

GCNに基づくクロスファイア攻撃の ターゲットエリア選定法

王 天嶼, 上山 憲昭
立命館大学大学院情報理工研究科

2024/09/12

背景

- 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: ターゲットサーバエリアと外部とのネットワーク通信を中断
 - CFAに対して脆弱なエリアの予測アルゴリズムを提案した[1]
 - CFAを受けやすいネットワークポロジの脆弱なエリアを見つけることができる
- ⇒効率的、高精度な方法**存在しない**

目的と貢献

- GCN (graph convolutional network)
 - GNN (graph neural network) の一種
 - グラフ畳み込みを使用してグラフデータの空間的特徴を抽出[2]
- 目的
 - 複数のネットワークトポロジを対象に, GCNを用いて高精度予測モデルを設計
- 貢献
 - CFA に対する脆弱性を測る尺度として, 変数を定義
 - GCNを用いてトポロジ内のエリアの特徴を学習し, 学習モデルを設計

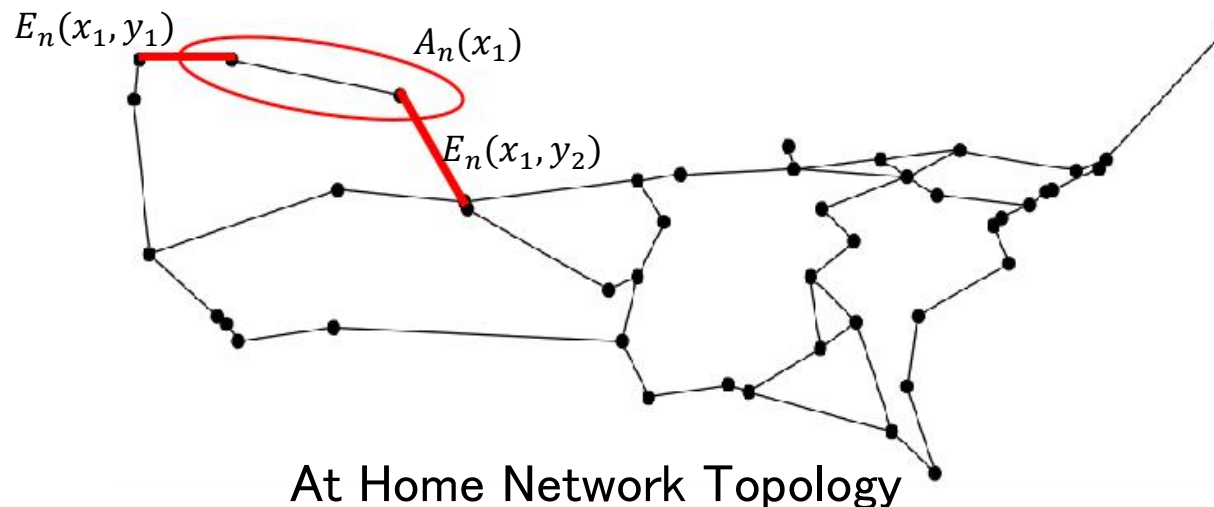
評価尺度

■ CFAの潜在的な影響度

- ターゲットエリア x 内と x 以外の領域を跨ぐリンクを 1 本や2 本削除した際に、エリア x の外部との間の通信不能となるトラフィックの割合

■ 変数

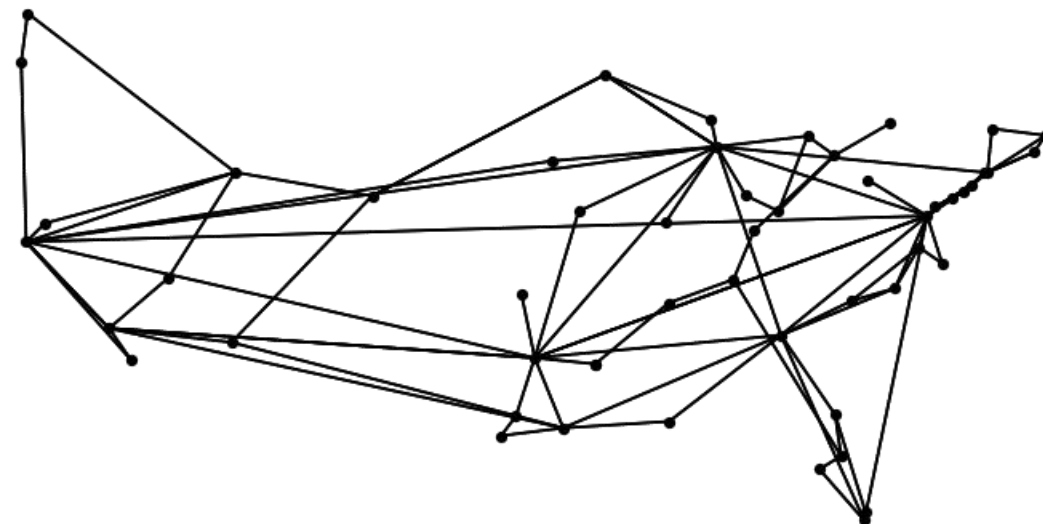
- $A_n(x)$: n 個の隣接ノードで構成される**エリア x**
- $E_n(x, y)$: 任意の $A_n(x)$ に対して, $A_n(x)$ と他エリアを跨る任意の**リンク y**
- $R_n(x, y)$: 任意の $A_n(x)$ 以外の任意のノードと $A_n(x)$ の間の最短ホップ経路のうち, リンク $E_n(x, y)$ を通る**割合**
- $Max_2 R_n(x)$: 任意の $A_n(x)$ に対して, $R_n(x, y)$ の最大値と 2 番目に大きな値との合計値



GCN学習モデル

■ 教師データセット

- Allegiance Telecom トポロジのノードとリンク
- ノード特徴
 - 次数中心性
 - 媒介中心性
 - 近接中心性
 - クラスタリング係数
- 5ノードのエリアとラベル(脆弱なエリアか否か)



Allegiance Telecom Topology
(hub-spoke network)

■ 損失関数

- CrossEntropyLoss (クロスエントロピー損失)

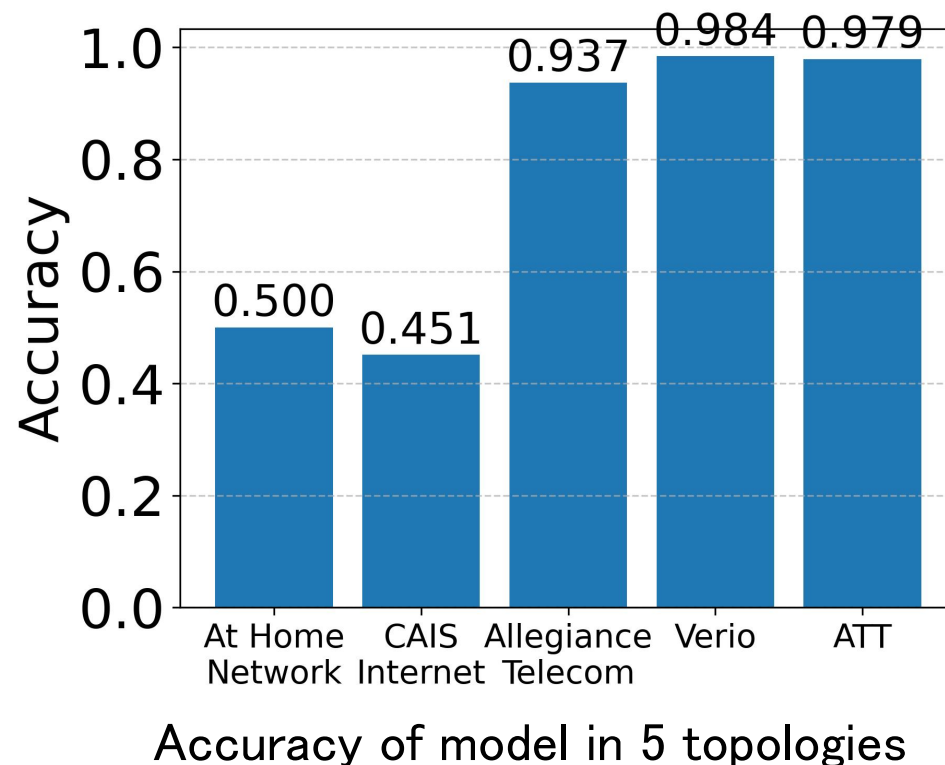
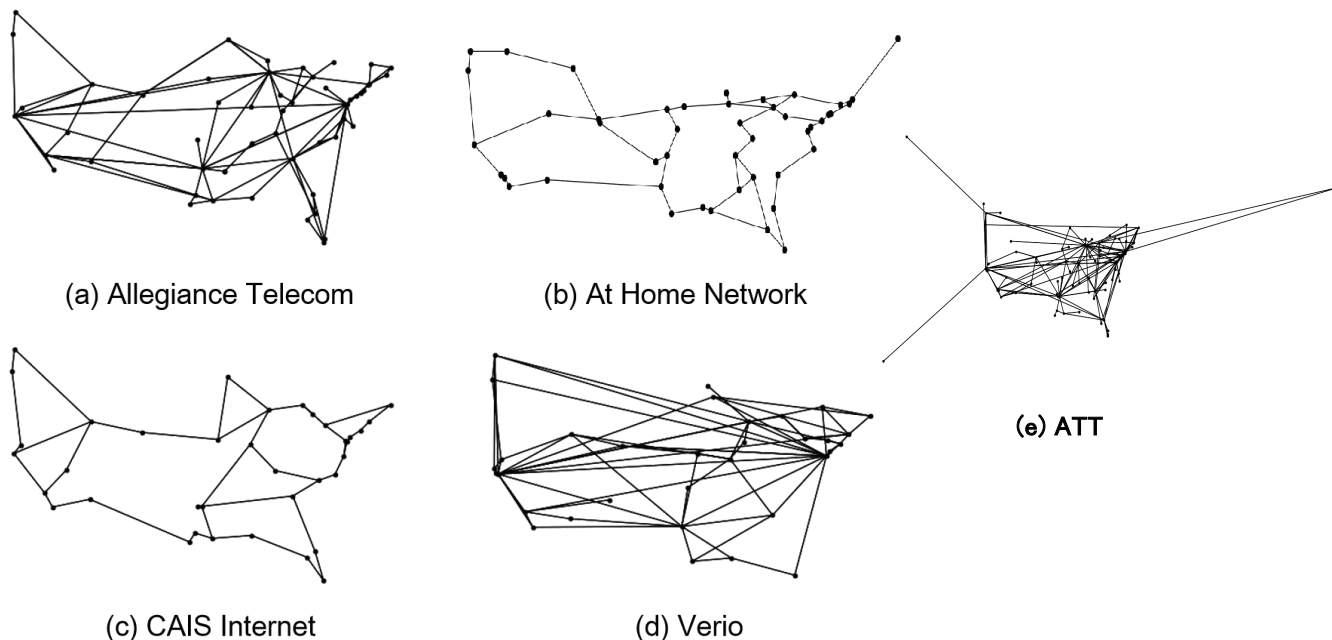
■ オプティマイザー

- Adam (アダム)

性能評価

- シミュレーションより
- Allegiance Telecom, ATT, Verioのhub-spokeネットワークでCFA攻撃に対して脆弱なエリアを正確に予測
 - hub-spoke ネットワークの構造に基づいて学習

- ladderネットワークでは, 予測精度が0.5以下
 - ノードの次数が低く, 均等に分布する傾向がある



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
- GCNを用いて予測モデルを訓練
- 予測モデル
 - hub-spokeネットワークの予測精度が0.9以上
 - ladderネットワークの予測精度が0.5以下
- 今後の予定
 - GCNの学習サンプルを増やし、より多様なトポロジに対応できる高精度な予測モデルを訓練