NDNでのプライバシー保護を目的としたアクセス制御法の検討

A Study of Access Control for privacy 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 [1]．NDN では，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る．特にアクセス制御を必要とするコンテンツに対してはコンテンツ名に対する秘匿性も望まれると推測される．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つけることで，コンテンツ名を特定する頻度攻撃が可能である [2]．

著者らは，ICN での Publisher でのアクセス制御方式を提案した [3]．しかし，NDN 上での具体的な実装については未検討である．そこで本検討では，コンテンツを要求するたびに発生させる初回 Interest を常にコンテンツ事業者 (Publisher) に到達させることで，Publisher でのアクセス制御を行うことにより，コンテンツ名の暗号化を行い，頻度攻撃の問題を減少させる方式を NDN 上での動作を考慮して提案する．

2. 提案方式の概要

本節では，本稿で提案するアクセス制御方式の概要について述べる．各コンテンツにコンテンツ鍵と呼ばれる鍵で暗号化を行い対応するコンテンツ鍵を取得しなければコンテンツを復号化できないという手法をとる．このコンテンツ鍵を取得するためにコンテンツ要求に先立って初回 Interest を送信する．NDN では Interest のパケットヘッダに存在する $MustBeFresh$ フラグをセットすることで，常に新しいデータのみが返答される．同時に Data のパケットヘッダには $MetaInfo$ 要素の中に $FreshnessPeriod$ 要素があり，この要素を 0 に設定することで $nonfresh$ データとなり，$MustBeFresh$ フラグがセットされた Interest に対する応答パケットとして返せなくなる．これらパケットヘッダを利用することで，初回 Interest で $MustBeFresh$ を使用し，初回 Interest の応答パケットであるコンテンツ鍵のパケットヘッダでは $nonfresh$ に設定しておくことで，常に初回 Interest は Publisher へと到達する．

提案方式では Publisher がコンテンツに対して任意につけたランダムな名前を実コンテンツ名と呼び，全ての人が知っているような URL などの名前を公開コンテンツ名と呼ぶ．さらに Consumer や Publisher がコンテンツ名をやり取りする際に使用する名前を仮コンテンツ名と呼ぶ．

また Interest パケットの名前に ConsumerID を含めて Interest パケットを送信することで，Publisher はどの Consumer からの要求なのかを判別することができる．そのためアクセス制御に必要な情報を Publisher に提供することが可能となる．

3. 提案方式の動作

本節では，NDN 上での本稿の提案方式の具体的な動作を図 1 を用いて説明する．ここでは 1 人の Consumer が Publisher に対してコンテンツを要求する流れを例として考える．

Publisher は，$ContentA$ という公開コンテンツ名から $aser09$ という実コンテンツ名をランダムに選択する．さらに，コンテンツ鍵 $KeyA$ でコンテンツを暗号化し，$Publisher/aser09$ という名前でコンテンツを公開する．

次に Consumer は，要求したいコンテンツの公開コンテンツ名 $ContentA$ を自身の秘密鍵で暗号化を行い，$9fe8b$ という仮コンテンツ名を生成する．さらに，自身の認証を行ってもらうための情報である $ConsumerID$ を Publisher の公開鍵で暗号化し，$ap08w$ を得る．これらの要素を組み合わせ，$Publisher/9fe8b/FOR/ap08w$ としてコンテンツ鍵を要求する初回 Interest を送信する．

初回 Interest を受信した Publisher は，$ap08w$ という情報を自身の秘密鍵で復号化し，Consumer のアクセス制御に必要な $ConsumerID$ を取得する．この情報を用いて認証を行い，コンテンツへのアクセス許可を行う．次に Publisher はどのコンテンツが要求されたかを知るために，仮コンテンツ名 $9fe8b$ を Consumer の公開鍵で復号化し，要求公開コンテンツ名 $ContentA$ を取得する．Publisher は公開コンテンツ名と実コンテンツ名の変換方法を知っているため，$ContentA$ から $aser09$ を変換する．次に実コンテンツ名 $aser09$ を Consumer の公開鍵で暗号化し，仮コンテンツ名 $af76d$ を得る．最後に，要求されたコンテンツに対応するコンテンツ鍵を Consumer の公開鍵で暗号化し，$Publisher/9fe8b/FOR/ap08w/KeyA/af76d$ という名前でコンテンツ鍵を返送する．

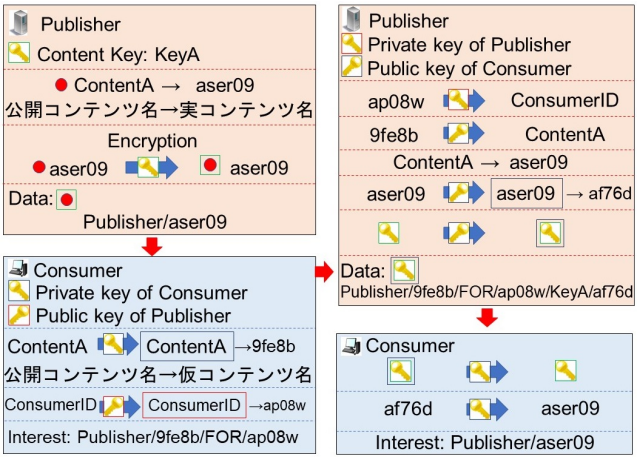

図 1: NDN 上で提案方式の動作

最後に，コンテンツ鍵を受けとった Consumer はコンテンツ鍵を自身の秘密鍵で復号化する．次に，仮コンテンツ名 $af76d$ を自身の秘密鍵で復号化し実コンテンツ名 $aser09$ を取得する．これらの情報から Consumer は $Publisher/aser09$ の名前で Interest を送信することで，暗号化されたコンテンツを取得可能である．暗号化されたコンテンツはコンテンツ鍵で復号化することで，Consumer はそのコンテンツを視聴可能となる．

4. まとめ

NDN 上での頻度攻撃による影響を減らし，コンテンツ名に対するプライバシーを保護するアクセス制御方式を提案した．本稿では提案方式の頻度攻撃に対する防御効果の詳細には触れていないが，頻度攻撃は十分な量の暗号化コンテンツ名の収集が必要なため [2]，提案方式は実コンテンツ名などを定期的に更新することで頻度攻撃の防御が期待される．今後は NDN 上で提案されている既存手法との比較評価や頻度攻撃に対する評価を行う予定である．

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] L. Zhang, et al. Named data networking. ACM SIGCOMM CCR, 2014, 44.3: 66-73.
[2] C. Ghali, G. Tsudik, CA. Wood, When encryption is not enough: Privacy attacks in content-centric networking. ACM ICN, 2017, p. 1-10.
[3] Y. Fukagawa, N. Kamiyama, Access Control with Individual Key Delivery in ICN, IEEE LANMAN 2022, July 2022.

Copyright © 2022 IEICE