

SDN を用いた NDN のアクセス制御方式の性能評価

Performance Evaluation of Access Control Using SDN in Named Data Networking

楊 湛斌¹

上山 憲昭²

Zhanbin Yang

Noriaki Kamiyama

立命館大学 情報理工学研究科¹

Graduate School of Information Science and Engineering, Ritsumeikan University

1. はじめに

Information-Centric Networking (ICN) が、コンテンツを効率的に転送するネットワークとして検討されている。ICN のアーキテクチャの一つに Named Data Networking (NDN) があり、NDN のキャッシュ技術は重要な研究分野である。NDN では要求パケットが到着したルータでコンテンツがキャッシュされている場合、そのルータからコンテンツが配信されるため、コンテンツのオリジナルを提供するパブリッシャに、常に配信要求が届くとは限らず、パブリッシャはコンテンツの要求に対するアクセス制御を行うことができない。

そのため NDN では新たなアクセス制御の仕組みが必要となるが、アクセス制御を NDN の従来の自律分散型の通信方式で実装した場合、制御情報の伝達効率が低くなる。一方、Software Defined Networking (SDN) は制御情報を交換するレイヤと、ユーザデータが転送されるデータレイヤとを分離し、制御情報の交換効率を向上させることができる。そこで筆者らは、パブリッシャによるデータのアクセス制御を可能にし、効率的なアクセス効率とキャッシュセキュリティを確保する、SDN ベースの NDN アクセス制御方式を提案した [4]。本稿ではその有効性を確認するため、本方式の計算機シミュレーションによる性能評価結果を示す。

2. 提案方式

図 1 に [4] で提案した SDN を用いた NDN のアクセス制御方式の動作を示す。

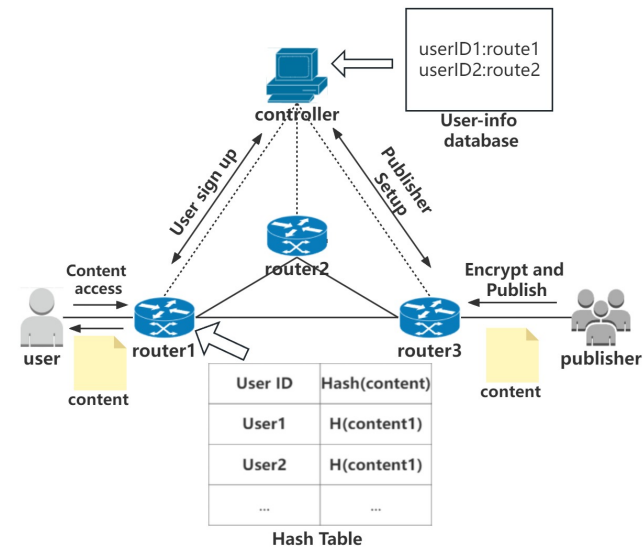


図 1: Overview of proposed method

2.1 初期化 パブリッシャはコンテンツを配信する前に、コンテンツ名をコントローラに登録し、コントローラで生成した Public Key (PK) を受け取る。新しいユーザがアプリケーションに参加するとき、コントローラは状況に応じて対応する属性のセットをユーザに割り当てる。同時にルータはユーザの対応ポートを記録し、コントローラがユーザと対応ルータを記録する。そしてコントローラは、ユーザの属性と MK に基づいて、対応する復号化キー Secret Key (SK) とユーザ ID を生成する。

2.2 暗号化 パブリッシャ側でコンテンツを暗号化して配信する。暗号化はコンテンツを大小 2 つの部分に分けて行うが、1 つ目 (パート 0) は属性アクセスポリシーと PK であり、小さい部分を暗号化する。2 つ目は対称鍵暗号方式で大きい部分を暗号化する。そのためコンテンツの大きい部分はどのようなユーザでも復号可能となり、NDN におけるキャッシング機能を活用する

ことが可能である。

2.3 アクセス制御

実際のアクセス制御はルータで行う。まずユーザは ID サインとして、Interest パケットのランダム数 Nonce とユーザ ID をスプライスして暗号化する。そして、これを名前パラメータとして Interest パケットに追加する。ルータは ID サインをハッシュテーブルのユーザ ID と Interest の Nonce に署名することで検証する。またアクセス制御の要求を応答するとき、CPABE で暗号化した部分 (パート 0) のみ返送する。残りのデータは別途要求する必要がある。また認証が通らない場合、直接要求パケットを破棄する。パート 0 は SK で復号化するため、ルータにキャッシュすることが許可されている。

2.4 権限更新

パブリッシャがアクセス権限を更新したい場合、まずコントローラに変更点を送る。コントローラが変更要求を受け取った後すぐにデータベースの情報を更新し、新しいアクセス制御情報が対応するルータに送られる。ルータのストレージスペースを節約するため、ルータの管理下に権限があるユーザのみがハッシュテーブルに記録される。ユーザが別のルータに移動した場合、再登録とルータへの再バインドのために、ユーザ ID をコントローラに送信する必要がある。

3. 性能評価

本稿では [1] で提案したアクセス制御方式の制御パケット量を評価する。提案方式と既存方式 [2] で、Allegiance Telecom トポロジ上の全ユーザが目的コンテンツを 1 回要求した場合に、各ノード n に到着する Interest パケット数 B_n を計算機シミュレーションにより比較評価する。

従来方式ではパート 0 を取得する前に、ユーザはパブリッシャでアクセス制御を完了する必要がある。一方、提案方式では、アクセス制御をルータで行うことができ、パート 0 をキャッシュすることで、完全なコンテンツに対する要求は 1 回のみで、2 回目以降の要求ユーザはルータでコンテンツを取得できる。ユーザ数が m のとき、従来方式はユーザの Interest パケットを m 回、隣接ノードに転送する必要がある。そのため従来方式の各ノードの到着 Interest パケット数は、提案方式の m 倍となる。

図 2 に単一パブリッシャの場合における 2 つの各方式の各ノードの B_n を、ノード番号に対してプロットする。パブリッシャのトラフィックの削減率は最大で 68 % と高い。リクエストの転送に関与するノードはすべてトラフィック量が削減するが、なかでも主要ハブノードであるノード 6 は、トラフィック量が 66 % 減少している。これは提案方式が負荷の高いノードが処理する必要のあるリクエストを効果的に削減できることを意味する。

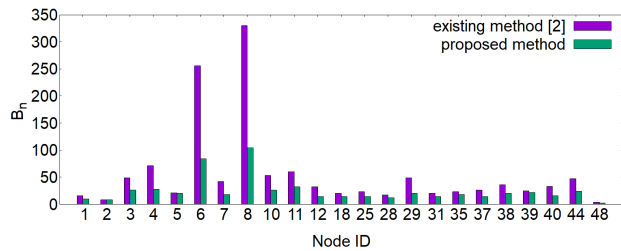


図 2: Number of Interest packets B_n at each node n in one user request

謝辞 本研究成果は JSPS 科研費 21H03436 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] 楊湛斌, 上山憲昭, “SDN を用いた NDN のアクセス制御方式”, 信学会 2023 年ソ大会, B-14-8
- [2] Y. Fukagawa and N. Kamiyama, “Access Control Method with Privacy Preservation in NDN,” IEEE ICNP 2023 (Poster)