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

Frequency Attack 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 [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 [1]．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，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 NAC[3] と比較を行い，性能評価を行った [4]．本稿では，頻度攻撃に対する性能評価を行い，その有効性を明らかにする．

2. 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，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．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．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．

3. 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の性能評価を行う．

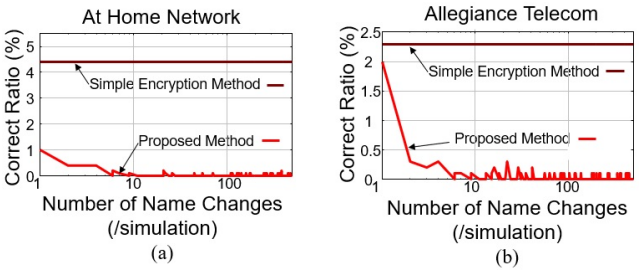

図 1: コンテンツ名変更回数に対する攻撃者の正答率

図 1(a)(b) に提案方式の頻度攻撃に対する性能評価結果を示す．特徴のある二つのネットワークトポロジを使用してシミュレーションを行った．図 1(a) は，各ノードが均等に近い次数をもつネットワークである．図 1(b) は，特定のノードが他ノードに比べて高い次数をもつネットワークである．攻撃者はネットワークトポロジ内における要求到着数が一番高いノードで盗聴情報を収集し，コンテンツ 10,000 個の内，人気上位 100 個のコンテンツを対象に特定を行う．また，提案方式がシミュレーション実行中に行ったコンテンツ名の変更回数を横軸に示し，コンテンツ名変更を一度も行わない単純な暗号化方式と比較評価を行った．

どちらのネットワークトポロジにおいても提案方式は単純な暗号化方式と比較し攻撃者の正答率が減少していることがわかる．また，シミュレーション時間ごとに 10 回の鍵交換を実施することで攻撃者の正答率を 0%近くまで減少させることが可能である．シミュレーション時間を 1,000s に設定した場合，100s に一回のコンテンツ名変更周期となる．

また，攻撃者はどちらのトポロジも提案方式は数%と低い正答率である．これは対象コンテンツを上位 100 個のコンテンツとしているため，正答率の低い下位コンテンツが多く含まれていることによって低くなっていると考えられる．

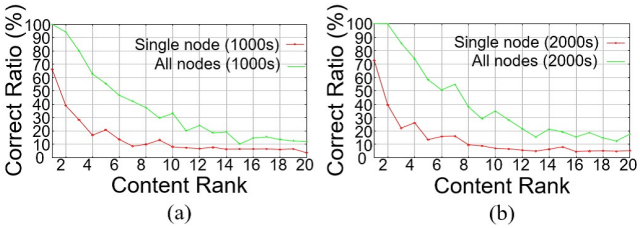

図 2: 上位 20 個のコンテンツに対する攻撃者の正答率

これまでの評価では上位 100 個のコンテンツを対象としたが，図 2(a)(b) に単純な暗号化方式における上位 20 個のコンテンツの盗聴成功率の評価結果を示す．各コンテンツのオリジンサーバ配置位置を 50 パターン用意し，各パターンにおいて 50 回シミュレーションを実行し合計 2,500 回の平均値を使用した．また，要求到着数が一番多いノードと全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をシミュレーションした．図 2(a) はシミュレーション時間を 1000 秒で実行し 1000 秒時点の結果を出力し，図 2(b) はシミュレーション時間を 2000 秒で実行し 2000 秒時点の結果を出力した．

頻度攻撃は人気のコンテンツほど特定されやすいという特徴を持つため，シミュレーション結果もおおよそその通りであることがわかる．全ノードから収集した情報を元に攻撃者が特定を実施した場合，1 位コンテンツは常に 100%の正答率となっている．単一ノードから収集した情報を元に攻撃者が特定を実施した場合，図 2(a) の 1 位コンテンツは 66.16%であり，図 2(b) は 72.86%であるため増加しており，2 位コンテンツも 38.96%から 39.40%と増加しているため，シミュレーション時間の増加とともに盗聴数も増加するため正答率が上昇している．しかし，3 位コンテンツは 22.82%から 22.04%と減少している．これは攻撃者の盗聴情報数が十分に足りていないことによって特定率が揺らいでいると考えられる．また，単一ノードの場合 4 位以降のコンテンツの正答率は一定の値に停滞する．

今後は，1 位～4 位コンテンツを対象に提案方式に対する性能評価を行い，攻撃者の盗聴回数と正答率との関係を分析する予定である．また，その結果から適切なコンテンツ名変更周期を数値評価で導出する予定である．

謝辞　本研究成果は JSPS 科研費 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 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, 2023 信学会 NS 研究会, NS2022-221, 2023 年 3 月