複数攻撃者配置における ICN のコンテンツポイズニング攻撃の影響分析

Investigating Influence of ICN Content Poisoning Attack with Multiple Attack Locations

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パケットを転送しルータでコンテンツをキャッシュし配信することでコンテンツを効率的に配信するネットワーク (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 に対する対処法を確立するには，CPA が NW の性質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]．そこで著者らは，Fake コンテンツ及び Bot の配置数が各々 1 の場合において，攻撃者が独自の名称の不当コンテンツをキャッシュに注入する独自 Fake 型 CPA の脅威を分析した [2]．本稿では，Fake コンテンツ及び Bot の数が 2 以上の場合における独自 Fake 型 CPA の脅威を分析する．

2. Fake コンテンツと Bot の配置方式

独自 Fake 型 CPA は Bot から攻撃者の用意した Fake コンテンツを要求し，NW 上に Fake コンテンツを配信することで，キャッシュに Fake コンテンツを注入する．Fake コンテンツか Bot のうち先に配置する方の配置方式を先行配置方式として，以下の二つを想定する．

BC: Betweenness Centrality が大きいノードから順に配置

DC: Degree Centrality が大きいノードから順に配置

先行配置されるノード集合を $\boldsymbol{U}$，ノード m からノード n までの最短経路のホップ長を $h(m,n)$ とするとき，先行配置される全てのノードからのホップ長の和 $z(n)$ を $z(n) = \sum_{m \in \boldsymbol{U}} h(m,n)$ と定義する．ここでは，$z(n)$ の値が最大となるノードに後に配置することを提案し，後続配置方式とする．2 つ目以降の配置は文献 [2] の PC (path count) を使用し，このアルゴリズムを HC とする．本稿では，先行配置方式を左側に表記し，方式の末尾に Fake コンテンツの割り当ては f，Bot の割り当てであれば b を表記する．また，先行配置数を X_1，後続配置数を X_2 と定義し，$X_1 = 2$，$X_2 = 2$，4 を想定する．

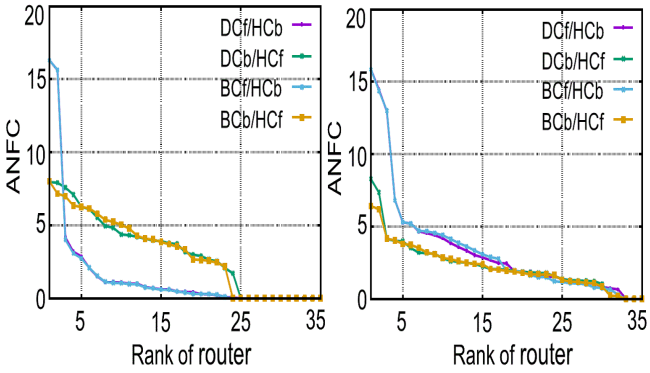
3. 性能評価

本稿では計算機シミュレーションによって評価する．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，At Home Network を評価に用いる．キャッシュ方式は経路上の全ルータでキャッシュする AllCache を想定し，キャッシュサイズは 100 とする．正当なコンテンツ数 $M = 10000$ に対し Fake コンテンツ数 F は 32 を想定する．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のに対し，Bot はランダムに Fake コンテンツを要求し，Bot の要求比率 ρ は全要求比率に対して 10%を想定する．

図 1 (a)，図 2 (a) に $X_2 = 2$，図 1(b)，図 2 (b) に $X_2 = 4$ における，各ノードの平均 Fake コンテンツ注入数 (ANFC: average number of Fake contents) を降順に示す．X_2 が同じ場合，先に Bot を，続いて Fake コンテンツを配置することで多数のノードに多くの Fake コンテンツを注入可能である．Bot を BC や次数が大きな主要ノードに配置することで，キャッシュの入れ替わりが激しくなり，Interest がオリジナルまで転送される機会が増え，NW 全体に Fake コンテンツを拡げることが可能である．

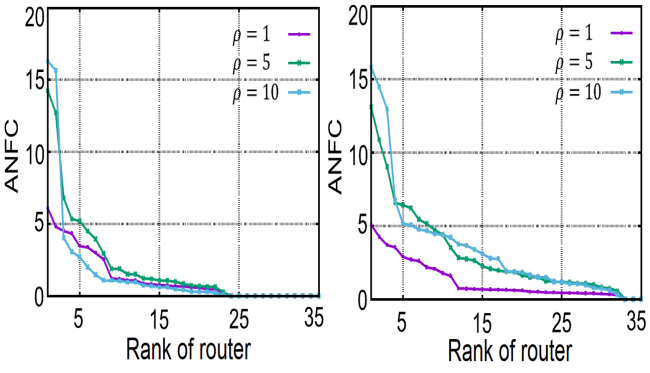
一方で，X_2 が増加した場合，1 つの Bot から発生する要求数が減少するため 1 ノードあたりの ANFC は減少することが予想される．しかし Bot を後続配置した青色と紫色の曲線では $X_2 = 4$ のときの方が 2 の時と比べ，ANFC は増加している．これは Interest がオリジナルまで転送される機会が増加することが要因である．図 2 に BCf/HCb において，$X_2 = 2$ 及び $X_2 = 4$ における ρ が 1%，5%，10%の場合の ANFC を示す．図 2 (a) より平均注入 Fake コンテンツ数が 3 位 (rank 3) 以降のノードでは，ρ が 5%の場合において ANFC が大きい．要求比率が大きい場合 Bot 付近のノードのみ Interest が転送されるため，全体的なノードへの注入数が減少する．一方で，要求比率が少ないことで，Bot 付近のノードに Fake コンテンツが残らず，オリジナル付近のノードへより多くの Interest が転送される．そのため，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，今回の配置方式において後続配置されるノードは NW 内の主要ではないノードであることも影響している．したがって ρ が 10%において X_2 を増やすことでより多くの Fake コンテンツを注入することが可能である．

また図 2 (b) より，$X_2 = 2$ の場合と比べて ρ が大きい方がより多くの Fake コンテンツを注入可能である．これは 1 つの Bot から発生する要求数が少ないためである．ρ を 10%から 5%まで減らした場合，総注入 Fake コンテンツ数は 10 個程度の差であることから，Bot の数や Bot が存在するノードの人口比などを考慮して，要求比率を定めるほうが良い．



(a) $X_2 = 2$　　**(b)** $X_2 = 4$

図 1: 各配置方式の各ノードの平均注入 Fake コンテンツ数



(a) $X_2 = 2$　　**(b)** $X_2 = 4$

図 2: 各要求比率の各ノードの平均注入 Fake コンテンツ数

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, ”ICN における Fake 型コンテンツポイズニング攻撃の影響分析”, 電子情報通信学会 コミュニケーションクオリティ（CQ）研究会, CQ2022-23, 大阪/オンライン, 2022 年 7 月