ICNの共通鍵暗号を用いたアクセス制御方式の性能解析

Performance Analysis of Access Control Using Symmetric Key in ICN

深川 悠馬[1]　　上山 憲昭[2]
Yuma Fukagawa　　Noriaki Kamiyama
福岡大学 工学部 電子情報工学科[1]
Faculty of Engineering, Fukuoka 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，コンテンツを効率的に転送するネットワークとして注目されている．従来インターネットでは，有料や会員限定のコンテンツなど特定ユーザだけがコンテンツを消費できる配信サービスに対し，通信開始時に配信要求が必ずコンテンツ事業者 (Publisher) のサーバに届くため Publisher によるアクセス制御が可能である．しかし ICN では配信要求 (Interest) の転送経路上のルータで要求コンテンツがキャッシュされている場合，ルータから配信されるため Interest が Publisher に到達せず，Publisher によるアクセス制御が困難である．

そこでアクセス権を有するすべてのユーザ (Consumer) に鍵を配布し，アクセス権を持たない Consumer は閲覧を不可能とする方式が提案されている (一括鍵配布方式)[1]．本方式はコンテンツ単位ではなく，該当 Publisher のコンテンツ全体を対象にアクセス制御を同じ鍵で行うため，鍵を定期的に変える必要がある．そのため鍵を変えるたびにアクセス権を有する全 Consumer への鍵の再配布と更新が必要なので，処理・トラヒックのオーバヘッドが大きく，不当配信も可能である．そこで著者らは，コンテンツの配信に先立ち Consumer から共通鍵暗号方式で暗号化された Consumer の ID を含む Interest を常に Publisher に到達させることで，Publisher にてアクセス制御を可能とする方式を提案した [2]．本稿では本方式の有効性を明らかにするため，制御トラヒック量や不当トラヒック量を一括鍵配布方式と定量的に比較する．

2. 提案方式の特徴

データパケットのヘッダにキャッシュ可否を示すフラグ (CPF: cache permission flag) を用意し，データパケットを受信したルータは CPF が 1 の場合にのみデータパケットをキャッシュする．Consumer はコンテンツ m の先頭チャンク $I_{m,1}$ の要求に先立ちアクセス承認要求のための Interest パケット $I_{m,0}$ を送信するが，本パケットに対するデータパケット $D_{m,0}$ の CPF を 0 にセットし，コンテンツのチャンク $D_{m,1}$, $D_{m,2}$, …のパケット送信時は CPF を 1 にセットする．その結果，アクセス要求の Interest は常に Publisher に到達するため，Publisher はアクセス権を有する場合にのみコンテンツを配信可能である．

Publisher はコンテンツを DES 等の共通鍵暗号方式で暗号化するが，Publisher は定期的に共通鍵を変更し，アクセス要求に対する応答として最新の共通鍵を要求 Consumer に配信する．そのためアクセス権を喪失した Consumer の視聴を防ぐことができる．提案方式では先頭チャンクの配信時にのみアクセス制御のオーバヘッドが発生するが，定期的に共通鍵を変えても鍵の再配布が不要であり，オーバヘッド処理やトラヒック量を抑えることができる．

3. 性能解析

提案方式の制御トラヒック量は，アクセス要求 Interest $I_{m,0}$ と Publisher からの応答パケット $D_{m,0}$ のトラヒック量となるため，平均ホップ長 h，総ユーザ数 n，1 日あたりのコンテンツ要求数 λ_r，$I_{m,0}$ のサイズ $L_{I,m,0}$，$D_{m,0}$ のサイズ $L_{D,m,0}$ を用いて，1 日の制御トラヒック量は $(L_{I,m,0}+L_{D,m,o})\times 2h\lambda_r n$ となる．次に一括鍵配布方式の 1 日あたりの制御トラヒック量を導出するが，すべてのルータにコンテンツがキャッシュされている場合 (Min) と，すべてのルータにコンテンツがキャッシュされていない場合 (Max) の 2 つの極端な場合を考える．ルータ数 n_r，鍵配布によるコンテンツのパケットサイズ L，鍵の交換周期 T_m を用いて，$L(n+n_r h)/T_m$ (Min) と，Lnh/T_m (Max) となる．

一括鍵配布方式の不当配信によるトラヒック量を考えるために，不当配信率を導出する．各ユーザが各日に退会する確率を p とすると，各日に退会するユーザ数はパラメタ (n,p) の二項分布に従う．二項分布は n が十分に大きいときは期待値が np，分散が $np(1-p)$ の正規分布に近似できるため，1 日の退会者数が x 人である確率 $f(x)$ は，

$$f(x)=\frac{1}{\sqrt{2\pi}}e^{-\frac{1}{2}(\frac{x-np}{\sqrt{np(1-p)}})^2} \quad (1)$$

となる．ただし数値評価では x を 1 から $np+3\sqrt{np(1-p)}$ の範囲で考える．

鍵の配布周期 T_m をタイムスロット TS とみなし，さらに各日をサブタイムスロット STS とみなすと，各 TS は T_m 個の STS から構成される．退会したユーザのうち不当配信を行う割合を y，退会後に各 STS で不当配信を行う確率を r とすると，TS の先頭から k 番目の STS で退会した人が，その TS 内で行う不当配信回数 G_k は，

$$\sum_{x=1}^{np+3\sqrt{np(1-p)}} xf(x)yr(T_m-k) \quad (2)$$

となる．よって不当配信によるトラヒック量は，コンテンツの総 interest パケット長 $L_{I,all}$，総コンテンツパケット長 $L_{D,all}$ を用いて，$\sum_{k=1}^{STS} G_k h(L_{I,all}+L_{D,all})$ となる．

4. 性能評価

n を 6,000,000，λ_r を 0.1，$L_{I,m,0}$ を 520 (byte)，$L_{D,m,0}$，L を 264 (byte)，$L_{I,all}$ を 621.25 (KB)，n_r を 200，h を $\sqrt{200}/2$，$L_{D,all}$ を 4.97 (GB)，r を 0.5 とする．図 1(a) は提案方式と一括鍵配布方式の制御トラヒック量である．提案方式は鍵の交換周期によらず 1 日あたり約 7GB の制御トラヒック量が発生している．一括鍵配布方式は鍵の交換周期が増えるほど 1 日あたりの制御トラヒック量が減少する．しかし鍵の交換周期が増えると不当配信トラヒック量も増える．図 1(b)($T_m=30$) に一括鍵配布方式の不当配信によるトラヒック量を示す． 最大で 10×10^5〜2.5×10^5 (GB) の不正トラヒック量が 1 日で発生しており，不当配信トラヒックもオーバヘッドトラヒックとみなすと，提案方式よりもオーバヘッドトラヒック量が大きくなる．

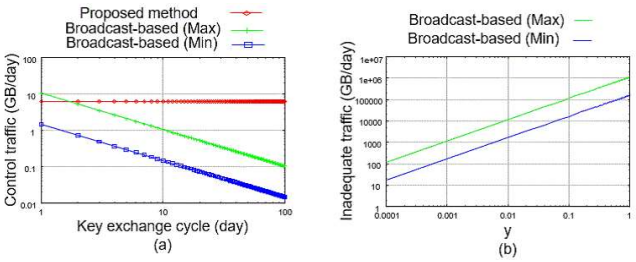

図 1: (a) 鍵の交換周期に対する制御トラヒック量，(b) 一括鍵配布方式の不当トラヒック量

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] S. Misra, et al., AccConF: An access control framework for leveraging in-network cashed data in the ICN-enabled wireless edge, IEEE Trans. Dependable and Secure Computing, 16(1), Jan./Feb. 2019
[2] 深川悠馬, 上山憲昭, ICN における公開鍵暗号を用いたアクセス制御方式, 信学会 2021 年総合大会, B-6-25, 2021 年 3 月