SDNを用いたNDNのアクセス制御方式

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．そこで本稿では，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する．提案方式では，ユーザ情報をサインとして暗号化し，Interest パケットのパラメタとして追加することで，SDN コントローラの管理下でルータに要求パケットを認証する機能を与える．また，[2] を用いることで，一旦ファイルがキャッシュされるとデータは安全に保護される．

2. 提案方式

図 1 に，NDN 上での本稿の提案方式の動作を示す．

2.1 初期化 コントローラはユーザの情報，関連ルータと属性アクセス構造 (Access Structure (AS)) を格納するデータベースを管理する．もし変更がある場合，新しいバージョンの情報を含むハッシュ値を生成し，担当するルータへ通知することで，すべてのルータが所持している情報を常に最新のままに保つ．また提案方式では，データプレーンとコントロルプレーンがそれぞれ独立しており，お互いに干渉できない．すなわちユーザがコントローラにアクセスできず，またコントローラもルータ上のデータにアクセスできない．このような仕組みとすることで，アクセス情報とデータの安全性を保証する．

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．なお PK の生成には Master Key (MK) が必要である．

新しいユーザがアプリケーションに参加するとき，そのユーザは既存の属性をコントローラに提出するか，何もなければ空のセットを提出し，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 そしてパブリッシャ側でコンテンツを暗号化して配信する．暗号化で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ィと 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 アクセス制御リストの配布は，コントローラ内部のデータベースそのものではなく，ルータの該当ユーザの情報を記載しているハッシュテーブルを送る．コントローラは，ハッシュテーブル (ユーザ ID をもとに，このユーザに対して許可されたアクセスコンテンツを探し出す) の更新のみルータに送ることになる．

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し，一致すれば身元認証はパスする．．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 で復号化する必要があるので，ルータにキャッシュすることが許可されている．

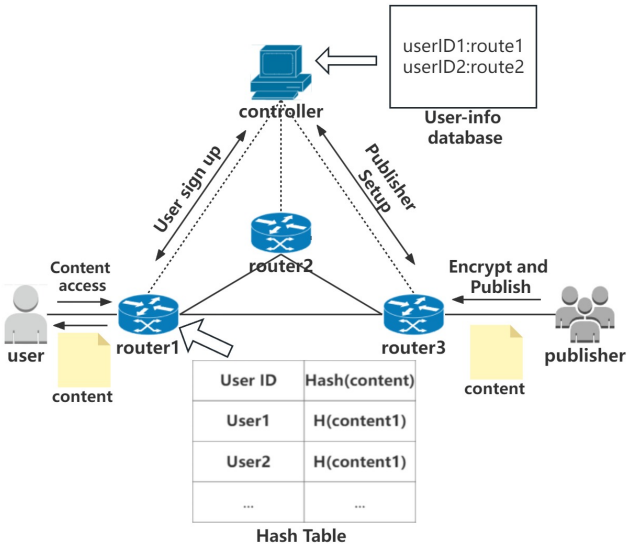

図 1: Overview of proposed method

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する．そして、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遷移する場合，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．

属性暗号化技術を用いたアクセス制御では，権限の取り消しが二種類に分けられる．例えば，パブリッシャが認可されたユーザのアクセスを無効にする指示を受け取った場合，そのユーザを管理するルータに対して個別に失効アップデートを送信することができる．この場合，取り消し指示を受け取ったコントローラは，自身のデータベース上に保存しているユーザエントリの情報を更新するだけで済む．取り消されたユーザの権限がまだ失効していない場合，コンテンツの再暗号化はルータによって実行される．[2] の手法に従うと．このプロセスで取り消されたユーザ ID は，キャンセルリストに追加され，そのユーザがコンテンツを復号できないことを保証する．これにより，パブリッシャの重複暗号化負荷が軽減される．二種類目はグループ単位の取り消しである．つまり，あるコンテンツから，許可が下りた属性のいくつを削除することである．この場合，属性アクセス構造を更新する必要がある．コントローラはこれを受け取り，許可情報を更新して新しいハッシュテーブルを生成し，ハッシュテーブルを対応するルータに送る．ルータは地元の対応キャッシュを削除し，再度パブリッシャに対応コンテンツをリクエストする必要がある．

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] Z.Wu, E.Xu, L.Liu and M.Yue, ”CHTDS: A CP-ABE Access Control Scheme Based on Hash Table and Data Segmentation in NDN, ” 2019 18th IEEE International Conference On Trust, 2019
[2] Z.Liu, F.Wang, K.Chen, F.Tang, and K.Liang. A New User Revocable Ciphertext-Policy Attribute-Based Encryption with Ciphertext Update. Sec. and Commun.Netw.2020