クロスファイア攻撃のターゲットエリア選定法

Target area selection method for 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

DDoS（Distributed Denial of Service）攻撃とは，大量のデータパケットやリクエストを対象サーバに送信し，そのサーバを過負荷にさせてネットワークサービスを利用不能にする行為である．一般的な DDoS 攻撃とは異なり，Crossfire Attack（CFA）の主な特徴は，攻撃の目標がサーバではなく，ネットワーク内のリンクである．目標サーバエリア外のリンクに過負荷をかけることで，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 [1] を含め既存の CFA の研究は，主に準備や攻撃段階における CFA を検出することを目的としており，CFA に対して脆弱なエリアを事前に予測し，重点的な設備投資などで事前に CFA に備える研究は見られない．そこで筆者らはこれまでに，CFA に対して脆弱なトポロジ上の部位を予測するため，CFA に対しての脆弱性を測る尺度を提案した [2]．本稿では，将来攻撃され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することを目的として，CFA の TA の高速で効率的な選択アルゴリズムを提案する．そして提案アルゴリズムで選択されたエリアと理想的なエリア選択とを比較することで，提案アルゴリズムの性能を評価し，TA 選択アルゴリズムの精度を検証する．アルゴリズムにより脆弱なエリアを特定することで，将来的にはこれらのエリアに対する防御をより効果的に展開することを目指す．

2　CFA の影響度の評価尺度

CFA の攻撃者は少量のトラフィックを大量の Bot から TA 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し，TA 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 TA と外部とののトラフィックの多くが通過するリンクを攻撃目標として選定する．ネットワークの隣接する複数のノードを CFA の TA x としたときに，x と x 以外の領域とを跨ぐ少数のリンクを削除したときに，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が高いエリア x ほど，CFA に対して脆弱なエリアと考えられる．そのため著者らは [2] で，CFA に対する脆弱性を測る尺度として，以下の変数を定義した．

(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) $R_n(x,y)$: $A_n(x)$ 以外の任意のノードと，$A_n(x)$ の任意のノードとの間の最短ホップ経路のうち，リンク $E_n(x,y)$ を通るものの割合

(iv) Max $R_n(x)$: $R_n(x,y)$ の最大値

ただし CFA では $A_n(x)$ に隣接しないリンクを攻撃対象とすることも考えられるが，本稿では便宜上，$A_n(x)$ と外部のエリアとの境界に存在するリンクを攻撃対象の候補として考える．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．実際の攻撃では，攻撃者は単一のリンクを選択だけではなく，複数のリンクを選択して攻撃することを考慮し，本稿ではさらに以下の変数を定義する．

(v) $Max_2\ R_n(x)$: $R_n(x,y)$ の最大値と 2 番目に大きな値との最大値

3　TA 選択アルゴリズム

本稿ではトポロジの特徴に基づいて CFA に対して脆弱な TA を抽出するアルゴリズムを提案する．多くの場合，CFA の TA は多くのノードを含まないため，本稿では TA を 5 つの隣接ノードから構成されるエリアと仮定する．理想的には，トポロジ上の隣接する 5 つの全てのエリア x について $Max_2\ R_n(x)$ を計算し，その値が与えられた閾値 T より大きな全てのエリアを抽出できればよい (理想法)．しかし $Max_2\ R_n(x)$ の計算には全てのノード間の最短ホップ経路が必要であるため，ノード数が多い大規模ネットワークでは計算量が大きくなる．そこで，より少ない計算量で効果的に $Max_2\ R_n(x)$ が大きなエリアを抽出するアルゴリズムを検討する．

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する．TA 内の高次数ノード数の増加に伴い，TA 内のノードの平均次数は増加し，TA と外部との接続リンク数が増加する．そのため TA 外から TA 内に送信されるトラフィックは多数のリンクに分散しやすくなり，$Max\ R_n(x)$ や $Max_2\ R_n(x)$ は減少する．したがって，TA 内の高次数ノードの数が少ないほど TA は CFA に対して脆弱になる．

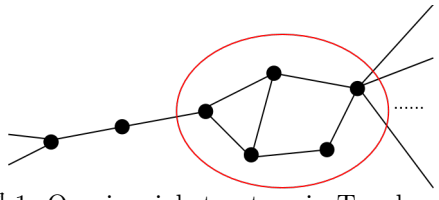


図 1: Quasi-serial structure in Topology of Allegiance Telecom

また筆者らはこれまでに，次数が 2 のノードが直列に連結した直列構造となったエリアの $Max_2\ R_n(x)$ が大

きなことを発見している [2]．本稿の選択アルゴリズムでは，直列構造に加えて准直列構造の判定を追加する．ただし准直列構造を次数が 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と定義する．Allegiance Telecom の一部のエリアを図 1 に示すが，赤色で示すエリアが准直列構造である．

これらの特徴から，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 CFA に対して脆弱なエリアとして抽出する．

$$S(x) = s_1(x) + s_2(x) + s_3(x) \quad (1)$$

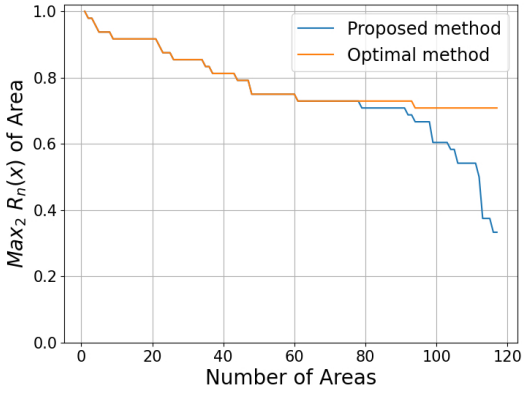
ただし $s_1(x)$，$s_2(x)$，$s_3(x)$ を以下のように定義する．

(i) $s_1(x)$: エリア x と隣接する直列構造の数

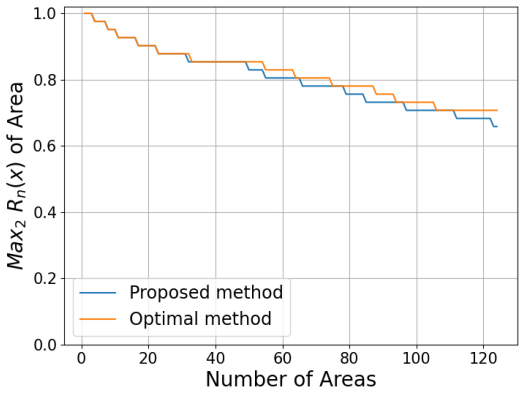
(ii) $s_2(x)$: エリア x と隣接する準直列構造の数

(iii) $s_3(x)$: エリア x 内の高次数ノード数の逆数

提案アルゴリズムは各ノードの次数のみで計算できるため，最適法と比較して計算時間を大幅に低減することが可能である．



(a) Allegiance Telecom

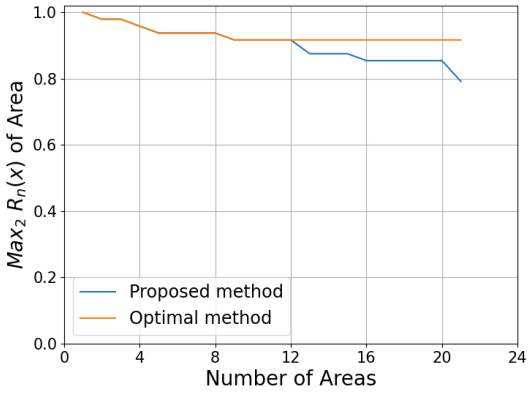


(b) At Home Network

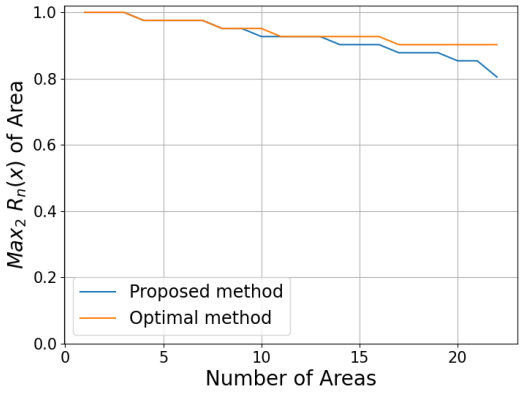
図 2: $Max_2\ R_n(x)$ of each area selected by each method in descending order when setting $T = 0.7$

4 性能評価

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．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することで提案アルゴリズムの有効性を確認する．ただし提案アルゴリズムではスコア $S(x)$ が大きな順に，最適法で発見された個数と同じ個数のエリアを選択した．図 2 に，最適法の閾値を $T = 0.7$ に設定したときの，各方式で選択されたエリアの $Max_2\ R_n(x)$ を値を降順にプロットする．同様に図 3 に最適法の閾値を $T = 0.9$ に設定した場合の結果を示す．



(a) Allegiance Telecom



(b) At Home Network

図 3: $Max_2\ R_n(x)$ of each area selected by each method in descending order when setting $T = 0.9$

図 2(a) に示すように Allegiance Telecom で $T = 0.7$ の場合，上位 80 個程度の $Max_2\ R_n(x)$ の値が大きなエリアは提案方式で正しく抽出できるが，残る 40 個程度のエリアについては抽出精度が低下する傾向がある．これは Allegiance Telecom のような複雑なネットワークトポロジで，特に $Max_2\ R_n(x)$ の値が 0.8 程度未満の場合，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ためである．しかし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する．

謝辞 本研究成果は JSPS 科研費 21H03436 と 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)

[2] 王 天嶼，上山 憲昭, 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, 信学会 2023 年ソ大会, B-6-57