---|---|---|
| 2015年3月 | 4日以上 | Github | 改竄された第三者Webサイトから2秒毎にGithubへ大量アクセスが発生．攻撃が繰り返され，都度対策を実施 |
| 2016年10月 | 約6時間 | Dyn (Managed DNS 基盤) | IoT機器向けマルウェア「Mirai」によるDDoS攻撃により，Amazon, PayPal, Twitterなど多くのサービスに支障. (1.2Tbps) |

・IoT機器を踏み台にした攻撃
・DDoS攻撃代行サービスの登場 → DDoS攻撃の規模，件数の増大．対策をとることが，より重要に．

## 既存の防御手法と課題

**DDoSミティゲーション**

・ミティゲーション装置を経由させる
・攻撃を検知，遮断
・正常な通信のみ通す対策手法




**既存手法の課題**

・攻撃の規模が大きくなる程，広帯域のネットワーク上流でのミティゲーションが必要．

→ ・数百Gのパケットを仮想回線で送るための処理(MTUの設定等)が必要．

・通信事業者は，負荷，到達性の面で巨大なパケットをあまり触りたくない．

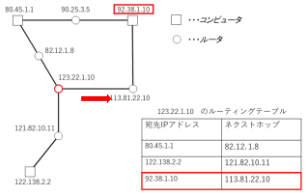

・20byteの新たなIPヘッダとGREのヘッダ4byteの合計24byteのオーバーヘッドが発生

## 問題設定と提案手法

ルーティング(経路制御)によって，DDoSミティゲーションを可能にするアルゴリズムを提案する．

・Tier-1等のネットワーク上流でのDDoS攻撃の対策，キャリアがすべきDDoS攻撃の対策を想定．
・グラフ理論を用いたアルゴリズムの提案を行う．

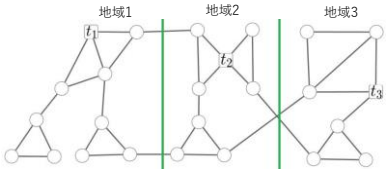
通常のルーティングテーブル




本研究で扱うルーティングテーブル


・VRF(ルーティングテーブルの仮想化)で実現可能

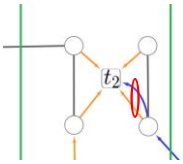
**問題設定**



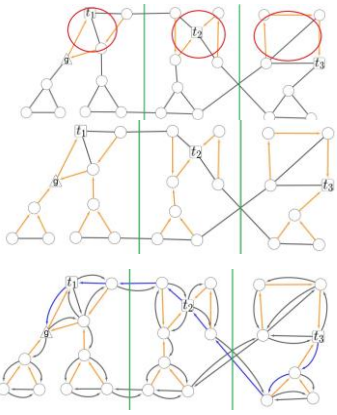

・頂点数: $n$ ($i = 1, 2, \cdots, n$)
・辺数: $m$ ($m \geqq n - 1$)
・地域数: $r$ ($k = 1, 2, \cdots, r$)
・各地域にミティゲーション装置 $t_k$ が1つ存在
・任意の宛先$g$(どの頂点も宛先になりうる)

**条件**:
・送信元の地域の$t_k$を経由して一度だけミティゲーションの処理を行う
・同じ地域に2度入らない．

**・全ての送信元から，$t_k$への経路**
**・全ての $t_k$ から，$g$への経路**
**が互いに独立となる経路を各宛先$g$毎に求める．**




**アルゴリズム**




1. $t_k$を含む二辺連結成分において，$t_k$を根とする深さ優先探索を行い，内向木をとる．

2. その他の連結成分において，各地域でミティゲーション装置に向かう橋の根元の頂点を根とする幅優先探索を行う．1.と2.のグラフ，およびこの地域内の橋をとる．

3. 2.で構築した枝を全て取り除いた有向グラフに対して，全ての$t_k$から宛先$g$まで幅優先探索を行う．

**実験環境:**
OS: Windows 10 Pro
CPU:Intel(R)Core(TM)i78550U(1.99GHz)
メモリ: 16.00 GB
言語: Python
使用ソフトウェア: Cytoscape

**数値実験**

頂点数 $n = 50$, 辺数 $m = 75$, 地域数 $r = 3$