

クロスファイア攻撃に脆弱な トポロジ上の位置に関する分析

王 天嶼, 上山 憲昭
立命館大学大学院情報理工研究科

2023/09/15

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
- tracerouteの発生間隔に基づくクロスファイア攻撃ホストの検知法を提案した[1]
 - CFAに対して脆弱なリンクを予測し, 的確な防御策を展開するための手法
⇒存在しない

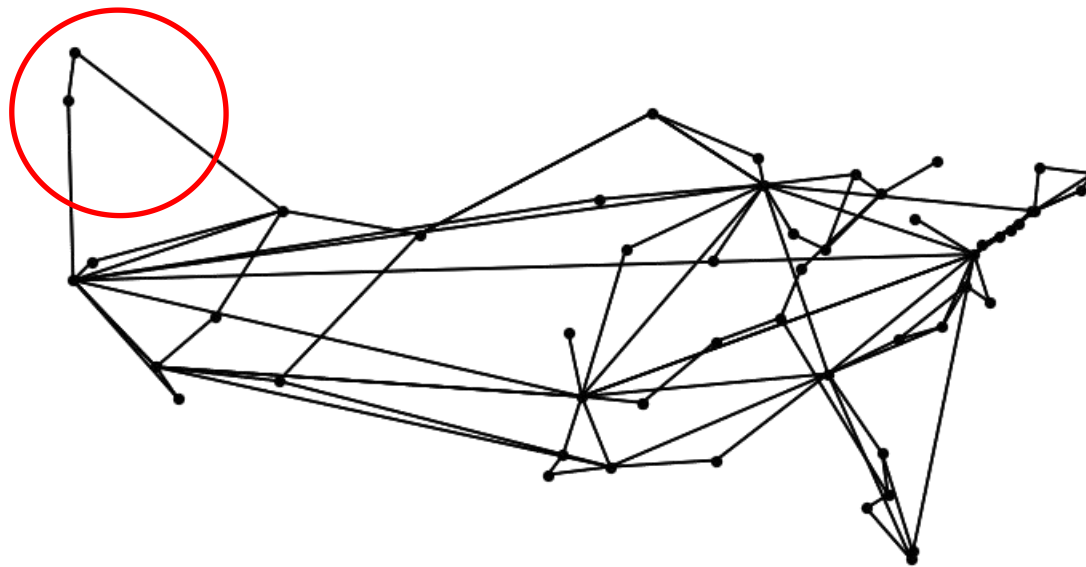
目的と貢献

■ 目的

- 複数のネットワークトポロジを対象に, CFAによる分断の影響度を定量的に分析

■ 貢献

- 直列構造がCFAの目標となりやすいことを明らかにする
 - 直列構造: 各ノードは前後の隣接ノードにのみ接続されている



Allegiance Telecom Topology

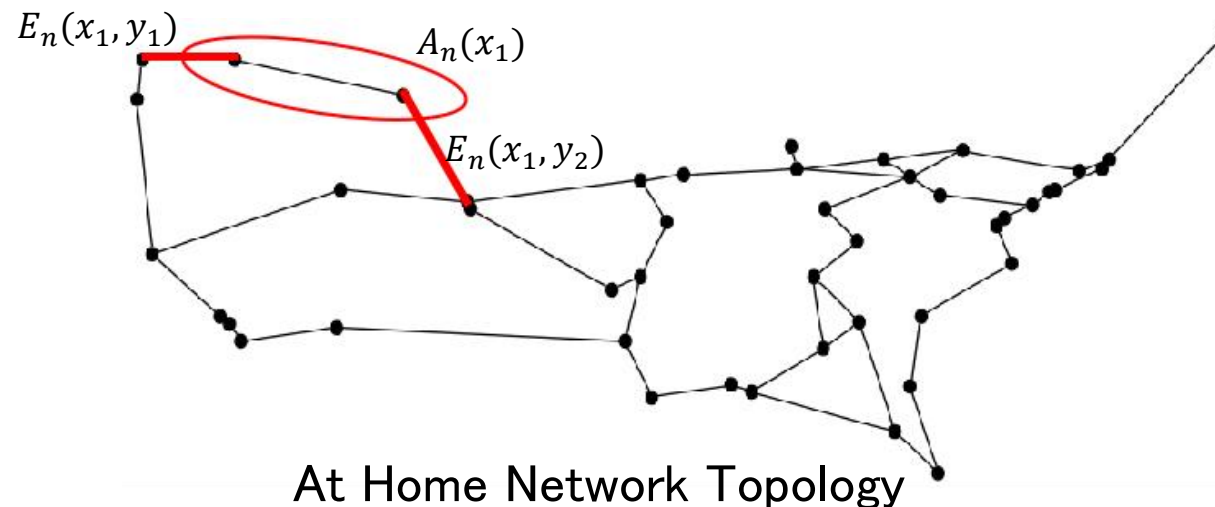
評価尺度

■ 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

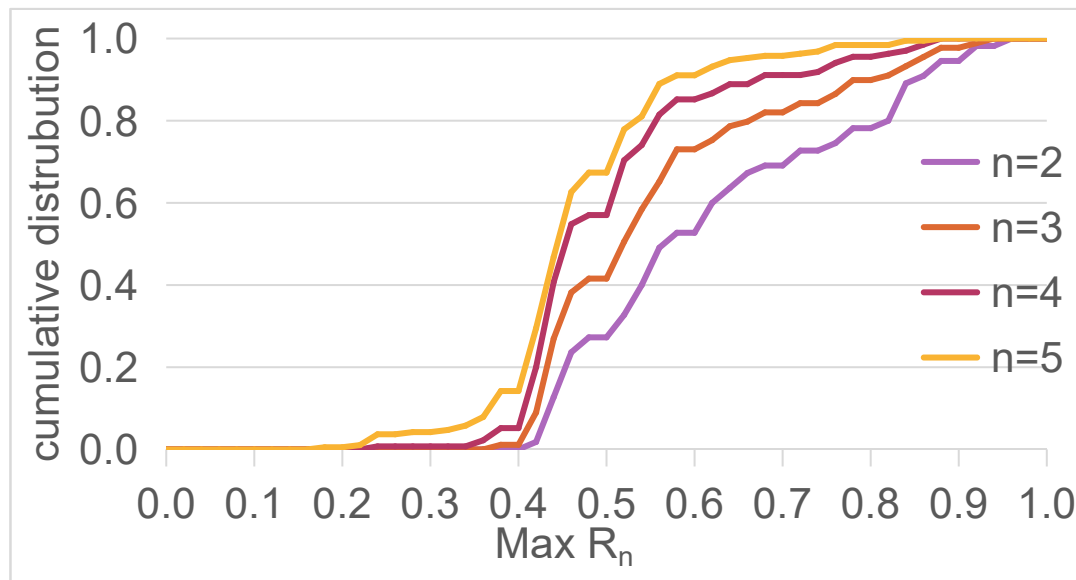
- $A_n(x)$: n 個の隣接ノードで構成される**エリア x**
- $E_n(x, y)$: 任意の $A_n(x)$ に対して, $A_n(x)$ と他エリアを跨る任意の**リンク y**
- $R_n(x, y)$: 任意の $A_n(x)$ 以外の任意のノードと $A_n(x)$ の間の最短ホップ経路のうち, リンク $E_n(x, y)$ を通る**割合**
- $Max R_n(x)$: 任意の $A_n(x)$ に対して, $R_n(x, y)$ の最大値



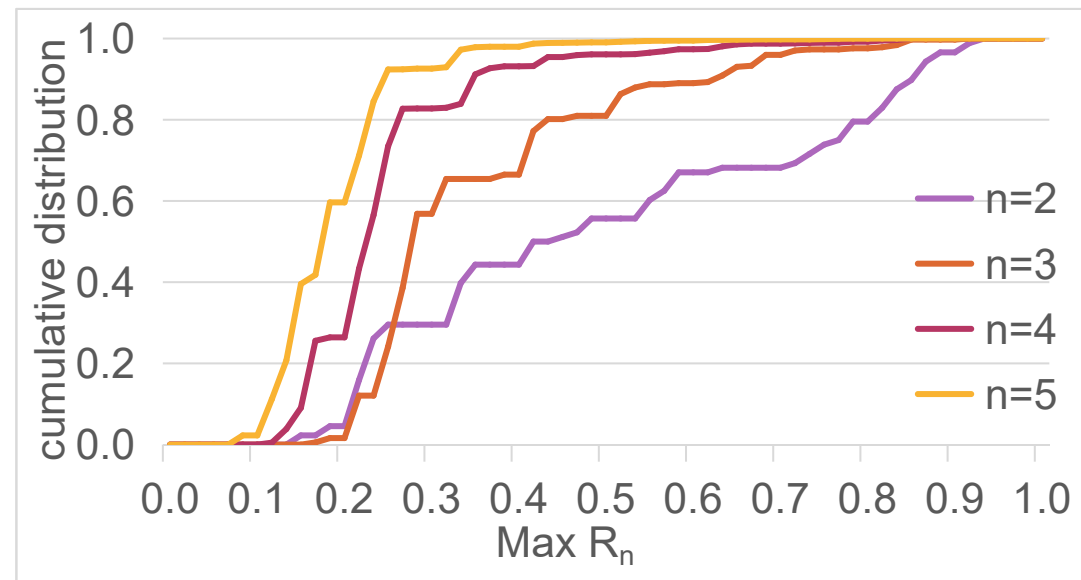
数値評価(1)

■ 累積分布

- 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



At Home Network



Allegiance Telecom

- n の増加に伴い, $Max R_n(x)$ の分布はより値の小さいものに集中
- トラフィックが各境界リンクに分散される度合いが大きい
- より低いコストで攻撃を達成する可能⇒少ないノードを含むエリアを攻撃

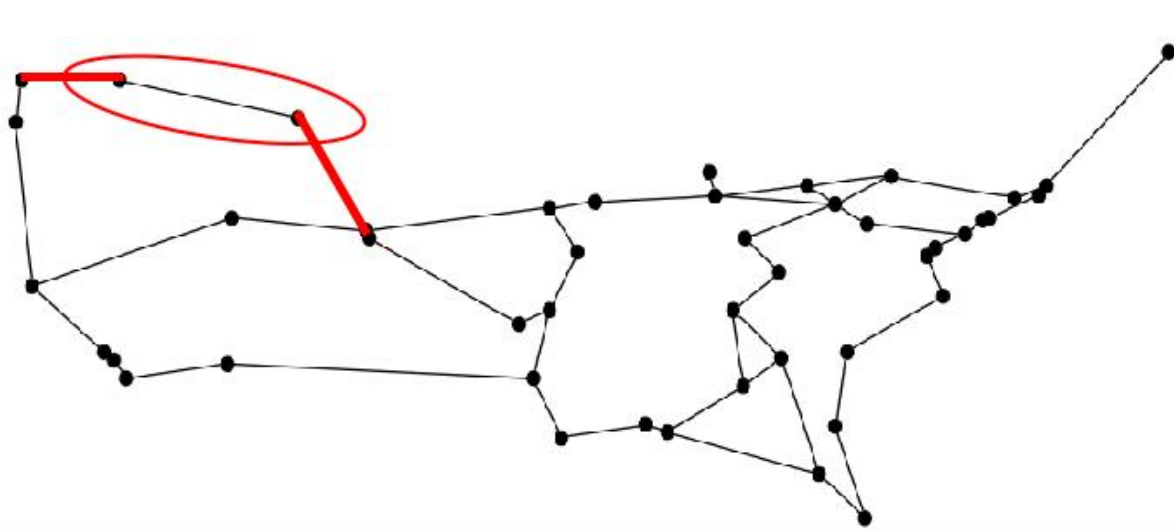
数値評価(2)

■ $Max R_n(x)$ が90%を超えるエリア

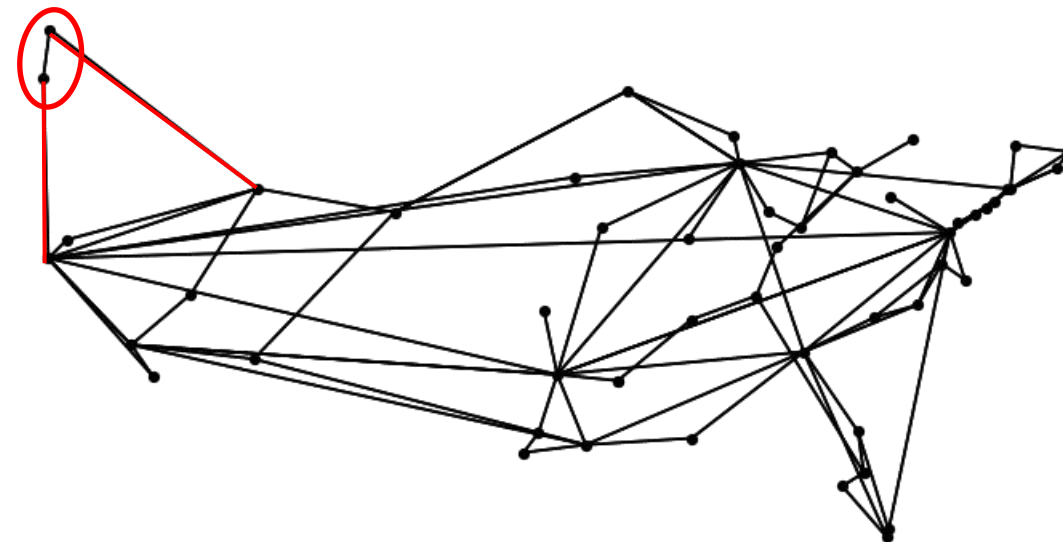
- 攻撃者はこのようなエリアを攻撃ターゲットとした場合
⇒ターゲットエリアに対する疎通性を容易に遮断

■ 直列構造

- エリアへのリンクは2~3本しかなく, トラフィックがそのうちの1本のリンクを通して送信される場合が非常に多い
- n が大きくなる⇒ターゲットエリア内に含まれるノード数が増加, 直列の部分が減少



At Home Network Topology



Allegiance Telecom Topology

まとめ

- CFA攻撃者はエリア間のトラフィックの多くが通過するリンクを目標と選定
- CFA攻撃者はより低いコストで攻撃を達成
⇒より少ないノードを含むエリアを攻撃
- 直列構造はネットワークのトポロジにおいて相対的に脆弱な部分
⇒容易にCFAの対象となる
- 今後の予定
 - $Max R_n(x)$ だけではなく, 複数の変数によってネットワークトポロジを分析
 - 攻撃者が目標を選定するパターンに基づき, 攻撃アルゴリズムを構築