Named Data Networkingにおける Interestのフラグを用いたContent Poisoning Attack 攻撃検知の検討

小林 諒二郎[1]　篠原 涼希[1]　重野 寛[1]

概要：コンテンツ指向型ネットワークである Named Data Networking（NDN）において，NDN の特徴を悪用して通常ユーザやネットワークに悪影響を及ぼす Content Poisoning Attack(CPA) の存在が指摘されている．いくつかの対策手法が提案されているが，それらの手法ではコンテンツを要求するパケットが攻撃サーバに転送される可能性があるため不正なコンテンツの拡散防止には不十分である．本論文では，ネットワーク上から不正なコンテンツを除外し攻撃サーバへの経路情報を変更する CPA 対策手法である CRCI を提案する．提案手法の目的は CPA の検知・対策であり，これを実現するために各ルータはコンテンツの信頼度を算出し，信頼度に応じてキャッシュとルーティング制御を行う．また，コンピュータシミュレーションにより提案手法の攻撃検知や抑制の性能評価を行った．

Consideration of Detection against Content Poisoning Attack by Utilizing the Flag for Named Data Networking

RYOJIRO KOBAYASHI[1]　RYOKI SHINOHARA[1]　HIROSHI SHIGENO[1]

1. はじめに

近年，ネットワークの主な利用目的が音声や映像などのコンテンツ取得に変化していることに対応するため，現在の IP ベースのネットワークに代わる次世代のネットワークアーキテクチャが考えられている．次世代のネットワークアーキテクチャの一つとして，コンテンツ名を使用して通信を行う Named Data Networking（NDN）[1] が研究されている．コンテンツを取得する際は「どこから」よりも「どの」コンテンツを取得するかが重要であるため，コンテンツ名を使用する NDN は今日のユーザの利用目的に合致したネットワークアーキテクチャである．

NDN において，データ要求パケットを Interest，応答パケットを Data と呼ぶ．Interest を受け取ったルータは，その Interest に含まれる Data 名を参照して転送する．ルータは Interest を転送する際にその Interest の転送情報を記録し，Data の転送先を決定する際に使用する．各ルータは Content Store（CS）と呼ばれるキャッシュ領域を保持しており，CS を用いることによってサーバの代わりにデータのコピーを提供することができる．

一方で NDN の特徴を悪用した，既存の IP ネットワークにおいては存在しない新たな攻撃の一つとして，Content Poisoning Attack（CPA）[2] が挙げられる．CPA は攻撃者が不正なコンテンツを意図的に配布することにより，通常ユーザのコンテンツ取得を妨害する攻撃である．NDN の特徴より，ユーザがコンテンツを要求すると不正なコンテンツが CS にキャッシュされて汚染が拡大するという問題がある [2]．

NDN において，全てのコンテンツは提供者によって署名が行われており，コンテンツの完全性やその出所が明確になっている．しかし，署名を確認するオーバヘッドの問題や署名確認時に必要となる公開鍵をいかにして入手するかという問題が指摘されている [3]．これらの問題に対応した手法としてランキングアルゴリズム [4] がある．ランキングアルゴリズムでは，ユーザからの Interest を集計することで不正なコンテンツのキャッシュを優先的に置換す

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University

る．しかしながら，そのプロトコルを利用していないユーザがコンテンツを要求すると再び不正なコンテンツがルータにキャッシュされるという問題がある．

本稿では，ネットワーク上から不正なコンテンツを除外し以降も不正なコンテンツのキャッシュを防ぐ Content Poisoning Attack 対策手法である CRCI（Cache and Route Control method from Interest）を提案する．CRCI において，ルータはキャッシュされているコンテンツの不信度を計算し，不正なコンテンツを検知する．この不信度はデータ要求パケット数，受信したインタフェース数，そして下流インタフェース数という三つの指標によって決定される．これらの指標で評価した際に，不信度が一定値を超えていた場合は不正コンテンツと判断して CS から除外し，そのコンテンツを避けるように不正なコンテンツへの経路情報の優先度を変更する．

以下本稿では，2 章において関連研究について述べ，3 章で CRCI を提案し，4 章でシミュレーション評価により提案手法の有用性を示す．最後に 5 章で結論を述べる．

2. 関連研究

本章では NDN の概要や NDN における CPA 攻撃について説明し，その対策における関連研究をあげる．

2.1 Named Data Networking

NDN [1] はコンテンツ指向のネットワークアーキテクチャ [5] の一つである．NDN において，データ要求パケットである Interest の転送先は，Interest が要求するデータ名に基づいて決定する．一方で，応答パケットである Data の転送先は対応する Interest の転送情報に基づいて決定される．このように Data は対応する Interest が転送された経路と同一の経路を逆方向にたどって返信される．

コンテンツ指向の通信を実装するために，NDN ルータは Forwarding Information Base（FIB），Pending Interest Table（PIT），Content Store（CS）の三つを利用する．FIB は Interest の転送方向を決定する際に使用される．転送する際に，ルータは Interest が要求する Data 名や入力元インタフェースといった情報を PIT に記録する．ルータは Data を受信すると，PIT を参照して対応する Interest が転送されてきたインタフェースを通じて Data を返送する．CS は Data の複製を保存するキャッシュ領域であり，CS によりルータは Data 発行者の代わりに Data を提供することが可能となる．複製の活用により Data が広く拡散し，ユーザは Data の素早い取得が可能となる．

2.2 Content Poisoning Attack

NDN において，コンテンツ指向の特徴を悪用した，既存の IP ネットワークにおいては存在しない新たな攻撃の一つとして Denial-of-Service(DoS) 攻撃 [6] が挙げられる．DoS 攻撃の対策として，Data を評価する方法 [7,8] やインタフェースを評価する方法 [9,10] がある．その DoS 攻撃の 1 つとして Content Poisoning Attack（CPA）[2] がある．CPA は攻撃者が不正なコンテンツを流すことで通常ユーザのコンテンツ取得を妨害する攻撃である．NDN の特徴より，ユーザがコンテンツを要求すると不正なコンテンツが CS にキャッシュされて汚染が拡大するという問題がある [2]．

CPA は攻撃者の行動モデルにより攻撃サーバが転送中の Interest 情報を集める方法，これから要求されるコンテンツ名を予測する方法がある．不正なコンテンツの送信方法として，現在転送中の Interest 情報を集め，不正なコンテンツを送信するものがある．これは情報を収集するためにルータに協力してもらう必要がある．また，これから要求されるコンテンツ名を予測するものがある．NDN におけるコンテンツ名は階層構造となっているため，主要な OS において配信が予想されているパッチ等はコンテンツ名が予測しやすい [3]．攻撃者サーバは予測したコンテンツ名を持つコンテンツをあらかじめルータに広告することで，攻撃者サーバへの経路情報を登録させる．次にユーザがこのコンテンツを要求する Interest を送信することで不正なコンテンツが返されて汚染が拡大する．この方法は攻撃者サーバがコンテンツ名を予測するだけで実行可能であり他のルータの協力を必要としないため実行が容易である．また，名前を予測しやすいコンテンツは人気のあるコンテンツであることから，多くのユーザがコンテンツを要求して汚染が広がりやすい．したがって，この攻撃方法は影響が大きく対策が必要であるといえる．

また，CPA は不正なコンテンツの種類によっても分類することが可能であり，偽と汚染にわけられる．偽コンテンツとはコンテンツの署名が無効，あるいは署名の中身が損壊しているものである．偽コンテンツはコンテンツ生成が容易である反面検知されやすいという特徴を持つ．汚染コンテンツとは他サーバの鍵を用いて署名を生成したコンテンツである．汚染コンテンツは他サーバの鍵を入手する必要があるためコンテンツの生成に手間がかかるが，署名自体が有効であるため検知されにくいという特徴を持つ．

2.3 Content Poisoning Attack への対策とその問題点

NDN において，全てのコンテンツは発行者によって署名が行われており，署名によってコンテンツの完全性やその出所が明確化されている．したがって，コンテンツの署名を確認することにより，CPA によって拡散された不正なコンテンツを除外することが可能である．しかしながら，全てのコンテンツの署名を確認することにより計算オーバヘッドが増大するという問題や，署名を確認する際に必要となる公開鍵をいかにして入手するかという信頼性の問題が指摘されている [3]．

計算オーバヘッドを軽減した手法として Self-Certifying Interest / Content (SCIC) [3]，Check on cache-hit [2]，ランキングアルゴリズム [4] がある．SCIC は事前に入手したいコンテンツのハッシュを取得し，実際に得られたコンテンツのハッシュと比較することでコンテンツの確認を行う．SCIC ではハッシュを用いることにより計算オーバヘッドを軽減しているが，正しいハッシュをいかに取得するかという点に課題がある．Check on cache-hit は署名の確認なしで CS にキャッシュし，CS のキャッシュヒット時に署名を確認する手法である．Check on cache-hit ではコンテンツの確認回数を減らすことにより計算オーバヘッドを軽減しているが，CS のサイズが大きくなるにつれて計算量が増大するという課題がある．ランキングアルゴリズムでは，各ユーザは Interest パケットの Exclude 領域に不正コンテンツ情報を記録する．各ルータは Exclude 情報を集計し，不正である確率が高いコンテンツほど置換されやすくなるようにコンテンツの置換順序を決定する．ランキングアルゴリズムでは情報を集計することによって通信の信頼性を向上させており，その計算量は CS のサイズに大きく左右されない．

これらの関連手法によってキャッシュからコンテンツを取得する際にそのコンテンツが不正である可能性は低くなる．しかし，関連研究の手法ではコンテンツ取得の経路情報に変更を加えない．不正なコンテンツに関する情報を持たない新たなユーザが Exclude 領域を用いずにコンテンツを要求すると，その要求は攻撃サーバへと転送される可能性がある．すると不正なコンテンツがネットワーク上に流入するため，再び不正なコンテンツを CS から除外する必要が生じる．したがって，CS から不正なコンテンツを除外するだけでは攻撃の対策は不十分であると考えられる．

また，各ルータが近隣ルータの評価値を算出し，転送先を決定する ROM [11] という手法が提案されている．この手法ではルータは不正なコンテンツを転送している近隣ルータに対して低い評価値をつけ，評価値が低いルータを転送先から除外することで攻撃の影響を抑制する．しかしながら，この手法ではネットワークトポロジ上重要な位置にいるルータへの転送を止めると多くのパケットが転送されなくなるという問題がある．したがって，経路情報の変更は最低限にとどめ，ネットワーク上の不正なコンテンツを除外することで攻撃に対処する必要があると考えられる．

3. CRCI の提案

本章では，本稿の提案手法である CRCI（Cache and Route Control by Interest）を提案する．

3.1 CRCI の概要

CRCI は各ユーザが不正なコンテンツに関する情報を送信し，その情報をもとに各ルータが不正なコンテンツの対策を行う手法である．CRCI の目的は，以下の三点にある．

- ユーザからの情報を基に不正なコンテンツの特定を行う．
- 特定した不正なコンテンツのコピーを CS から削除する．
- 不正なコンテンツへの経路情報の優先度を変更し，Interest が攻撃サーバへと転送されないようにする．

上記の目的を実現するため，CRCI では各ルータがユーザからの不正なコンテンツに関する情報を集計する．各ルータは，集計した情報をもとに不正なコンテンツを特定する．不正なコンテンツのコピーが CS にキャッシュされていた場合，ルータはそのコンテンツを削除する．さらに，ルータは FIB を参照し，Interest が攻撃サーバへと転送されないように不正なコンテンツへの経路情報の優先度を変更する．

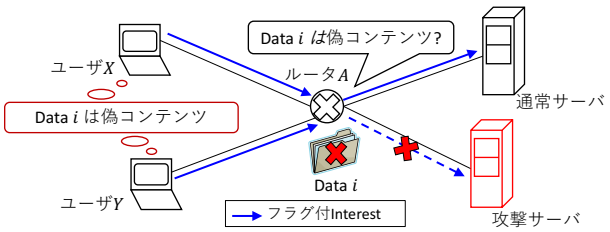

図 1　CRCI の概要

3.2 ユーザによる不正コンテンツ情報の送信

CRCI では各ユーザが受信したコンテンツが正しいコンテンツであるか不正なコンテンツであるかを署名を用いて確認できるという前提に立っている．この前提はランキングアルゴリズムにおいても使用されている．各ユーザは受信したコンテンツを確認し，コンテンツが不正であった場合はコンテンツ名を不正コンテンツテーブルに記録する．ユーザが Interest を送信する際は不正コンテンツテーブルを確認し，同名のコンテンツが記録されている場合は Interest に不正コンテンツ受信フラグを付けて送信する．このフラグは以前同名のコンテンツを要求した際に不正なコンテンツが返信されたことを示す．フラグ領域は Interest パケットにあるオプション領域 [12] を用いる．また，不正コンテンツテーブルにあるコンテンツをユーザが再度受信した際にそのコンテンツの署名を確認し，正しいコンテンツであった場合は不正コンテンツテーブルからコンテンツ名を削除する．このように，不正なコンテンツを受信したユーザは再度正しいコンテンツの要求を行い，その際に不正なコンテンツに関する情報を同時に送信する．

3.3 ルータによる不正なコンテンツの特定と攻撃対策

ルータは各ユーザから送信された不正コンテンツ情報を集計し，不正なコンテンツを特定した後に攻撃の対策を

行う．

Interest を受信したルータは Interest に不正コンテンツ受信フラグが付いているかを確認する．フラグが付いていた場合，ルータは CS を参照せずに PIT の参照を始める．これにより，CS にキャッシュされているコンテンツが不正なコンテンツであった場合にキャッシュヒットで不正なコンテンツが再度返信されることを防ぐ．ルータはフラグが付いていた Interest をもとに不正なコンテンツに関する情報を集計する．集計する情報はコンテンツ名，およびその名前を持つコンテンツが不正コンテンツとして報告された回数，そしてその報告を受信したインタフェース数である．

集計した情報をもとに，ルータは各コンテンツに対して不信度を算出する．コンテンツ i の不信度 D_i は以下の式によって算出する．

$$D_i = \begin{cases} 0 & (R_i = 0) \\ (1 - \frac{1}{R_i}) \times \frac{I_i}{S} & (R_i > 0) \end{cases} \quad (0 \leq D_i \leq 1) \quad (1)$$

ここで，R_i はコンテンツ i に関する情報の受信数，I_i はコンテンツ i に関する情報を受信したインタフェース数，S は下流インタフェース数である．下流インタフェース数とはコンテンツ i を要求する Interest が転送されうるインタフェース数のことを指す．今回は S の値をルータに接続している全インタフェース数から FIB に登録されているコンテンツ i の転送先インタフェース数を引いた数とした．不信度 D_i の式より，コンテンツ i に関する情報の受信数が多いかつ情報を受信したインタフェース数が多いほど値が大きくなるようになっていることがわかる．

このように，ルータは各ユーザによる情報の信頼性を向上させたうえで各コンテンツの不信度を算出する．ルータはフラグ付きのコンテンツ i の要求 Interest を受信するたびにコンテンツ i に対する不信度 D_i を更新する．ルータは不信度 D_i を更新後に D_i の値を閾値 T_F と比較し，以下の式を満たす場合にコンテンツ i が不正なコンテンツであると判断する．

$$D_i > T_F \quad (2)$$

コンテンツ i が不正なコンテンツであった場合，ルータは不正なコンテンツへの対策を行う．初めにルータは CS を参照する．そして CS にコンテンツ i がキャッシュされていた場合，それは不正なコンテンツである可能性が高いため，ルータは CS からコンテンツ i を削除する．さらに，ルータは FIB を参照し，コンテンツ i の転送先として登録されているインタフェース数を調べる．インタフェースが複数登録されている場合，優先的に転送が行われるインタフェースが攻撃サーバへつながっている可能性が高い．なぜなら，これまでユーザが多数の不正コンテンツを受信したサーバだからである．

コンテンツ i の転送先が複数存在した場合に，ルータは

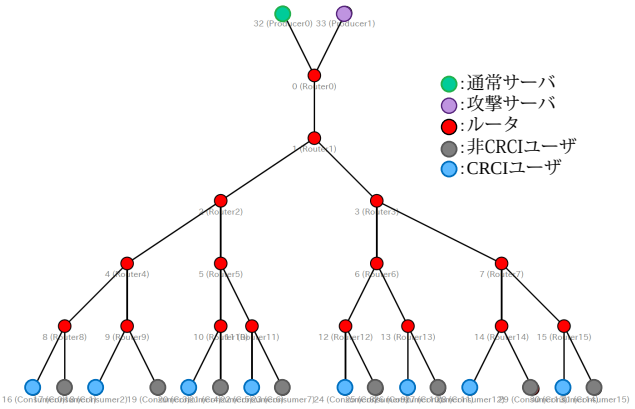

図 2　二分木トポロジ

FIB の情報を変更し優先度が低かったインタフェースに Interest が転送されるように設定する．これにより，一度不正なコンテンツが返信された Interest が同一の攻撃サーバに転送され，結果として不正なコンテンツが再度拡散することを防止する．

4. シミュレーション評価

提案手法 CRCI の有用性を確認するためにコンピュータシミュレーションによる評価を行った．

4.1 シミュレーションモデル

今回の評価では，ネットワークシミュレータとして ns-3 [13] を用いた．NDN のシミュレーションを行うため，ndnSIM [14] によってネットワーク層に NDN の機能を実装した．シミュレーションに用いたトポロジは二分木トポロジである．図 2 にその概形を示す．CRCI ユーザや非 CRCI ユーザは一定の割合で Data を要求する．一方で非 CRCI ユーザはコンテンツ受信後にコンテンツの確認を行わず，Interest をフラグ付きで送信することもない．非 CRCI ユーザを設定することにより，不正コンテンツに関する情報を持たないユーザがコンテンツ要求をおこなった際に，どれだけ不正なコンテンツが返送されるかを調べる．各ユーザは要求するコンテンツをランダムに決定し，その確率分布は一定となっている．通常サーバと攻撃サーバは同様のデータセットを所持しているものとし，不正なコンテンツはコンテンツの署名が無効である偽コンテンツとする．攻撃サーバはシミュレーション開始と同時にコンテンツの提供を開始し，通常サーバはシミュレーション開始から 1 秒後にコンテンツの提供を開始する．攻撃サーバが通常サーバよりも早くコンテンツ提供を開始することにより，あらかじめネットワークが不正コンテンツで汚染されている状況を再現する．

表 1 にユーザの基本的なパラメータについて示す．ユー

表 1　通常ユーザパラメータ

パラメータ	値
要求時間	200[sec]
Data の種類数	100
要求の強度	800[pkt/sec]

表 2　シミュレーションパラメータ

パラメータ	値
ネットワークシミュレータ	ns-3 [13]
NDN モジュール	ndnSIM 1.0 [14]
シミュレーション時間	200[sec]
キャッシュ置換アルゴリズム	LFU
ルータの CS サイズ	31[pkt]
ルータの PIT サイズ	1000[pkt]
Data サイズ	1100[byte]
リンクの帯域	10[Mbps]
リンクの遅延	10[ms]
T_F	0.6

ザのコンテンツ要求時間は 200 秒とした．最初の 10 秒間は通常ユーザのみがコンテンツ要求を行い，それ以降は攻撃者もコンテンツ要求を行う．CRCI ユーザ数と非 CRCI ユーザ数は同数とした．

表 2 に基本的なシミュレーションパラメータを示す．キャッシュ置換手法には LFU を用いた．Data を各々のキャッシュから返信しないようにするために各ユーザとサーバにはキャッシュ容量を設けていない．CPA の影響と CRCI の性能を評価するために，以下の評価項目を設ける．

- コンテンツ取得数
  非 CRCI ユーザが取得した単位時間あたりの正しいコンテンツおよび不正なコンテンツの取得数である．
- コンテンツの種類
  非 CRCI ユーザが取得したコンテンツの種類である．

4.2　不信度の算出

提案手法において，正しいコンテンツと不正なコンテンツでどの程度不信度に差がでるのか，シミュレーション上で確認する．今回のシミュレーションでは CRCI ユーザがコンテンツの確認を行い，不正コンテンツに対してはフラグ付きで Interest を再送する．今回は正しいコンテンツと不正コンテンツの不信度の差を調べることを目的としているため，不信度の値が高い場合でもコンテンツの除外や経路情報の変更は行わない．図 3 に図 2 の二分木トポロジにおける不信度のグラフを示す．この図より，正しいコンテンツの不信度は 0 のままであるのに対し，不正コンテンツの不信度は高い値で収束していることがわかる．また，この不信度の値は全ルータの平均値であるため，不正コンテンツの不信度はネットワーク全体で高くなっていることがわかる．したがって，提案手法はユーザからの情報をもとにコンテンツの不信度を算出し，その結果不信度から正しいコンテンツと不正コンテンツを判別できることがわかった．今回のトポロジでは不正コンテンツの不信度が 0.7 あたりで収束していることを踏まえ，提案手法における不正コンテンツ判定の閾値である T_F の値を 0.6 に設定する．

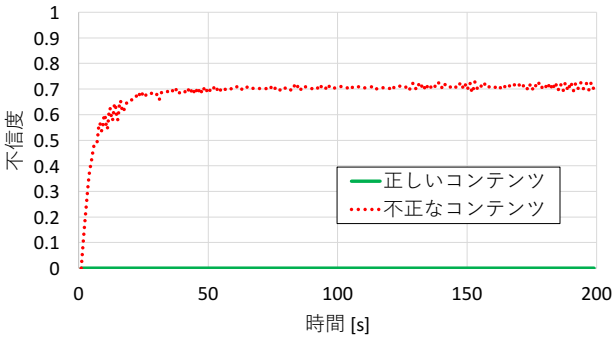

図 3　それぞれのコンテンツの不信度の平均値

4.3　Content Poisoning Attack の抑制性能の評価

今回のシミュレーションでは，コンテンツの確認を行わない非 CRCI ユーザのコンテンツの取得数と取得するコンテンツの種類を調べる．

図 4 は非 CRCI での単位時間あたりの正しいコンテンツおよびの不正なコンテンツ取得数の時間経過を示す．この図より，ユーザが受信しているコンテンツはすべて不正なコンテンツとなっていることがわかる．これは攻撃サーバが通常サーバよりも早くコンテンツを提供したため，不正なコンテンツがネットワーク上に広く拡散したことが原因である．また，その後もルータの経路情報が変更されず，先に登録された攻撃サーバへ Interest が転送され続けたことも確認できた．

図 5 は CRCI での単位時間あたりの正しいコンテンツおよびの不正なコンテンツの取得数の時間経過を示す．この図より，図 4 において全く取得出来ていなかった正しいコンテンツが，約 10 秒後には速やかに増加し，以降も高い数値で正しいコンテンツ取得数を維持出来たことを確認した．不正なコンテンツを約 10%の割合で取得し続けてしまう理由として，閾値をネットワーク内の全てのルータの平均値から定めたことが考えられる．特定のルータでは不正なコンテンツの不信度が閾値よりも低くなっていることで，不正なコンテンツとして判定されずにキャッシュ置換やルーティングの優先度が変更されなかった可能性がある．

以上のことより，提案手法は CPA の影響を抑制することが可能であり，以降も再び不正なコンテンツがキャッシュされることを防いでいることが確認できた．

5.　おわりに

本論文では，NDN における CPA の対策手法である CRCI

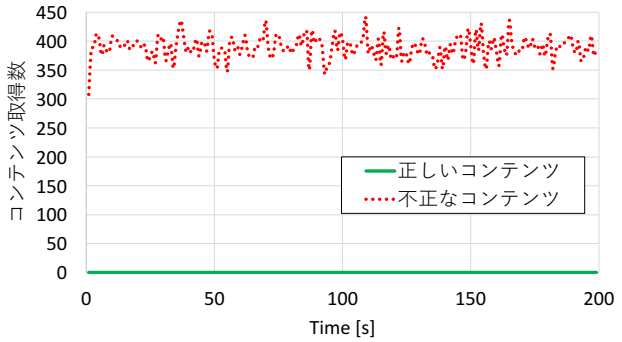

図 4　CRCI 非動作時のコンテンツ取得数

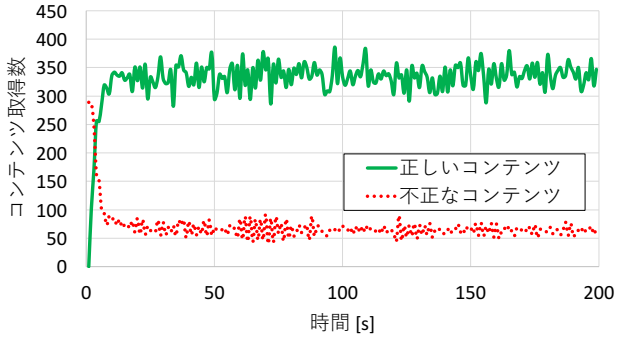

図 5　CRCI 動作時のコンテンツ取得数

を提案した．

CRCI では各ユーザが判定した不正なコンテンツの情報を集める．Interest を受信したルータはフラグ情報を集計し，コンテンツに対して算出した不信度をもとに不正なコンテンツを推定する．不正なコンテンツは CS から除外し，そのコンテンツを避けるように不正なコンテンツへの経路情報の優先度を変更する．

シミュレーションを用いて CRCI の不正コンテンツ抑制性能を評価した．シミュレーション結果より，フラグ情報を用いて不信度を算出することで正しいコンテンツと不正なコンテンツを判別できることを確認した．さらに，不正なコンテンツへの経路情報の優先度を変更することで，それ以降も不正なコンテンツの流出を抑制できていることを確認した．

以上より，提案手法は Content Poisoning Attack 攻撃を抑制することが可能であり，有用性があることを示した．

謝辞　本研究は JSPS 科研費 16H02811 の助成を受けたものです．

参考文献

[1] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., claffy, k., Crowley, P., Papadopoulos, C., Wang, L. and Zhang, B.: Named Data Networking, *ACM SIGCOMM Computer Communication Review (CCR)*, Vol. 44, No. 3, pp. 66–73 (2014).

[2] Kim, D., Nam, S., Bi, J. and Yeom, I.: Efficient content verification in named data networking, *Proceedings of the 2nd International Conference on Information-Centric Networking*, pp. 109–116 (2015).

[3] Gasti, P., Tsudik, G., Uzun, E. and Zhang, L.: DoS and DDoS in Named Data Networking, *Proceedings of 2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–7 (online), DOI: 10.1109/ICCCN.2013.6614127 (2013).

[4] Ghali, C., Tsudik, G. and Uzun, E.: Needle in a haystack: Mitigating content poisoning in named-data networking, *Proceedings of NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, pp. 1–10 (2014).

[5] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H. and Braynard, R. L.: Networking Named Content, *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, CoNEXT '09, pp. 1–12 (2009).

[6] Saxena, D., Raychoudhury, V., Suri, N., Becker, C. and Cao, J.: Named Data Networking: A survey, *Computer Science Review*, Vol. 19, pp. 15 – 55 (2016).

[7] Xie, M., Widjaja, I. and Wang, H.: Enhancing cache robustness for content-centric networking, *Proceedings of the IEEE INFOCOM 2012*, pp. 2426–2434 (2012).

[8] Karami, A. and Guerrero-Zapata, M.: An ANFIS-based cache replacement method for mitigating cache pollution attacks in Named Data Networking, *Computer Networks*, Vol. 80, pp. 51 – 65 (2015).

[9] 篠原涼希，神本崇史，　重野寛：Named Data Networking における要求フローの特徴を使用した DoS 攻撃の検知分類手法，第 25 回マルチメディア通信と分散処理ワークショップ論文集，pp. 85–91 (2017).

[10] 篠原涼希，神本崇史，　重野寛：Named Data Networking における要求フローの影響度を用いた DoS 攻撃対策手法，情報処理学会論文誌，Vol. 59, No. 2, pp. 564–573 (2018).

[11] Wu, D., Xu, Z., Chen, B. and Zhang, Y.: What If Routers Are Malicious? Mitigating Content Poisoning Attack in NDN, *Proceedings of the 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUSTCOM-16)*, pp. 481–488 (2016).

[12] : NAMED DATA NETWORKING, `https://named-data.net/` (2018).

[13] Henderson, T. R., Roy, S., Floyd, S. and Riley, G. F.: Ns-3 Project Goals, *Proceeding of the 2006 Workshop on Ns-2: The IP Network Simulator (WNS2 '06)* (2006).

[14] Afanasyev, A., Moiseenko, I. and Zhang, L.: ndnSIM: NDN simulator for NS-3, Technical report, NDN (2012).