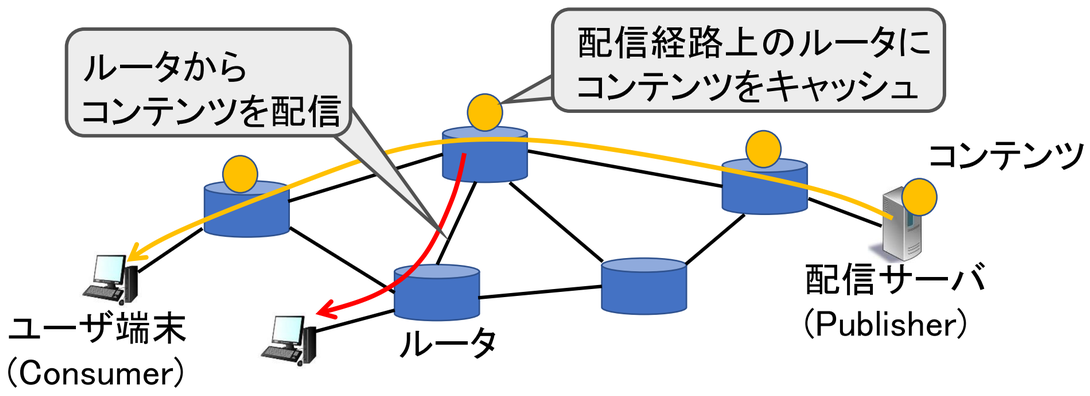
ネットワークトポロジがコンテンツポイズニング攻撃に与える影響の分析

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

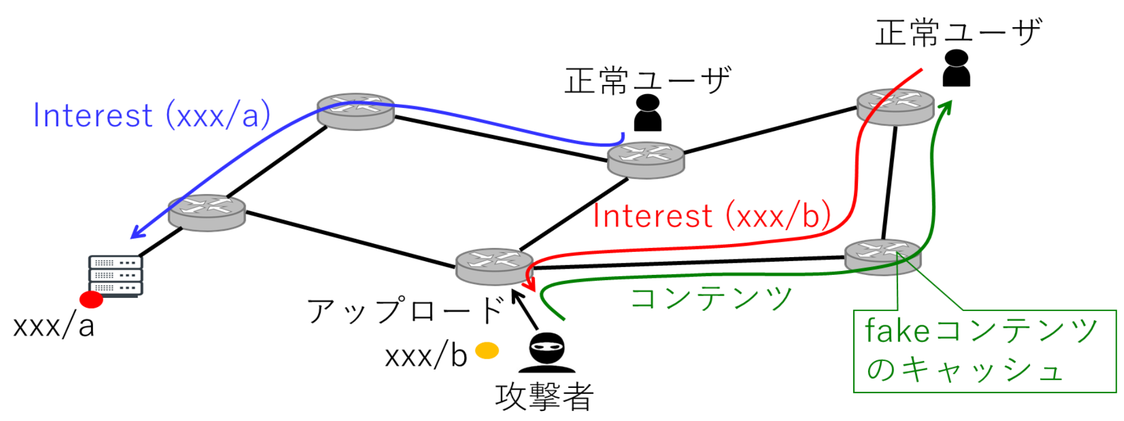


- ICNでは誰もがNWにコンテンツをアップロードできるため，コンテンツポイズニング攻撃(CPA: Content Poisoning Attack)の問題が指摘

本研究：
NWトポロジが独自fake型CPAの脅威に与える影響を分析

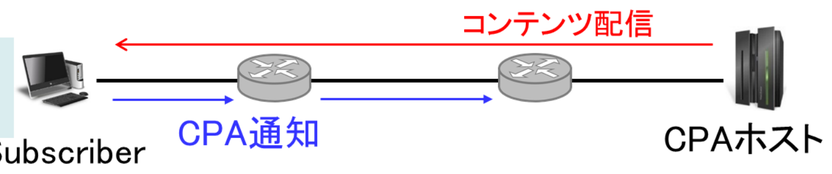
2. CPAとは

- CPAの仕組み
  - 攻撃者が偽のコンテンツをアップロードすることで，ルータのContent Store (CS)に無効コンテンツを注入

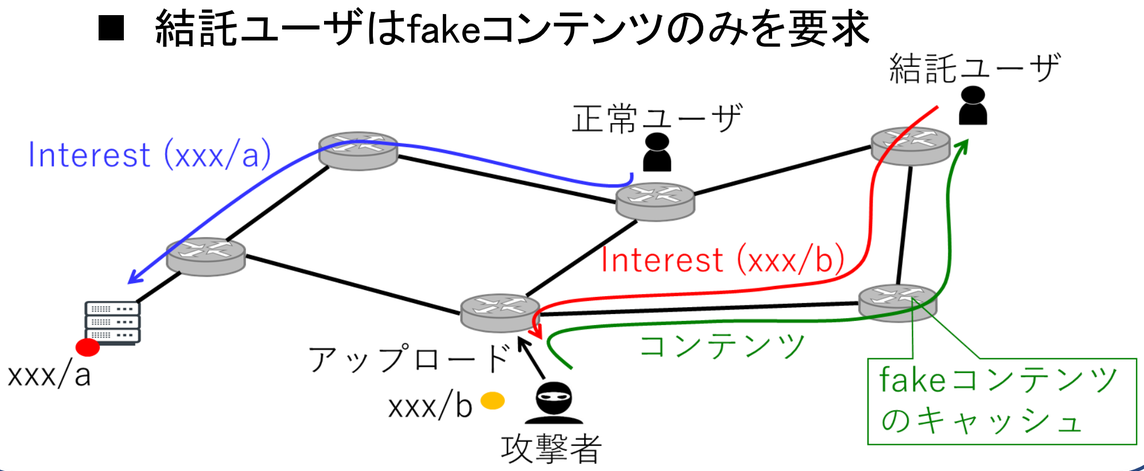


- コンテンツ要求者(Subscriber)は受信コンテンツの正当性を，公開鍵暗号を用いたディジタル署名により判断可能
- 2種類のCPA: corrupted型，fake型
  - corrupted型：ディジタル署名と一致しない偽のコンテンツをCSに注入 ⇒ ディジタル署名の検査で容易に検出可能
  - fake型：ディジタル署名と一致する偽のコンテンツをCSに注入 ⇒ディジタル署名の検査で検出不可

ディジタル署名によるCPAの検知



- 独自fake型
  - ディジタル署名と一致するfakeコンテンツを独自に作成
  - 攻撃者と結託ユーザとが連携して動作
    - 正常ユーザは通常通り正当なコンテンツを要求
    - 結託ユーザはfakeコンテンツのみを要求



3. 攻撃者配置方式

- fakeコンテンツの配置方法
  - NW上の多数のノードにfakeコンテンツを拡散できる位置が望ましい
    - AVH方式： 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方式： Betweenness Centralityが最大のノードに配置
- 結託ユーザの配置方法
  - 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たい
    - PC：パス数のみを考慮
    - PAH：パス数及びホップ長を考慮

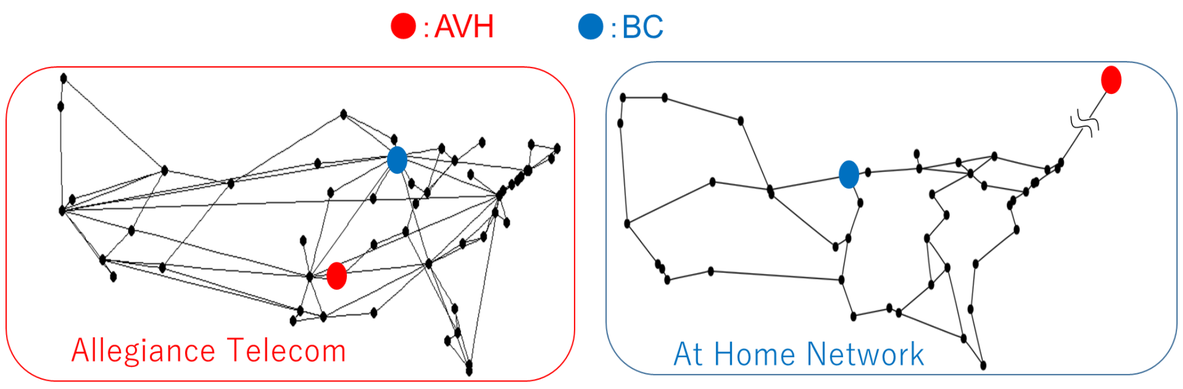
Algorithm 1 Placement of colluded users

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

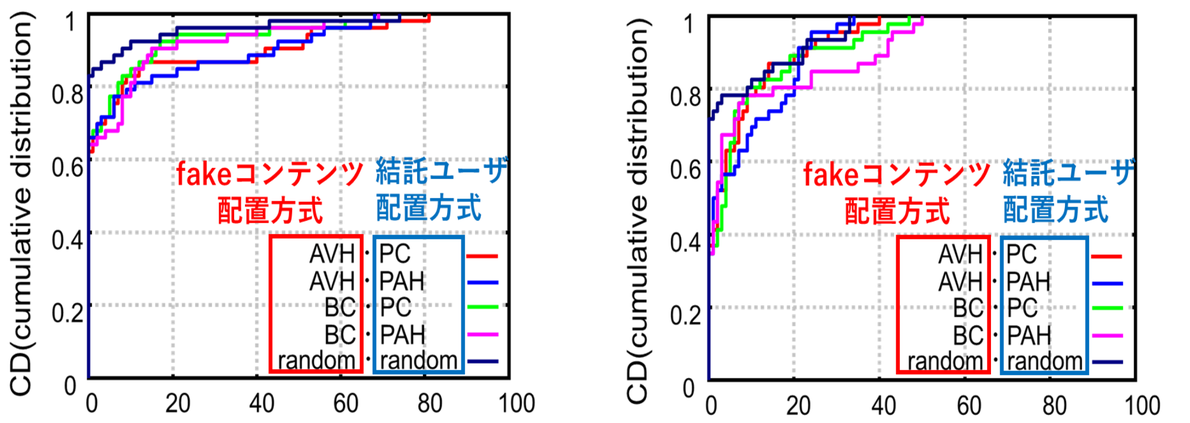
- C：結託ユーザの数(C=5)
- N：全ノード集合
- U：結託ユーザの配置ノード集合
- M_n：ノードnの接続リンク集合
- $f(l)$：リンク重み
  - PC：$f(l) = 1/x(l)$
  - PAH：$f(l) = 1/\{x(l)h(l)\}$
  - $x(l)$：リンクlを経由するfake contentパス数
  - $h(l)$：リンクlのfake contentからのホップ長

4. 性能評価

- fakeコンテンツ配置結果



- 各ルータにキャッシュされたfakeコンテンツ数の累積分布



(a) Allegiance Telecom　(b) At Home Network

- (a) Allegiance Telecom ⇒ AVH方式の効果が大
- (b) At Home Network ⇒ BC方式の効果が大
- ラダー型のNWトポロジ ⇒ CPAの影響が大
  - ノード間の経由ノード数が多い傾向があるため
- NWの中央付近にfakeコンテンツを配置することで，CPAの影響が拡大

5. 今後の予定

- 最適なfakeコンテンツ数や最適な攻撃者の数について分析