ネットワークトポロジがコンテンツポイズニング攻撃に与える影響の分析

Investigating Influence of Network Topology on Content Poisoning Attack

工藤 多空飛[1]　　上山 憲昭[2]
Takuto Kudo　　Noriaki Kamiyama
福岡大学大学院 工学研究科 電子情報工学専攻[1]
Graduate School of Engineering, Fukuoka University
立命館大学 情報理工学部[2]
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

コンテンツの名称でデータ通信を行い，コンテンツ配信を効率的に行うネットワーク (NW) アーキテクチャとして情報指向ネットワーク (ICN: information-centric networking) が注目を集めている．しかし，悪意を持ったユーザが不当なコンテンツを NW に展開することでキャッシュの効果を低下させるコンテンツポイズニング攻撃 (CPA: content poisoning attack) の問題が指摘されている [1]．CPA には，独自に作成した fake コンテンツを結託ユーザから要求する独自 fake 型，実在コンテンツの fake データをオリジナルとして配信する詐称 fake 型，ユーザの要求直後に fake データを配信する自然 corrupted 型，結託ユーザから実在コンテンツの fake を要求し配信する結託 corrupted 型が存在する [2]．CPA に対する対処法を確立するには，CPA が NW の性能に与える影響を明らかにする必要があるが，既存研究はその多くが小規模な NW トポロジや限定された攻撃者の位置のみで評価を行っている [1]．そこで文献 [2] では fake 型 CPA がキャッシュヒット率に与える影響分析を，文献 [3] では ICN のキャッシュ方式が独自 fake 型 CPA の脅威に与える影響を評価した．本稿では，NW トポロジが独自 fake 型 CPA の脅威に与える影響を分析する．

2. 独自 fake 型 CPA の攻撃者配置方式

fake コンテンツの配置方法として，以下の二つを想定する [3]．
AVH: 他のノードに至る平均ホップ長が最大となるノードに配置
BC: Betweenness Centrality が最大のノードに配置

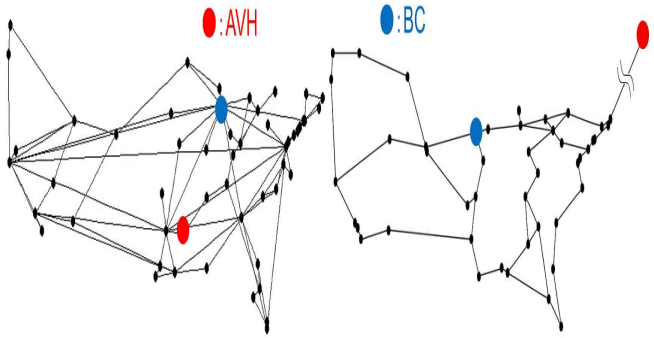
C を結託ユーザの配置数とし，$\boldsymbol{N}$ を全ノード集合，$\boldsymbol{U}$ を結託ユーザの配置ノード集合，$x(l)$ をリンク l を経由する fake コンテンツパス数，$h(l)$ をリンク l の fake コンテンツからのホップ長の最小値，$z(n)$ をノード n が接続された全リンク l の $f(l)$ の総和と定義する．攻撃者は fake コンテンツが多数のルータに展開されるノードに結託ユーザを配置し，できるだけ fake コンテンツ のキャッシュ位置が重ならずに拡散させたい．そこで $f(l)$ をリンク重みとし，2 つの設定法 PC (path count) と PAH (path count and hop length) を考え，PC では $f(l) = 1/x(l)$ に，PAH では $f(l) = 1/\{x(l)h(l)\}$ に設定する [3]．$z(n)$ が最大のノードから順番に結託ユーザを配置する．

3. 性能評価

NW トポロジが独自 fake 型 CPA の脅威に与える影響を計算機シミュレーションにより評価する．CAIDA で公開されている米国の商用 ISP のバックボーン NW トポロジのうち，Allegiance Telecom 及び At Home Network を評価に用いる．図 1 にこれら 2 つの NW トポロジと，各 fake コンテンツ配置方式において fake コンテンツが配置されたノードを赤色と青色の丸で示す．AVH 方式の場合，Allegiance Telecom のようなハブ・スポーク型の NW トポロジでは，ハブノードが存在するためハブノードではない NW トポロジの中心付近のノードに fake コンテンツが配置される．At Home Network のようなラダー型の NW トポロジでは，ハブノードが存在せずノードが一様に分布しているため，NW の端のノードに配置される．BC 方式の場合，ハブ・スポーク型ではハブノードに，ラダー型では NW トポロジの中心付近のノードに配置される．

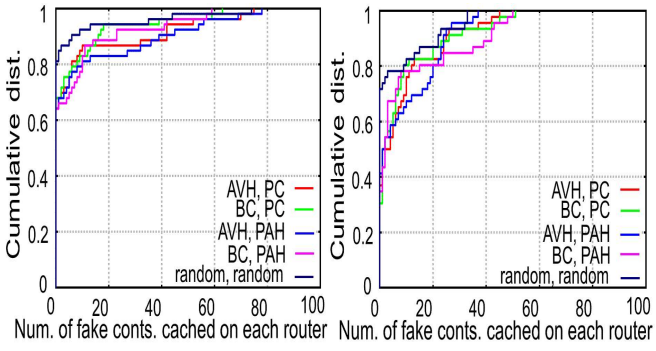
キャッシュ方式は配信ルータの 1 ホップ下流ルータでキャッシュを行う Leave Copy Down (LCD)[4] を想定する．コンテンツ数 $M = 10,000$ に対しキャッシュサイズは 100 とする．正常ユーザはパラメタ $\theta = 0.8$ の Zipf 分布に従いランダムに選択したコンテンツを要求する．fake コンテンツ数は 100，結託ユーザの総要求比率は全要求比率に対して 10%を想定する．2 節で述べた fake コンテンツ及び結託ユーザの配置法の 4 つの組み合わせに加え，両者をランダムに配置した場合の 5 つを比較する．

図 2 に，独自 fake 型における LCD に対し，結託ユーザが異なる 5 ノードに存在している 2 つの NW において，各ルータにキャッシュされている fake コンテンツの累積分布を示す．図 2(a) の赤及び青の曲線が他の曲線に比べて下に位置する傾向が確認できる．ハブ・スポーク型の NW トポロジでは，fake コンテンツを AVH 方式を用いて，ハブノードではない NW の中心付近に配置することで，ハブノード以外の多数のノードに fake コンテンツを経由させ，より多くのノードに fake コンテンツを注入可能である．一方，図 2(b) の緑及び紫の曲線が他の曲線に比べて x 軸が 25 程度以上の領域では下に位置する傾向が確認できる．ラダー型の NW トポロジでは，fake コンテンツを BC 方式に従って NW の中心付近に配置することで，重複せずに多くのノードに fake コンテンツを経由させ，より多くのノードに fake コンテンツを注入可能である．また，ラダー型の NW トポロジはハブ・スポーク型に比べて，ノード間の経由ノード数が多い傾向があるため，CPA の影響が大きい．



(a) Allegiance Telecom　　**(b)** At Home Network

図 1: NW トポロジ



(a) Allegiance Telecom　　**(b)** At Home Network

図 2: 各ルータのキャッシュ fake content 数の累積分布

謝辞 本研究成果は JSPS 科研費 18K11283 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．

[1] T. Nguyen, et al., "Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment", IM 2017, 2017.
[2] 工藤多空飛, 上山憲昭, "コンテンツポイズニング攻撃の影響分析", 2021 信学総大, B-6-24, 2021 年 3 月.
[3] 工藤多空飛, 上山憲昭, "攻撃者の位置がコンテンツポイズニング攻撃の脅威に与える影響の分析", 2021 信学ソ大, B-11-18, 2021 年 9 月.
[4] N. Laoutaris, H. Che, and I. Stavrakakis, "The LCD interconnection of LRU caches and its analysis," Elsevier Performance Evaluation, Vol. 63, Issue 7, pp. 609-634, July 2006.