NDN におけるプライバシィ保護を考慮したアクセス制御方式の性能評価

Performance Evaluation for Access Control with Privacy Preservation in Named Data Networking

深川 悠馬[1]　　上山 憲昭[2]
Yuma Fukagawa　　Noriaki Kamiyama
立命館大学大学院 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 [8]．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ィを守るために，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 [5]．そのため，ただ暗号化するだけでは不十分である．

著者らは，ICN におけるアクセス制御方式を提案し，NDN におけるプライバシィ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，既存のアクセス制御方式である name-based access control (NAC)[7] と比較を行い，制御トラヒック量は NAC と比べると大きいがトラヒック量全体で考えると許容範囲であり，Publisher への負担の差異は小さいことを確認した [3][4]．さらに，人気上位 4 個のコンテンツが攻撃者にとってより有益であることを確認した [2]．本稿では，上位 4 個のコンテンツに対して頻度攻撃に対する提案方式の防御効果とキャッシュヒット率の評価も行い，その有効性を明らかにする．

2. 関連研究

これまでに NDN のアクセス制御機構として，アクセス権限を有する Consumer に対してのみ復号を行うための暗号鍵を共有する Encryption-based 方式のアクセス制御法が提案されている．Encryption-based 方式では，コンテンツ名に基づくアルゴリズムを使用してアクセス制御を行う Name-based 型のアクセス制御 [1] [6] [7] が提案されている．

[7] では，NAC を提案し，コンテンツを暗号化するコンテンツ鍵とアクセス制御を実行するためにコンテンツ鍵を暗号化する key-encrypt key, key-decrypt key (KEK/KDK) を使用して，粒度の細かいアクセス制御を実現している．しかし，コンテンツ名によってアクセス制御を行うためコンテンツ名に Consumer 情報やコンテンツ情報を載せなければならない．

[1] では，secure distribution of protected content (SDPC) を提案し，Consumer を識別できる番号を付与しその番号をハッシュした値と，KEY_{MSG} と呼ばれる鍵の生成情報から生成した鍵を使用して要求コンテンツ名の暗号化を行う．ハッシュ値と暗号化名で要求することによって攻撃者からの盗聴を防ぐことでプライバシィの保護を実現している．また，KEY_{MSG} に基づいて生成された鍵によりコンテンツも暗号化されているため，コンテンツも保護されている．しかし，Consumer の識別番号のハッシュ値を要求コンテンツ名に使用しているため，攻撃者から同一ハッシュ値を使用して Consumer を間接的に特定するプライバシィ問題が残る．

[6] では，Web アプリケーションなどを提供する Content Provider が使用する online social networking (OSN) 上で NDN を考慮した session-based access control (SAC) を提案している．ユーザと OSN 間の接続が維持されている間，セッション鍵と呼ばれる鍵を保持する．セッション鍵を使用して Consumer 情報や要求コンテンツ情報を送信することで，セッション鍵を持っていない第三者はその内容を知ることができない手法を実現している．この手法は頻度攻撃の防御は可能であるが Publisher から Consumer に Interest を送る必要がある．そのため，FIB の更新処理などに大きな負荷を与える可能性がある．

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ィ漏洩の問題に対して，コンテンツ名を暗号化するといった対策が考えられる．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 [5] が可能である．そのため，ただ暗号化するだけでは対策が不十分である．

4. 提案方式

本節では [4] で著者らが提案した方式を紹介する．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，応答パケットから取得し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ィは保護されている．頻度攻撃は同一名が繰り返し使用されるほど特定率が上昇する．提案方式ではコンテンツの要求時のみ全 Consumer で共通の暗号コンテンツ名を使用するため，頻度攻撃による影響が大きい．しかし，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抑制させることが可能である．Consumer は変更後のコンテンツ名を初回 Interest の応答パケットであるコンテンツ鍵の名前から再度取得する．

5. 性能評価

本節では独自に作成したシミュレータを使用して頻度攻撃に対する提案方式を評価する．

図 1(a)(b) にシミュレーション時間に対する攻撃者の正答率を 10,000 個のコンテンツの内，人気上位 4 個のコンテンツを対象とした評価結果を示す．図 1(a) は提案方式を使用しない場合の攻撃者の正答率推移である．図 1(b) は提案方式を使用し，コンテンツ名の変更周期を 100s に一回に設定した場合の攻撃者の正答率推移である．さらに，シミュレーション時間を 2,000 秒で行い，攻撃者が全ノードから盗聴情報を収集した場合で評価した．

図 1(a) より，コンテンツ名を変更しない場合，時間経過後に一定の正答率に収束することがわかる．1 位コンテンツは約 100%，2 位コンテンツは約 93%，3 位コンテンツは約 82%，4 位コンテンツは約 81%に収束する．一方，提案方式を用いた場合，図 1(b) より，攻撃者の正答率はコンテンツ名を変更した後に時間の経過に伴い増加するものの，コンテンツ名を変えたときに急減する結果，攻撃者の正答率は 1 位コンテンツが約 7%，2 位コンテンツは約 0.04%，3 位コンテンツは約 0.04%，4 位コンテンツは約 0.03%と大幅に頻度攻撃の影響を抑制させていることがわかる．

図 2(a)(b) も同様の条件で攻撃者が単一ノードから情報を収集した場合における攻撃者の正答率推移を示す．図 2(a) より，コンテンツ名を変更しない場合，同様に時間経過後一定の値に収束する．1 位コンテンツは約 71%，2 位コンテンツは約 40%，3 位コンテンツは約 30%，4 位コンテンツは約 20%に収束する．図 2(b) より提案方式を使用した場合，こちらも同様に 1 位コンテンツは約 4%，2 位コンテンツは約 0.8%，3 位コンテンツは約 0.1%，4 位コンテンツは約 0.1%となり，単一ノードで攻撃者が情報を収集した場合でも大幅に頻度攻撃の影響を抑制可能である．

図 1(b)，2(b) よりコンテンツ名の変更周期とともに攻撃者の正答率は 0%まで低下する．その後，時間と共に盗聴数が増加するにつれ次のコンテンツ名変更周期までに徐々に正答率が

増加することがわかる．しかし，シミュレーション時間の 0s から最初のコンテンツ名変更までにおいて，各コンテンツの正答率はコンテンツ名変更後の最大正答率と比べ高くなっていることがわかる．これは攻撃者が初期段階に盗聴情報を持っていないため，初めは盗聴した暗号化コンテンツ名が Zipf 分布に従い人気順で暗号化コンテンツ名を盗聴できるためである．しかし，一度コンテンツ名が変更されると盗聴できる暗号化コンテンツ名の数が増加するため，攻撃者の正答率が減少する．

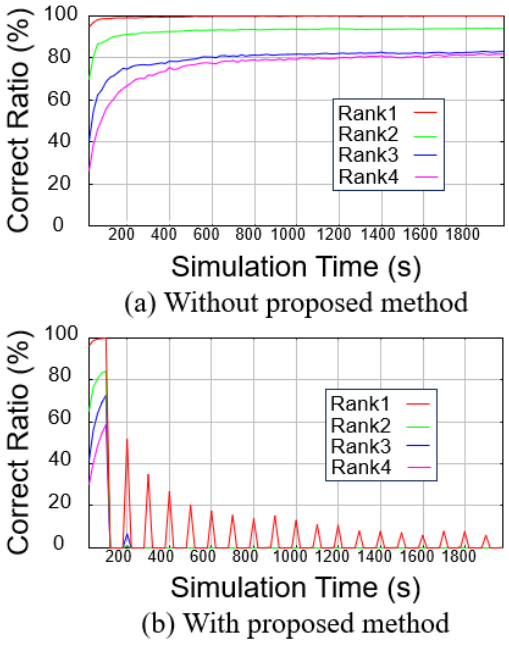

図 1: 上位 4 位コンテンツに対する攻撃者の正答率 (攻撃者が全ノードで要求情報を得た場合)

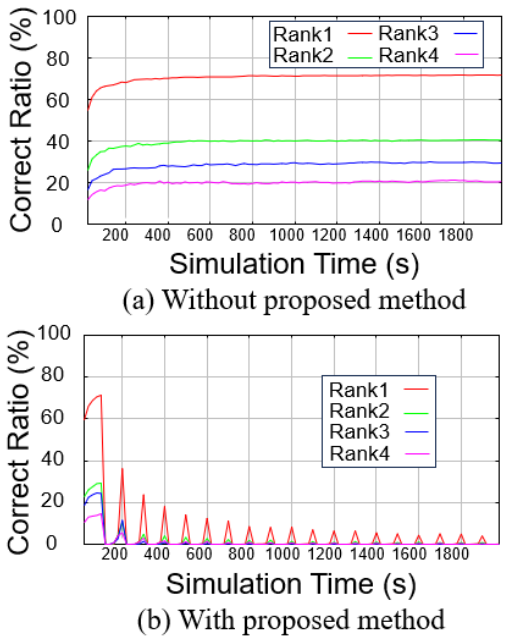

図 2: 上位 4 位コンテンツに対する攻撃者の正答率 (攻撃者が単一ノードで要求情報を得た場合)

提案方式では全てのコンテンツに対して同じ周期でコンテンツ名を変更している．しかし，攻撃者がコンテンツ名の変更周期を知っていた場合，攻撃者は周期が来る度に収集した情報をリセットすることで，初期状態の高い正答率を維持できる．そのため，各コンテンツに対してコンテンツ名変更周期をそれぞれ設定することが望ましい．さらに，頻度攻撃はより人気のコンテンツに対して影響が大きいため，人気の高いコンテンツのコンテンツ名変更周期を短くし，人気の低いコンテンツのコンテンツ名変更周期を長くすることで Publisher の負担を減らしながら頻度攻撃の影響を抑制させることが可能である．

提案方式はコンテンツ名変更により，既にルータ上にキャッシュされているコンテンツが使用できなくなる．そのためコンテンツ名変更周期に応じてルータ上のキャッシュヒット率が減少する可能性がある．そのため，コンテンツ名変更周期を 100s と 200s に設定し，評価した．表 1 にコンテンツ名を一度も変更しない場合と提案方式をそれぞれの周期で行った場合のキャッシュヒット率評価結果を示す．シミュレーション時に使用したトポロジ全体のすべてのノードのキャッシュヒット率は約 19.46%であり，提案方式を使用した場合は約 19.38%と約 19.33%である．最大でもキャッシュヒット率の差は約 0.13%であるため，提案方式を使用したとしてもキャッシュヒット率に影響を大きく及ぼしていないことがわかる．単一ノードのキャッシュヒット率の場合も提案方式を使用しても最大で約 0.19%の低下である．そのため，提案方式はネットワークの効率を下げずに頻度攻撃の影響を抑制可能であることがわかる．

表 1: キャッシュヒット率

	Simple Encryption	Proposed Method (200s)	Proposed Method (100s)
All nodes	0.1946	0.1938	0.1933
Single node	0.0431	0.0425	0.0412

6. まとめ

これまでに NDN 上での頻度攻撃の影響を抑制し，コンテンツ名に対するプライバシィを保護するアクセス制御方式を提案した．本稿では頻度攻撃に対する提案方式の防御効果とキャッシュヒット率を評価した．100s に一回の鍵交換周期で攻撃者の正答率推移を評価し，攻撃者が全ノードにいる場合と単一ノードにいる場合のいずれも十分に影響を抑制可能であることを確認した．また，提案方式はコンテンツ名の変更周期が短いほど頻度攻撃の影響を抑制できるが，ネットワーク全体への影響も大きくなる．しかし，提案方式はキャッシュヒット率に大きな影響を及ぼすことなく頻度攻撃による影響が抑制可能であることが確認できた．今後は最適なコンテンツ名変更周期を数値評価により導出する予定である．

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] M. Bial, S. Pack, Secure Distribution of Protected Content in Information-Centric Networking, IEEE SYSTEM JOURNAL, June. 2020.
[2] 深川悠馬, 上山憲昭, NDN におけるプライバシィ保護を考慮したアクセス制御方式の頻度攻撃評価, 信学会 ソサイエティ大会, 2023 年 9 月
[3] Y. Fukagawa, N. Kamiyama, Access Control with Individual Key Delivery in ICN, IEEE LANMAN 2022, July. 2022.
[4] Y. Fukagawa, N. Kamiyama, Poster: Access Control Method with Privacy Preservation in NDN, IEEE ICNP 2023, Oct. 2023.
[5] C. Ghali, G. Tsudik, CA. Wood, When encryption is not enough: Privacy attacks in content-centric networking, ACM ICN, 2017.
[6] Y. Wang, M. Xu, Z. Feng, Q. Li, and Q. Li, Session-based Access Control in Information-Centric Networks: Design and Analyses, IEEE IPCCC 2014, Dec. 2014.
[7] Y. Yu, A. Afanasyev, L. Zhang, “Name-Based Access Control”, Technical Report NDN-0034, Jan 2016.
[8] L. Zhang, et al. Named data networking. ACM SIGCOMM CCR, 2014.