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

Analysis of vulnerable topological location against crossfire attacks

王　天嶼
Wang Tianyu

上山　憲昭
Noriaki Kamiyama

立命館大学大学院情報理工研究科
Graduate School of Information Science and Engineering, Ritsumeikan University

立命館大学情報理工学部
Collage of Information Science and Engineering, Ritsumeikan University

1　はじめに

一般的な DDoS 攻撃とは異なり，Crossfire Attack（CFA）はサーバではなくネットワーク内のリンクを目標として攻撃し，目標サーバエリアと外部とのネットワーク通信を中断することを目的とする．筆者らはこれまでに，CFA に先立ち攻撃者がターゲットリンクを選定するため大量の traceroute を行うことに着目し，traceroute の発生間隔に基づく攻撃ホストの検知法を提案した [1]．しかし 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はまだ存在しない．そこで本稿では，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する．そして直列構造が CFA 攻撃の目標となりやすいことを明らかにする．

2　CFA の潜在的な影響度の評価尺度

CFA の攻撃者は少量のトラフィックを大量の Bot からターゲットエリア周辺のデコイサーバ間で転送することで，目標エリア周辺に存在するリンクを高負荷にすることで，ターゲットエリアとそれ以外のエリア間のトラヒック流通を妨害する．そのため，攻撃者はより多くのこれら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する．そのためネットワークの隣接する複数のノードを CFA のターゲットエリア x としたときに，x と x 以外の領域とを跨ぐリンクの 1 本や 2 本を削除したときに，x の外部との間のトラヒック量のうち通信不能となるものの割合を評価する．そのため以下の変数を定義する．

(i) $A_n(x)$: n 個の隣接ノードで構成されるエリア x

(ii) $E_n(x,y)$: 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

(iii) $R_n(x,y)$: 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

(iv) Max $R_n(x)$: 任意の $A_n(x)$ に対して，$R_n(x,y)$ の最大値

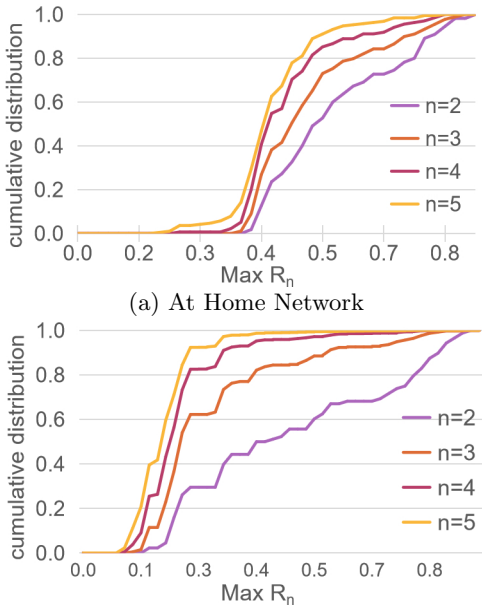
各 $A_n(x)$ には対応する Max $R_n(x)$ が存在し，CFA の攻撃者は $A_n(x)$ の CFA を行う際に，このリンクを攻撃対象としてい選択することで，最も効率的・効果的に CFA を行うことが可能となる．そのため本稿では本尺度を CFA の潜在的な影響度合いを評価する尺度に用いる．

3　数値評価

米国の商用バックボーン ISP である At Home Network と Allegiance Telecom のネットワークトポロジを評価に用いる．

図 1 に，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 $R_n(x)$ の累積分布を示す．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する．すなわちターゲットエリアに至る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くなる．そのため CFA 攻撃者はより低いコストで攻撃を達成するためには，より少ないノードを含むエリアを攻撃する必要がある．

また両方のネットワークトポロジにおいて，Max $R_n(x)$ が 90% を超えるエリアが存在する．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，対応する $R_n(x,y)$ が大きいリンクを攻撃対象とすることで，ターゲットエリアに対する疎通性を比較的容易に遮断することができる．図 1(a) の Max $R_n(x)$ が 90% を超えるエリアを図 2 に赤色で示すが，本エリアは複数のノードが直列に接続した構造であることがわかる．直列構造では，各ノードは前後の隣接ノードにのみ接続されているためである．すなわちターゲットエリアが直列構造にある場合，その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 本のリンクを通って送信される場合が非常に多いためである．一方で n が大きくなると，ターゲットエリア内に含まれるノード数が増え，直列の部分が少なくなるため，Max $R_n(x)$ は減少する．したがって，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であり，容易に CFA の対象となる．



(a) At Home Network

(b) Allegiance Telecom

図 1: Cumulative distribution of Max $R_n(x)$

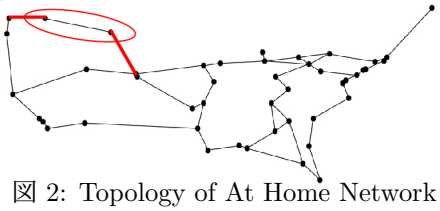


図 2: Topology of At Home Network

謝辞

本研究成果は JSPS 科研費 21H03437 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] Manami Nakahara and Noriaki Kamiyama, “Detecting Crossfire-Attack Hosts in Search Phase,” APNOMS 2022 (Poster Session)