クロスファイア攻撃における攻撃戦略と費用対効果の分析

立命館大学　情報理工学部
先進ネットワーク研究室
上田和輝　上山憲昭

目次

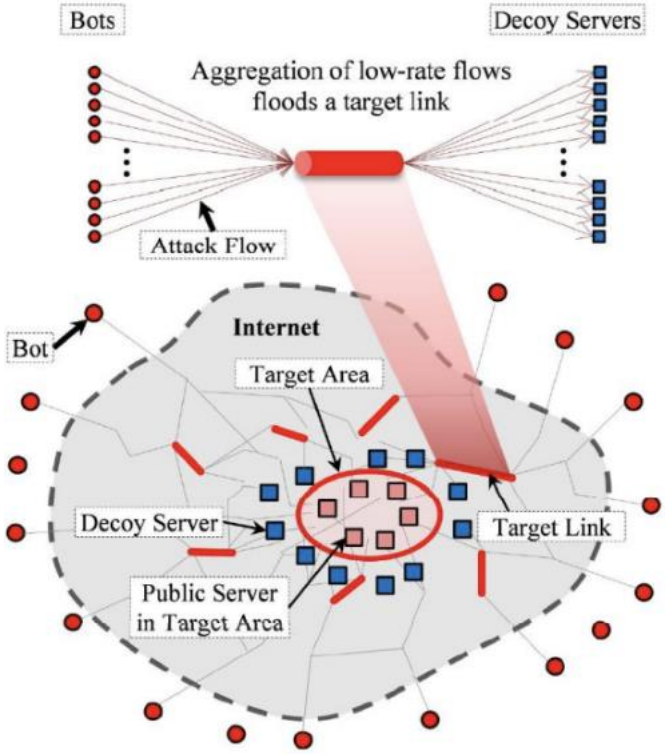
- Crossfire attack (CFA)について
- 先行研究・本研究の目的
- 提案指標
- 研究概要
- 結果・考察
- 今後の展望

Crossfire attack (CFA)

- Crossfire attack (CFA)

  ターゲットエリア(TA)内のホストを宛先とする外部からのフローの多くが経由するリンクを過負荷にすることで，TA内のホストを通信不能にする攻撃

- CFAの特徴：検知困難性
  - 従来のDDoS攻撃の検知手法は，攻撃対象サーバで検知するが，TA内のサーバは直接攻撃されない
    - 被攻撃サーバでの検知が困難
  - 各ボットが各デコイサーバに対して送付するトラヒック量は少量かつ，正常ユーザと区別がつかない
    - トラヒック量やパケットのペイロードによる識別が困難

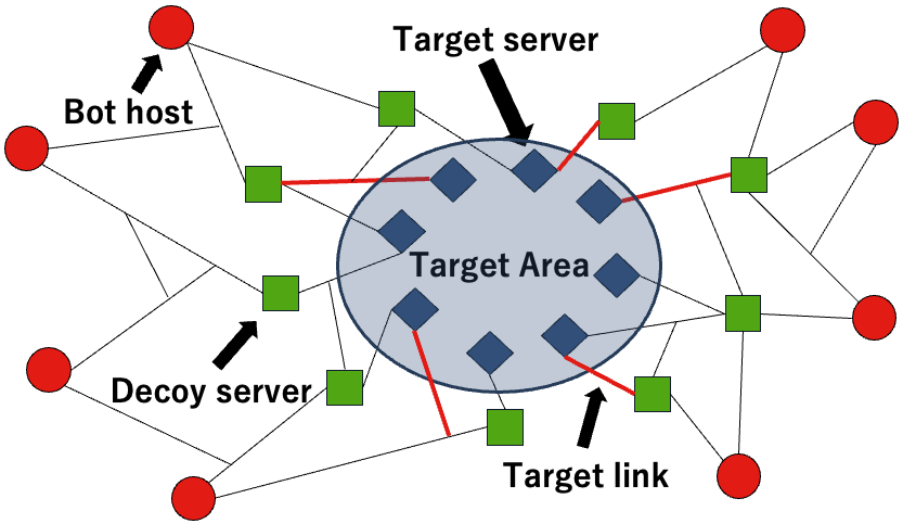


CFAの攻撃メカニズム

- 探索フェーズ
  - 多数のBot hostを利用
  - TA周辺のDecoy serverに向けて，tracerouteパケットを送信
  - ネットワークの経路情報を収集・リンクマップの構築

- 攻撃フェーズ
  - 得られた経路情報をもとに，Target linkを選定・攻撃

- Target linkの選定基準
  - 赤線のように，TAに向かう多数の通信が集中している，ボトルネックとなるリンク



先行研究

- 課題:
  - CFAの脅威・影響・効果は攻撃エリアの選定に強く依存するが，攻撃エリアの選定法を議論した研究は見られない

- 研究の目的:
  - CFAに対して脆弱なネットワーク上のエリア推定法を提案

  ⇨ 検出したエリアに対して重点的な設備増設が可能

  - エリアの境界を跨ぐリンクのトラヒック量上位2本のリンクを経由する，トラヒック量の比率が高いエリアを脆弱なエリアと定義
  - グラフ(トポロジ)構造の学習が可能なGCN（graph convolutional network)を用いて，CFAに脆弱なエリアを推定

本研究の目的

- 着目課題:
  - CFAの攻撃者にとっての効率を図る尺度が未定義
  - 効率性の観点でCFAに対して脆弱なエリアの推定法は未検討
  - CFAに脆弱なエリアの効果的・効率的な対策が未検討

- 本研究の目的:
  - CFAの攻撃者にとっての費用対効果に基づく尺度を提案
  - 上記尺度が高い，CFAに対して脆弱なエリアの推定法を提案
  - CFAに脆弱なエリアのCFA効率性を，小コストで効果的に低減する技術を提案

Regular Traffic Ratio (RTR)

- 定義
  - 攻撃の効果を表す指標
  - 正規トラヒックの分布を表す平常時の通信において，Target linkの占有割合を示す
- 算出アルゴリズム
  1. TAと外部エリア間の全ノードペアについて，最短経路を導出
  2. 対象リンクを通過する経路数を，総経路数で除算して正規化
- 攻撃者視点
  - RTRが高い：そのリンクを遮断すれば，TAへの通信の大部分を遮断できる

  → TAに対して深刻な通信障害を引き起こすことが可能

Attack Concentration Ratio (ACR)

- 定義
  - 攻撃効率を表す指標
  - 各攻撃シナリオにおいて，対象のTarget linkにどれだけ攻撃トラヒックが集中しているかを示す
- 算出アルゴリズム
  1. モンテカルロ法 (N=1,000)を用いる
  2. ランダムに抽出したボット・デコイ間の最短経路を導出し，リンクごとの通過フロー数を計測・集中率を算出して平均化
- 攻撃者視点
  - ACRが高い：ネットワークの構造上，攻撃トラヒックが集まりやすいボトルネックなリンク
  - これらのリンクに対して少数のボットを動員

  → 容易に帯域幅を枯渇

Blocked Traffic Ratio (BTR)

- 定義
  - 攻撃成功度を表す指標
  - 予算(ボット数)制約下で攻撃を実行した結果，TAに流入出する正規トラヒックの何割が遮断されるか

  → 遮断トラヒック量比率を示す

- 算出アルゴリズム：貪欲法・費用対効果を最大化
  1. 攻撃コスト(ACR：攻撃効率に反比例すると定義)を設定
  2. 費用対効果(ROI)=攻撃効果 (RTR)/攻撃コストを算出
  3. ROIが高い順にリンクを選定し，予算内で攻撃を最大化
  4. 選定リンク全てのRTRをカウントし，BTRとする

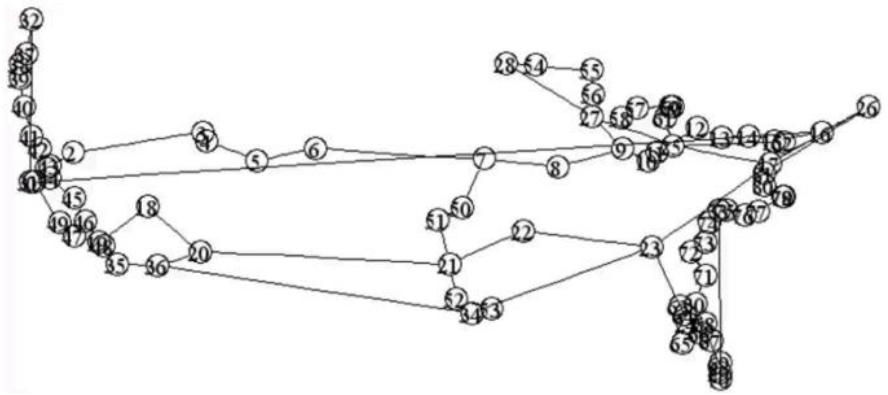
- 攻撃者視点
  - RTRとACRを統合した，限られた予算内でネットワークに最大の被害を与えるための指標

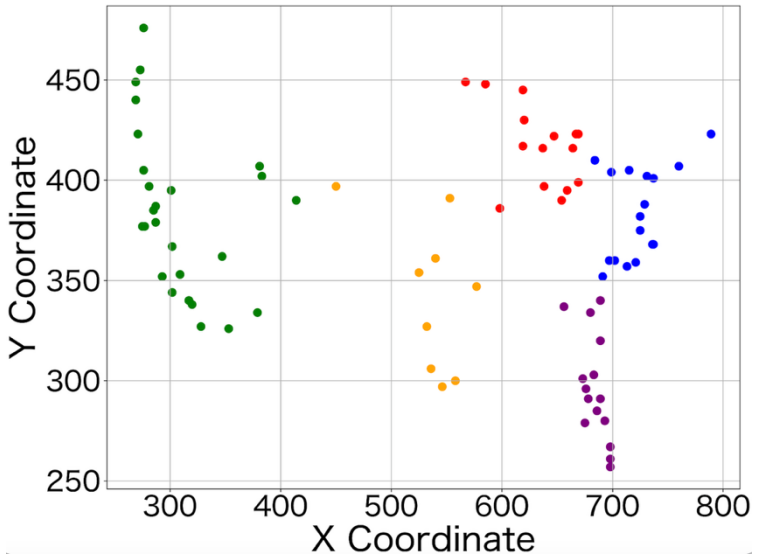
ボットの相対コスト

- 背景
  - 先行研究のPPI (Pay-Per-Install)市場調査に基づき，各地域によってボットの獲得単価が異なる事実に着目
- 定義
  - 同じネットワーク内でも，地理的配置によって価格が異なる
  - トポロジをk-means法で5分割し，各エリアの獲得費用について，エリアごとに$0.1-0.18/1ボットで設定
- 本研究の独自性
  - 攻撃者の規模によってCFAに導入可能な予算は変化すると考察し，攻撃者の攻撃能力をコストとして数値評価

評価対象ネットワーク

- 3つのネットワークトポロジ（AGIS, Allegiance_Telecom, At_Home_Netowork）について，位置座標を特徴量として分類





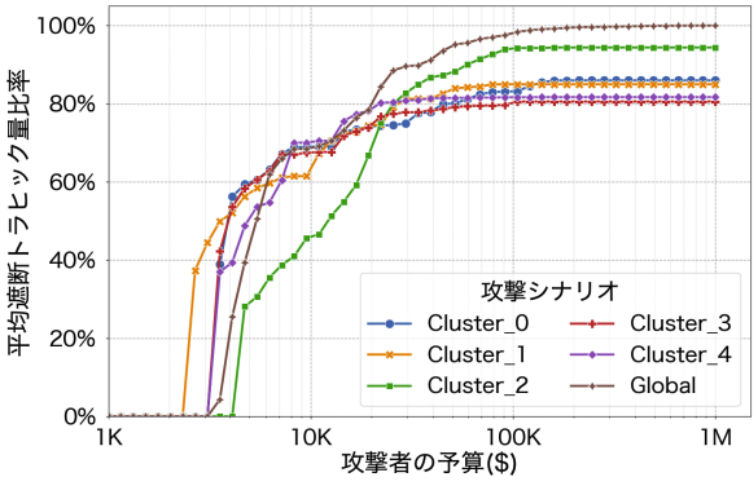
Cluster	Color	Location ・ Cost per Install
0	Blue	東海岸北部・$0.1376
1	Orange	大陸中央部・$0.1000
2	Green	西海岸・$0.1800
3	Red	大陸北部・$0.1282
4	Purple	東海岸南部・$0.1282

研究概要

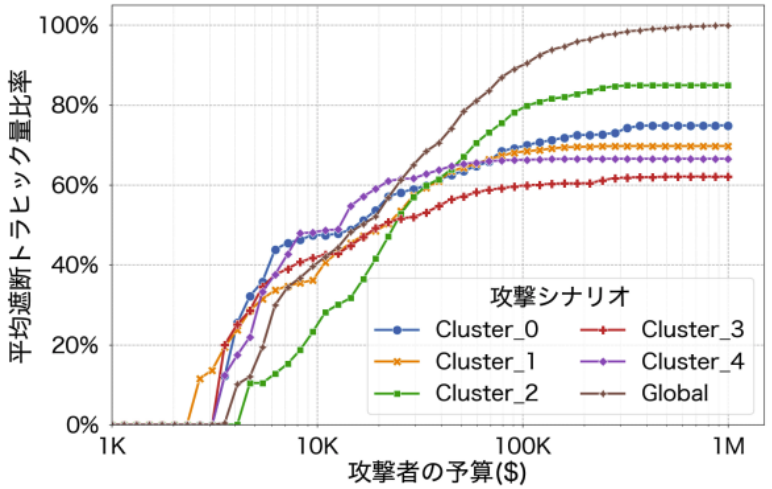
- 攻撃者の予算規模
  - 小規模：$10,000
  - 中規模：$100,000
  - 大規模：$1,000,000
- 攻撃シナリオ
  - Cluster0-4シナリオ：k-means法で分類した特定エリアに限定
  - Globalシナリオ：ネットワークトポロジ全体からランダムに選択
- 数値評価
  - 攻撃者が標的エリア（TA）を拡大した場合における，
    攻撃効果・費用対効果の関係性を分析

研究結果1

- 攻撃者の予算増加に伴う最適な攻撃戦略の変化(AGIS)



(a)TA サイズ 2

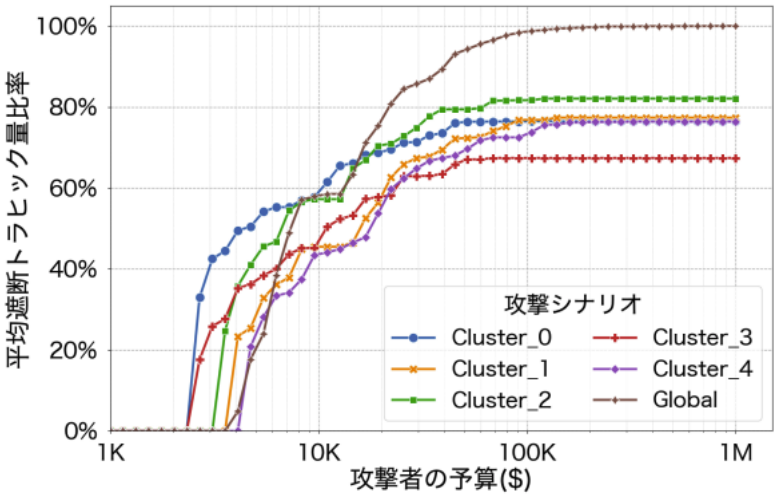


(c)TA サイズ 5

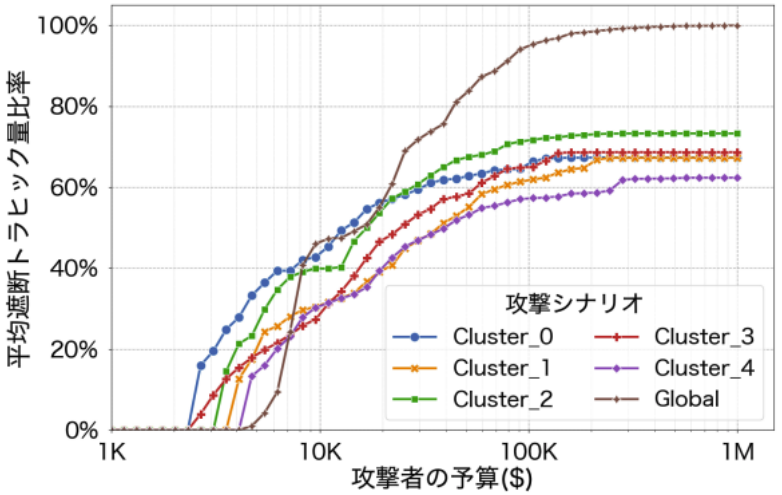
- 基本的には，予算増加に伴いBTR(攻撃成功度・平均遮断トラヒック量比率)は上昇
- Cluster2(緑・西海岸)
  - 低予算時：BTR最下位→高予算時：BTR2番目
- 予算規模に応じて最適な攻撃戦略は変化する

研究結果2

- ボットの地理的分布と攻撃可能エリアの推移（At Home）



(a)TA サイズ 2

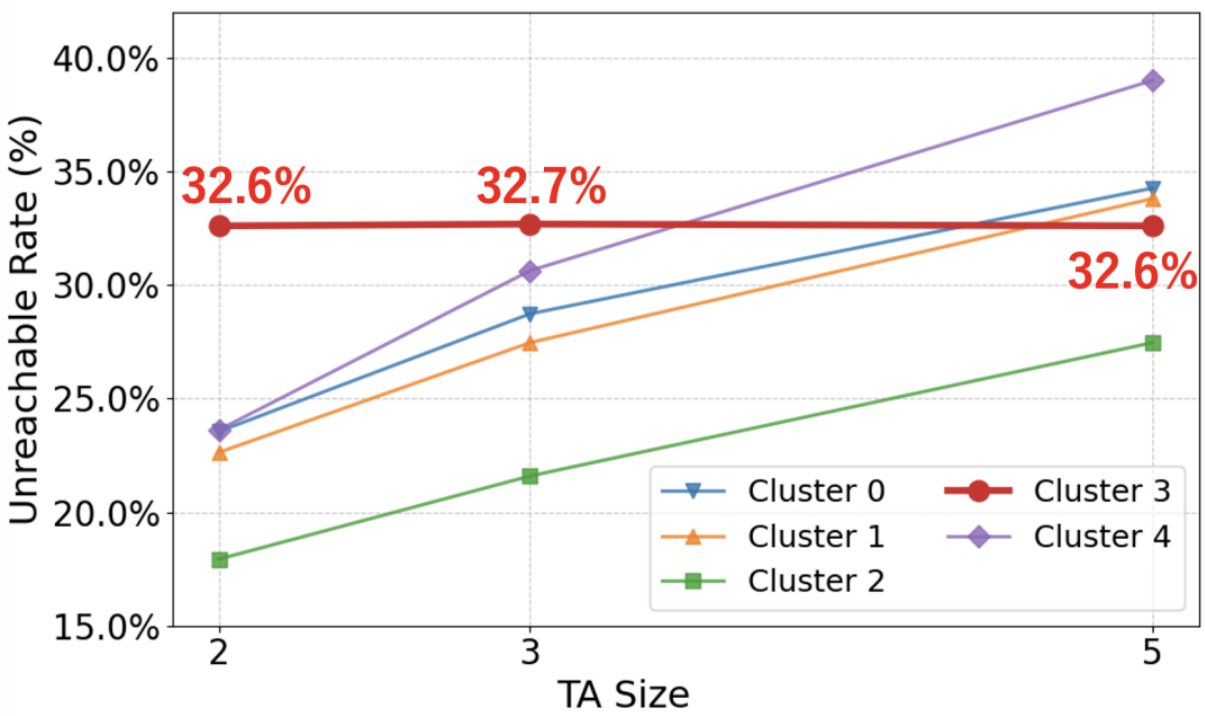


(c)TA サイズ 5

- Cluster3(赤・大陸南部)の特異性
  - TAサイズを2→5に拡大しても，同じBTR(攻撃成功度)で横ばい
  - 特定の地理的条件下において，TAの拡大は攻撃の到達性を低減させる比率が限定的

到着不能通信トラフィック

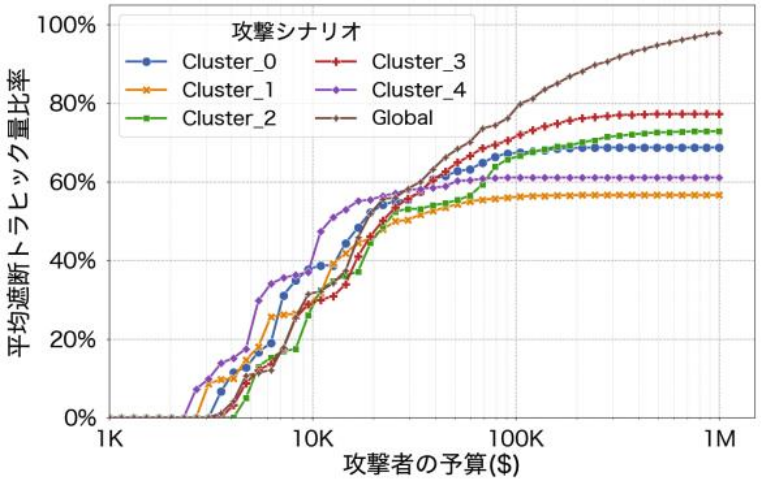
- 各攻撃シナリオにおける，TA拡大に伴う攻撃不能率の推移
  - Cluster0,1,2,4：攻撃者がTAサイズを拡大すると，TAに届かない通信の割合が増加（右肩上がり）
  - Cluster3：値が約33%で横ばい



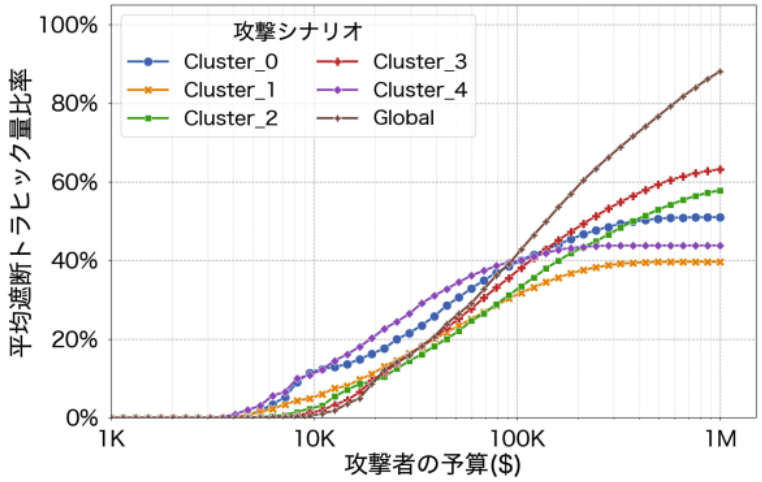
- 攻撃者にとって，Cluster3は標的エリアを拡大させても攻撃効果が低下しない→地理的に優れたエリア

研究結果3

- ネットワーク構造と堅牢性の関係 (Allegiance Telecom)



(a)TA サイズ 2



(c)TA サイズ 5

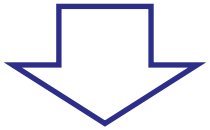
- 他のネットワーク2つと比較して，全体的にBTR(攻撃成功度)が低い
  - 攻撃者にとって費用対効果が低く，攻撃に対して堅牢である
  - リンク密度(ノード数に対するエッジ数の割合)が関係していると考察

リンク密度

- トポロジ全体における，ノード数に対するエッジ数の割合

Network	Nodes ($\|V\|$)	Edges ($\|E\|$)	Ratio (R)	連結 TA 数
AGIS	82	92	1.12	478
At Home Network	46	55	1.20	232
Allegiance Telecom	53	88	**1.66**	**7817**

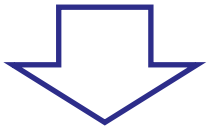
- Allegiance Telecomの特異性
  - AGISおよびAt Home Networkはリンク密度Rの値が1.1−1.2であるのに対し，Allegiance Telecomは1.66と突出して高い



  - 1つのノードから接続されるエッジ数が多く，ネットワーク構造が複雑・迂回経路が豊富に存在するため，ネットワーク全体で平均遮断トラヒック比率が低く抑えられている

今後の展望

- CFAに対する，ネットワークの脆弱性を数値評価
  - 他のネットワークにも共通した特徴・脆弱性が判明



- GCNを用いた高CFA効率エリアの推定技術を詳細化
- リンク容量増設，経路制御，トラヒック分散等の対策に要するコストを定義し，総コストの制約条件化におけるCFA効率の低減効果を最大化する制御法の選択法を検討

ご清聴ありがとうございました