

ICN の Fake 型コンテンツポイズニング攻撃に 攻撃者配置ノード数が及ぼす影響の分析

工藤多空飛[†] 上山 憲昭^{††}

[†] 福岡大学 大学院工学研究科
〒 814-0180 福岡市城南区七隈 8-19-1
^{††} 立命館大学 情報理工学部
〒 525-8577 滋賀県草津市野路東 1-1-1

E-mail: [†]td212005@cis.fukuoka-u.ac.jp, ^{††}kamiaki@fc.ritsumeikan.ac.jp

あらまし コンテンツを効率的に配信するための新しい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) が広く研究されている。しかし、悪意を持ったユーザが正当な名前で偽のコンテンツを大量にネットワークに挿入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。CPA にはその攻撃の性質から四つの型が想定される。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。しかし既存研究は限定された CPA 方式を想定しており、その多くが小規模なネットワークトポロジや攻撃者の位置で評価を行っており、汚染コンテンツ数や汚染ノード、攻撃者の位置などが CPA の脅威に与える影響が明らかにされていない。そこで本稿では独自 fake 型の CPA を想定し、複数攻撃者配置において、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。

キーワード ICN, コンテンツポイズニング攻撃, キャッシュ

Impact Analysis of Attacker Location Count on Fake-Type Content Poisoning Attack in ICN

Takuto KUDO[†] and Noriaki KAMIYAMA^{††}

[†] Graduate School of Engineering, Fukuoka University
8-19-1, Nanakuma, Jounan, Fukuoka 814-0180
^{††} College of Information Science and Engineering, Ritsumeikan University
1-1-1, Nojihigashi, Kusatsu 525-08577
E-mail: [†]td212005@cis.fukuoka-u.ac.jp, ^{††}kamiaki@fc.ritsumeikan.ac.jp

Abstract Information-centric networking (ICN) has been widely studied as a new network architecture for efficient content delivery. However, the problem of content poisoning attack (CPA), in which a malicious user inserts a large amount of fake content into the network under a legitimate name, thereby reducing the effectiveness of the cache, has been pointed out. However, existing studies assume a limited number of CPA schemes, and most of them are based on small network topologies and attacker locations, and do not consider the number of contaminated contents, contaminated nodes, and attacker locations. The impact of the number of contaminated contents, contaminated nodes, and attacker locations on the CPA threat has not been clarified. In this paper, we assume a original fake type CPA and analyze the impact of various factors on the effectiveness of CPAs and clarify the threat of CPAs by conducting multifaceted evaluations in a large network topology and at various attacker locations.

Key words ICN, Content Poisoning Attack, Cache

1. はじめに

YouTube などのユーザ生成コンテンツや、映画やドラマなどのコンテンツプロバイダによって生成されたリッチコンテンツを配信することによって生成されるトラフィックは、インターネット上のトラフィックの大部分を占めている。インターネットでは IP アドレスを用いてパケットを転送するため、配信に先立ち配信元となるサーバの IP アドレスをコンテンツの名称から解決するオーバーヘッドが発生する。そこでコンテンツをネットワーク (NW) 内のルータでキャッシュし、コンテンツの名称を用いて配信要求 (interest) を転送し、転送経路上で要求コンテ

ンツを保持しているルータからコンテンツを配信する情報指向ネットワーク (ICN: Information-Centric Networking) が注目され、精力的な研究が進められている [4]。ICN の思想を用いた具体的な NW アーキテクチャとしては、Named Data Networking (NDN) [13] などが提案されている [12]。ICN を用いることで名前解決処理のオーバーヘッドを回避し、ユーザに近い位置からコンテンツを配信することで遅延時間や NW 負荷の低減が期待される。

しかし悪意を持ったユーザが正当な名前で偽のコンテンツを大量にネットワークに挿入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]. 実在するコンテンツの名称で偽りのコンテンツをアップロードすることで、ルータのキャッシュに無意味なコンテンツをキャッシュさせることが可能である。CPA によって正当なコンテンツのキャッシュ配信が減少し、キャッシュの効果が減少するなどの問題がある。CPA は、注入する fake コンテンツなどの攻撃の方法からいくつかの型が想定される。そこで著者らは 4 つの各 CPA タイプを、独自 fake 型、詐称 fake 型、結託 corrupted 型、自然 corrupted 型と定義した [2].

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。しかし既存研究は限定された CPA 方式を想定しており、その多くが小規模なネットワークポロジや攻撃者の位置で評価を行っており、汚染コンテンツ数や汚染ノード、攻撃者の位置などが CPA の脅威に与える影響が明らかにされていない [1]. そこで著者らは、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、正当なユーザの要求比率やキャッシュサイズが CPA の効果に与える影響を分析し、独自 fake 型 CPA の脅威を明らかにする。

以下 2. 節では CPA の詳細について述べ、3. 節では独自 fake 型における fake コンテンツ及びボット (bot) の配置アルゴリズムについて述べる。そして 4. 節では、独自 fake 型における影響分析結果について述べ、最後に 5. 節で全体をまとめる。

2. コンテンツポイズニング攻撃

ICN ではコンテンツの正当性を、パケットのヘッダに付与された公開鍵暗号を用いたデジタル署名により判断できる。しかし経路上のルータでは大量のパケットが到着するため、処理負荷が大きく、デジタル署名による検査が困難である。そのため CPA の検知法としては、コンテンツの要求者 (subscriber) が受信コンテンツの正当性を検査し、不当コンテンツをルータに通知する方式が提案されている [3]. CPA は、コンテンツと紐づいた公開鍵から生成されたデ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 型と、デジタル署名と一致しない無意味なコンテンツを CS に注入する corrupted 型の二つに大別されるが [2], デジタル署名により検知可能な CPA は corrupted 型に限定される。さらにそれぞれにおいて、攻撃者と結託したユーザの有無によって CPA の攻撃方法は四つのタイプを想定することができる。以下にそれぞれについて示す。

- **独自 fake 型:** 攻撃者が独自に作成した fake コンテンツを攻撃者の指示に従って bot から要求することで CS に注入
- **詐称 fake 型:** 実在するコンテンツの fake コンテンツを正当なユーザからの要求時に配信することで CS に注入
- **結託 corrupted 型:** 実在するコンテンツを騙ったデジタル署名と一致しない fake コンテンツを攻撃者の指示に従って bot から要求することで CS に注入
- **自然 corrupted 型:** 実在するコンテンツを騙ったデジタル署名と一致しない fake コンテンツを正当なユーザからの interest 到着直後に配信することで CS に注入

詐称 fake 型では、攻撃者のコンテンツに subscriber からの interest が転送されるよう FIB が設定される。実在する高人気コンテンツの fake コンテンツであるためアクセス数が非常に多く、攻撃の影響が非常に大きいことが予想される。正当なコンテンツ配信者 (publisher) の公開鍵を管理している CA の職員と結託するなど、公開鍵を攻撃者の公開鍵に書き換えることで本タイプの攻撃が可能である [2]. 正当な publisher の公開鍵を乗っ取って書き換える結果、攻撃者のコンテンツの方が正当化される。

corrupted 型においては、fake コンテンツはコンテンツに紐づいた公開鍵から生成されたデジタル署名と一致しないため、subscriber が署名検証を行うことで容易に検知可能である。そこで本稿では、実現が容易でかつ検知が困難な独自 fake 型に着目し、ICN のキャッシュ方式や正当なユーザの要求比率、CS や攻撃者の位置が CPA の効果に与える影響について分析し、CPA

の脅威を明らかにする。

3. 配置アルゴリズム

独自 fake 型 CPA においては、fake コンテンツ及び bot の配置を行う必要がある。独自 fake 型においては、攻撃者が独自に作成した fake コンテンツに interest を転送するのは攻撃者と結託したユーザ (bot) のみであり、interest の転送機会も少ない。そのため独自 fake 型 CPA においては、fake コンテンツ及び bot の配置が CPA の効果に大きく影響する。しかしこれまでに、fake コンテンツ及び bot の配置法に關した研究は見られない。そこで本節では、fake コンテンツおよび bot の配置方式を検討する。fake コンテンツと bot のうち、先に割り当てるものを先行配置、次に割り当てるものを後続配置と呼ぶ。

3.1 先行配置方式

NW において重要なノードの CS に fake コンテンツが注入されることで、CPA の効果が大きくなることが想定される。そこで NW 内の重要なノードの概念として中心性を考える。 X_1 を先行配置ノード数、各ノード n の中心性を w_n とするとき、 w_n が最大のノードから順に配置する。Algorithm 1 に、先行配置アルゴリズムを示す。

Algorithm 1 Preceding placement

```

1:  $c = 0$ 
2: while  $c \leq X_1$  do
3:    $n^* = \operatorname{argmax} w_n$ 
4:   Allocate fake content/bot at node  $n^*$ 
5:    $c++$ 
6: end while

```

中心性 w_n の具体例として、任意のノードペア間の最短パスの経由数である媒介中心性 (BC: betweenness centrality) 及び、各ノードの隣接ノード数である次数中心性 (DC: degree centrality) の二つを考える。

以後、fake コンテンツを先行配置する場合には BCf および DCf と表記し、bot を先行配置する場合には BCb および DCb と表記する。

3.2 後続配置方式

CPA の効果を高めるには、先行割当ノードからより遠いノードに fake コンテンツまたは bot を配置することで、より多くのノードを fake コンテンツが経由させることが有効である。そこで本稿では、以下の配置アルゴリズムを提案する。先行配置されたノード集合を U_1 、既に後続配置されたノード集合を U_2 、そして $x(l)$ を既に後続配置ノードとして選択された任意のノードと任意の先行配置ノードペア間の最短ホップ径路のうちリンク l を経由するパスの数と定義する。そして任意のノードペア i, j 間の最短経路上の $1/x(l)$ の総和を $y_{i,j}$ とすると、ノード i からノード j までの最短経路が通るリンクの集合 L_{ij} に対して、

$$y_{i,j} = \sum_{l \in L_{ij}} 1/x(l) \quad (1)$$

となる。 $y_{i,j}$ が大きな経路に要求パケットを転送した方が、より多くのノードに fake コンテンツを注入することができる。ここで、ノード n に接続するリンクの集合を E_n 、先行配置ノード i と既に後続配置されたノード j との間の最短経路がリンク l を経由するときに 1 を、そうでないときに 0 をとる 2 値変数を $b_{i,j}(l)$ とする。そして z_n を

$$z_n = \sum_{e \in E} \sum_{i \in U_1} \sum_{j \in U_2} b_{i,j}(e) y_{i,j} \quad (2)$$

と定義し、 z_n が最大のノードから順番に後続配置する。後続配置ノード数を X_2 とし、Algorithm 2 に、後続配置アルゴリズムを示す。

Algorithm 2 Subsequent placement

```

1:  $U_2 = \phi, c = 0$ 
2: while  $c \leq X_2$  do
3:   for  $i \in N, j \in N$  do
4:     Calculate  $y_{i,j} = \sum_{l \in L_{ij}} 1/x(l)$ 
5:   end for
6:   for  $n \in N \setminus U_1 \setminus U_2$  do
7:     Calculate  $z_n = \sum_{e \in E} \sum_{i \in U_1} \sum_{j \in U_2} b_{i,j}(e) y_{i,j}$ 
8:   end for
9:    $n^* = \operatorname{argmax} z_n, U_2 += \{n^*\}, c++$ 
10: end while
  
```

4. 性能評価

4.1 評価条件

4.1.1 ネットワークトポロジ

CAIDA の Web ページで公開されている米国の商用 ISP のうち、At Home Network のバックボーンネットワークトポロジを評価に用いた [8]. 図 1 にこの NW トポロジを示す. また, 表 1 に, ノード数 N , リンク数 E , 人口比で重みづけたノード間の平均ホップ長 H , 平均次数 D をまとめる.

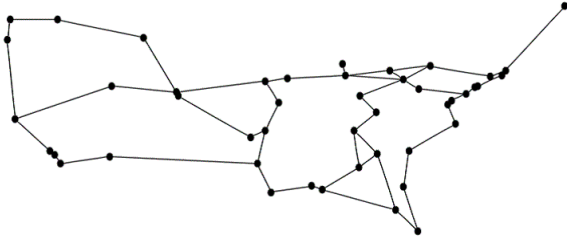


図 1: Network topologies used for numerical evaluation

表 1: Summary of properties of a networks evaluated

Network	N	E	H	D
At Home Network	46	55	6.83	2.41

4.1.2 コンテンツ要求

コンテンツ数 M を 10,000 に設定する. Web ページやユーザー生成ビデオなどの様々な種類のデジタルコンテンツの要求数分布は Zipf 分布に従うことが報告されている [9] [10]. 例えば Web ページの要求数分布はパラメタ θ が 0.64~0.83 の, YouTube 動画は約 0.8 の Zipf 分布に従う [10]. そこでコンテンツ m の要求比率 Q_m をパラメタ θ の Zipf 分布で与え, 本稿では $\theta = 0.8$ もしくは $\theta = 2.0$ と設定し, 影響の違いを分析する. 以降, 特に明記しない限り $\theta = 0.8$ に設定する [11]. また, fake コンテンツ数 F は 32 もしくは 1,024 に設定し, bot の要求比率 ρ は全要求比率に対して 1% から 10% を想定する. 以降, 特に明記しない限り bot の要求比率 ρ は 0.1 に設定する.

4.1.3 キャッシュ方式

経由ルータでのコンテンツのキャッシュ判断を行うキャッシュ方式に関し, 以下の 3 つの方式を想定する.

AC (all cache): 発ルータ s から目的ルータ u に至るコンテンツ配信経路 (default path) 上のすべてのルータでキャッシュ [5]

EC (edge cache): default path 上の最終ホップノードでのみキャッシュ [7]

LCD (leave copy down): コンテンツ配信ノードから default path 上の次ホップのルータでのみキャッシュ [6]

4.1.4 ルータの Content store の容量

CS の容量を次数で重みづけして設定する場合と, 全ノード統一で 100 と設定する場合の 2 つを考える. 両方の場合において, NW 内の総 CS 容量は同じになるように設定する. 以降, CS の容量を次数で重みづけたものを $weight$, 全ノード統一して 100 と設定したものを $unweight$ と定義する.

4.2 各ノードの平均 Fake コンテンツ注入数

4.2.1 Fake コンテンツや Bot の配置ノード数や Bot トラヒック比率が及ぼす影響

図 2, 図 3 に各配置方式において, X_1 と X_2 の値を 3 つのパターンに設定した場合の各々における, 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. 配置数が同じ場合, 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, bot 配置ノードのキャッシュの入れ替わりが激しくなり, fake コンテンツが長時間, これら bot 配置ノードにとどまらずに, 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.

図 2(b) 及び (d) より, bot を先行配置した場合は, X_2 の増加に伴って, 1 ノードあたりの ANFC は減少する. これは, 1 つの bot から発生する要求数が減少するためである. しかし図 2(a) 及び (c) より, fake コンテンツを先行配置した場合は, X_2 の増加に伴い, 1 ノードあたりの ANFC が増加している. 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 4 に BCf において, $X_1 = 1, X_2 = 1$ 及び $X_1 = 2, X_2 = 2$ において, ρ が 1%, 5%, 10% の場合の各ノードの ANFC を同様に示す.

図 4(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 1% 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 4(b) より, $X_2 = 1$ 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. $X_2 = 2$ の場合においても rank3 以降のノードでは, ρ が 10% よりも 5% の場合において ANFC が大きいことから, 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.

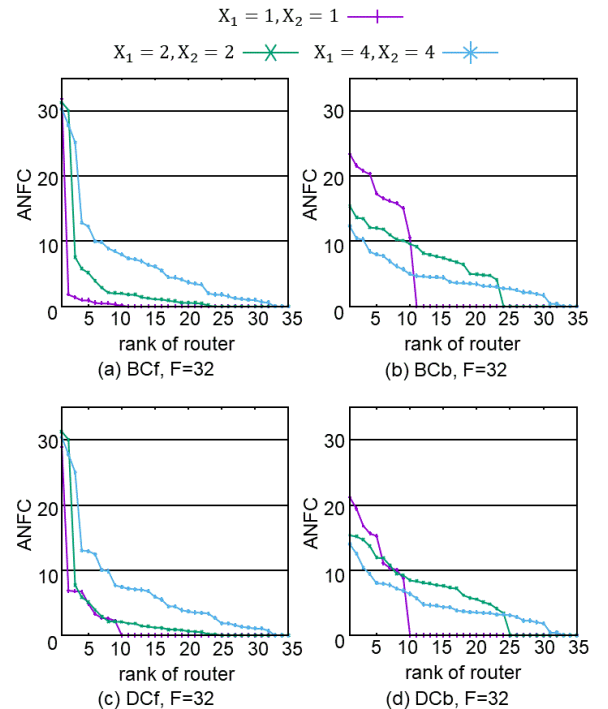


図 2: Average number of fake contents injected at each node at $F = 32$

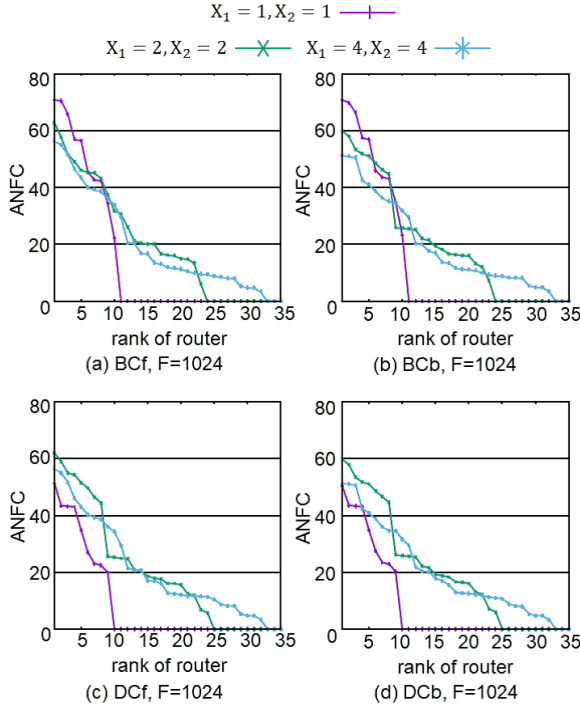


図 3: Average number of fake contents injected at each node at $F = 1,024$

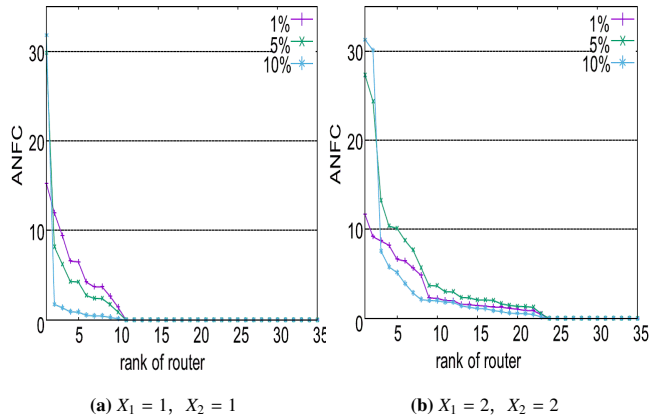


図 4: Average number of fake contents injected at each node for three values of ρ

4.2.2 コンテンツの人気の偏りが及ぼす影響

図 5 及び図 6 に CS を weight で設定した場合における, $\theta = 0.8$ 及び $\theta = 2.0$ における各ノードの ANFC を降順に示す. 図 5, 図 6 より, $\theta = 0.8$ の場合と比較すると $\theta = 2.0$ において ANFC が増加している. 正当なユーザが集中的にコンテンツを要求することで, 各ノードにキャッシュされる正当なコンテンツの種類が減少する. その結果, より多くの fake コンテンツが各ノードにキャッシュされる.

また, F が少ない場合, 配置方式によって fake コンテンツの注入数は異なる. $\theta = 2.0$ において, bot を先行配置方式で複数ノードに割り当てた場合, 上位 rank ノードと下位 rank ノードでの ANFC の差が大きい. これは, bot が NW の中心付近に割り当てられており, 正当なユーザの要求コンテンツの種類が少ないことから, bot が存在するノード内のキャッシュに多くの fake コンテンツが残っており, fake コンテンツへの interest がオリジナルまで転送される機会が減少するためである.

一方, $\theta = 2.0$ において bot を後続配置した場合, 配置数が増加するにつれて ANFC が多いノードが増加する. これは bot を NW の主要ではないノードに複数配置することで, fake コンテ

ンツへの interest が分散され interest がオリジナルまで転送される機会が増加しており, 正当なユーザの要求が集中していることから多くのノードにおいて fake コンテンツが残りやすいためである. また, F が大きい場合においては正当なユーザの要求比率によって ANFC に大きな差が生じるが配置方式間での違いは見られなかった.

4.2.3 キャッシュサイズが及ぼす影響

図 7 及び図 8 に $\theta = 0.8$ における, CS を weight 及び unweight で設定した場合における各ノードの ANFC を降順に示す. 図 7 より, CS を weight で設定したほうが ANFC が増加している. 提案配置方式により, fake コンテンツもしくは bot のいずれかが BC や DC の大きなノードに配置されており, CS が大きくなっている高次数ノードを fake コンテンツへの interest が通過する機会が多いためである. またその影響は直接高次数ノードに攻撃者を割り当てる DC 方式が大きい. また, 図 7 より bot の数が少なく F が小さいときは bot の配置が重要となる. bot の配置されるノードが高次数の場合, CS が大きいため bot 付近のノードでの ANFC が大きくなり, fake コンテンツへの interest がオリジナルまで転送される機会が減少する. 一方, bot が配置されるノードが低次数の場合, CS が小さいため, bot 付近のノードでの ANFC が小さくなり, interest がオリジナルまで転送される機会が増加する. 一方, 図 8 より, F が大きい場合は CS や bot の配置による影響はほとんど見られない. これは, fake コンテンツへの interest が分散されており, interest がオリジナルまで転送される機会が多いためである.

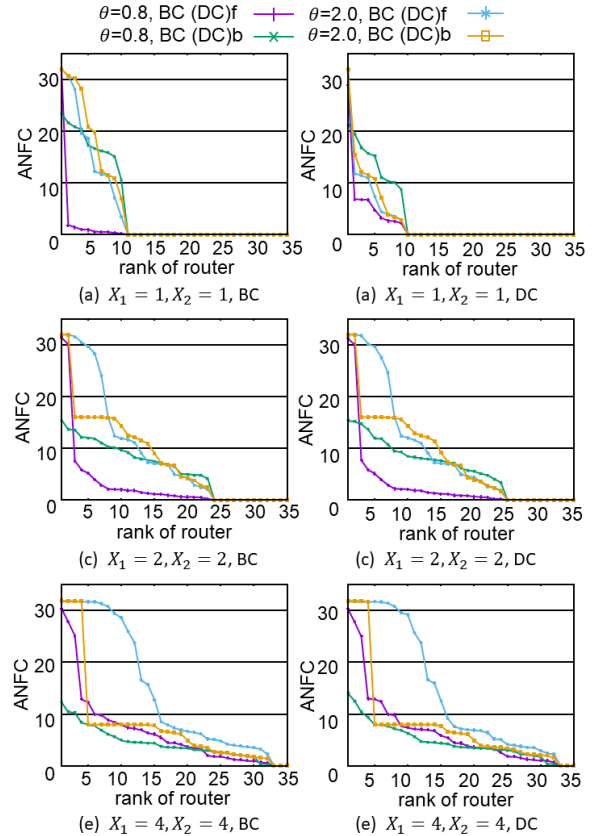


図 5: Average number of fake contents injected at each node at $F = 32$ for two values of θ

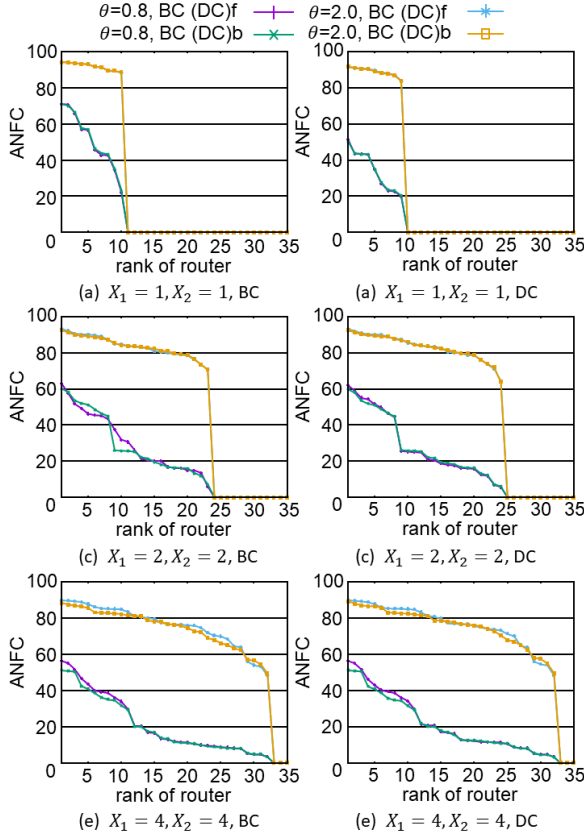


図 6: Average number of fake contents injected at each node at $F = 1,024$ for two values of θ

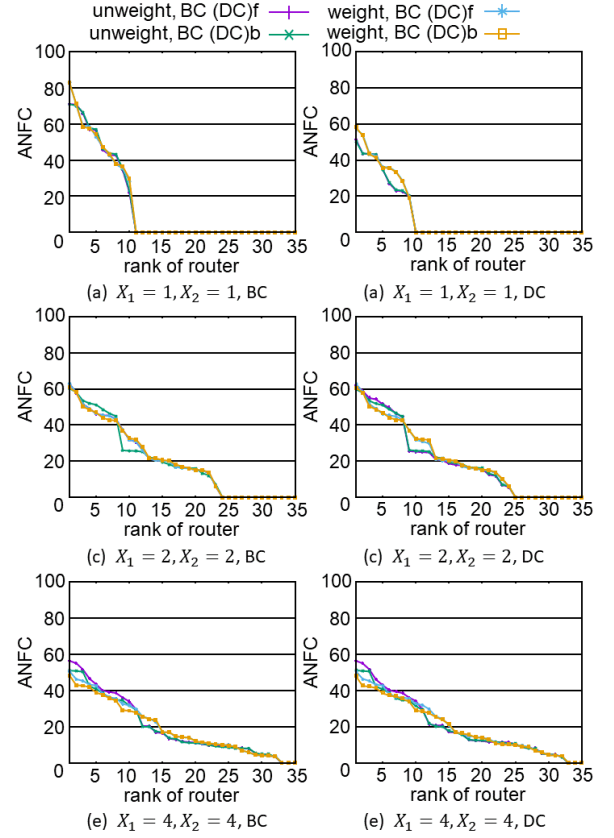


図 8: Average number of fake contents injected at each node at $F = 1,024$ for two cases of CS sizes

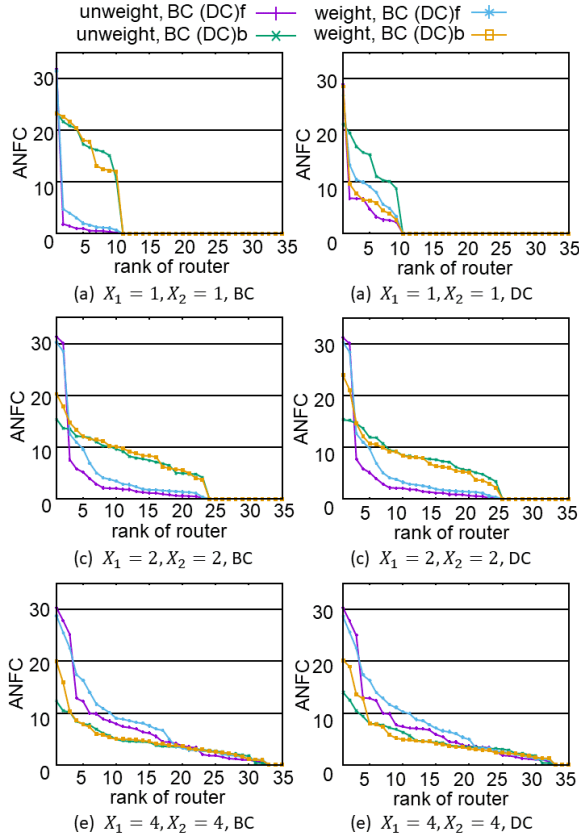


図 7: Average number of fake contents injected at each node at $F = 32$ for two cases of CS sizes

4.3 キャッシュヒット率

表 2 から表 5 に各 CS, 各配置数, 各配置方式, 各キャッシュ方式において, ANFC が 1 位から 3 位のノードにおけるローカルキャッシュヒット率 (LCHR) の変化率を示す。ただしローカルキャッシュヒット率を, 対象となるノードに到着した正常コンテンツに対する interest 数のうち, そのノードに要求コンテンツがキャッシュされていた割合と定義する。表 2 より, 攻撃者が単数の場合, bot を DC または BC 方式で先に割当て, fake コンテンツを方式で後続配置することで fake コンテンツ数が少ない場合でも rank1 だけではなく, rank2, rank3 ノードにおけるローカルキャッシュヒット率を大きく低減させることが確認できる。一方, fake コンテンツ数が多い場合, bot の配置が重要ではなく, 主要なノードに fake コンテンツや bot を割当てていることが重要となる。これは fake コンテンツへの interest が分散され, interest がオリジナルまで転送される機会が増加するためである。

表 2 より, bot を先行配置する方式において配置数の増加に伴って, LCHR の変化率が減少している。これは X_1 の増加に伴い, fake コンテンツへの interest が分散するためである。一方, bot を後続配置する方式において, 配置数の増加に伴って, rank2 以降のノードでの LCHR の変化率が増加している。これは X_2 の増加に伴って, fake コンテンツへの interest が分散し, rank1 ノードにキャッシュされている fake コンテンツの数が減少する。その結果, interest がオリジナルまで転送される機会が増加し, rank2 以降のノードでの ANFC が増加するためである。

また, 表 3 より, 配置数の増加に伴って, rank3 ノードにおいて LCD の LCHR の変化率が増加している。これは fake コンテンツのオリジナルの次ホップノードの数が増加することにより, ANFC が増加するためであり bot を先行配置する方式に顕著に表れている。これは LCD の性質が関係しており, bot を先行配置することで配信ルータは NW 内の中心性が低いノードに配置される。その結果, fake コンテンツがキャッシュ内に残りやすいため LCHR への影響が大きい。

また、表 4, 表 5 より、CS を次数で重みづけることで LCHR への影響が大きいことが確認でき、表 5 では、rank1, rank2 ノードでの LCHR 変化率が減少し、rank3 ノードでは増加している。これは、高 rank ノードでは CS が大きいノードとなるため、キャッシュヒット率への影響が小さくなり、キャッシュが全体へ分散するためである。しかし、NW 全体のキャッシュヒット率を考えるとその影響は僅かである。従って、攻撃者は影響を与えたいノードの数や位置に応じて fake コンテンツ及び bot の配置数や配置位置を設定する方が良い。

表 2: Local cache hit ratio (F=32, unweight)

X_1, X_2	placement method	rank1			rank2			rank3		
		AC	EC	LCD	AC	EC	LCD	AC	EC	LCD
1	DCf	-41.0	-26.3	-21.5	1.2	0.0	-0.3	-50.2	0.0	0.6
	DCb	-19.3	-25.8	-9.6	-20.3	0.0	-3.1	-23.6	0.0	-1.2
	BCf	-21.0	-22.4	-14.2	18.5	0.0	3.5	-4.3	0.0	-74.9
	BCb	-28.0	-24.5	-3.3	-18.9	0.0	1.1	-28.9	0.0	0.9
2	DCf	-40.6	-3.5	-9.6	-19.8	-22.7	-14.0	-4.7	0.0	-1.6
	DCb	-17.9	-24.0	-4.4	-16.4	-10.0	-8.5	-13.9	0.0	-5.7
	BCf	-42.7	-11.9	-11.3	-19.3	-20.0	-13.0	5.5	0.0	-2.0
	BCb	-16.8	-22.2	-10.4	-13.4	-19.7	-4.4	-10.4	0.0	-2.1
4	DCf	-21.8	-6.0	-14.0	-36.8	-15.1	-9.2	-16.1	-17.8	-14.4
	DCb	-13.0	-6.5	-6.7	-11.7	-21.3	-3.4	-3.5	-22.9	-4.0
	BCf	-22.6	-1.3	-11.8	-37.3	-19.2	-9.0	-15.1	-19.7	-13.3
	BCb	-11.3	-12.7	-6.0	-19.4	-21.3	-2.9	-7.8	-22.1	-5.3

表 3: Local cache hit ratio (F=1024, unweight)

X_1, X_2	placement method	rank1			rank2			rank3		
		AC	EC	LCD	AC	EC	LCD	AC	EC	LCD
1	DCf	-51.2	-72.1	-22.2	-51.1	0.0	-28.8	-48.3	0.0	14.2
	DCb	-51.3	-88.4	-51.0	-48.4	0.0	-44.3	-50.3	0.0	11.8
	BCf	-58.5	-77.8	-54.5	-60.9	0.0	-28.4	-58.2	0.0	0.7
	BCb	-60.2	-89.1	-60.4	-59.9	0.0	-69.3	-57.8	0.0	-5.7
2	DCf	-60.0	-87.4	-20.5	-53.2	-60.4	-10.4	-48.1	0.0	-34.2
	DCb	-56.0	-89.1	-54.8	-52.6	-80.0	-44.1	-45.3	0.0	-46.5
	BCf	-61.6	-87.6	-28.9	-53.2	-60.5	-17.8	-47.0	0.0	-13.3
	BCb	-54.7	-79.0	-57.6	-52.6	-37.1	-45.4	-47.9	0.0	-46.8
4	DCf	-46.8	-78.7	-23.8	-44.0	-48.8	-13.5	-33.9	-43.8	-6.0
	DCb	-32.2	-76.8	-45.3	-47.4	-60.3	-33.6	-33.1	-49.1	-59.0
	BCf	-49.2	-77.7	-15.9	-45.8	-49.7	-7.7	-34.3	-45.6	-18.6
	BCb	-43.0	-68.0	-45.1	-38.4	-60.0	-35.6	-32.2	-61.6	-59.6

表 4: Local cache hit ratio (F=32, weight)

X_1, X_2	placement method	rank1			rank2			rank3		
		AC	EC	LCD	AC	EC	LCD	AC	EC	LCD
1	DCf	-43.8	-30.8	-24.5	-7.2	0.0	-0.3	-5.0	0.0	-0.6
	DCb	-13.4	-10.0	-7.2	-3.9	0.0	-1.5	-16.0	0.0	-0.3
	BCf	-30.1	-25.8	-18.7	-5.0	0.0	-4.2	-17.2	0.0	-2.5
	BCb	-11.2	-15.5	-8.8	-12.9	0.0	-1.9	-12.9	0.0	-2.2
2	DCf	-44.4	-13.5	-12.7	-24.1	-26.0	-20.9	-10.4	0.0	-25.7
	DCb	-9.4	-8.9	-6.0	-9.7	-4.5	-5.9	-6.5	0.0	0.2
	BCf	-43.7	-14.5	-14.3	-23.5	-26.7	-21.7	-8.9	0.0	-49.6
	BCb	-7.0	-13.7	-6.5	-7.3	-12.5	-2.6	-7.3	0.0	-3.9
4	DCf	-28.9	-8.1	-16.0	-36.8	-22.1	-15.0	-17.3	-25.2	-18.8
	DCb	-7.8	-4.2	-3.2	-5.9	-7.5	-3.8	-3.6	-16.8	-8.1
	BCf	-28.7	-14.7	-17.4	-37.1	-22.0	-15.3	-17.7	-25.5	-18.6
	BCb	-7.6	-13.4	-3.6	-5.4	-7.2	-2.3	3.6	-23.8	-2.6

表 5: Local cache hit ratio (F=1024, weight)

X_1, X_2	placement method	rank1			rank2			rank3		
		AC	EC	LCD	AC	EC	LCD	AC	EC	LCD
1	DCf	-24.5	-71.4	-25.3	-36.5	0.0	-29.7	-15.4	0.0	-7.1
	DCb	-23.3	-82.4	-53.8	-39.2	0.0	-41.5	-20.8	0.0	-11.9
	BCf	-54.8	-78.2	-27.7	-44.6	0.0	-46.9	-62.9	0.0	12.5
	BCb	-52.2	-87.5	-73.8	-43.1	0.0	-59.4	-62.7	0.0	2.2
2	DCf	-39.3	-89.9	-13.1	-38.2	-62.3	-18.5	-61.7	0.0	-23.4
	DCb	-37.0	-69.0	-56.6	-38.8	-81.4	-49.2	-57.6	0.0	-44.3
	BCf	-40.4	-88.8	-18.4	-36.2	-63.3	-13.1	-62.3	0.0	-12.1
	BCb	-39.0	-76.1	-56.4	-38.7	-34.8	-48.7	-57.7	0.0	-44.8
4	DCf	-35.5	-80.8	-18.4	-50.2	-52.4	-7.0	-47.7	-44.1	-18.1
	DCb	-31.2	-66.7	-48.4	-47.8	-48.3	-35.4	-39.1	-46.5	-70.2
	BCf	-34.0	-79.7	-13.7	-48.9	-50.1	-15.0	-48.0	-46.5	-5.7
	BCb	-31.7	-48.8	-48.7	-43.9	-56.7	-35.0	-39.6	-72.7	-71.9

5. ま と め

ICN における CPA に対する対処法を確立するには、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ことが望ましい。そこで本稿では独自 fake 型の CPA を想定し、複数攻撃者配置において、大規模なネットワークボ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、様々な要素が独自 fake 型 CPA の効果に与える影響を分析し、CPA の脅威を明らかにした。本稿で得られた知見を以下に示す。

- fake コンテンツや bot の配置数が少ない場合、特定のノードに集中的に fake コンテンツを注入可能である。一方、fake コンテンツや bot の配置数が増加するにつれて fake コンテンツへの interest が分散されるため、複数のノードに平均的に多くの fake コンテンツを注入可能である。

- 独自 fake 型 CPA においては、fake コンテンツへの interest がオリジナルまで転送される機会が重要である。bot の数が増加するにつれ、fake コンテンツへの interest が分散するため、各 bot/fake コンテンツ配置ノード組間の interest 発生レートは、bot/fake コンテンツの配置ノード数と bot の要求比率の両方の影響を受ける。そのため bot の要求比率は bot の数や bot が存在するノードの人口比などを考慮して定める必要がある。

- 正当なユーザの要求比率は独自 fake 型 CPA の効果に影響を与え、人気の偏りが大きいほど CPA の影響は大きくなる。

- CS を次数で重み付けして設定した場合、提案配置方式によって fake コンテンツまたは bot を betweenness centrality や次数の大きい NW の主要なノードに割当てすることで、CPA の影響は大きくなる。

謝辞 本研究成果は、JSPS 科研費 18K11283 および 21H03437 の助成を受けたものである。ここに記して謝意を表す。

文 献

- [1] T. Nguyen, et al., "Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment." IFIP/IEEE IM 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, 2022 年 7 月
- [3] W. Cui, et al., "Feedback-Based Content Poisoning Mitigation in Named Data Networking." IEEE ISCC 2018
- [4] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, "A Survey on Content-Oriented Networking for Efficient Content Delivery," IEEE Commun. Mag., vol.49, 3, pp.121-127, Mar. 2011.
- [5] K. Cho, et al., "WAVE: Popularity-based and Collaborative In-network Caching for Content-Oriented Networks," IEEE NOMEN 2012.
- [6] 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.
- [7] V. Sourlas, L. Tassioulas, I. Psaras, and G. Pavlou, "Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks," IFIP Networking 2015.
- [8] CAIDA web page, <http://www.caida.org/data>
- [9] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, "Web Caching and Zipf-like Distributions: Evidence and Implications," IEEE INFOCOM 1999.
- [10] M. Cha, H. Kwak, P. Rodriguez, Y. Ahn, and S. Moon, "Analyzing the Video Popularity Characteristics of Large-Scale User Generated Content Systems," IEEE/ACM ToN, Vol.17, NO.5, pp.1357-1370, Oct. 2009.
- [11] H. Yu, D. Zheng, B. Y. Zhao, and W. Zheng, "Understand-ing User Behavior in Large-Scale Video-on-Demand Systems," ACM EuroSys 2006.
- [12] G. Xylomenos, et al., "A Survey of Information-Centric Networking Research," IEEE Communications Survey and Tutorials, Vol. 16, No. 2, pp.1024-1049, 2014.
- [13] L. Zhang, et al., "Named Data Networking (NDN) Project," Technical Report NDN-0001, Oct. 2010.