

クロスファイア攻撃に対して 脆弱なエリアの選定法

王 天嶼 上山 憲昭 (立命館大学)

研究背景: Crossfire Attack (CFA)

■ DDoS攻撃の一つ: クロスファイア攻撃(CFA)

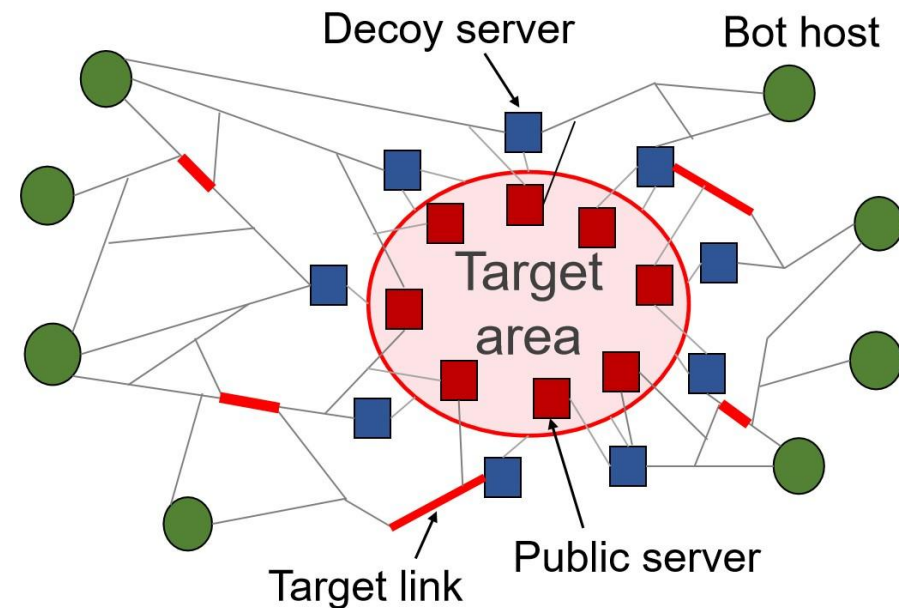
- ターゲット: サーバではなくネットワーク内のリンク
- 目的: ターゲットエリア (TA) 内のホストへの通信を外部から遮断してサービスを妨害

■ 探索フェーズ

- ボットホストからターゲットエリア(TA)内の公開サーバにtracerouteパケットを送信
- 経由するルータのリストを得る

■ 攻撃フェーズ

- ボットからデコイサーバに少量のトラフィックを生成し, TAと外部との通信を遮断



研究目的

- CFAの発生を未然に防御するためには、攻撃フェーズ前で検知・防御を行う
- 将来CFAのターゲットとなる可能性の高いエリアに対してより効果的な防御を展開
- CFAに対して脆弱なエリアの選択アルゴリズムを提案
- 提案アルゴリズムの有効性を検証

CFAに対して脆弱なエリア検知の課題

■ 検知の困難さ

- 既存のCFAの防御策では, CFAのTAを予測することができない

■ CFAの特徴

- トラフィックが頻繁に通過するリンク
 - 攻撃コストが低い

➡トラフィックのルーティング頻度に基づくCFAに対するエリアの脆弱性を定義

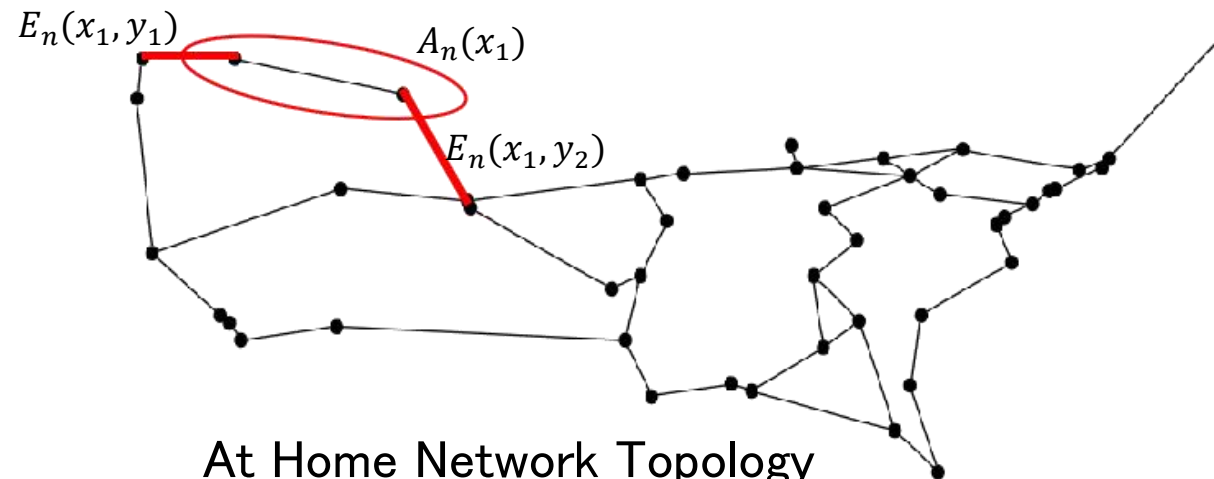
CFAに対する脆弱さを測る尺度

■ CFAの潜在的な影響度

- ターゲットエリア x 内と x 以外の領域を跨ぐ少数のリンクを削除した際に、エリア x が外部と通信不能となるトラフィックの割合

■ 定義

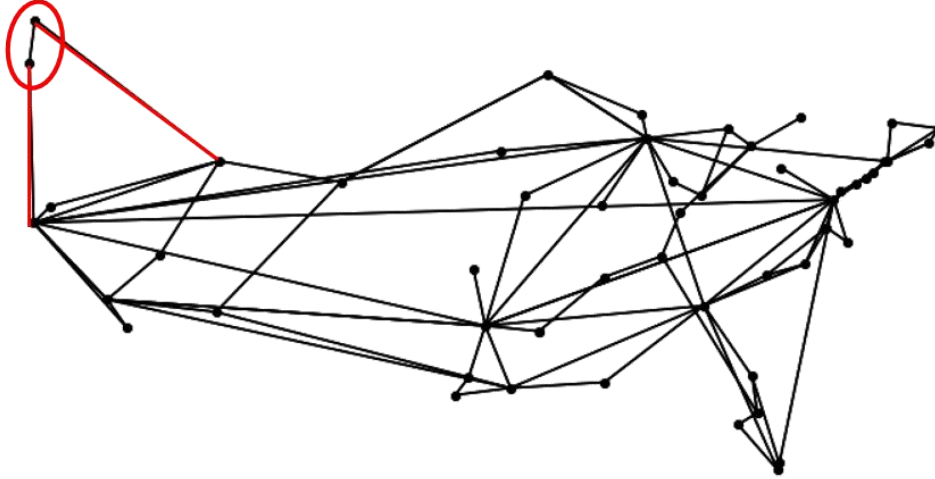
- $A_n(x)$: n 個の隣接ノードで構成されるエリア x
- $E_n(x, y)$: 任意の $A_n(x)$ に対して, $A_n(x)$ と他エリアを跨る任意のリンク y
- $R_n(x, y)$: 任意の $A_n(x)$ 以外の任意のノードと $A_n(x)$ の間の最短ホップ経路のうち, リンク $E_n(x, y)$ を通る割合
- $Max_2 R_n(x)$: 任意の $A_n(x)$ に対して, $R_n(x, y)$ の最大値と 2 番目に大きな値との合計値



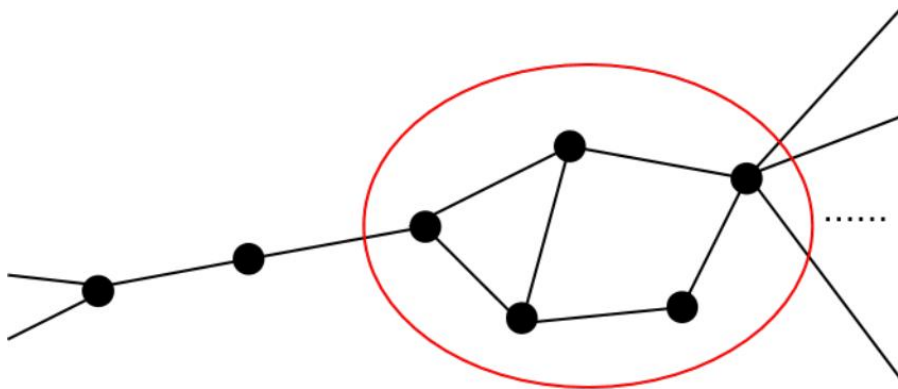
At Home Network Topology

CFAに対して脆弱なエリア特徴

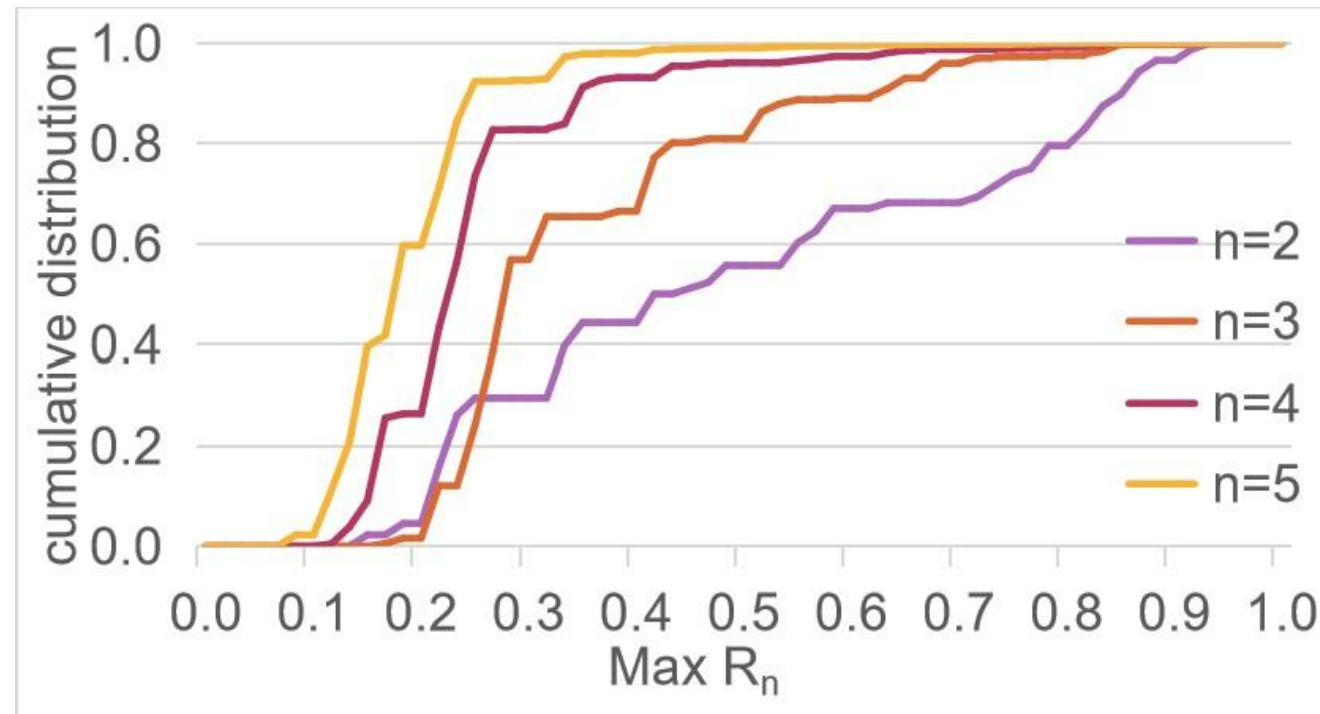
- 直列構造: 次数が2のノードが直列に連結したエリア



- 准直列構造: 次数が3以上のノードが複数連結したもので、エリア内外が2個のノードでのみ連結しているエリア



各ネットワークトポロジの任意の n 個の隣接ノードからなるエリア x に対する
 $Max R_n(x)$ の累積分布



(a) Allegiance Telecom

提案アルゴリズム

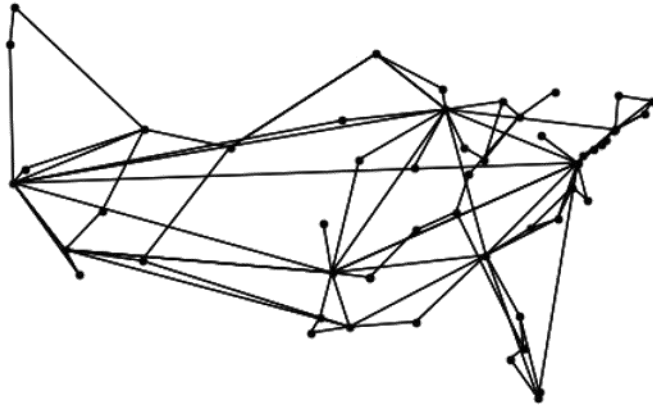
- 各エリア x に対して以下で定義するスコア $S(x)$ を計算し, その値が大きなエリアを脆弱なエリアとして抽出
 - $S(x) = s_1(x) + s_2(x) + s_3(x)$
 - $s_1(x)$: エリア x と隣接する直列構造の数
 - $s_2(x)$: エリア x と隣接する准直列構造の数
 - $s_3(x)$: エリア x 内の高次数ノード数の逆数
- TA: 5個の隣接ノードから構成されるエリア
- 高次数ノード
 - ネットワークトポロジ内の全ノードの中で, 上位30%以内の次数を有するノード
 - TA内の高次数ノードの数が少ないほどTAはCFAに対して脆弱

性能評価

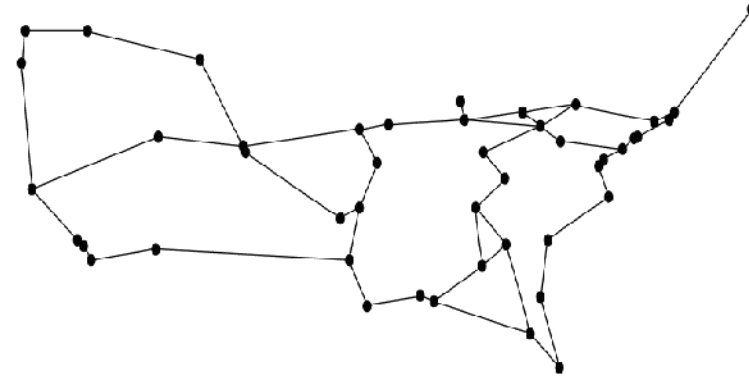
- 提案アルゴリズムで発見した各エリアの $Max_2 R_n(x)$ を最適法の発見エリアと比較
- 最適法
 - $Max_2 R_n(x)$ が任意に与えた閾値 T 以上となるエリアを全て選択
 - 計算量が大きい
 - $Max_2 R_n(x) \Rightarrow$ 全てのノード間の最短ホップ経路を計算
- 提案アルゴリズム
 - スコア $S(x)$ が大きな順に最適法同じ個数のエリアを選択

評価が用いるトポロジ

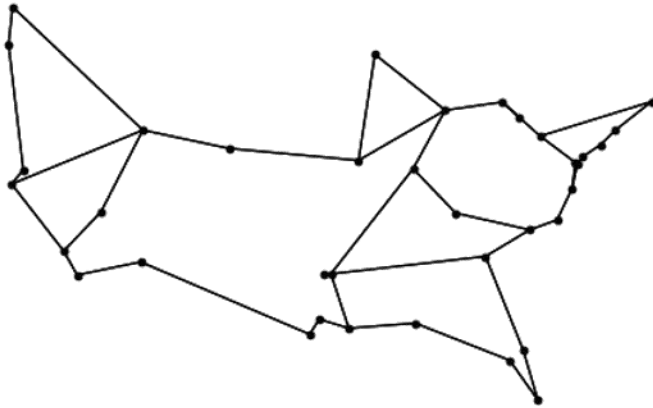
■ 米国の商用バックボーンISPである4つのネットワークのトポロジ



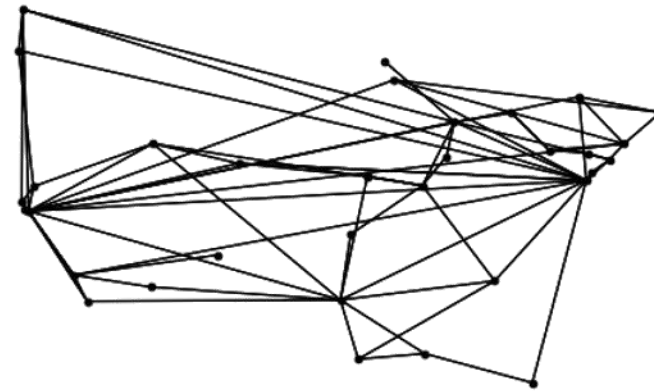
(a) Allegiance Telecom



(b) At Home Network



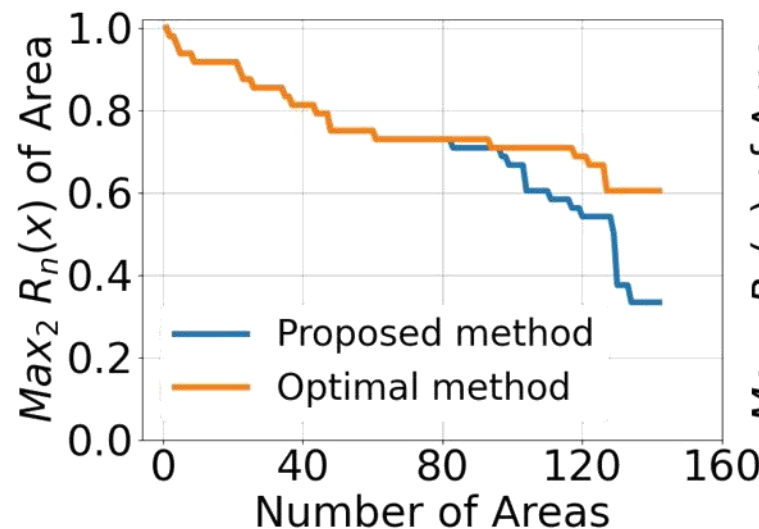
(c) CAIS Internet



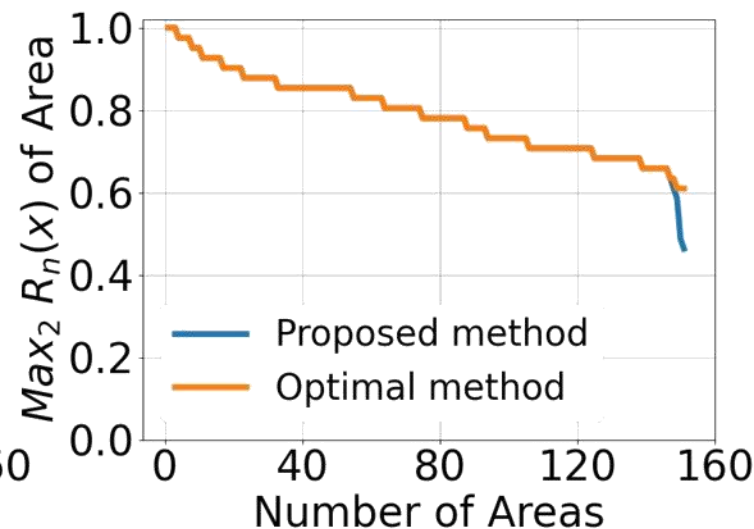
(d) Verio

有効性評価

- 図に、最適法の閾値を $T = 0.6$ に設定したときの、各方式で選択されたエリアの $Max_2 R_n(x)$ を降順に示す
- Allegiance Telecomで $T = 0.6$ の場合
 - 上位80個程度
 - 正しく抽出
 - 残る60個程度
 - 抽出精度が低下する傾向
 - $Max_2 R_n(x)$ が0.6以下のエリアに対しては誤検出が大きい
 - 複雑なネットワークトポロジ
 - ノード次数のみでは脆弱なエリアを特定することが難しい



(a) Allegiance Telecom



(b) At Home Network

抽出精度の定義

■ 尺度

■ FPR(false positive ratio)

■ $\text{Max}_2 R_n(x)$ が T 未満(抽出すべきでないエリア)の中で, 誤って抽出されたエリアの割合

■ FNR(false negative ratio)

■ $\text{Max}_2 R_n(x)$ が T 以上(抽出すべきエリア)の中で, 誤って抽出されなかったエリアの割合

抽出精度: Hub & Spoke(H&S)ネットワーク

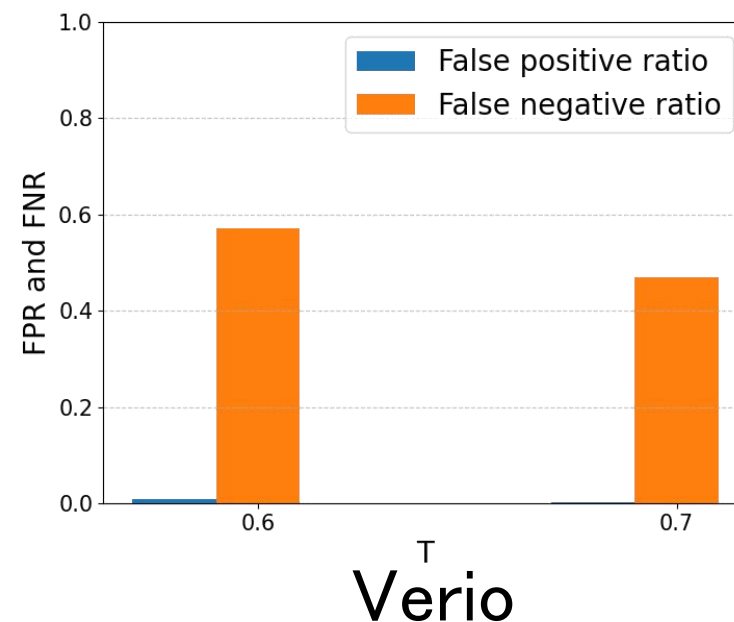
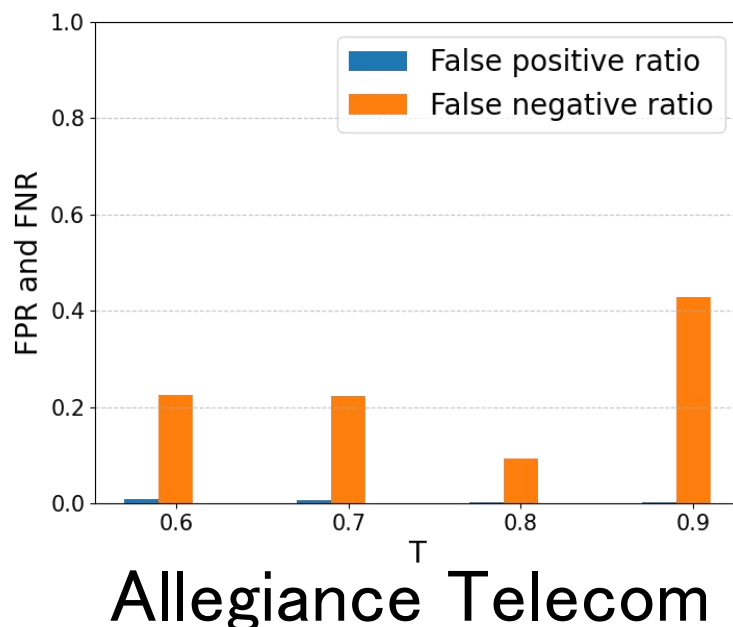
■ Allegiance TelecomとVerio

■ FNRが高い傾向

- 複雑なネットワークトポロジ: 提案アルゴリズムは多くのCFAに脆弱なエリアを見逃す

■ FPRは常に低くゼロに近い値

- 誤抽出する可能性が小さい



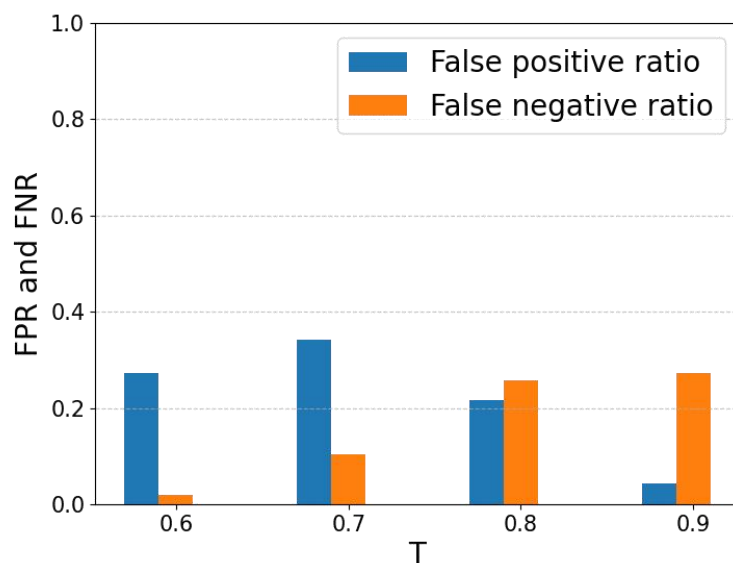
抽出精度: ladderネットワーク

■ At Home NetworkとCAIS Internet

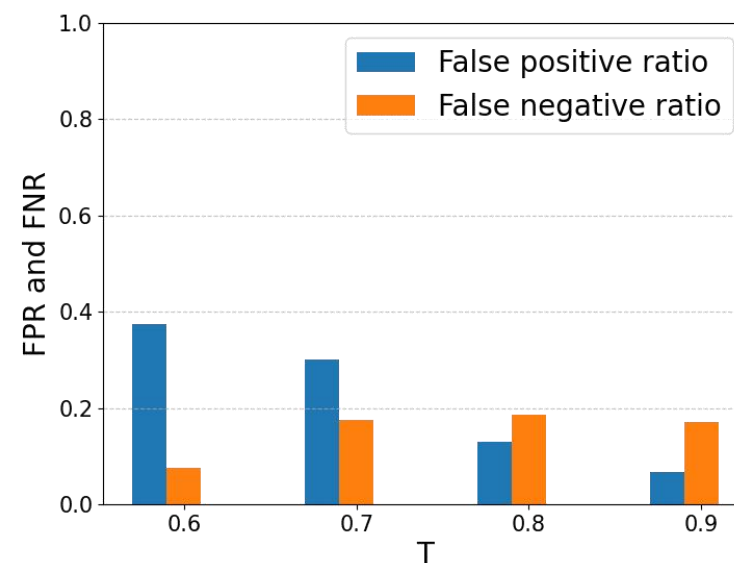
- FNRはH&Sと比較的低い

- FPRは $T = 0.6, 0.7$ のとき0.2以上

- 単純なネットワークトポロジでは, 提案アルゴリズムは条件を満たさないエリアを誤って選択する可能性が高い



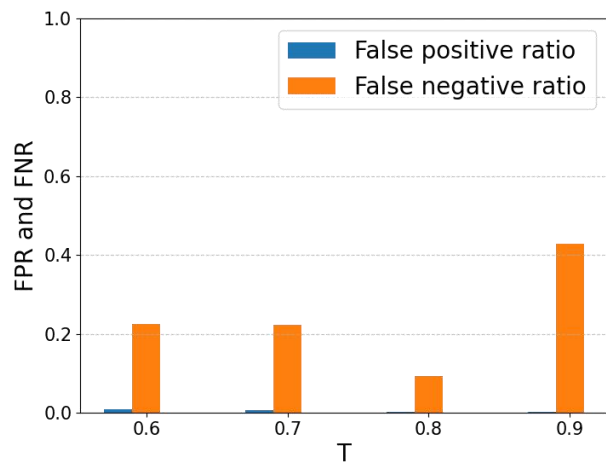
At Home Network



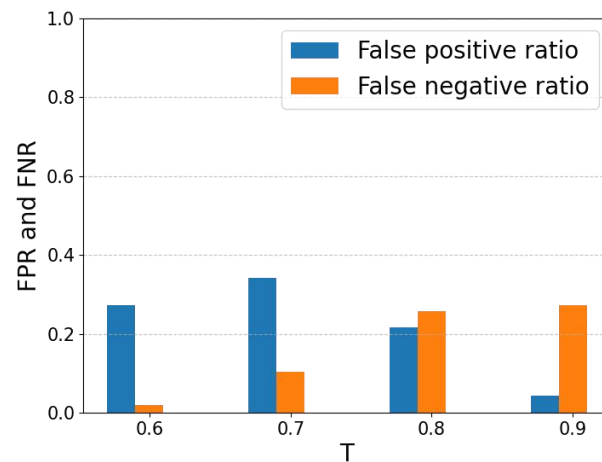
CAIS Internet

Tが精度に与える影響

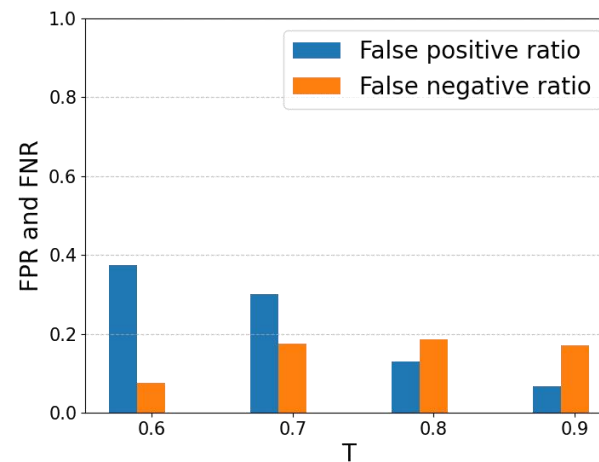
- 4つのトポロジのFPRが全体的に閾値 T の増加とともに減少する
 - $\text{Max}_2 R_n(x)$ の値が0.4~0.6の範囲で多くのエリアが存在
 - 小さな閾値 T の場合, 提案アルゴリズムはこれらのエリアを誤抽出する可能性が高い



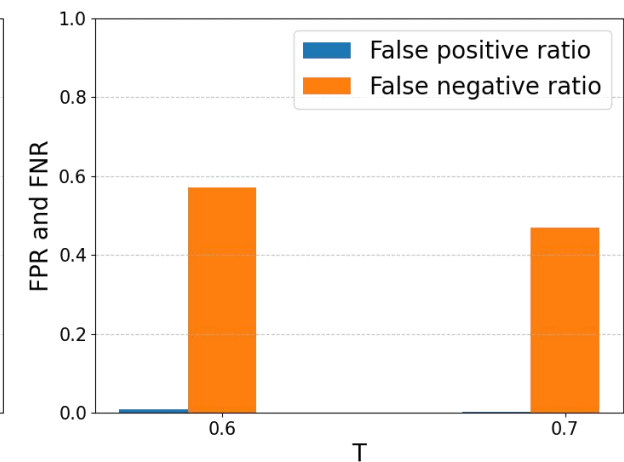
Allegiance Telecom



At Home Network



CAIS Internet



Verio

まとめ

- CFAに対して脆弱なエリアを測るための指標を定義
- 少ない計算量で脆弱エリア抽出アルゴリズムを提案
- 提案アルゴリズムがネットワークポロジのCFAに対し脆弱なエリアを高精度に抽出できる
- 今後の予定
 - ネットワークポロジの複雑さを表す新たな指標を導入
 - 複雑さの異なるネットワークポロジに対して異なる閾値を設定