GCN を用いた Fake 型 CPA に対する脆弱ノード検出法

Vulnerable Node Detection Method for Fake-type CPA of ICN using GCN

上野 優衣　　上山 憲昭
Yui Ueno　　Noriaki Kamiyama
立命館大学 情報理工学部
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

コンテンツ名を用いてパケットを転送するネットワーク (NW) である情報指向ネットワーク (ICN) が研究されている．しかし，悪意を持ったユーザが不当なコンテンツをルータにキャッシュさせることで，キャッシュヒット率を低下させるコンテンツポイズニング攻撃 (CPA: content poisoning attack) が指摘されている [1]. 既存研究では，攻撃者が自身でオリジナルの無意味なコンテンツを生成し，bot から無意味なコンテンツを要求しキャッシュさせる独自 Fake 型攻撃が NW に与える脅威が分析されている [2]．本稿では，独自 Fake 型攻撃に対して脆弱なノードの GCN (graph convolusional neural network) を用いた検出法を提案する．

2. 提案手法

従来のニューラルネットワークが画像やテキストを学習するモデルであるのに対し，グラフニューラルネットワーク (GNN: graph neural network) はグラフ構造データを学習させる機械学習モデルである．GNN の中でも代表的な，近傍ノードの特徴量を畳み込みながら学習させる手法であるグラフ畳み込みニューラルネットワーク (GCN) を用いることで，ノードのクラス分類が可能である．ノードのクラス分類は，グラフ，全ノードのそれぞれの特徴量，一部のノードが属するクラス（ラベル）が入力として与えられた際に，ラベルが未判明であるノードのラベルを予測する．

GCN のラベルに，各ノードのキャッシュにおける Fake コンテンツの平均注入率（AIRF: average injection ratio of fake content）を使用する．これにより，Fake コンテンツが注入される可能性のある脆弱なノードを推測する．AIRF を算出するには，各ノードのキャッシュを全て確認し，キャッシュされている Fake コンテンツの数を調べる必要がある．そのため，少ない正解ラベルから脆弱なノードを効率よく推測できることが望ましい．また，全ノードの特徴量として，ネットワーク内で人気の高い上位 5 つのコンテンツについて，各ノードにおけるキャッシュヒット率を利用する．

3. 性能評価

計算機シミュレーションによって，GCN で使用する特徴量とラベルを作成する．シミュレータには，米国の商用 ISP のバックボーン NW トポロジである At Home Network を使用する．キャッシュは転送経路上の全てのルータでキャッシュを行い，キャッシュ容量は 100 とする．正当コンテンツ数は $M = 10,000$ とし，Fake コンテンツ数は $F = 1,024$ とする．正常ユーザは $\theta = 0.8$ の Zipf 分布に従い正当コンテンツを要求し，Bot は全体要求比率の 50%の割合で Fake コンテンツを要求する．シミュレーション時間は 10,000 秒とし，1,000 秒に 1 回，各ノードの Fake コンテンツの注入率を測定し，測定した 10 回の平均値を AIRF とする．

本稿では，各ラベルがなるべく均等な数になるよう教師データをランダムに選択して GCN を学習する．教師データを与える数を 3 から 6 に変化させたときの，偽陰性率 (FNR: false negative rate)，偽陽性率 (FPR: false positive rate)，精度を表 1 に示す．ただし FNR はラベル 1 ($AIRF > 0$) のノードを誤ってラベル 0 ($AIRF = 0$) と判定する割合で，FPR はラベル 0 のノードを誤ってラベル 1 と判定する割合である．また精度を次式で定義する．

$$\text{精度} = \frac{TP + TN}{TP + FP + TN + FN}$$

ただし，TP(TN) をラベル 0(1) のノードを正しく判定した数とし，FP(FN) をラベル 0(1) のノードを誤って判定した数とする．

与える教師データ数が 4 個以下のときは精度が低いが，教師データ数が 5 個以上になると FPR が低下し精度が 70%以上に上昇している．シミュレーションに使用している At Home Network は全体のノード数が 46 の NW である．このことから NW 全体のうち約 10%以上の正解ラベルを与えることで高い精度での予測が可能であると推測される．

表 1: GCN の予測精度

教師データ数	FNR	FPR	精度
3	0.3684	0.7500	0.4186
4	0.1111	0.8750	0.4524
5	0.2778	0.2609	0.7317
6	0.2353	0.3478	0.7000

図 1 は，シミュレータで作成した正解ラベルをラベルごとに色付けしてトポロジを出力したものである．また図 2 は，表 1 の中で最も精度の良かった教師データ数が 5 の場合の予測ラベルを同様に出力したものである．GCN は近傍ノードの特徴量を畳み込み学習する性質上，与えられる教師データの位置が予測精度に与える影響は大きい．

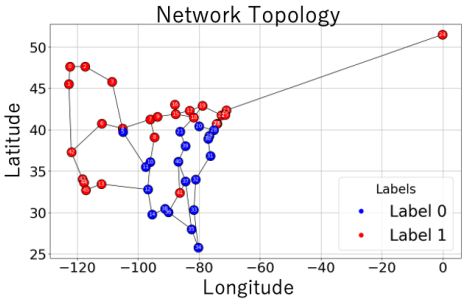

図 1: 正解ラベルトポロジ

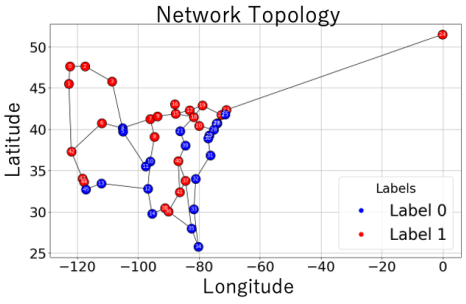

図 2: 予測ラベルトポロジ

謝辞

本研究成果は JSPS 科研費 23K11086, 23K21664, 23K28078 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] T. Nguyen, et al., Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment, IM2017, 2017.

[2] Noriaki Kamiyama and Takuto Kudo, Investigating Impact of Fake-Type Content Poisoning Attack on NDN, GRASEC 2023

Copyright © 2025 IEICE