NDN におけるプライバシー保護と個別鍵配送を用いたアクセス制御方式

Access Control with Privacy Preservation Using Individual Key Delivery in Named Data Networking

深川 悠馬[1]　　上山 憲昭[2]
Yuma Fukagawa　　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
立命館大学 情報理工学部[2]
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

ICN (information-centric networking) が，コンテンツを効率よく転送するネットワークとして注目されている．ICN のアーキテクチャの一つに NDN (Named Data Networking) が存在する [2]．NDN は，コンテンツを要求する際に要求コンテンツ名で配信要求 (Interest) を送信する．そのため攻撃者がスニッフィングにより，Interest の情報からどのコンテンツを取得しているのかを盗聴できる問題があり，ユーザのプライバシーを守るために，要求されたコンテンツ名に対する秘匿性も望まれる．そのため，この問題を回避するためにコンテンツ名を暗号化するといった対策をとることが考えられる．しかしコンテンツ名を暗号化するだけでは，暗号化コンテンツ名を収集し，統計的に要求頻度の高い暗号化コンテンツ名と人気コンテンツ名を結び付けることで，コンテンツ名を特定する頻度攻撃が可能である [1].

著者らは，NDN におけるプライバシー保護を目的としたコンテンツ名暗号化，Publisher でのアクセス制御方式を提案した [4]．本稿では，本アクセス制御方式に必要な制御トラヒック量，暗号化，復号化回数や使用する鍵の生成数を，既存の NDN アクセス制御手法である NAC (Name-based Access Control)[3] と数値比較し，その有効性を明らかにする．

2. Name-based Access Control

NAC ではコンテンツを暗号化するコンテンツ鍵に Key-Encrypt Key (KEK)，Key-Decrypt Key (KDK) を使用することで Consumer 毎に粒度の高いアクセス制御を実現している [3]．また，鍵生成の処理を分散させることが可能である．Consumer はコンテンツを要求することでコンテンツの名前からコンテンツ鍵の名前を取得し，コンテンツ鍵を要求する．コンテンツ鍵は KEK で暗号化されているため，コンテンツ鍵の名前から KDK の名前を取得し要求を行う．各コンテンツの取得に必要な名前に対して平文を使用しているため，Consumer の各要求コンテンツが攻撃者に知られるプライバシー漏洩の問題がある．

3. 頻度攻撃

コンテンツを平文の名前で要求することで発生するプライバシー漏洩の問題に対して，コンテンツ名を暗号化して要求する対策が考えられる．しかしスニッフィングを行う攻撃者が各暗号化コンテンツ名を収集し，コンテンツの人気順位などのコンテンツを特定化可能な情報と比較することで暗号化コンテンツ名からコンテンツ名を特定する頻度攻撃 [1] が可能である．そのため，ただ暗号化するだけでは不十分である．

4. 提案方式

[4] で著者らが提案した方式では，初回 Interest と呼ばれるコンテンツ鍵要求を固有の名前で行い，常に Publisher へと要求を到着させることで Publisher はアクセス制御を実行する．また，コンテンツ鍵の名前からコンテンツの名前を取得することでコンテンツを要求可能となる．各要求に使用するコンテンツ名はすべて暗号化されているためプライバシーは保護されている．また，Publisher はコンテンツの名前を定期的に変更することで頻度攻撃の影響を減少させることが可能である [4].

5. 性能評価

提案方式では NAC[3] で問題であったプライバシーの問題を解決するが，一方で制御トラヒック量の増加，暗号化，復号化の処理の増加が懸念される．そこで本節では，NAC との配信要求あたりの制御トラヒック量，暗号化，復号化の回数，使用する鍵の生成数の数値評価を行う．制御トラヒック量はコンテンツ鍵のやり取りに発生するトラヒック量とする．

制御トラヒック量の評価の条件として，コンテンツ鍵の交換周期を 1 時間，KEK/KDK の交換周期を 24 時間，コンテンツの数を 10000，Interest，コンテンツ鍵，KEK/KDK のトラヒック量を 100 (Byte) とする．また，各コンテンツの要求分布として Zipf 分布を想定した．

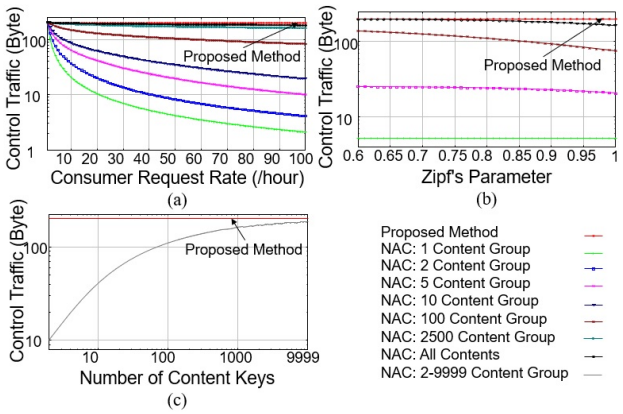

図 1: 制御トラヒック量

図 1 に制御トラヒック量の数値評価結果を示す．提案方式ではどのパラメータにおいても，初回 Interest は常に発生するため約 200 Byte の制御トラヒック量が発生している．図 1(a), (b), (c) から NAC は 1 時間に Consumer が要求する回数が増加し，Zipf 分布のパラメータの偏りが大きく，コンテンツ鍵の数が減少するほど制御トラヒック量が減少する．そのため提案方式は NAC よりも制御トラヒック量が増加することが確認できる．しかし制御トラヒック量はコンテンツのデータ量と比較すればごく僅かな量であり，1 回の配信要求において発生するトラヒックの大部分はコンテンツデータであり問題はないと考えられる．

暗号化，復号化の評価の条件としてコンテンツ鍵の交換周期を 1 時間，KEK/KDK の交換周期を 24 時間，鍵を生成する Publisher の数を N_{P_k}，Publisher のコンテンツに 1 日にアクセスが許可されている Consumer の数を $N_{C_{24}}$ とする．

1 要求あたりの，暗号化，復号化の回数は，NAC では $2+2N_{P_k}$ 回となり，提案方式では鍵生成を分散させる機構がなくコンテンツ名暗号化も行うため固定で 10 回となる．そのため，暗号化や復号化に伴う処理時間などは回数に比例した値になる．

次に暗号化，復号化に使用する鍵の生成数を 1 日当たりで評価する．NAC では 24 回のコンテンツ鍵生成に加え，KDK が 1 日に $N_{C_{24}}$ 人分生成されるため，$24+N_{C_{24}}$ 個となる．提案方式は 1 時間毎に $N_{C_{24}}$ 人にコンテンツ鍵を生成するため，$24N_{C_{24}}$ 個となる．そのため，どちらの方式も $O(N_{C_{24}})$ となり，Consumer の数によって鍵生成数が増加する．

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] C. Ghali, G. Tsudik, CA. Wood, “When encryption is not enough: Privacy attacks in content-centric networking”, ACM ICN, 2017, p1-10.
[2] L. Zhang, et al. “Named data networking”. ACM SIGCOMM CCR, 2014, 44.3: 66-73.
[3] Y. Yu, A. Afanasyev, L. Zhang, “Name-Based Access Control”, Technical Report NDN-0034, Jan 2016.
[4] 深川悠馬, 上山憲昭, “NDN でのプライバシー保護を目的としたアクセス制御方式の検討”, 2022 信学会ソ大, B-11-9, 2022 年 9 月