ICN における IOTA を用いたコンテンツ名管理方式

Management System of Content Name of ICN Using IOTA

岡田 鉄平　　上山 憲昭
Teppei Okada　　Noriaki Kamiyama
立命館大学 情報理工学部 情報理工学科
College of Information Science and Engineering, Ritsumeikan University

1. はじめに　要求されたコンテンツの名称をもとにパケットを転送し，ルータにてコンテンツをキャッシュしコンテンツ要求者 (Consumer) に配信する情報指向ネットワーク (ICN: information-centric networking) が，次世代のネットワークとして注目を集めている．ICN では誰もが Publisher としてコンテンツをアップロード可能だが，正当な Publisher を騙る攻撃者が，実在するコンテンツ名で fake コンテンツをアップロードすることでキャッシュの機能を低下させる CPA (content poisoning attack) の問題が指摘されている [1]．CPA の対策として，Consumer が公開鍵暗号を用いたディジタル署名によりコンテンツの正当性を判断し，不当なコンテンツをルータに通知する方式が提案されている [2]．しかしコンテンツに紐づいた公開鍵により生成されたディジタル署名と一致する fake 型 CPA[3] では，[2] の方式では検知は困難となる．中でも，公開鍵を管理する認証局の職員が攻撃者と結託し，攻撃者の公開鍵と書き換えることにより，実在する高人気コンテンツを騙る fake コンテンツをキャッシュに注入する詐称 fake 型 CPA は対策が困難である．本攻撃はアクセス数が多い人気コンテンツを詐称されると攻撃の影響が大きいことが推測される [4]．また，正当な Publisher の公開鍵を乗っ取って書き換えているため，攻撃者のコンテンツの方が正当化される．

そこで本稿では，Publisher によるコンテンツのアップロードに際し，登録データの改ざんが困難な分散型台帳技術の一つである IOTA[5] でコンテンツ名を管理することで詐称 fake 型 CPA を未然に防ぐ方式を提案する．分散型台帳としては Blockchain が代表的であるが，Blockchain はスケール性に課題があるのに対し，IOTA はスケール性が高い．提案方式では，台帳内でコンテンツ名を検索する四つの探索手法の検索時間と，必要メモリ量の比較を行った．その結果，検索時間と必要メモリ量のトレードオフの関係を確認した．

2. 提案方式 IOTA では，新しい transaction が未承認の transaction である tip の中から二つ選択し，有向非巡回グラフ (DAG: directed acyclic graph) を形成することで分散型台帳が実装される [5]．その tip 選択アルゴリズムは，tip の中からランダムに二つ選択する URS (uniform random selection)，最初の transaction であるジェネシス transaction から等確率に tip を選択する URW (uniform random walk)，transaction の重みを考慮して選択する WRW (weighted random walk) の三つである．WRW においては，H_x, H_y を transaction x および y の累積重み，$\alpha(\geq 0)$ を累積重みのパラメタとすると，transaction y から x への遷移確率 P_{xy} は以下の式で定義される．

$$P_{xy} = \frac{e^{-\alpha(H_x - H_y)}}{\sum_{z:z\to x} e^{-\alpha(H_x - H_z)}} \quad (1)$$

Publisher は，コンテンツのアップロードに際して，コンテンツの Prefix，ID，公開鍵，ディジタル署名，コンテンツ名を transaction に登録する．その際，重複するコンテンツ名の管理を防ぐため，既に同じコンテンツ名が管理されているか IOTA 台帳内で探索し，存在していなければ登録する．アップロードが終了した後，Consumer がコンテンツの Prefix を要求し，それを基に台帳内で検索する．そして発見したコンテンツ名を Consumer に回答し，Consumer はそのコンテンツ名で要求パケットである Interest を送信し，コンテンツを要求する．

DAG 内でコンテンツ名を検索するタイミングは，Publisher によるコンテンツ名登録時と，Consumer による名前解決時の二つである．DAG の検索法として，ハッシュチェイン法，二分探索木 (bst: binary search tree)，幅優先探索 (bfs: breadth-first search)，深さ優先探索 (dfs: depth-first search) の四つを考え，次節ではこれら手法間で検索時間と，必要メモリ量を比較する．ハッシュチェイン法，bst では Prefix と ID をハッシュテーブルや二分木で管理するため，発見後，DAG 上に直接アクセスしてコンテンツ名を取得する必要があるのに対し，bfs，dfs では，transaction にコンテンツ名が管理されているため，発見した時点で探索が終了する．

3. 性能評価　提案方式を計算機シミュレーションにより評価する．transaction 数 N_t を 100, 1000 の二通りで，WRW の tip 選択アルゴリズムで DAG を生成する．新規コンテンツ名登録による transaction 生成はレート $\lambda_1 = 50(/秒)$ の指数分布に従い発生させる．また遷移確率の式 (1) における α を 0.1 とする．Consumer による要求は，総要求数を 5000 とし，発生レートを $\lambda_2 = 50(/秒)$ の指数分布に従い発生させる．またハッシュチェイン法におけるテーブルのバケット数 B を 100 とする．

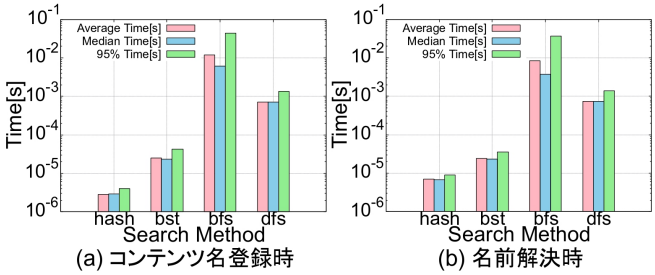

図 1: transaction 検索時間

図 1 に該当 transaction の探索に要する検索時間の平均値，中央値，95%値を示す．(a)，(b) のいずれの場合もハッシュチェイン法が最も検索時間が小さく，bfs が最も大きい．また，WRW ではジェネシス transaction からのホップ数が大きい transaction が多いため，URS，URW に比べて bfs に時間を費やすことも確認した．

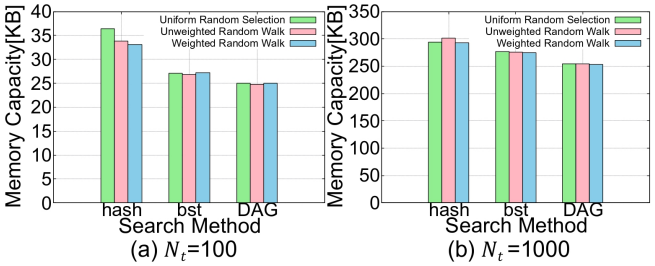

図 2: 必要メモリ量

図 2 に必要メモリ量を示す．ハッシュチェイン法ではハッシュテーブルで最大の容量を持つバケットの容量が全てのバケットで確保されるため，大量のメモリを必要とするが，DAG では他のテーブルなどで管理する必要がないため，最も必要メモリ量が少ない．また，transaction 数が増加するとハッシュチェイン法と bst の必要メモリ量の差が縮まることが確認できる．これはハッシュチェイン法では生成データ数にかかわらず，ハッシュテーブルで固定的に大量のメモリが必要となるためである．

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.”, IFIP/IEEE IM 2017.
[2] W. Cui, et al., “Feedback-Based Content Poisoning Mitigation in Named Data Networking”, IEEE ISCC 2018.
[3] P. Gasti, et al., ”DoS and DDoS in Named Data Networking”, IEEE ICCCN 2013.
[4] 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”, 信学会 CQ 研究会, CQ2022-23, 2022 年 7 月
[5] S. Popov, et al., Equilibria in the Tangle, Computers & Industrial Engineering, 136, pp.160-172, Oct. 2019.