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

Target area selection method for crossfire attacks based on GCN

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に対して脆弱なトポロジ上の部位を予測することに着目し，CFAに対しての脆弱性を測る尺度を提案した (1)．しかし一部の条件においては十分な予測精度を達成できない．そこで本稿では，GCN (graph convolutional network) を用いてトポロジ内のエリアの特徴を学習し，畳み込みを繰り返すことでエリアのトポロジ上の特徴に基づき高精度かつ効率的にCFAに脆弱なエリアを推定する方法を提案する．GCNはグラフ畳み込みを行う複数の層から構成され，その基本的な目的は，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することである (2)．

そして提案学習モデルの性能を評価し，予測アルゴリズムの精度を検証する．提案アルゴリズムによりCFAに対し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行うことを目指す．

2　CFAの影響度の評価尺度

CFAの攻撃者は通信量が多いリンクを攻撃目標として選定する．ネットワーク内の複数のノードをCFAのTA x としたときに，x をつなぐ少数のリンクを削除すると，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 [1] 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

(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合計値

本稿ではCFAに対するエリアの脆弱性の評価指標として $Max_2\ R_n(x)$ を用いる．

3　学習モデル

教師データセットは，トポロジ内のノード情報とノード関係から構成される．ノード情報には，各ノードの4つの固有値（次数中心性，媒介中心性，近接中心性，クラスタリング係数）が含まれる．このデータセットに基づいて，5つの隣接ノードからなるすべてのエリアサンプルに，脆弱なエリアか否かのラベルを付ける． あるエリアがCFA攻撃に対して脆弱かどうかは，そのエリアの $Max_2\ R_n(x)$ の値によって決定される．

CrossEntropyLossを損失関数として，Adamをオプティマイザーとして選択する． そして，学習モデルを得るために，hub-spokeネットワークであるAllegiance Telecomを学習用教師データセットとして用いる．

4　性能評価

米国の商用バックボーンISPであるVerio，ATT，Allegiance Telecom，At Home Network，CAIS Internetの5つのネットワークのトポロジを評価に用いる．

図1に示すように，予測モデルがVerio，ATT，Allegiance Telecomのhub-spokeネットワークでで CFA攻撃に対して脆弱なエリアを正確に予測できることがわかる．一方，At Home NetworkやCAIS Internetなどのladderネットワークでは，予測精度が0.5以下にとどまる．これは，モデルがhub-spokeネットワークの構造に基づいて学習しているためであり，両者のネットワーク構造の違いが原因である．ladderネットワークはノードの次数が低く，均等に分布する傾向があるが，hub-spokeネットワークはノードの分布がべき乗分布になる．これにより，予測モデルの精度に大きな差が生じる．

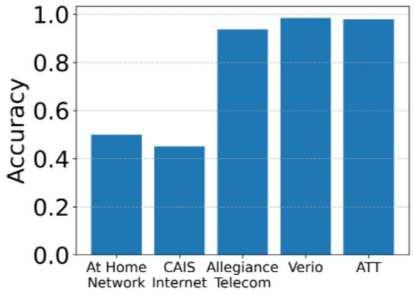

図 1: Accuracy of model in 5 topologies

謝辞　本研究成果はJSPS科研費23K21664と23K21665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] 王　天嶼, 上山 憲昭, クロスファイア攻撃に対して脆弱なエリアの選定法, NS研究会, NS2023-195, 沖縄, 2024年2月

[2] Max Welling and Thomas N. Kipf, Semi-supervised classification with graph convolutional networks, J. ICLR 2017, 2016.