2023年度

修　士　論　文

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

指導教員: 上山 憲昭

立命館大学大学院 情報理工学研究科
情報理工学専攻 博士課程前期課程
計算機科学コース

学生証番号: 6611220031-3

氏名: 深川 悠馬

概要

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．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コンテンツがある．後者のコンテンツ要求時には，要求したユーザが試聴できるか否かを判断するアクセス制御が必要になる．従来のインターネットでは多くの場合，コンテンツ事業者の権威 DNS (domain name system) サーバに配信要求が届く．そのため Publisher でアクセス制御が容易に可能である．しかし ICN では，コンテンツがルータ上から配信されるため Publisher でアクセス制御を行うことが困難である．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，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．そのため，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 からどのコンテンツを取得している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．そこで本論では，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アクセス制御方式を提案する．また，NAC 方式との比較により，提案方式は制御トラヒック量が多く発生するがトラヒック全体で考えると許容範囲であり，遅延時間なども差は小さいことを確認する．さらに，頻度攻撃評価により提案方式は頻度攻撃に対して有効であることを確認する．

目 次

第1章　序論

1.1　研究の背景

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．しかし図 1.1 に示すように 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 [4]．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 [7] などの別の攻撃が発生す

る可能性も残る．

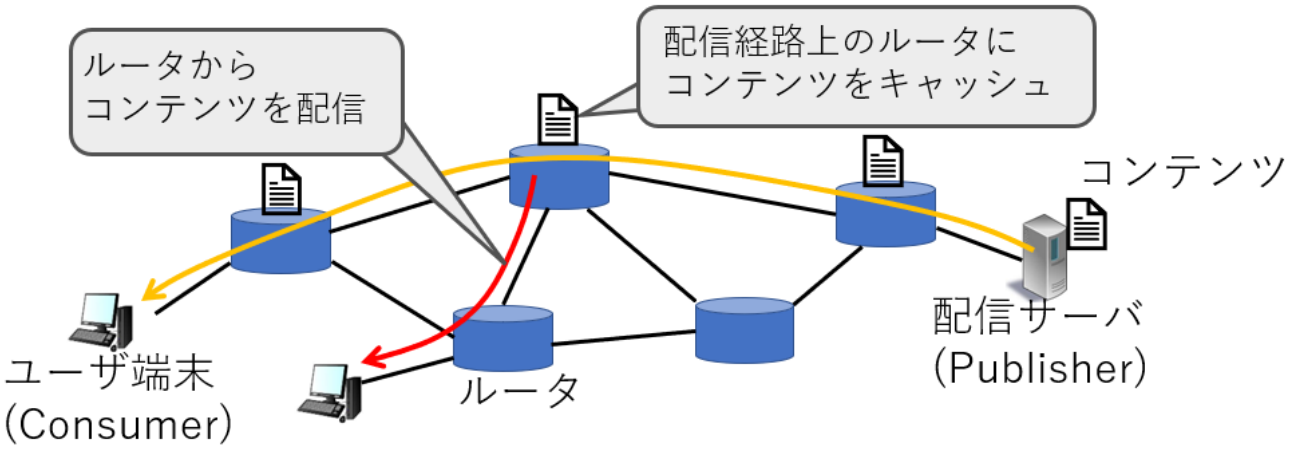

図 1.1: NDN のコンテンツ配信システム

1.2 研究の目的

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．

そこで本論では，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，NDN での Publisher によるアクセス制御を実現し，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する．さらに，提案方式を既存の NDN アクセス制御方式である NAC と比較することで，必要な制御トラヒック量や遅延時間，Publisher への負担を評価する．また，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．

第2章　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

図 2.1 に示すように，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 [5] 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]．

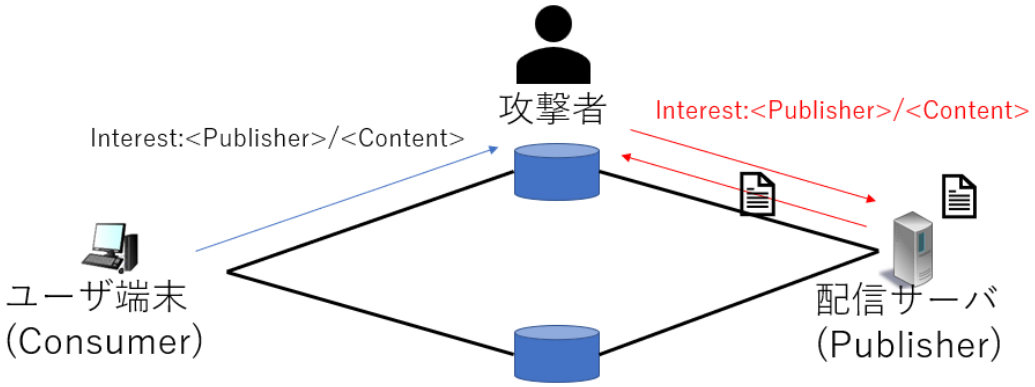

図 2.1: リプレイ攻撃

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．しかし図 2.2 に示すように，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]．

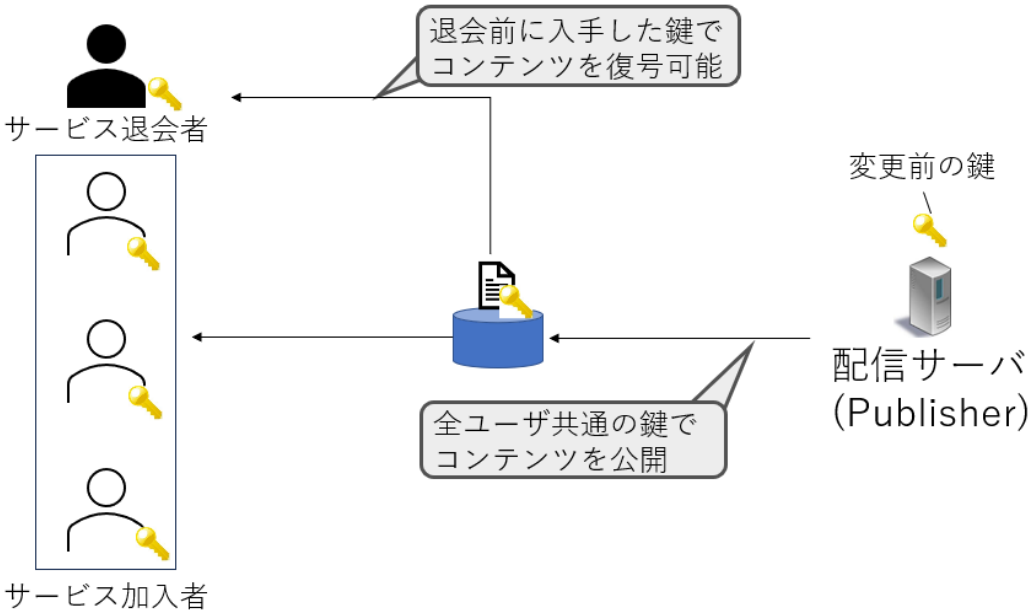

図 2.2: 前方秘匿性

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．しかし図 2.3 に示すように，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 [4] 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 [7] 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．

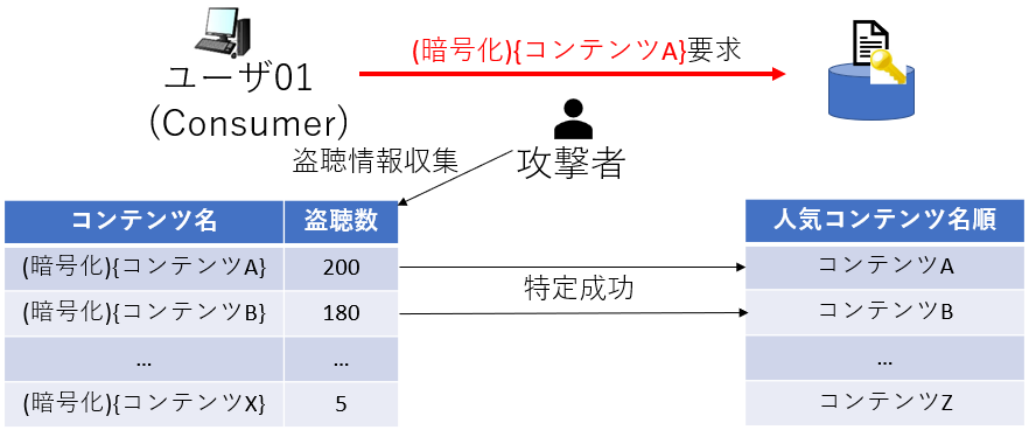

図 2.3: 頻度攻撃

第3章　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．

第4章　提案方式

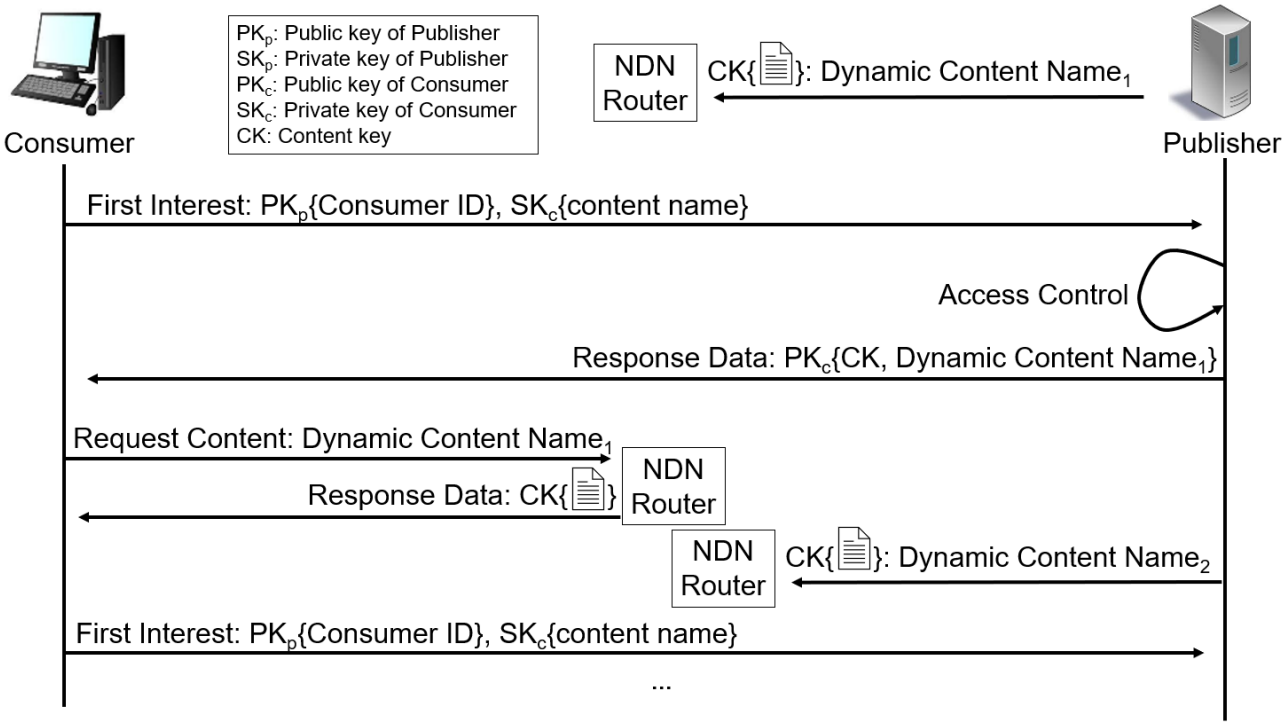

図 4.1: 提案方式の制御フロー

提案方式は，NDN 上での Publisher によるアクセス制御を達成し，頻度攻撃による問題を減少させることが可能なコンテンツ名暗号化を行う手法である．本節では，アクセス制御方式の概要について述べる．図 4.1 に提案方式の制御フローを示す.

4.1　NDN のパケット仕様の活用

本節では，NDN の Interest パケットや Data パケットの仕様 [6] について述べ，提案方式がどのようにこれらパケットのヘッダ情報を活用するか述べる．なお NDN の詳細は [13] で述べられている．

提案方式では，コンテンツ要求時に Consumer の秘密鍵を使用し，要求するコンテンツ名を暗号化して送信する．このとき同一のコンテンツ名に対して，Consumer 毎に異なる固有な暗号化コンテンツ名が生成される．固有な暗号化コンテンツ名により，ルータ上に同一の名前のコンテンツが存在しないため，キャッシュヒットせず常に Publisher に要求が到達するが，同一の Consumer が自身の秘密鍵により生成した暗号化コンテンツ名や各 Consumer が生成

する暗号化コンテンツ名が競合しないとは限らない．そのため提案方式では，NDN Packet Format Specification v0.3 [6] における Interest パケット，Data パケットの仕様を以下のように活用する．

4.1.1 Interest Packet Format

図 4.2 に NDN の Interest パケットヘッダを示す．提案方式では，Publisher によるアクセス制御を実現するために $MustBeFresh$ フラグを使用する．$MustBeFresh$ フラグが設定されている Interest に対して，4.1.2 節で述べる $FreshnessPeriod$ 要素が新しいデータであることを示すコンテンツのみをキャッシュから選択し，応答パケットとして転送する．キャッシュされているコンテンツが古い場合，キャッシュを無視して Interest を次ノードへと転送する．提案方式では，初回 Interest の要求コンテンツを常に古いコンテンツとして扱い，$MustBeFresh$ フラグを設定した初回 Interest を送信することで，既にキャッシュされている要求コンテンツには応答せず，常に Publisher に要求を到達させる．

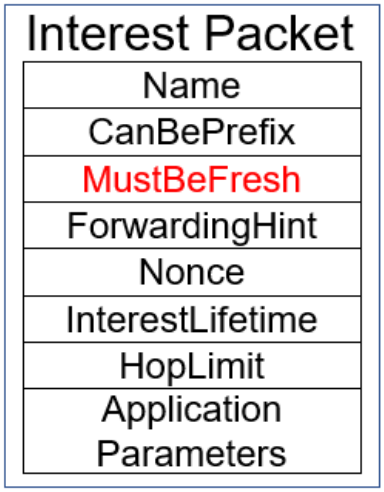

図 4.2: NDN における Interest パケットフォーマット v0.3

4.1.2 Data Packet Format

図 4.3 に Data パケットヘッダを示す．提案方式では，初回 Interest の応答パケットがルータ上で応答しないように $MetaInfo$ 要素の中の $FreshnessPeriod$ 要素を使用する．$FreshnessPeriod$ 要素はコンテンツがルータに到着してから $fresh$ なデータとして扱う期間を指定可能である．この要素を 0 に設定するか，設定時間を過ぎると $non\text{-}fresh$ なデータとして扱われる．この時，4.1.1 節で述べた $MustBeFresh$ 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．提案方式では初回 Interest の応答パケットの $FreshnessPeriod$ を常に 0 に設定することで，初回 Interest を常に Publisher に到達させる．

4.2 コンテンツ名

NDN では (A–Z, a–z), (0–9), (-), (.), (_), (~) が名前として使用でき，その他の文字はパーセントエンコーディングを行うことが NDN URI Scheme [6] に定義されている．コンテンツ名はこの定義に順守するものとする．ま

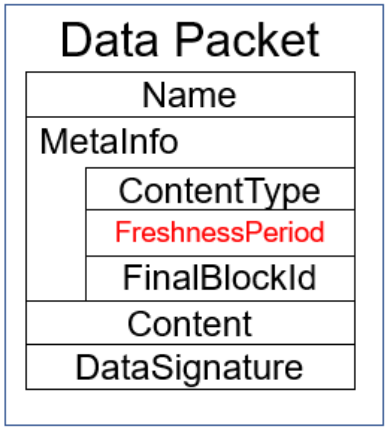

図 4.3: NDN における Data パケットフォーマット v0.3

た，提案方式で使用するコンテンツ名は以下の 3 つに分類される．

4.2.1 Content Name

前提として，“youtube/watch/content1” といった URL に含まれる “content1” のような名前を *ContentName* と呼び，全ての Consumer はこのコンテンツ名を知っている．提案方式では，プライバシィ保護のためコンテンツの名前には *ContentName* が使用されない．しかし，Consumer が要求したいコンテンツ名を指定するのに *ContentName* を使用する．

4.2.2 Dynamic Content Name

ContentName を Publisher が独自に暗号化したコンテンツ名を *DynamicContentName* と呼ぶ．4.2.1 節で述べたように，コンテンツの名前に *ContentName* を使用しないが，Publisher はすべてのキャッシュされるコンテンツの名前に *DynamicContentName* を使用する．Consumer は *DynamicContentName* を知らないため，Publisher に対して暗号化した *ContentName* で要求を行うことで，サービスに加入している正常な Consumer であれば，その応答として *DynamicContentName* を取得する．

また，*DynamicContentName* は全ての Consumer がコンテンツを要求する際に共通して使用する名前であり，攻撃者にとってコンテンツ要求は同一の *DynamicContentName* 情報が収集しやすくなっている．そのため，コンテンツ要求のみ頻度攻撃の影響が大きくなるが，*DynamicContentName* は Publisher が管理しているため，定期的にコンテンツ名を変更することが可能である．そのため *DynamicContentName* が動的に変化し，同一暗号化コンテンツ名が継続的に使用されないため頻度攻撃の影響を抑制させることが可能である．

4.2.3 Encrypted Content Name

コンテンツやコンテンツ鍵を *ContentName* や *DynamicContentName* で要求を行う場合，スニッフィングを行う攻撃者にとって，どちらもコンテンツ名を特定する情報として有益である．そこで提案方式では Consumer と Publisher 間でパケットを送信する際，コンテンツ名を Consumer の秘密鍵や公開鍵を使用して暗号化する．これに

より攻撃者はスニッフィングを行っても暗号化されているため，*ContentName* や *DynamicContentName* が知られることはない．この時のコンテンツ名をそれぞれ *EncryptedContentName*, *EncryptedDynamicContentName* と呼ぶ．

また，初回 Interest とその応答パケットでは *ContentName* や *DynamicContentName* を各 Consumer の秘密鍵や公開鍵で暗号化を行うため，Consumer 毎に異なるコンテンツ名で要求を行う．そのため初回 Interest とその応答パケットの通信においては攻撃者が特定の一人の要求を監視しない限り頻度攻撃のような推測は難しくなる．さらに，2 節で述べたように NDN の特性上，Interest から要求 Consumer の特定ができないため特定の Consumer の監視が難しく，初回 Interest の通信においては頻度攻撃の影響が最小であることが推測可能である．

4.3 Consumer ID

2 節で述べたように，NDN では Interest に Consumer の情報を載せないため，アクセス制御を行うための *ConsumerID* が必要である．*ConsumerID* はサービス加入時に Publisher から Consumer に対して交付される Consumer 判別のための ID である．*ConsumerID* の配布方式については本論の範囲外であるが，*ConsumerID* 配布においても RSA 暗号等を使用して配布することで，*ConsumerID* の第三者への漏洩を防ぐことを想定する．

提案方式では，*ConsumerID* を Publisher の公開鍵で暗号化して初回 Interest を送信することを想定しているが，頻度攻撃を *ConsumerID* に対して行うと *ConsumerID* を復号できなくとも暗号化された同一の *ConsumerID* が継続して使用されるため，Interest の要求者を識別できる問題がある．そのため，Diffie–Hellman 鍵交換プロトコル [3] のような一時的な公開鍵を使用することで，要求毎に異なる暗号化を行うことが望ましい．

4.4 提案方式の動作

Consumer は Publisher のサービス加入時に，Publisher から Publisher 名と *ConsumerID* を取得する．さらに Consumer は Publisher の公開鍵を取得し，Publisher も Consumer の公開鍵を取得しているものとする．

4.4.1 コンテンツ公開

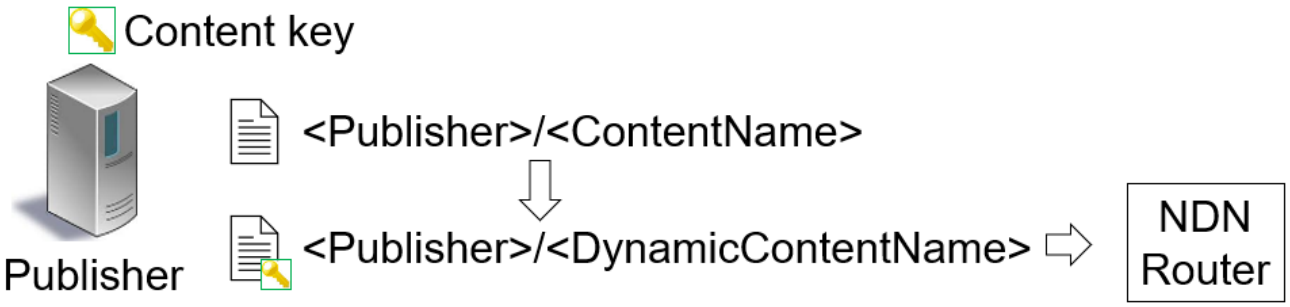

図 4.4: コンテンツ公開時の処理フロー

Publisher はあらかじめコンテンツを公開しなければならない．公開するコンテンツの名前に *ContentName* を使用する場合，Consumer は平文のコンテンツ名で要求しなければならないためプライバシィ漏洩の問題が発生する．そのため，図 4.4 に示すように Publisher は暗号化コンテンツ名である *DynamicContentName* を使用し

てコンテンツを公開する．また，$DynamicContentName$ は Publisher から認証を受けたのちに取得しない限り Consumer は知ることができない．また，コンテンツ鍵を使用してコンテンツの暗号化も行う．

4.4.2 初回 Interest

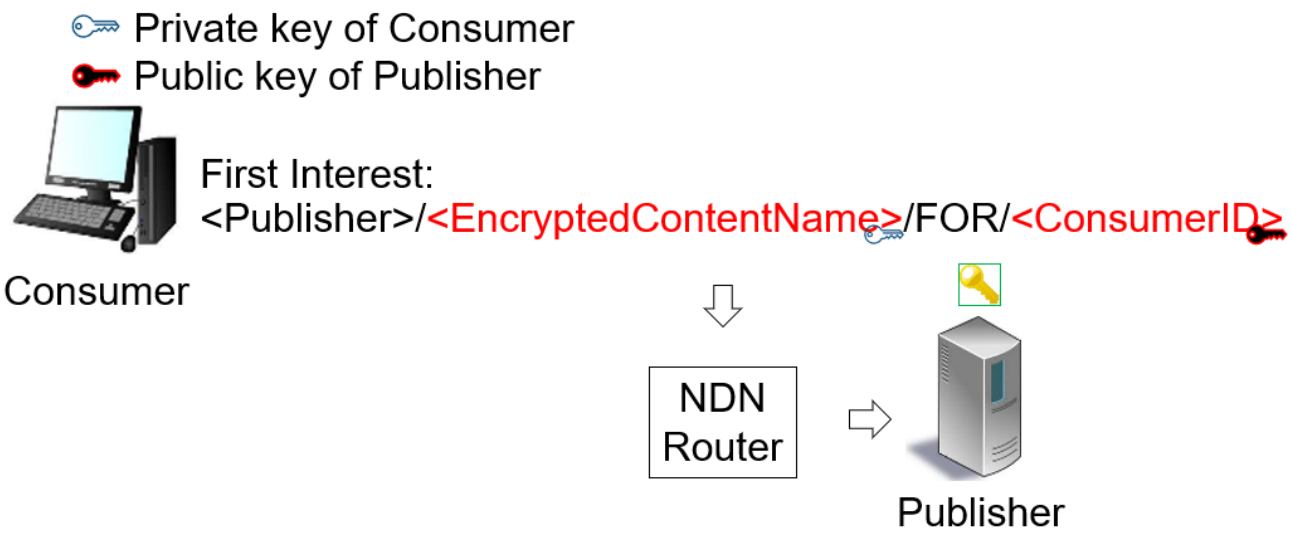

図 4.5: 初回 Interest 送信時の処理フロー

Consumer はコンテンツ要求に先立ってコンテンツ鍵に対して Publisher に初回 Interest を送信する．同時に初回 Interest を用いてアクセス制御を行う．図 4.5 に示すように，初回 Interest のコンテンツ名には Consumer の認証情報である $ConsumerID$，要求したいコンテンツの $ContentName$ を挿入する．$ConsumerID$ は Publisher の公開鍵で暗号化し，$ContentName$ は Consumer の秘密鍵で暗号化し $EncryptedContentName$ として要求する．また，“FOR” は同一コンテンツ名の競合を防ぐための予約語として定義する．この暗号化した要求名は固有の名前であり，ルータ内に同一コンテンツ名が存在しない．さらに，この初回 Interest のパケットヘッダには $MustBeFresh$ フラグを使用し，$non\text{-}fresh$ のコンテンツが応答しないように設定する．そのため，常に初回 Interest は Publisher へと到達する．

4.4.3 アクセス制御

コンテンツ鍵要求である初回 Interest を受信した Publisher は，アクセス制御を行うために図 4.6 に示すように，$ConsumerID$ を Publisher の秘密鍵で復号する．この時 $ConsumerID$ が正常な Consumer でなければ初回 Interest を棄却する．正常な Consumer であれば，Publisher は Consumer の公開鍵を特定できるため，$EncryptedContentName$ を Consumer の公開鍵を用いて復号し $ContentName$ を取得する．Consumer がこのコンテンツにアクセスが許可されている場合，Publisher は $ContentName$ から $DynamicContentName$ を生成する．要求されたコンテンツ鍵と $DynamicContentName$ を Consumer の公開鍵で暗号化し，$EncryptedDynamicContentName$ としてコンテンツ名に挿入し初回 Interest の応答パケットとして返送する．また，この応答パケットのパケットヘッダにある $FreshnessPeriod$ は 0 に設定することで，常に $non\text{-}fresh$ のデータとして扱い，初回 Interest に応答させない．

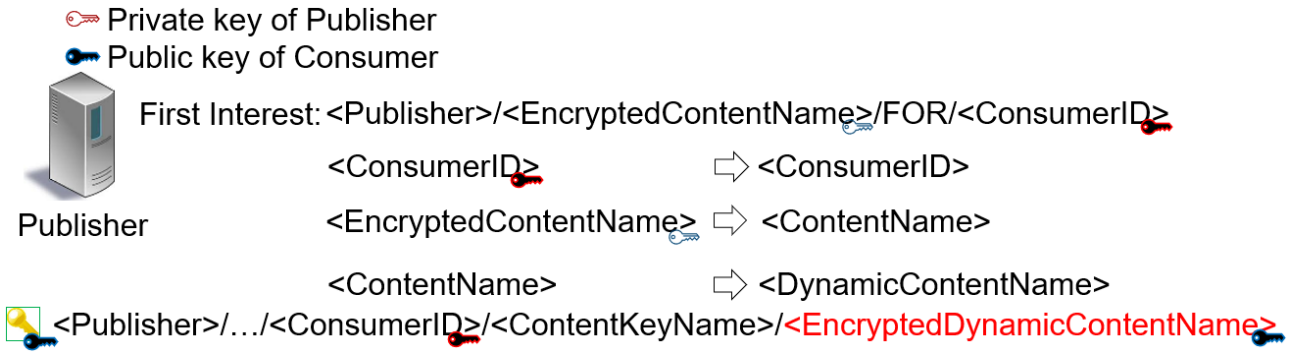

図 4.6: アクセス制御時の処理フロー

4.4.4　コンテンツ要求

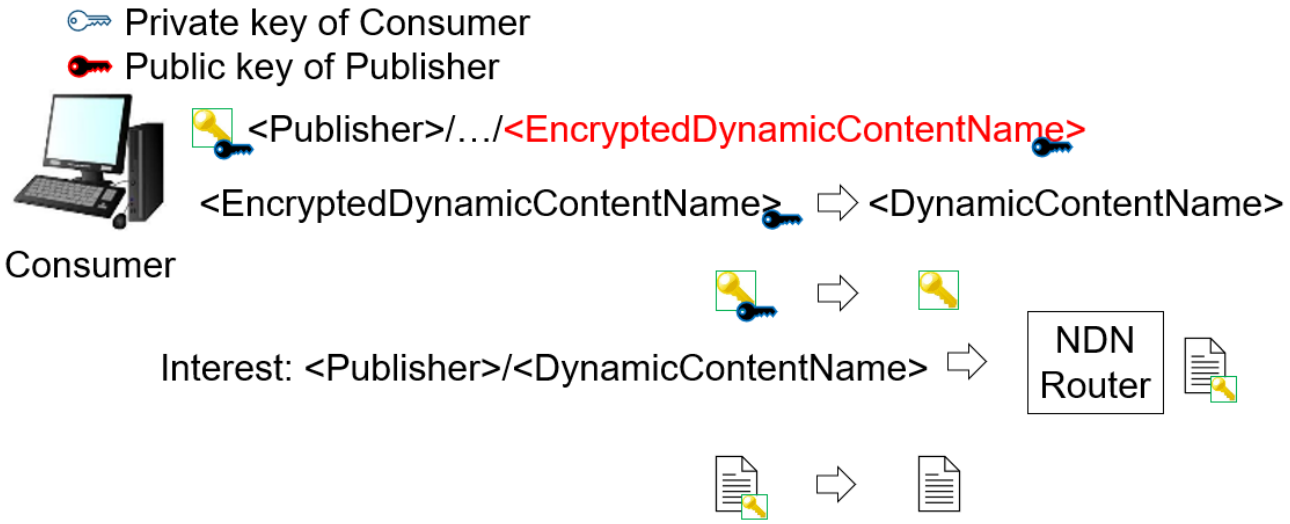

図 4.7: コンテンツ要求時の処理フロー

コンテンツ鍵を取得した Consumer は，図 4.7 に示すように，Consumer の秘密鍵を使用してコンテンツ鍵と *EncryptedDynamicContentName* を復号し，*DynamicContentName* を取得する．そのため，Consumer は *DynamicContentName* を用いてコンテンツを要求し，取得したコンテンツをコンテンツ鍵で復号する．初回 Interest と応答パケットにより，*DynamicContentName* はすべてのユーザ間で共有されるため，全ての Consumer が同一の *DynamicContentName* を使用して要求できるため，NDN のキャッシュ機能を利用してコンテンツを取得可能である．さらに，提案方式では前方秘匿性を満たすために Consumer はコンテンツ鍵を使用後すぐに削除する．そのため，コンテンツ要求時に毎回初回 Interest を Publisher に送信することでコンテンツ鍵と *DynamicContentName* を取得する．これにより，Publisher が *DynamicContentName* を変更しても，Consumer は初回 Interest により毎回最新の *DynamicContentName* が取得可能である．

4.5 アクセス制御における考察

4.5.1 アクセス失効

提案方式では初回 Interest を常に Publisher に到達させることでアクセス制御を行う．そのため，アクセス権を失った Consumer からの要求は $ConsumerID$ で判断可能である．アクセス権を失った Consumer に対して現在利用可能なコンテンツ鍵の配布が行われないため，アクセス失効が可能となる．また，$ConsumerID$ を不当に利用した第三者からの要求で認証が成功しコンテンツ鍵の配布が行われたとしても，コンテンツ鍵は $ConsumerID$ が割当てられている Consumer の公開鍵で暗号化されているため，第三者は Consumer の秘密鍵を所持していない限りコンテンツは復号不可能である．

4.5.2 緊急のアクセス失効

コンテンツ鍵を所持したままの Consumer が途中退会を行った結果，Publisher によってコンテンツ鍵の変更が行われるまでの間，不当にコンテンツを閲覧可能である．そのため，途中退会を行った Consumer に対してもアクセス権の失効を必要とする．Hulu や Netflix では，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しており，鍵を入手しても使用後に削除することで，Consumer が鍵を永続的に保持することを防いでいる．提案方式においてもこのような技術を使用することを推奨する．これにより Consumer は鍵の保持ができないため，途中退会を行っても即座にアクセス権を失効可能である．

4.5.3 Publisher によるアクセス制御

提案方式は Publisher レベルのアクセス制御を提案しているが，NDN では IoT データ等を効率的に転送するため，Publisher と独立したアクセス制御手法が望まれる [8]．しかし，既存の Netflix のような大規模な Publisher が Publisher と独立したアクセス制御を使用している NDN 環境に移行するのは容易ではない可能性がある．提案方式では Publisher によるアクセス制御を NDN 環境で実現しており，既存の認証システムを継続して使用することが可能である．さらに，図 4.2 に示すように，$ApplicationParameters$ 要素を使用することで認証に必要なアプリケーション層の情報を挿入することも可能である．

4.6 提案方式のセキュリティ

4.6.1 リプレイ攻撃

攻撃者が初回 Interest を傍受しリプレイ攻撃に使用した場合，コンテンツ鍵を不正に取得可能である．また，コンテンツ要求においても同様である．しかし，コンテンツはコンテンツ鍵で暗号化されており，コンテンツ鍵は Consumer の公開鍵で暗号化されている．そのため，攻撃者は Consumer の秘密鍵を所持していない限りコンテンツ鍵の復号ができず，同時にコンテンツの復号もできない．また，提案方式では各コンテンツに対して別々のコンテンツ鍵で暗号化を行っているため，一つの鍵を不当に取得したとしても不正取得可能なコンテンツは一つであり，鍵の復号に時間を要し，Publisher は定期的に自由にコンテンツ鍵の変更を行うことが可能なため，提案方式においてリプレイ攻撃は現実的ではない．

4.6.2 前方秘匿性

一度サービスに加入した Consumer が Publisher の所有するすべての鍵を正当に入手したのちに，Publisher によってコンテンツ鍵が変更されるよりも前に退会する場合を考える．このとき Consumer は正当に入手したコンテンツ鍵を用いて不当にコンテンツを復号可能である．そのため，4.5.2 節のようなブラックボックス化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．この対策はアプリケーション層で対応可能な場合に限るが，アプリケーション層で対処できない場合は，前方秘匿性を満たすことはできないがコンテンツ鍵の変更周期を短くすることで，不正アクセスの影響を抑制させることが可能である．しかし，コンテンツ鍵変更と同時にコンテンツを再暗号化する必要がある．そのため，キャッシュ済みのコンテンツが使用できなくなるため，キャッシュ効率が低下する．

4.6.3 頻度攻撃

Publisher が $DynamicContentName$ を動的に変更可能なため，変更されるたびに使用される $DynamicContentName$ の種類が増加し，攻撃者がコンテンツ名の特定に必要な要求サンプルが集まりづらくなる．そのため，頻度攻撃はコンテンツ名の変更回数を増加させると影響を抑制させることが可能である．しかし，提案方式ではコンテンツ名変更と同時にコンテンツを再暗号化する必要あるため，キャッシュを再度更新する必要があり，4.6.2 節と同様にキャッシュヒット率低下の問題が発生する．

第5章　性能評価

提案方式ではNAC[12]で問題であったプライバシィの問題を解決するが，一方で制御トラヒック量の増加，暗号化，復号化の処理の増加が懸念される．そこで本節では，NACとの配信要求あたりの制御トラヒック量，暗号化，復号化の回数，使用する鍵の生成数の数値評価を行う．制御トラヒック量はコンテンツ鍵のやり取りに発生するトラヒック量とする．また，頻度攻撃やネットワークに与える影響を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する．

5.1　評価条件

表 5.1: 評価に用いたパラメタ

Parameter	Value	Definition
T_{C_k}	1 (h)	interval of key exchange
T_k	24 (h)	interval of KEK/KDK exchange
N_c	10,000	number of contents
N_k	1–10,000	number of content keys
N_{R_c}	1–100 (/h)	number of consumer requests
V_I	100 (Byte)	traffic volume of interest packets
V_{C_k}	100 (Byte)	traffic volume of content keys
V_k	100 (Byte)	traffic volume of KEK/KDK

性能評価で使用するパラメタの設定値を表5.1にまとめる．

提案方式およびNACにおけるコンテンツ鍵の変更周期T_{C_k}を1時間とし，NACにおけるKEK/KDKの変更周期T_kを24時間とする．総コンテンツ数N_Cを10,000とし，各コンテンツにかけるコンテンツ鍵の数N_kを1–10,000の範囲で変化させる．さらに，Consumerからの要求数N_{R_c}を1時間あたり1–100回で変化させ，各リクエストで使用されるInterestのトラヒック量V_I，コンテンツ鍵のトラヒック量V_{C_k}，NACで使用されるKEK/KDKのトラヒック量V_kをそれぞれ100Byteとする．

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．評価に使用した特徴のある二つのネットワークトポロジを図5.1，5.2に示す．図5.1は合計ノード数が46個あり，各ノードが均等に近い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5.2は合計ノード数が53個あり，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しており，N_C個のコンテンツを，zipfパラメタを0.8に設定したzipf分布に従い人気順で要求する．

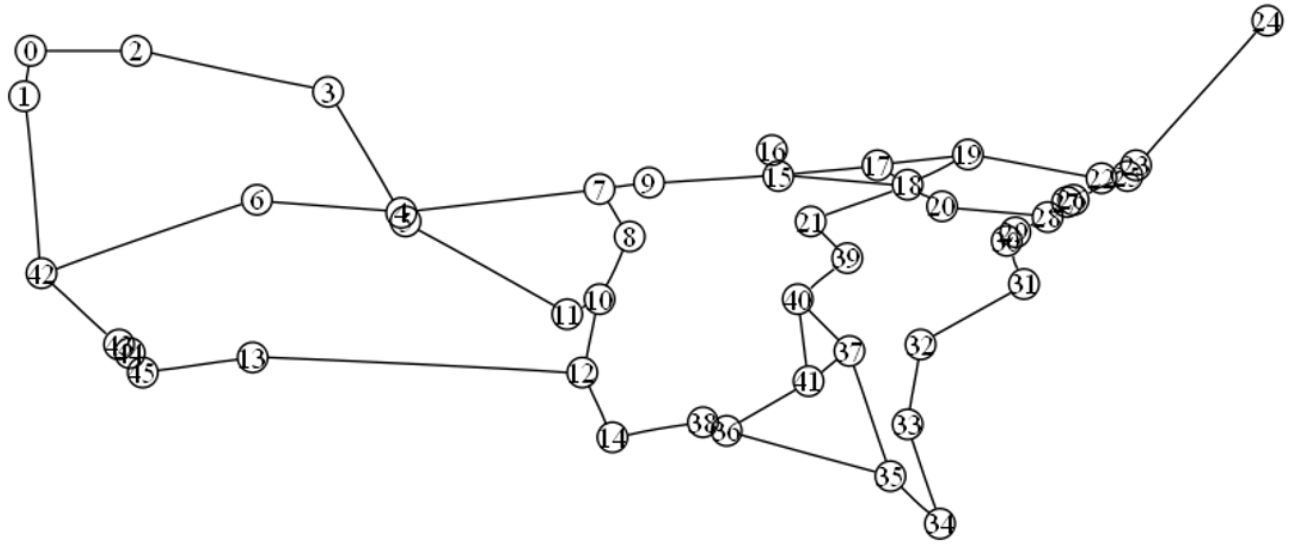

図 5.1: At Home Network

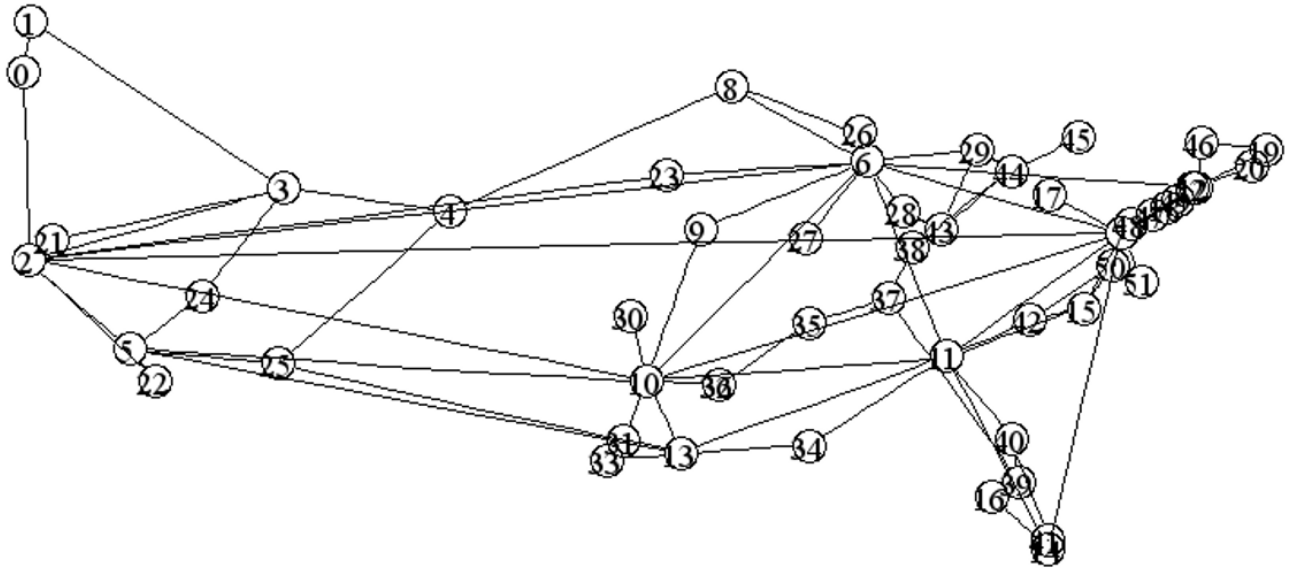

図 5.2: Allegiance Telecom

5.2 制御トラヒック量

提案方式では要求の度に初回 Interest としてコンテンツ鍵要求が発生するため，制御トラヒック量 V_p は次式で得られる．

$$V_p = V_I + V_{C_k} \tag{5.1}$$

NAC では，制御トラヒック量 $V_n(N_k)$ は，N_C 個のコンテンツを暗号化するために使用するコンテンツ鍵の数 N_k に依存する．すべてのコンテンツを単一のコンテンツ鍵で暗号化する場合，$N_k = 1$ であり，制御トラヒック量 $V_n(1)$ は次式で得られる．

$$V_n(1) = \frac{V_I + V_{C_k}}{N_{R_c}} + \frac{V_I + V_k}{24N_{R_c}} \tag{5.2}$$

N_k が 2 個以上の場合，NAC では N_c 個のコンテンツが N_k 個のコンテンツグループにグループ化され，各グループでそれぞれの共通の鍵で暗号化される．そのため，コンテンツ鍵 i を要求する確率 P_{c_i} を用いて，制御トラヒック量 $V_n(N_k)$ は次式で得られる．

$$V_n(N_k) = \frac{\sum_{i=1}^{N_K}(1-(1-P_{C_i})^{N_{R_c}})(V_i + V_{C_k})}{N_{R_c}} + \frac{V_I + V_k}{24N_{R_c}} \tag{5.3}$$

図 5.3 に 1 回のコンテンツ配信において発生する提案方式と各 N_k に対する NAC の制御トラヒック量の評価結果を示す．提案方式ではどのパラメタにおいても，初回 Interest は常に発生するため約 200Byte の制御トラヒック量が常に発生する．図 5.3 から NAC は 1 時間に Consumer が要求する回数が増加し，Zipf 分布のパラメタの偏りが大きく，コンテンツ鍵の数が減少するほど制御トラヒック量が減少する．そのため提案方式は NAC よりも制御トラヒック量が増加することが確認できる．しかしコンテンツのデータ量は数百 MB から数十 GB であり，制御トラヒック量はコンテンツデータ量と比較すればごく僅かな量であり，1 回の配信要求において発生するトラヒックの大部分はコンテンツデータであるため問題はないと考えられる．

5.3 暗号/復号評価

提案方式は，初回 Interest を毎回送信するためコンテンツ鍵要求が多く，暗号化や復号化にかかる処理時間，遅延時間などが NAC よりも多く発生する．そのため，提案方式と NAC との計算の複雑さを 1 要求あたりの暗号化，復号化の回数を導出することで比較評価する．評価条件としてコンテンツ鍵の交換周期 T_{C_k} を 1 時間，KEK/KDK の交換周期 T_k を 24 時間，鍵を生成する Publisher の数を N_{P_k}，Publisher のコンテンツに 1 日の間アクセスが許可されている Consumer の数を $N_{C_{24}}$ とする．NAC はコンテンツ鍵生成の分散機構を持つため，NAC の暗号化，復号化回数 N_{NAC_k} は以下になる．

$$N_{NAC_k} = 2 + 2N_{P_k} \tag{5.4}$$

提案方式は鍵生成を分散させる機構がなく，コンテンツ名暗号化も行うため常に 10 回発生する．そのため，N_{P_k} が増加しない限り，提案方式が多くなる．また，NAC は新規コンテンツ鍵を要求するときのみ N_{NAC_k} 回発生するのに対し，提案方式はすべての要求に対して 10 回発生するため，処理時間や遅延時間も比例して NAC よりも増加する．

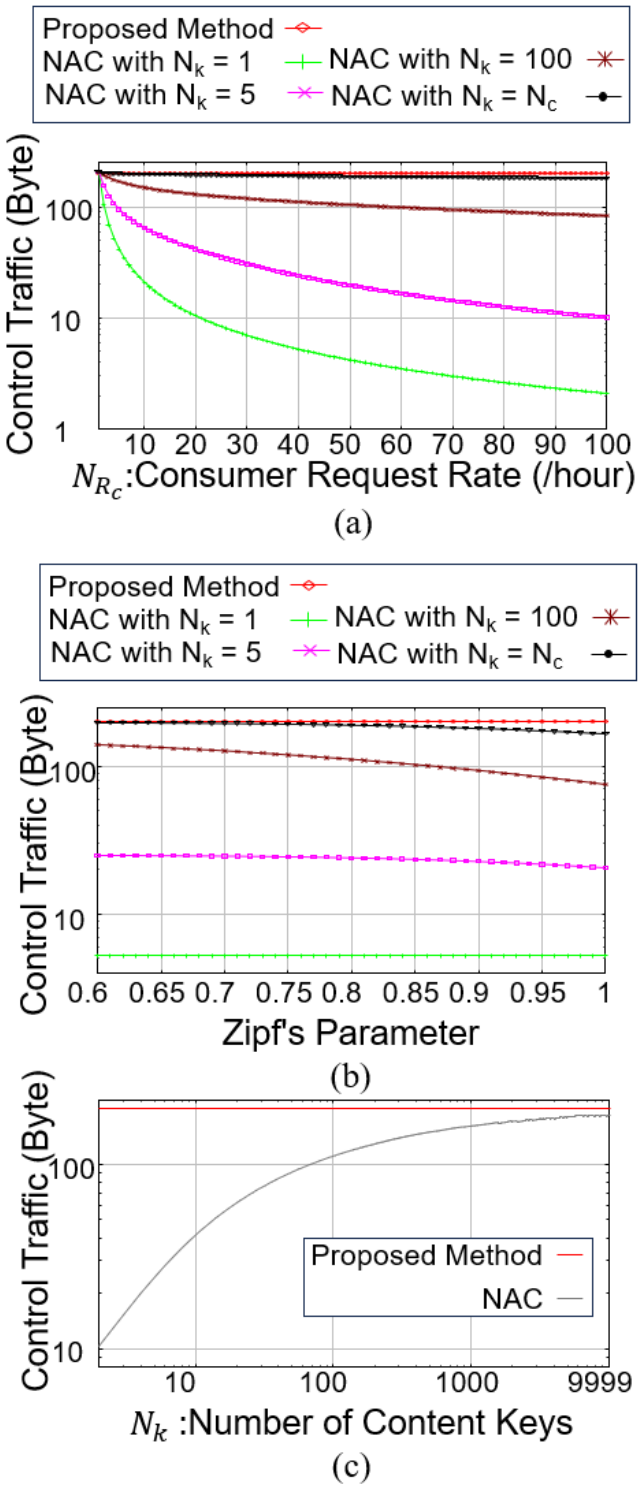

図 5.3: 制御トラヒック量

次に暗号化，復号化に使用する鍵の生成数を 1 日当たりで評価する．NAC では 24 回のコンテンツ鍵生成に加え，KDK が 1 時間毎に $N_{NAC_{24}}$ 人分生成されるため，NAC の 1 日当たりのコンテンツ鍵生成数 N_{NAC_g} は以下になる．

$$N_{NAC_g} = 24 + N_{C_{24}} \tag{5.5}$$

提案方式は，1 時間毎に $N_{C_{24}}$ 人にコンテンツ鍵を生成するため，提案方式の 1 日あたりのコンテンツ鍵生成数 N_{p_g} は以下になる．

$$N_{p_g} = 24N_{C_{24}} \tag{5.6}$$

どちらの方式も計算の複雑さは $O(N_{C_{24}})$ である．Consumer の数の増加とともに鍵生成数が増え，Publisher の負担が増加する．そのため，コンテンツ鍵の生成数による差異はみられない．

これら結果をまとめると提案方式と NAC の処理の複雑さの比較は以下となる．

- 提案方式の 1 要求毎の暗号化，復号化の処理回数は，$N_{P_k} < 4$ の場合，提案方式よりも NAC の方が小さくなり，$N_{P_k} \geqq 4$ の場合は提案方式の方が小さくなる．しかし，提案方式と NAC の処理回数の差異は小さい．
- 提案方式と NAC のどちらも Publisher への負担は $O(N_{C_{24}})$ で増加し，NAC との差異は小さい．

5.4 頻度攻撃評価

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．本節では提案方式の頻度攻撃に対する抑制効果を独自に作成したネットワークシミュレータを使用して数値評価を行う．シミュレーションでは，図 5.1 と図 5.2 に示す米国の商業バックボーン ISP の 2 つネットワークトポロジである At Home Network と Allegiance Telecom を使用した．頻度攻撃は人気であるコンテンツほど特定される可能性が高いため，N_C で定義した 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 $ContentName$ を特定した正答率を評価する．

5.4.1 攻撃者の正答率推移

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．評価基準として，攻撃者の正答率を上位 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 5.4 は simple encryption 方式と呼び，一度も $DynamicContentName$ を変更せずに各トポロジで頻度攻撃を行った場合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経過後に一定の正答率に収束することが分かる．そのため，攻撃者の正答率が収束するよりも前に $DynamicContentName$ を変更する必要がある．

5.4.2 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

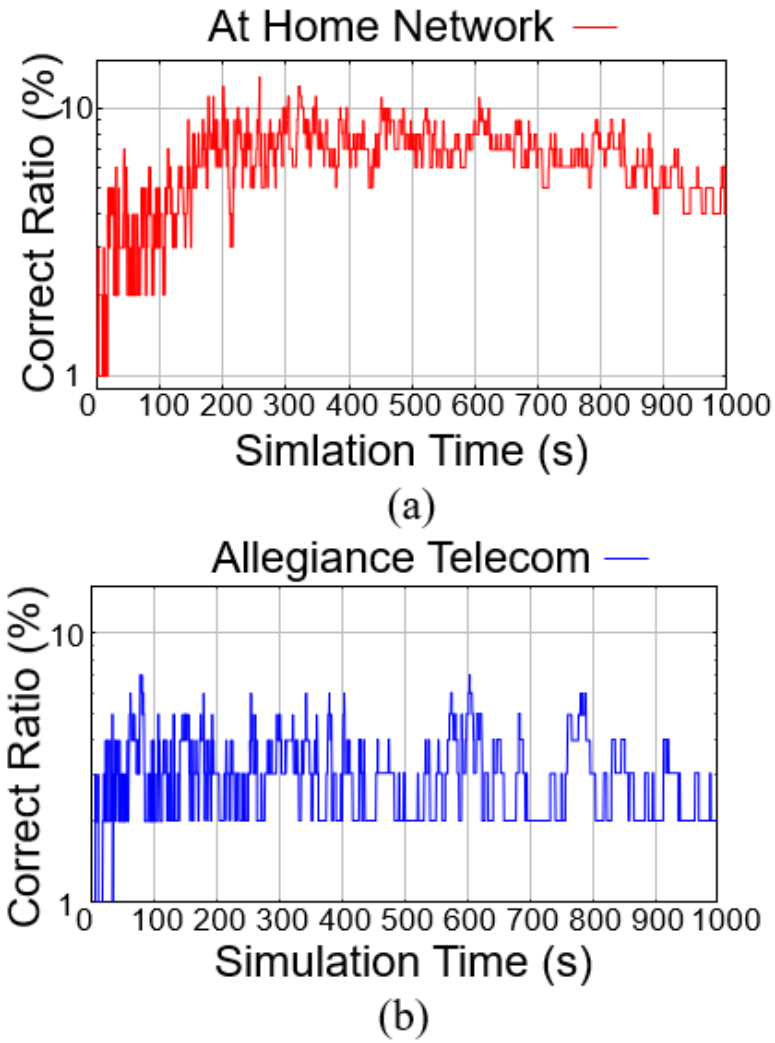

図 5.4: 各トポロジにおける攻撃者の正答率の時間変化

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 5.5 に，$DynamicContentName$ の変更回数に対する攻撃者の正答率をプロットする．図 5.4 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 5.5 の simple encryption 方式は収束時の平均値を示す．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収束する．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．

5.4.3 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 5.6 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，要求到着数が一番多い単一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 5.6(a) はシミュレーション時間を 1,000 秒で実行し，図 5.6(b) はシミュレーション時間を 2,000 秒で実行した．

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 5.6(a) の 1 位コンテンツは 66.16%であり，図 5.6(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上位 4 個のコンテンツを対象に評価を行う．

5.4.4 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 5.7(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 5.7(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 5.5 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 5.7(a) より，全ノードから情報を収集した場合，図 5.6 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 5.7(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 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．

図 5.8 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 5.8(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

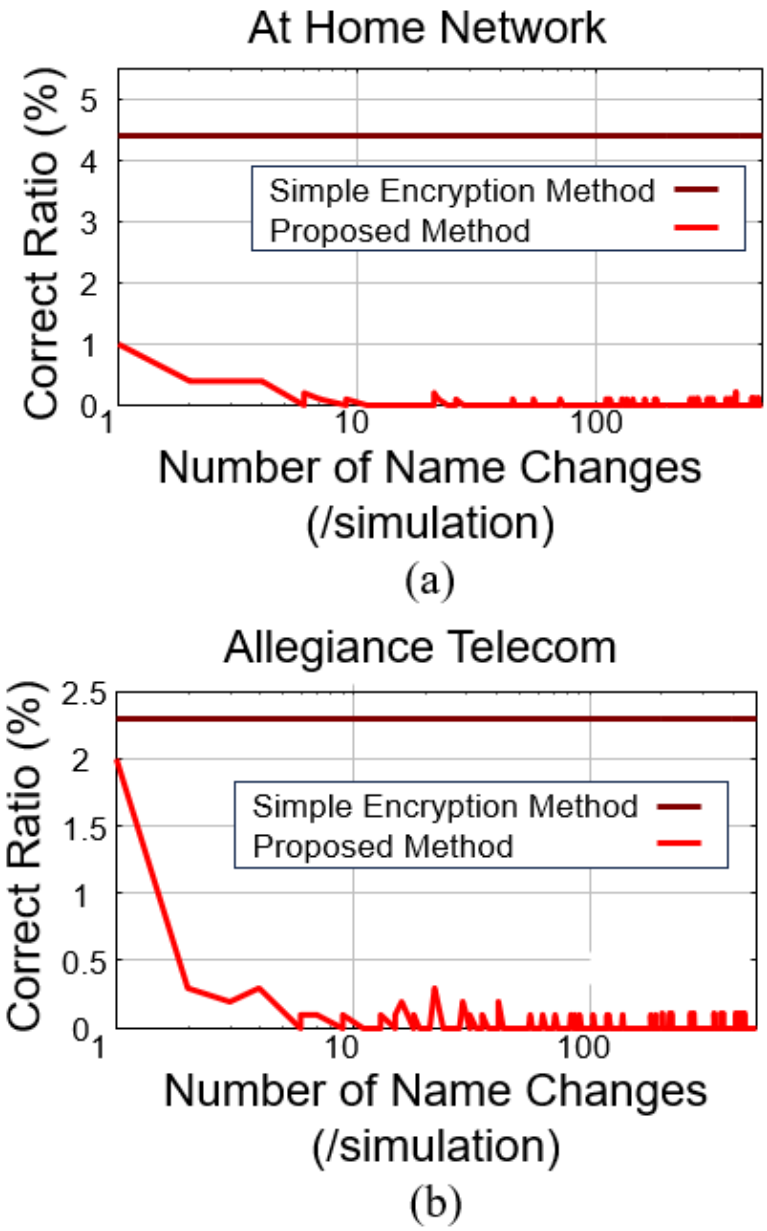

図 5.5: コンテンツ名変更回数に対する攻撃者の正答率

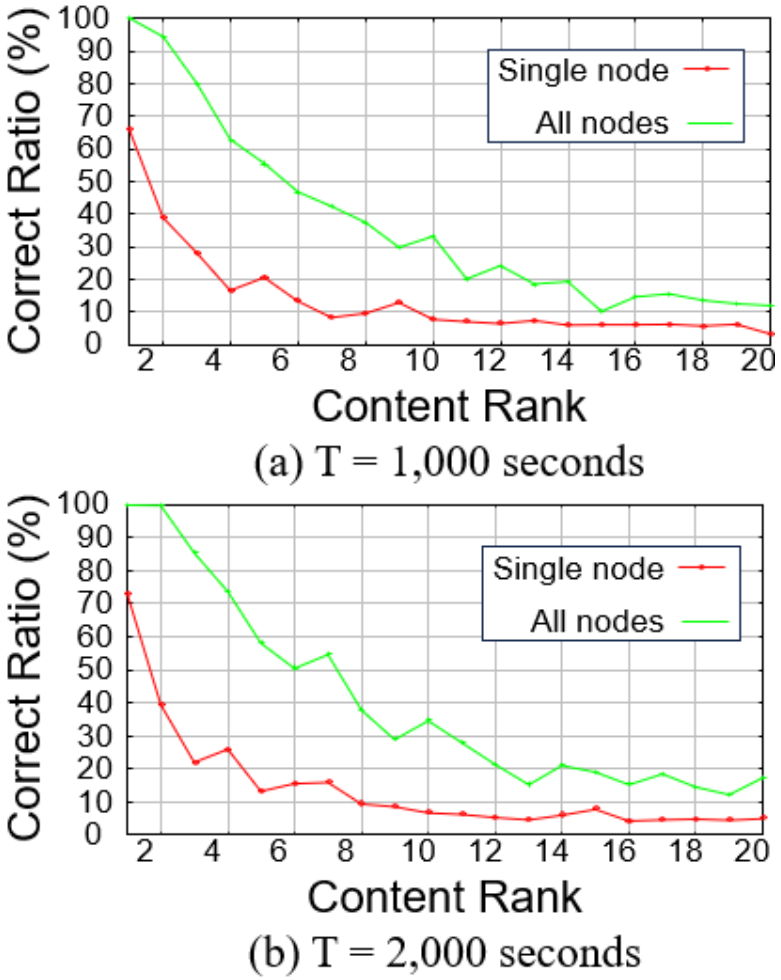

図 5.6: 上位 20 個のコンテンツに対する攻撃者の正答率

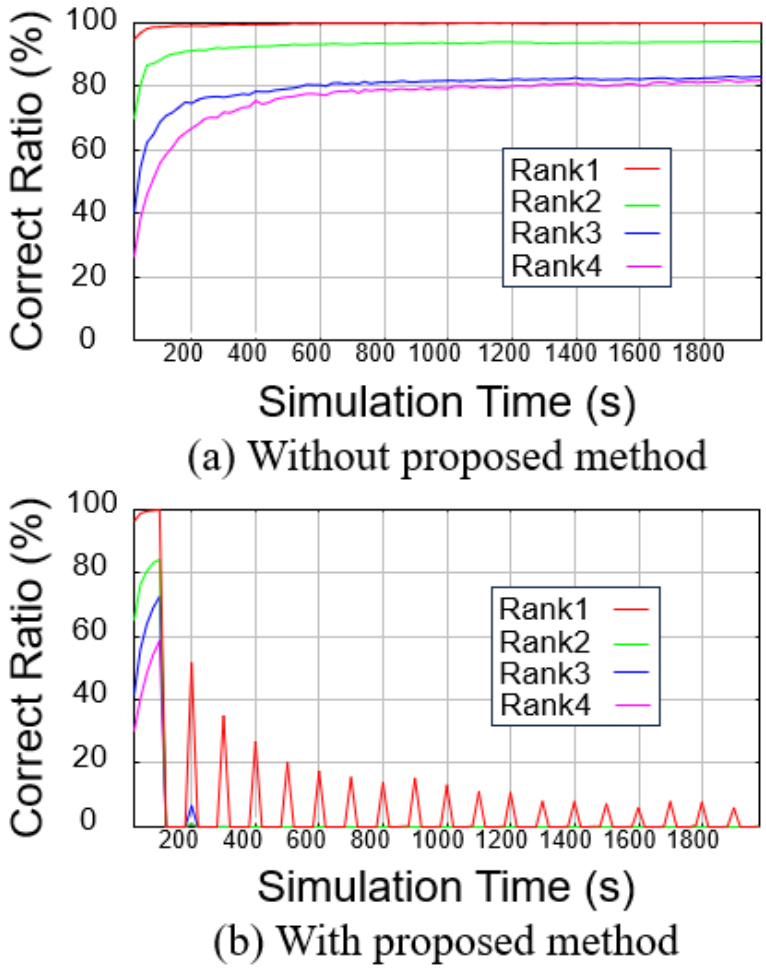

図 5.7: 上位 4 位コンテンツに対する攻撃者の正答率 (攻撃者が全ノードで要求情報を得た場合)

ある．図 5.8(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 5.8(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 5.8(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．

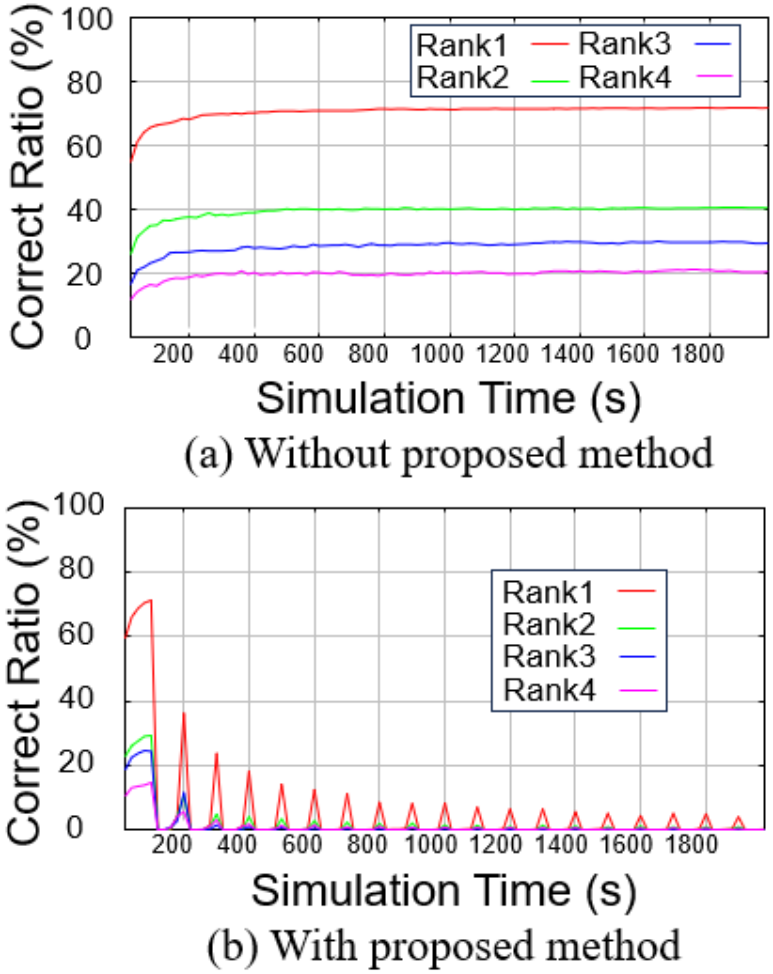

図 5.8: 上位 4 位コンテンツに対する攻撃者の正答率 (攻撃者が単一ノードで要求情報を得た場合)

図 5.7，図 5.8 の結果から提案方式は使用することで，単一ノードで情報を収集した場合，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 5.7(b)，5.8(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．

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．

5.5 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を 100 秒と 200 秒に設定し，評価した．表 5.2 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，提案方式は使用した場合は約 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 5.2: 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

第6章　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．そこで本論では，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提案した．

提案方式は制御トラヒック量や処理時間，遅延時間などが NAC 方式に比べて増加する．しかし，制御トラヒック量においては 1 回の配信要求に発生するトラヒックの大部分はコンテンツデータであるため問題はないと考えられる．また 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．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．

謝辞

本研究を行うにあたり，ご指導をいただいた上山教授に感謝します．また日常，有益な議論をしていただいた研究室の皆様に感謝します．

参考文献

[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] W. Diffie, M. E. Hellman, New direction in cryptography, *IEEE Trans. Inform. Theory.*, Nov. 1976.

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

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

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

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

[8] B. Nour, H. Khelifi, R. Hussain, S. Mastorakis, and H. Moungla, Access Control Mechanism in Named Data Networking: Comprehensive Survey, *ACM CS*, Apr. 2022.

[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*, Jan. 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*, Dec. 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*, Oct. 2018.

外部発表リスト

[1] 深川悠馬, 上山憲昭, ICN の公開鍵暗号を用いたアクセス制御方式の性能解析, 電子情報通信学会総合大会, 2021 年 3 月

[2] 深川悠馬, 上山憲昭, ICN の共通鍵暗号を用いたアクセス制御方式の性能解析, 電子情報通信学会ソサイエティ大会, 2021 年 9 月

[3] 深川悠馬, 上山憲昭, ICN における個別鍵配送を用いたアクセス制御方式, 電子情報通信学会コミュニケーションクオリティ (CQ) 研究会, 2021 年 11 月

[4] Yuma Fukagawa, Noriaki Kamiyama, Access Control with Individual Key Delivery in ICN, *IEEE LANMAN 2022*, July 2022

[5] 深川悠馬, 上山憲昭, 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, 電子情報通信学会ソサイエティ大会, 2022 年 9 月

[6] 深川悠馬, 上山憲昭, NDN におけるプライバシー保護と個別鍵配送を用いたアクセス制御方式, 電子情報通信学会総合大会, 2023 年 3 月

[7] 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, 電子情報通信学会ネットワークシステム (NS) 研究会, 2023 年 3 月

[8] 深川悠馬, 上山憲昭, NDN におけるプライバシィ保護と頻度攻撃防御を考慮したアクセス制御方式, 電子情報通信学会情報指向ネットワーク (ICN) 研究会, 2023 年 5 月

[9] 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, 電子情報通信学会ソサイエティ大会, 2023 年 9 月

[10] Yuma Fukagawa, Noriaki Kamiyama, Access Control Method with Privacy Preservation in NDN, *IEEE ICNP 2023 (Poster)*, Oct. 2023

[11] 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, 電子情報通信学会ネットワークシステム (NS) 研究会, 2024 年 2 月

[12] 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性能評価, 電子情報通信学会総合大会, 2024 年 3 月