

クロスファイア攻撃の 効率性分析

立命館大学 情報理工学部
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
- 現在の取り組み
- 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

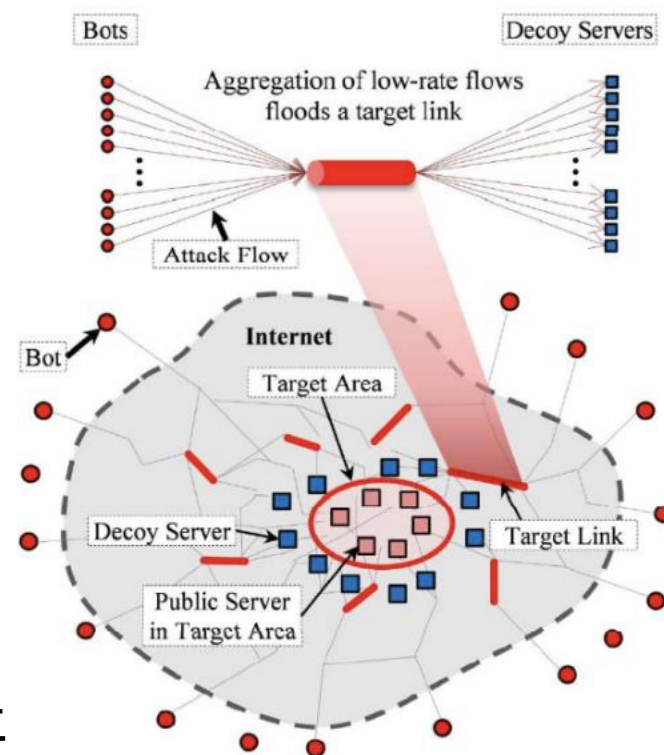
■ CFAの特徴: 検知困難性

- 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フィック量は少量かつ, 正常ユーザと区別がつかない

- トラフィック量やパケットのペイロードによる識別が困難



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フィック量上位2本のリンクを経由する, トラフィ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

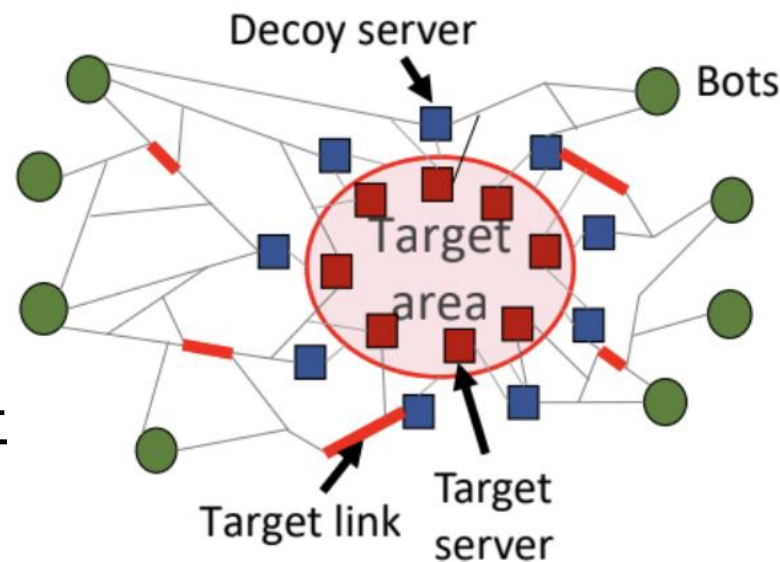


■ 本研究の目的:

- 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

現在の取り組み

- CFA効率の定義式を詳細化
- CFA効率: 攻撃者にとっての費用対効果を表す指標
 - $\frac{\text{遮断トラフィック量比率}}{\text{使用ボット数} \times \text{ボットの相対コスト}}$ で定義
- 遮断トラフィック量比率: ターゲットエリア(TA)の境界を横断するトラフィック量のうち, CFAにより遮断されたトラフィック量の比率
- ボットの相対コスト:
 - 攻撃に使用するボットについて回線速度とコストに基づく相対コストを定義
 - 使用ボット数と相対コストを元に複数の攻撃シナリオを作成



作成した攻撃シナリオ

■ 数値評価環境

- 対象ネットワーク: 米国商用ISPバックボーンネットワーク
(Allegiance_Telecom)
- リンク容量: 3Gbps
- デコイサーバ: 5台
- 試行回数: 100回

■ ボットのパターン

- Wi-Fiモデル(送信レート: 200Mbps・相対コスト: 1.0)
- 標準モデル(送信レート: 1Gbps・相対コスト: 1.0)
- 高性能モデル(送信レート: 4Gbps・相対コスト: 1.6)



■ 3つの攻撃シナリオを作成(総送信量: 8Gbps)

- A: 標準ボット8台の組み合わせ
- B: 高性能ボット2台の組み合わせ
- C: Wi-Fiボット40台の組み合わせ

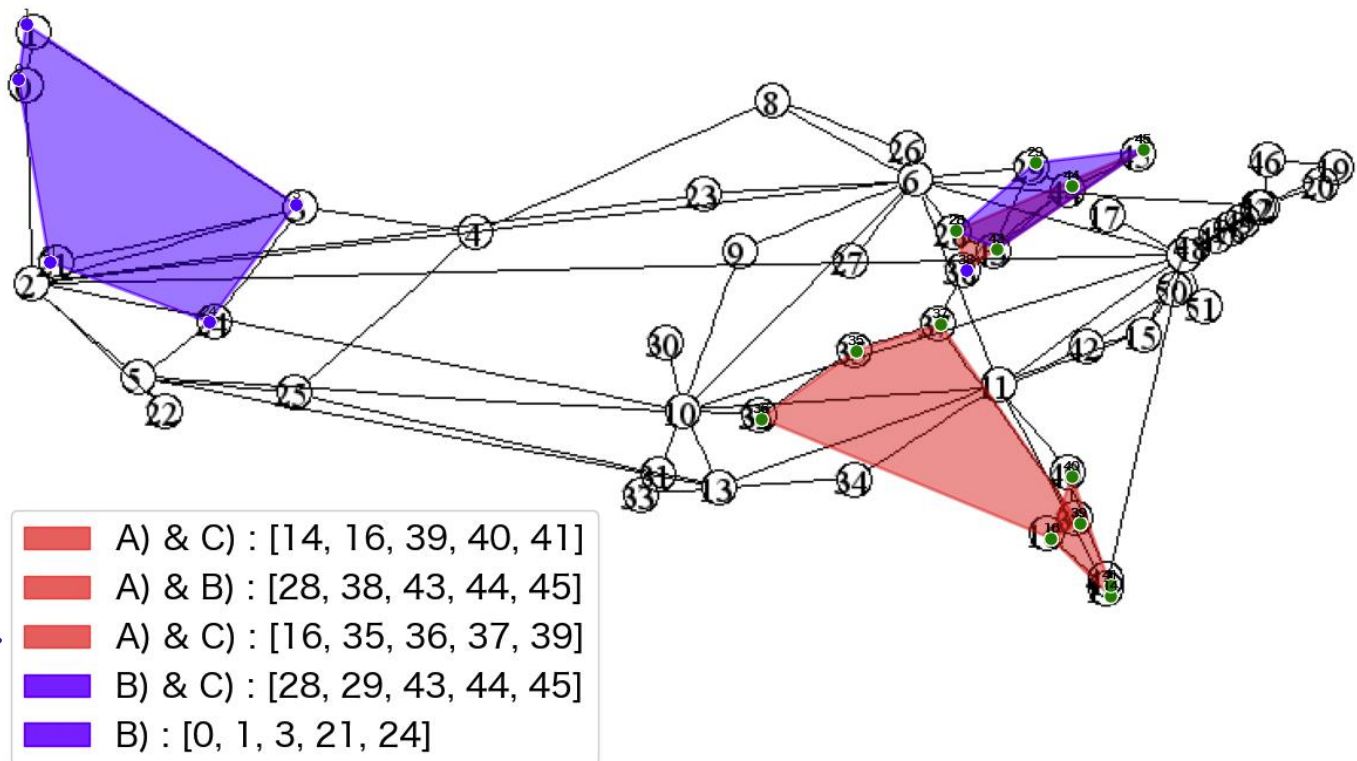
脆弱なTAの変化

- 作成したシナリオにおける, 各TAについてのCFA効率を調査
 - CFA効率の値が高い各TA(隣接する5ノード)のTOP3について, トポロジ図上に表示

脆弱なTA(隣接する5ノード)を色付けして表示

各攻撃シナリオのCFA効率値TOP3

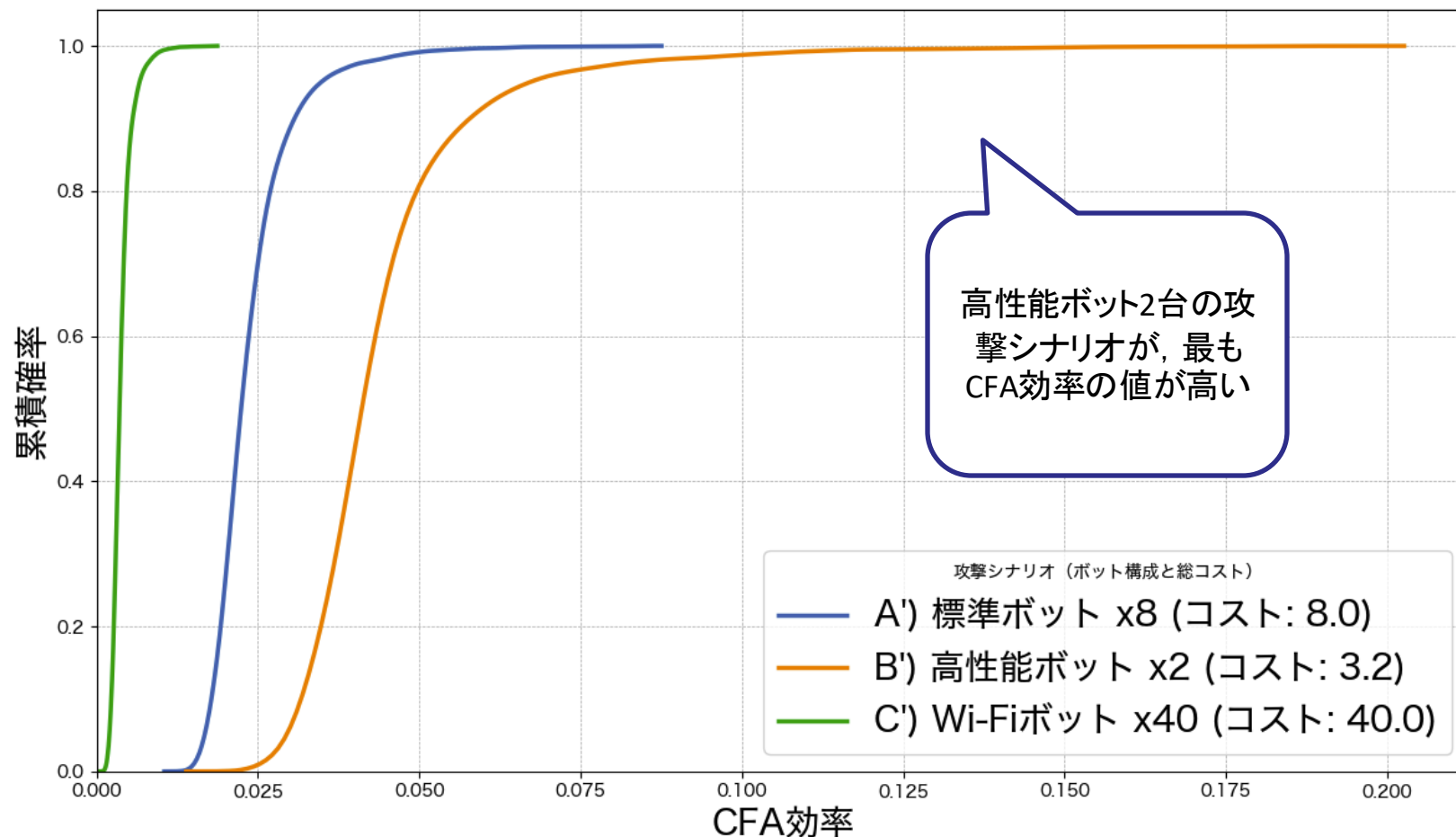
A:標準ボット×8
B:高性能ボット×2
C:WiFiボット×40



- 高性能ボット×2の組み合わせのみ左側をフラッディング
→境界リンクが他エリアと比較して少ないため

CFA効率の分布

■ 各攻撃シナリオにおける, CFA効率の値の累積分布



- 少ないボット数・コストで攻撃→CFA効率の値は上昇
- TAの選定によってCFA効率の値は大きく異なる

今後の展望

- CFA効率の定義式に基づく, 脆弱なエリアの選定
 - 用意した複数の攻撃シナリオごとに, 脆弱なTAは異なる



- 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