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

Investigating Influence of Attacker Location 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ネットワーク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ゾニング攻撃 (CPA: content poisoning attack) の問題が指摘されている [1]．CPA には，コンテンツと紐づいた公開鍵から生成されたディジタル署名と一致する偽のコンテンツをキャッシュ (CS: content store) に注入する fake 型が存在する．さらに fake 型には，攻撃者が独自に作成した fake コンテンツを結託した Client から要求することで CS に注入する独自 fake 型と，実在するコンテンツの fake コンテンツを正常な Client からの要求時に配信することで CS に注入する詐称 fake 型が考えられる．CPA に対する対処法を確立するには，CPA がネットワーク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ネットワーク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]．そこで本稿では独自 fake 型の CPA を想定し，大規模なネットワークトポロジで様々な攻撃者の位置で評価を多面的に行うことで，様々な要素が CPA の効果に与える影響を分析し，CPA の脅威を明らかにする．

2. 独自 fake 型 CPA の攻撃者配置方式

2.1 fake content の配置

fake content の配置方法として，以下の二つを提案する．
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

2.2. 結託ユーザの配置

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 content パス数，$h(l)$ をリンク l の fake content からのホップ長の最小値と定義する．$f(l)$ 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．Algorithm 1 に，結託ユーザの配置アルゴリズムを示す．

Algorithm 1 Placement of colluded users

1: $\boldsymbol{U} = \phi$, $c = 0$
2: **while** $c \leq C$ **do**
3:　**for** $n \in \boldsymbol{N} \setminus \boldsymbol{U}$ **do**
4:　　$z(n) = \sum_{l \in M_n} f(l)$
5:　**end for**
6:　$n^* = \text{argmax}\ z(n)$, $\boldsymbol{U} += \{n^*\}$, $c++$
7: **end while**

3. 性能評価

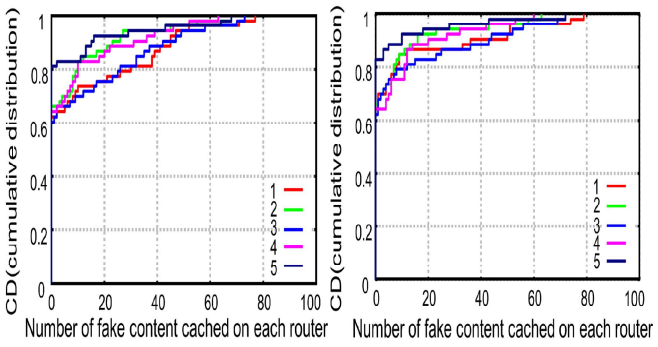
独自 fake 型の影響について計算機シミュレーションにより分析する．CAIDA で公開されている米国の商用 ISP のバックボーンネットワークトポロジのうち，Allegiance Telecom を評価に用いる．キャッシュ方式は経路上のすべてのルータでキャッシュを行う AllChace，配信ルータの 1 ホップ下流ルータでキャッシュを行う Leave Copy Down (LCD)[2] の 2 つを想定する．コンテンツ数 $M = 10,000$ に対しキャッシュサイズは 100 とする．正常ユーザはパラメタ $\theta = 0.8$ の Zipf 分布に従いランダムに選択したコンテンツを要求する．

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．fake content 及び結託ユーザの配置については表 1 に示す 5 つのパターンを想定する．

表 **1:** Attacker Location

case	fake content	colluded users
1	AVH	PC
2	BC	PC
3	AVH	PAH
4	BC	PAH
5	random	random

図 1 に独自 fake 型におけるキャッシュ方式 2 つに対し，結託ユーザが異なる 5 ノードに存在している NW において，各ルータにキャッシュされている fake content の累積分布を示す．All Cache においては，経由するすべてのノードにキャッシュする方式であることから汚染度が高いことがわかる．LCD においては，オリジナルの付近からキャッシュを行う方式であることから，All Cache に比べて汚染度は小さいことがわかる．fake content 及び結託ユーザの配置について，ランダムと比較してアルゴリズムに従って配置した方が攻撃の影響が大きいことがわかる．また，fake content のオリジナルの配置については，ホップ数を考慮して配置することで，より多くのノードを通過することで影響が大きくなる．結託ユーザの配置についても，パス数のみを考慮するのではなくホップ長も考慮することで攻撃の影響が大きくなる．ただし fake content の配置の影響が大きい．



(a) All Cache　　**(b)** LCD

図 **1:** 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．

参考文献

[1] T. Nguyen, et al., Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management(IM), pp.72-80, 2017.
[2] 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.