クロスファイア攻撃のターゲットエリア選定法

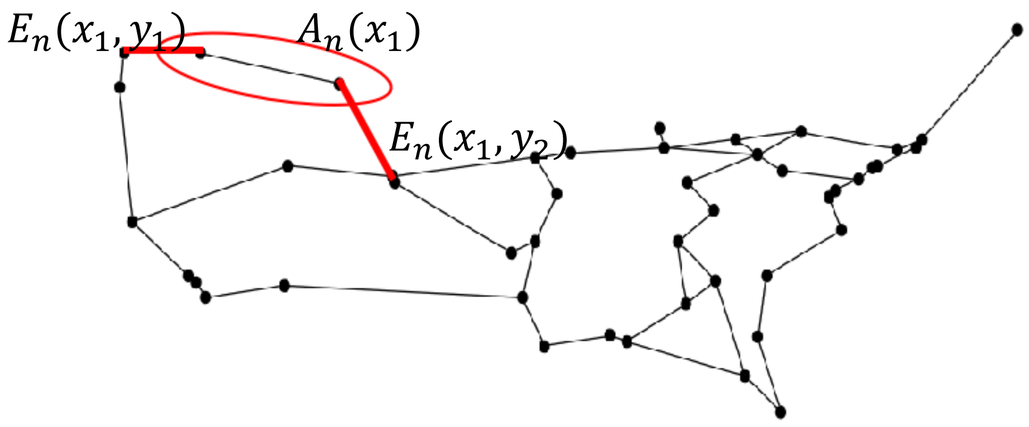
1. 背景

- 近年，Crossfire Attack（CFA）の問題が指摘されている
- CFAとは
  - DDoS攻撃の一つ
  - 攻撃の目標は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)と外部との通信を遮断し，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
  - CFA の発生を未然に防ぐ必要があり

既存のCFAの研究は，CFAに対して脆弱なエリアを事前に予測することができない

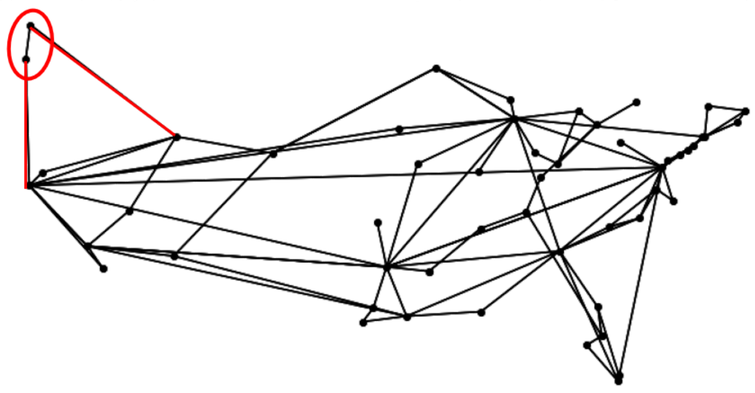
2. CFAの影響度の評価尺度

- CFAに対する脆弱性を測る尺度として以下の変数を定義
  - $A_n(x)$: 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

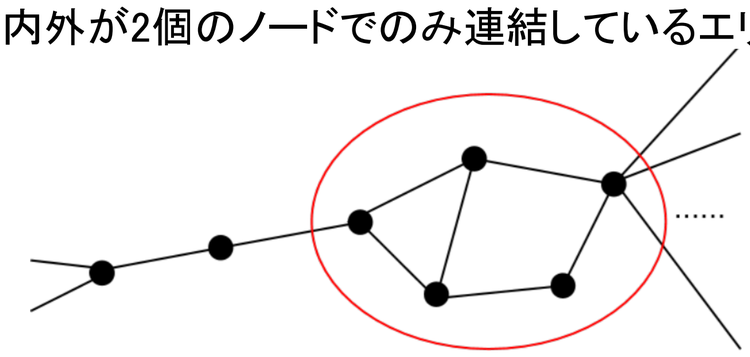


3. CFAに対して脆弱なエリア特徴

- 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



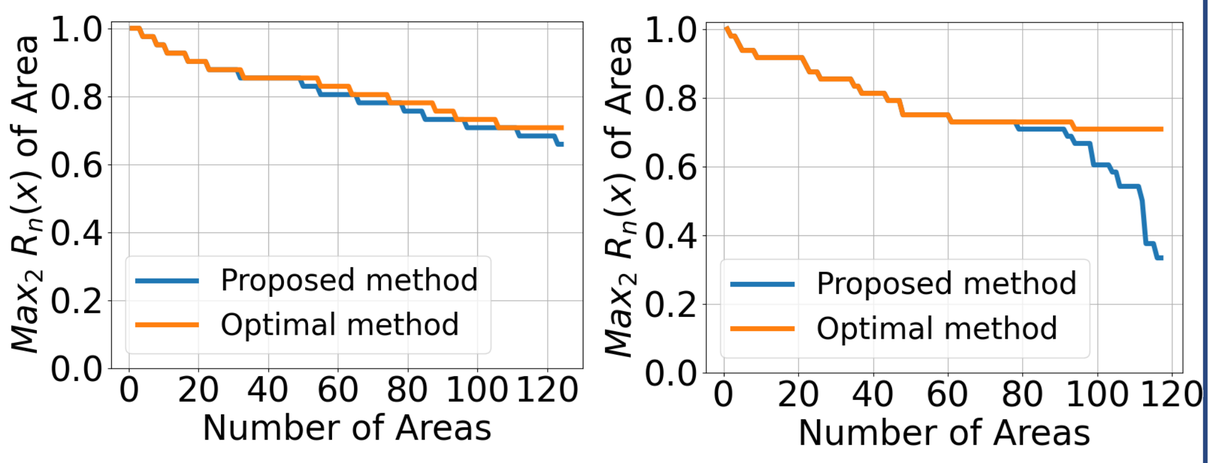
4. TA選択アルゴリズム

- 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を高次数ノードとして定義
- 提案アルゴリズムは以下の式に従って各エリアのスコア付けを行う：
  - エリアxのスコア = $S_1(x) + S_2(x) + S_3(x)$
    - $S_1(x)$: エリアxと隣接する直列構造の数
    - $S_2(x)$: エリアxと隣接する準直列構造の数
    - $S_3(x)$: エリアx内の高次数ノード数の逆数

5. 性能評価

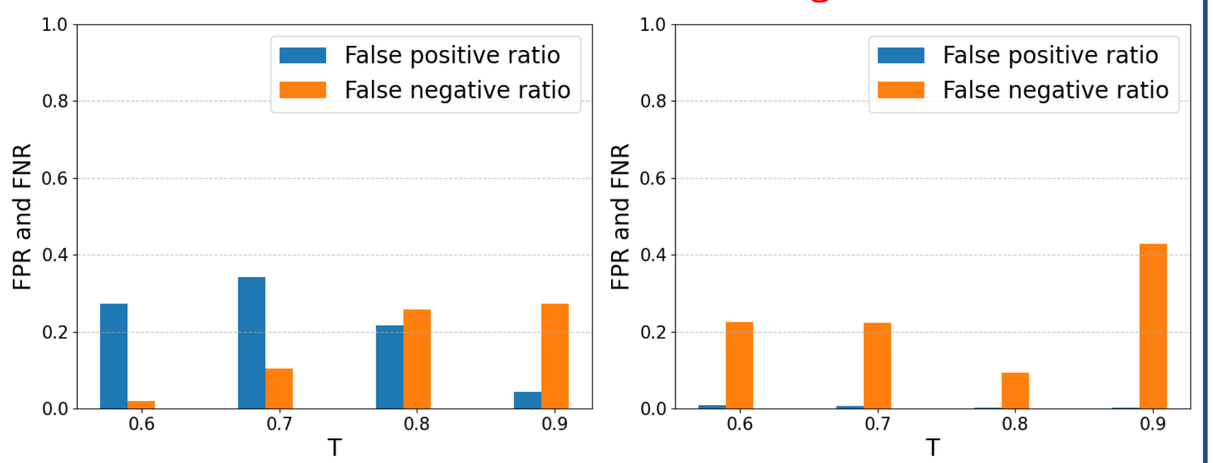
- 最適法
  - $Max_2\ R_n(x)$が任意に与えた閾値 T以上となるエリアを全て選択
  - 全てのノード間の最短ホップ経路を計算 → 計算量が大
- 提案アルゴリズム
  - スコア$S(x)$が大きな順に最適法と同じ個数のエリアを選択

At Home Network (T = 0.7)　　Allegiance Telecom (T = 0.7)



- 抽出精度
  - FPR(false positive ratio)
    - $Max_2\ R_n(x)$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)
    - $Max_2\ R_n(x)$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

At Home Network　　Allegiance Telecom



- 複雑なネットワークトポロジで，ノード次数のみでは脆弱なエリアとそれ以外のエリアを正しく区別することが難しい
- 提案アルゴリズムは$Max_2\ R_n(x)$が0.9以上といった特にCFAに対して脆弱なエリアを正確に識別