一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2023-182(2024-02)

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

深川　悠馬†　　上山　憲昭††

† 立命館大学 大学院 情報理工学研究科
〒 525–8577 滋賀県草津市野路東 1–1–1
† 立命館大学 情報理工学部
〒 525–8577 滋賀県草津市野路東 1–1–1
E-mail: †gr0579ri@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　通信開始に先立つ名前解決を行わずにコンテンツの名称で要求パケット (Interest) を転送し，Publisher からの応答コンテンツをルータでキャッシュする ICN (information-centric networking) が，IoT などのコンテンツを効率的に転送するネットワークとして着目されている．ICN のアーキテクチャの一つに NDN (named data networking) が提案されている．NDN では Publisher によるアクセス制御が困難であり，コンテンツ名に対するプライバシィ漏洩の課題がある．既存のアクセス制御手法である NAC (name-based access control) ではアクセス制御の課題を解決するが，プライバシィ漏洩の課題が残る．また，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対策が考えられるが，頻度攻撃により暗号化コンテンツ名が特定される問題が発生する．そこで筆者らは，初回 Interest を常に Publisher に到達させることで Publisher によるアクセス制御を実現し，コンテンツ名暗号化によってプライバシィ保護を行い，暗号化コンテンツ名を動的に変化させることで頻度攻撃の影響を減少させる方式を提案した．本稿では，頻度攻撃評価により，本方式がキャッシュヒット率に影響を与えずに頻度攻撃の影響を大幅に抑制できることを確認する．
キーワード　ICN，NDN，プライバシー保護，アクセス制御，頻度攻撃，コンテンツ名暗号化

Frequency Attack Evaluation for Access Control Method with Praivacy Preservation in Named Data Networking

Yuma FUKAGAWA† and Noriaki KAMIYAMA††

† Graduate School of Information Science and Engineering, Ritsumeikan University
1–1–1, Nojihigashi, Kusatsu, Shiga 525–8577
† College of Information Science and Engineering, Ritsumeikan University
1–1–1, Nojihigashi, Kusatsu, Shiga 525–8577
E-mail: †gr0579ri@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　Information-centric networking (ICN) has been attracting attention as a network that efficiently transfers content such as internet of things (IoT). Named data networking (NDN) is one of the architectures in ICN. In NDN, access control at Publisher is difficult, and privacy leakage for content names is a problem. Although an existing access control method of NDN called name-based access control (NAC) solves the access control problem in NDN, the problem of privacy leakage remains. Moreover, although we can avoid privacy leakage by encrypting content names, the encrypted content name can be still identified by a frequency attack. Therefore, we have proposed an access control method at Publisher which protects privacy by encrypting content names and reduces the impact of frequency attack by dynamically changing the encrypted content names. In this paper, we numerically confirm that the proposed method dramatically decreases the impact of frequency attack without degrading the cache hit ratio.
Key words　Access control, Content name encryption, Frequency attack, ICN, NDN, Privacy preservation.

1. はじめに

従来のインターネットでは通信開始に先立ち，配信ホスト (Publisher) の名前解決を DNS (domain name system) に依頼し，配信ホストの IP アドレスを取得することでデータの送受信を行っている．しかし普及が進む IoT (internet of things) の一部サービスでは，キーワードや条件などの曖昧な名称でデータを要求するため，DNS による名前解決が困難になることが想定される．そこで通信開始に先立つ名前解決を行わずにコンテンツの名称で要求パケット (Interest) を転送し，Publisher からの応答コンテンツをルータでキャッシュする ICN (information-centric networking) が，IoT などの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 [1]．ICN の概念を実現するためのアーキテクチャの一つに NDN (named-data networking) が提案されている [13]．NDN においてコンテンツはユーザ (Consumer) や Publisher から独立しており，さらに

コンテンツ要求時には要求コンテンツ名を平文で送信することでコンテンツを取得するため，Publisher によるアクセス制御とプライバシィに関して課題が存在する．

ネットワークで利用されるコンテンツには，誰もが自由に取得できるコンテンツと特定のユーザだけが取得できる閲覧者限定コンテンツがある．閲覧者限定のコンテンツには例えば，Hulu や Netflix などの月会費の支払いサービスを契約することが求められる有料コンテンツや，特定の会員のみがアクセスできるコンテンツがある．従来のインターネットでは閲覧者限定のコンテンツに対する配信要求時には，要求した Consumer が閲覧可能か否かを判断する Publisher によるアクセス制御を実行している．NDN においても閲覧者限定のコンテンツに対するアクセス制御が必要である．しかし NDN では，コンテンツはルータ上にキャッシュされている．そのため閲覧者限定のコンテンツに対して配信要求を行うと Publisher に配信要求が到達することなく，キャッシュされているルータからコンテンツが配信される可能性がある．そのため NDN では全ての配信要求が Publisher に到達しないため，従来のインターネットのように Publisher でアクセス制御を行うことが困難である．この問題に対処するためにルータでアクセス制御を行う手法が提案されている [10] [14]．しかし，ルータでアクセス制御を行う場合，ルータの処理負荷が増加する問題が残る．さらに Netflix のような既存の大規模 Publisher が NDN に移行する場合，Publisher によるアクセス制御が困難であるため，ルータでアクセス制御を行うとしても既存の制御方式を大幅に改良する必要があり，移行することが困難である．そのため，NDN での Publisher によるアクセス制御の実現が課題の一つである．

NDN では，コンテンツを要求する際に要求コンテンツ名で Interest を送信する．コンテンツが暗号化されていたとしても，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コンテンツ名の盗聴により特定できるプライバシィ漏洩の問題がある．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，NDN ではコンテンツ名暗号化によるプライバシィ保護の実現も課題である．プライバシィ漏洩の問題に対処するためにコンテンツ名を暗号化するといった手法が考えられる．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]．また，頻度攻撃によって特定されたコンテンツを使用してコンテンツポイズニング攻撃 [8] などの別の攻撃が発生する可能性も残る．

これまでにアクセス制御の課題を解決する手法として，NAC (name-based access control) [12] が提案されている．しかし NAC ではコンテンツ名を利用したアクセス制御を行い，コンテンツ名を平文で要求するため，プライバシィ漏洩の問題が存在する．

著者らは，NDN においても常に Publisher に到達させる初回 Interest をコンテンツ要求に先立って送信することで，Publisher によるアクセス制御を実現する方式を提案した [3]．さらに Publisher による暗号化コンテンツ名の動的な変更により頻度攻撃の影響を抑制させる方式を提案し，既存の NDN アクセス制御方式である NAC と性能比較を行い，制御トラヒック量は NAC に対し増加する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 [4]．本稿では，独自のシミュレータを使用し，頻度攻撃に対する提案方式の抑制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. NDN のセキュリティの課題

NDN では，従来のネットワークにある送信元 IP アドレスのような Consumer 情報を Interest に載せない．そのため，Interest から要求 Consumer の特定ができない．さらに署名機能を有しておりコンテンツの信頼性を高めているが，以下のようなセキュリティに関する問題が生じる．

2.1 リプレイ攻撃

Interest を盗聴した攻撃者が盗聴 Interest を利用し，再度同じ Interest を送信した場合，要求した攻撃者ノードにコンテンツが転送される．この時，攻撃者は不当にコンテンツを取得可能である．このような攻撃をリプレイ攻撃 [6] と呼ぶ．アクセス制御を必要とするような閲覧者限定のコンテンツも，攻撃者はリプレイ攻撃により取得可能である [9]．

2.2 前方秘匿性

鍵交換には，鍵が漏洩しても過去に暗号化されたコンテンツを復号できないという前方秘匿性を満たすことが求められる．しかし，NDN ではキャッシュされたコンテンツをすべての Consumer で共通で使えるようにするため共通鍵が使用されており，さらにコンテンツが Publisher から独立しているためコンテンツ鍵を変えない限り，Consumer がサービス加入時にコンテンツ鍵を取得し，サービス終了後もコンテンツ鍵を保持している場合，サービス終了後もコンテンツを復号可能であるため，前方秘匿性が満たされない [2]．

2.3 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．この場合，特に同一暗号化コンテンツ名が継続的に利用されるほど影響が大きくなる．さらに，特定されたコンテンツを利用して，攻撃者はコンテンツポイズニング攻撃 [8] などの別の攻撃に利用する可能性が残る．そのため，ただ暗号化するだけでは不十分である．

3. 関 連 研 究

3.1 NAC

NDN のアクセス制御を実現している手法の一つに NAC [12] が存在する．コンテンツを暗号化するコンテンツ鍵や，コンテンツ鍵を Consumer 毎に暗号化する KEK/KDK (key-encrypt key/key-decrypt key) を使用して，粒度の細かいアクセス制御を実現している．NAC ではまず初めにコンテンツの要求を行い，要求コンテンツを取得する．取得したコンテンツの名前からコンテンツ鍵の名前を推測し，コンテンツ鍵を要求する．取得したコンテンツ鍵の名前からコンテンツ鍵を暗号化している KEK の名前が分かるため，その名前から自身の情報を組み合わせて KDK の名前を推測して要求する．要求名の予測に取得済みのコンテンツ名を利用し平文でコンテンツを要求するため，スニッフィングを行う攻撃者はコンテンツが暗号化されていても，それがどんなコンテンツであるのかが把握可能である．本問題に対処するためにコンテンツ名の暗号化が考えられるが，2.3 節で述べたように頻度攻撃により暗号化コンテンツ名からコンテンツ名が特定される問題が残る．

3.2 関連アクセス制御手法

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 に対してのみに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暗号化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 [2] [11] [12] と属性ベース暗号を使用した attribute-based 型のアクセス制御 [10] [14] が提案されている．

[2] では，コンテンツとプライバシィを保護するために SDPC (secure distribution of protected content) を提案している．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 を間接的に特定されるプライバシィ問題が残る．

[11] 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 OSN (online social networking) 上で NDN を考慮した SAC (session-based access control) を提案している．Consumer 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抑制は可能であるが Publisher から Consumer に Interest を送信する必要がある．そのため，FIB (forwarding information base) の更新処理などに大きな負荷を与える可能性がある．

[10] では，コンテンツとそのコンテンツにアクセス可能な属性情報を載せたアクセスポリシーを利用してアクセス制御を行う手法を提案している．Consumer はコンテンツのアクセスに必要な属性を持っていない限りそのコンテンツにアクセスできない．[14] は [12] を属性ベース暗号に拡張した手法となる．

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 NDN のヘッダー [7] を利用することで，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 ($DynamicContentName$) 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．

提案方式はコンテンツ名を暗号化することでプライバシィ漏洩の問題に対処しているが，ただ暗号化するだけでは頻度攻撃により暗号化コンテンツ名からコンテンツ名が特定される問題が残る．そこで提案方式では Publisher が $DynamicContentName$ を Consumer と共有せずに管理することで，任意のタイミングで動的に変更可能とすることで頻度攻撃に対処可能とした．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 $DynamicContentName$ 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 $DynamicContentName$ 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．また，コンテンツをコンテンツ鍵で暗号化し，コンテンツ鍵を Consumer の公開鍵で暗号化しているため，リプレイ攻撃を行っても攻撃者が Consumer の秘密鍵を所持していない限りコンテンツを復号不可能である．提案方式では Hulu や Netflix が使用している鍵の入手などをアプリケーション層でブラックボックス化することで Consumer が鍵を保持することを防ぐなどの対策を施すことで前方秘匿性を満たすことが可能である．

5. 性能評価

5.1 評価条件

提案方式の頻度攻撃評価では独自に作成したネットワークシミュレータを使用して評価を行う．評価には，米国の商業バックボーン ISP (internet service provider) である二つのネットワークトポロジを用いたが，それらのトポロジを図 1，2 に示す．図 1 に示す At Home Network は，ノード数が 46 であり，各ノードがほぼ同一の次数をもつネットワークである．そのため各ノードから発生した要求はどのノードも等しく経由する．図 2 に示す Allegiance Telecom は，ノード数が 53 であり，特定のノードが他ノードに比べて高い次数を持つネットワークである．そのため，各ノードから発生した要求は次数の高いノードをより多く経由する．また，各ノードの要求発生確率は人口に比例させ，10,000 個のコンテンツを，skew パラメタを 0.8 に設定した zipf 分布に従い要求を発生させる．

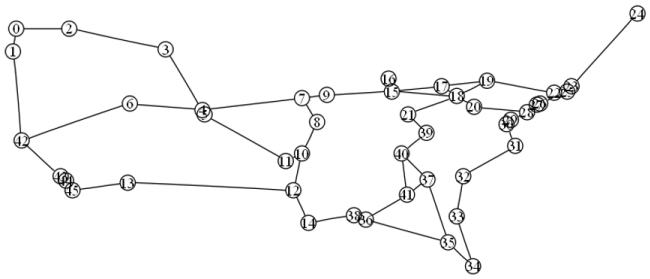


図 1　At Home Network のトポロジ

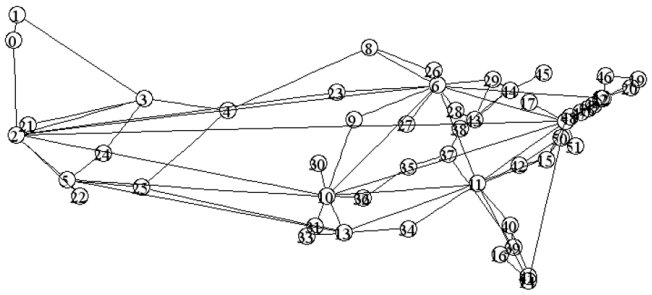


図 2　Allegiance Telecom のトポロジ

5.2 コンテンツ名を変更しないときの攻撃者の正答率の時間推移

本節では提案方式による頻度攻撃の抑制効果を評価する．頻度攻撃は人気コンテンツほど特定される可能性が高いため，10,000 個のコンテンツの内，上位 100 個の人気コンテンツを対象に攻撃者の $DynamicContentName$ から実際のコンテンツ名を特定した正答率を評価する．正答率は上位 100 個のコンテンツのうち攻撃者が特定したコンテンツの比率と定義する．

図 3 に，一度も $DynamicContentName$ を変更せずに頻度攻撃を行った場合 (simple encryption 方式) の攻撃者の正答率の時系列を示す．どちらのトポロジにおいても，時間の経過に伴い一定の正答率に収束することが分

かる．そのため，攻撃者の正答率が一定値に収束するよりも前に，*DynamicContentName* を変更する必要があることが確認できる．

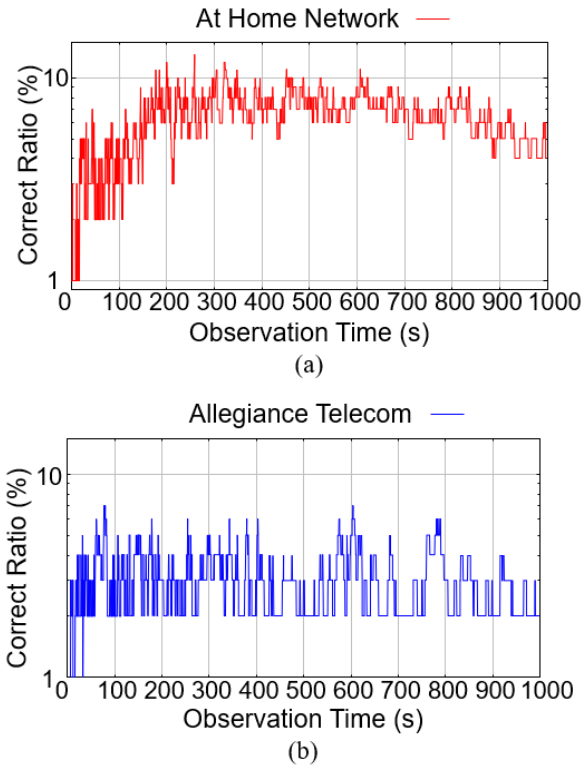


図 3　各トポロジにおける攻撃者の正答率の時間推移 (コンテンツ名を変更しない場合)

5.3　適切なコンテンツ名変更周期

提案方式は *DynamicContentName* を動的に変化させることで頻度攻撃の影響を抑制する．しかし，コンテンツ名の変更周期を短くした場合，コンテンツを再公開する必要がありキャッシュヒット率やネットワークへの負荷が増加する可能性がある．そこで，提案方式を使用した場合と一度も暗号化コンテンツ名を変更しない simple encryption 方式の攻撃者の正答率の時間推移を比較し，適切なコンテンツ名変更周期を評価する．図 4 に，*DynamicContentName* のシミュレーション期間中の変更総回数に対する攻撃者の正答率をプロットする．図 3 に示すように simple encryption 方式の攻撃者の正答率は収束するため，図 4 の simple encryption 方式は全期間の攻撃者の平均正答率を示す．また，シミュレーション時間は 1,000 秒に設定し，Consumer からの要求レートは 10.7 ミリ秒とする．

どちらのネットワークトポロジにおいても提案方式は simple encryption 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，*DynamicContentName* の変更回数がシミュレーションあたり 10 回時点で約 0%に攻撃者の正答率が減少する．そのため，今回はシミュレーション時間が 1,000 秒のため，100 秒に一回のコンテンツ名変更周期がネットワークへの負荷を最小限に抑えながら頻度攻撃の影響を抑制することが可能な値となる．同様にシミュレーション時間を 2,000 秒で行った場合も 100 秒に一回のコンテンツ名変更周期が適切であるという結果が得られた．

5.4　攻撃者の対象コンテンツ評価

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，頻度攻撃が有効な上位コンテンツの範囲を評価する必要がある．そのため，図 5 に simple encryption 方式における上位 20 個のコンテンツの攻撃者の正答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 回の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，各コンテンツに対する要求発生数の情報を，要求到着数が一番多い単一ノードから攻撃者が収集した場合と，全ノードから攻撃者が収集した場合の，各々における攻撃者の正答率を評価する．．図 5(a) はシミュレーション時間 T が 1,000 秒の，図 5(b) は T が 2,000 秒の場合の，各コンテンツの正答率をコンテンツの人気順にプロットする．

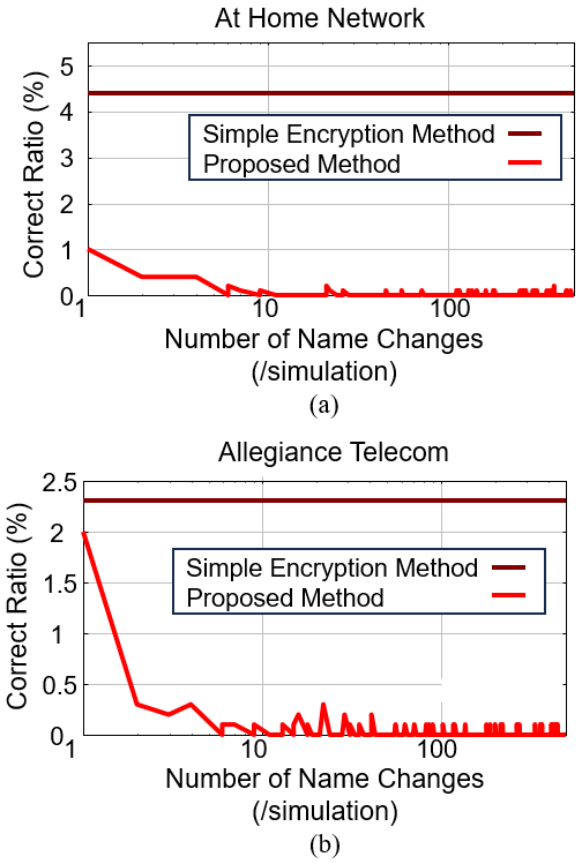


図 4　コンテンツ名変更回数に対する攻撃者の正答率

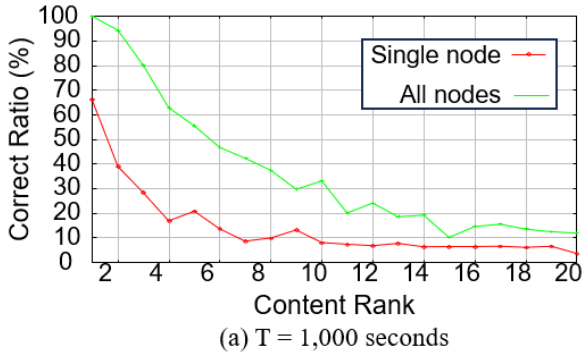
頻度攻撃は人気コンテンツほど特定されやすいという特徴を持つため，シミュレーション結果もおおよそその通りであることが分かる．全ノードから収集した情報を元に攻撃者が特定を実施した場合，1 位コンテンツは常に 100%の正答率となっている．単一ノードから収集した情報を元に攻撃者が特定を実施した場合，図 5(a) の 1 位コンテンツは 66.16%であり，図 5(b) は 72.86%であるため増加しており，2 位コンテンツも 38.96%から 39.40%と増加しているため，シミュレーション時間の増加とともに盗聴数も増加するため正答率が上昇している．しかし，3 位コンテンツは 22.82%から 22.04%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正答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収束する．これら結果を考慮し，以後は上位 4 個のコンテンツを対象に評価を行う．

5.5　上位 4 個のコンテンツに対する評価

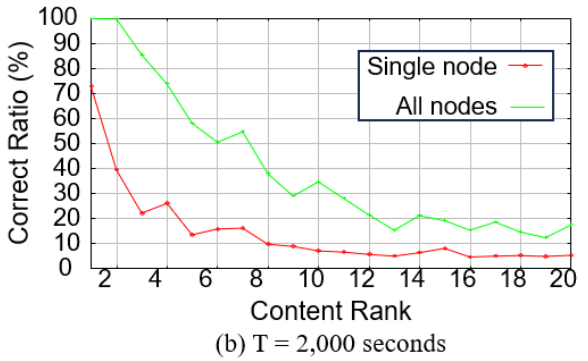
次に上位 4 個のコンテンツ毎の攻撃者の正答率の時間推移を評価する．図 6(a) は，攻撃者が全ノードから情報を盗聴した場合の上位 4 個のコンテンツのそれぞれの正答率推移を示す．図 6(b) は，提案方式を使用した場合の正答率推移を示す．また，図 4 の結果から *DynamicContentName* の変更周期を 100 秒

毎に設定し，シミュレーション時間を 2,000 秒で設定した．

図 6(a) より，全ノードから情報を収集した場合，図 5 の結果と同様に 1 位コンテンツは一定時間経過後約 100%の値に収束することがわかる．他の順位のコンテンツも同様に時間経過後に約 93%，約 82%，約 81%の値に収束することがわかる．図 6(b) において提案方式を使用することで 1 位コンテンツは最終的に約 7%の正答率に低下している．2 位コンテンツに対しても約 94%から約 0.04%の正答率に低下している．



(a) T = 1,000 seconds



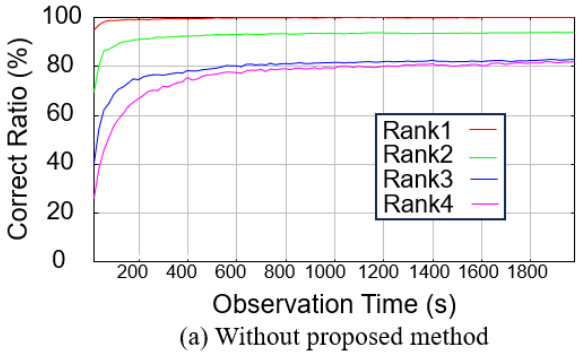
(b) T = 2,000 seconds

図 5　上位 20 個のコンテンツに対する攻撃者の正答率 (simple encryption 方式)

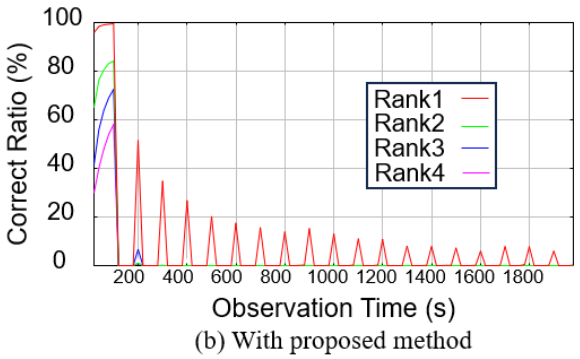
図 7 に攻撃者が単一ノードから情報を収集した場合におけるシミュレーション時間に対する攻撃者の正答率の評価結果を示す．図 7(a) は提案方式を使用しない場合の上位 4 個のコンテンツに対する攻撃者の正答率推移である．図 7(b) は提案方式を使用した場合の攻撃者の正答率推移である．図 7(a) より各コンテンツは最終的に約 71%，約 40%，約 30%，約 20%の値に収束する．図 7(b) において提案方式を使用することで 1 位コンテンツは最終的に約 4%に正答率が低下する．2 位コンテンツも同様に約 0.8%に正答率が低下する．

図 6，図 7 の結果から，提案方式を用いることで，単一ノードで情報を収集した場合は全ノードから情報を収集した場合に比べて正答率は低下するが，全ノードの場合においても頻度攻撃の影響を大きく抑制可能である．

図 6(b)，7(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が 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 0 秒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．

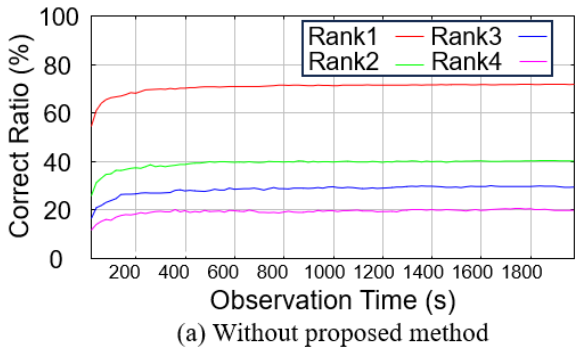


(a) Without proposed method

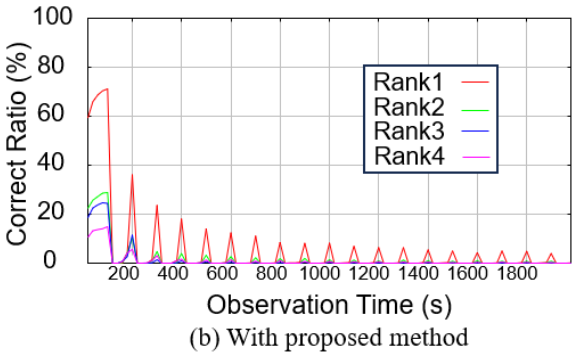


(b) With proposed method

図 6　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)



(a) Without proposed method



(b) With proposed method

図 7　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．

5.6 キャッシュヒット率評価

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 T_{C_k} を 100 秒と 200 秒に設定し，キャッシュヒット率を評価する．表 1 にコンテンツ名を一度も変更しない simple encryption 方式と，提案方式の T_{C_k} の各々の値における，キャッシュヒット率を示す．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，提案方式を用いた場合は約 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 **Cache Hit Ratio**

	Simple Encryption	Proposed Method (T_{C_k} = 200s)	Proposed Method (T_{C_k} = 100s)
All nodes	0.1946	0.1938	0.1933
Single node	0.0431	0.0425	0.0412

6. ま と め

NDN ではルータでコンテンツがキャッシュされるため，Publisher によるアクセス制御が困難である．そのため，閲覧者限定のコンテンツに対するアクセス制御が課題である．また，コンテンツ名が平文で要求されるため，コンテンツ名を盗聴することによるプライバシィ漏洩の問題がある．対策としてコンテンツ名暗号化が考えられるが，頻度攻撃が可能なため単純な暗号化だけでは不十分であることも課題である．既存方式である NAC ではアクセス制御の課題を解決するが，プライバシィ漏洩の問題が残る．そこで筆者らは，初回 Interest を常に Publisher に到達させることで Publisher によるアクセス制御を実現し，暗号化コンテンツ名を動的に変化させることで頻度攻撃の影響を抑制させる方式をこれまでに提案した．さらに，NDN のセキュリティの課題にはリプレイ攻撃，前方秘匿性もあるが，提案方式は適切な鍵管理によりリプレイ攻撃を防ぎ，前方秘匿性はアプリケーション層で対処可能な場合，暗号化や復号化処理などをブラックボックス化し Consumer に鍵を保持することを防ぐような対策を施すことで満たすことが可能である．

本稿では，提案方式の有効性を明らかにするための数値評価結果を示した．NAC ではプライバシィ漏洩の問題が残るが，提案方式ではコンテンツ名を暗号化することによりプライバシィを保護し，頻度攻撃による影響を，暗号化コンテンツ名を動的に変更することにより抑制させることが可能であることを確認した．また攻撃者の正答率を評価し，一定時間経過後に特定の正答率に収束することを確認し，提案方式は 100 秒に一回の鍵交換周期が適切であることを確認した．また，上位 100 個のコンテンツに対して攻撃者の正答率評価を行い，上位 4 個のコンテンツがより頻度攻撃の影響を受けやすいことを確認した．さらに，上位 4 個のコンテンツに対して 100 秒に一回のコンテンツ名変更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を抑制可能であることを確認した．今後は最適なコンテンツ名変更周期をシミュレーションで得られた結果をもとに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．

文 献

[1] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, Recent Adavances in Information-Centric Networking-Based Internet of Things (ICN-IoT), *IEEE Internet of Things Journal*, Apr. 2019.

[2] M. Bilal, S. Pack, Secure Distribution of Protected Content in Information-Centric Networking, *IEEE SYSTEM JOURNAL*, June. 2020.

[3] Y. Fukagawa and N. Kamiyama, Access Control with Individual Key Delivery in ICN, *IEEE LANMAN 2022*, July 2022.

[4] Y. Fukagawa and N. Kamiyama, Access Control Method with Privacy Preservation in NDN, *IEEE ICNP 2023 (Poster)*, Oct. 2023.

[5] C. Ghali, G. Tsudik, and CA. Wood, When encryption is not enough: Privacy attacks in content-centric networking, *ACM ICN 2017*.

[6] Y. Mo, B. Sinopoli, Secure Control Against Replay Attacks, *47th Annu. Allerton Conf. Commun., Control, Conput. (Allerton)*, Sep. 2009.

[7] NDN Packet Format Specification v0.3. Available: https://docs.named-data.net/NDN-packet-spec/0.3/. Accessed on: Jan. 15, 2024.

[8] T. Ngyen, X. Marchal, G. Doyen, T. Cholex, and R. Cogranne, Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment, *IFIP/IEEE IM 2017*.

[9] M. S. M. Shah, Y. Leau, M. Anbar, and A. A. Bin-salem, Security and Integrity Attacks in Named Data Networking: A Survey, *IEEE Access*, Jan. 2023.

[10] R. S. Silva, S. D. Zorzo, An Access Control Mechanism to Ensure Praivacy in Named Data Networking using Attribute-based Encryption with Immediate Revocation of Privileges, *IEEE CCNC 2015*.

[11] Y. Wang, M. Xu, Z. Feng, and Q. Li, Session-based Access Control in Information-Centric Networks: Design and Analyses, *IEEE IPCCC 2014*.

[12] Y. Yu, A. Afanasyev, and L. Zhang, Name-Based Access Control, *Technical Report NDN–0034*, Jan. 2016.

[13] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, K. Claffy, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley, and E. Yeh, Technical Report NDN–0001, *Named Data Networking (NDN) Project*, Oct. 2010.

[14] Z. Zhang, Y. Yu, S. K. Ramani. A. Afanasyev, and L. Zhang, NAC: Automating Access Control via Named Data, *IEEE MILCOM 2018*.