情報処理学会論文誌 Vol.60 No.2 440–448 (Feb. 2019)

Named Data Networkingにおける Content Poisoning Attack対策手法

小林 諒二郎[1,a)] 篠原 涼希 重野 寛[1]

受付日 2018年5月7日, 採録日 2018年11月7日

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 CFCM 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不信度を算出し，不信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．

キーワード：Named Data Networking，Content Poisoning Attack，Bad Mouthing Attack

Countermeasure against Content Poisoning Attack in Named Data Networking

Ryojiro Kobayashi[1,a)] Ryoki Shinohara Hiroshi Shigeno[1]

Received: May 7, 2018, Accepted: November 7, 2018

Abstract: In Named Data Networking (NDN), which is a content-oriented network, Content Poisoning Attack (CPA) affect normal users and networks. Countermeasures against CPA have been proposed, but it is impossible to prevent the fake content spreading because the router repeats forwarding data requests to the server which has the poisoned content. In this paper, we propose a countermeasure against CPA by the router by deleting cache on itself Content Store and changing the forwarding routing, called CFCM. The purposes of CFCM are detection and suppression of CPA. Each router calculates distrust value of cached data and deletes and limits spreading the data. We evaluate suppression performance of CFCM through computer simulation.

Keywords: Named Data Networking, Content Poisoning Attack, Bad Mouthing Attack

1. はじめに

近年，ユーザのコンテンツ取得要求がコンテンツ指向へと変化していることにともない，コンテンツ指向型のネットワークアーキテクチャ [1] が注目を集めている．コンテンツ指向型ネットワークアーキテクチャの 1 つに Named Data Networking（NDN）[2] がある．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

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio Uniersity, Yokohama, Kanagawa 223–8522, Japan
[a)] ryojiro@mos.ics.keio.ac.jp

においては存在しない新たな攻撃の 1 つとして，Content Poisoning Attack（CPA）[3] があげられる．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 [3]．

NDN において，すべ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 [4]．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 [5] 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，以降も不正なコンテンツのキャッシュを防ぐ CPA 対策手法である CFCM（Cache and Flow Controlling Method based on distrust value）を提案する．CFCM 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 3 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 から除外する．その後，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．

以下本論文では，2 章において関連手法について述べ，3 章で CFCM を提案し，4 章でシミュレーションによる評価結果を示す．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 [2] はコンテンツ指向のネットワークアーキテクチャ [1] の 1 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．

図 1 に NDN ルータの構造とパケット処理を示す．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 3 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 を返信する．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．

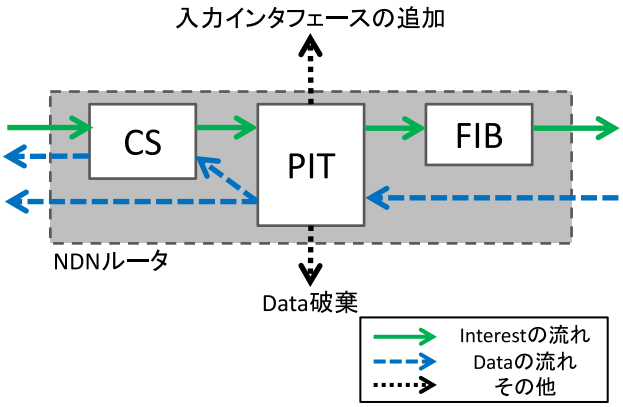

図 1 NDN ルータの構造とパケット処理
Fig. 1 The structure of NDN router and processing of packets.

2.2 Content Poisoning Attack

既存の IP ネットワークにおいて Denial-of-Service（DoS）攻撃が問題視されているが，NDN においてもそれは例外ではなく，NDN 特有の DoS 攻撃 [6] が存在する．DoS 攻撃の対策としては，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）[3] 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 [3]．

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 [4]．攻撃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ため，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る．不正なコンテンツは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，すべ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となっている．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，すべ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[4]．

計算オーバヘッドを軽減した手法としてSelf-Certifying Interest/Content（SCIC）[4]，Check on cache-hit[3]，ランキングアルゴリズム[5]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，不正なコンテンツを再びCSから除外する必要がある．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. 提案手法CFCM

本章では，本論文の提案手法であるCFCM（Cache and Flow Controlling Method based on distrust value）について説明する．

3.1 CFCMの概要

CFCM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．CFCMの目的は，以下の3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
- 特定した不正なコンテンツのコピーをCSから削除
- 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の変更

図2にCFCMの外形を示す．上記の目的を実現するため，CFCM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．不正なコンテンツの報告はエッジルータにのみ転送され，上位ルータへの転送は行われない．そのため上位ルータで不正コンテンツのキャッシュ置換が発生しないことが考えられる．しかし，エッジルータでコンテンツの経路情報の優先度が変更されること

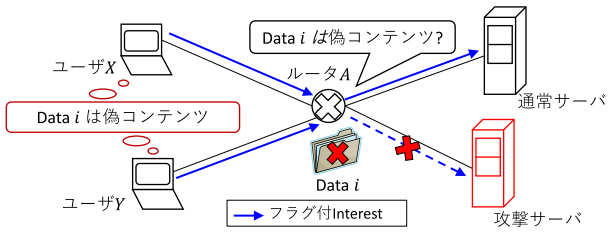

図 2 CFCM の概形
Fig. 2 Overview of CFCM.

により，その上位ルータへ Interest が転送されなくなる．その結果，上位ルータへは Interest が転送されなくなりキャッシュ置換が発生する．

また，ユーザからの評価値を算出する手法に対して Bad-Mouthing Attack（BMA）[12] が指摘されている．CFCM においても BMA を行うことは可能であることから対策が必要である．以下において，CFCM における具体的なユーザとルータの動作について詳細に説明する．

3.2 ユーザによる不正コンテンツ情報の送信

CFCM 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，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 [13] 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する．さらに，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．情報を集計することにより，BMA 等の悪意のあるユーザの影響を最小限とし，情報の信頼性の向上を目指す．

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 R_i は以下の式によって算出する．

$$R_i = \begin{cases} 0 & (I_i = 0) \\ \left(1 - \dfrac{1}{I_i}\right) \times \dfrac{F_i}{S_i} & (I_i > 0) \end{cases} \quad (0 \le R_i \le 1) \qquad (1)$$

ここで，I_i はコンテンツ i の不正に関する情報の受信数，F_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_i 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 R_i の式より，コンテンツ i に関する情報の受信数が多く，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分かる．

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 R_i を更新する．ルータは不信度 R_i を更新後に R_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．

$$R_i > T_F \qquad (2)$$

ルータがコンテンツ i を不正なコンテンツであると判断した場合，ルータは不正なコンテンツへの対策を行う．まず初めにルータは 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 に関する Interest 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は攻撃サーバに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 に関する Interest の転送先が複数存在した場合に，ルータは 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．

3.4 Bad-Mouthing Attack への対策

CFCM は Bad-Mouthing Attack（BMA）の影響を受けることが想定される．CFCM は各ユーザからの情報をもとに不正なコンテンツを推定し対策する手法である．ユーザからの情報をもとに評価値を算出する手法は有用であり，モバイルアドホックネットワーク（MANET）のような従来のネットワークにおいてもトラストモデルとして研究されている [14], [15]．しかしながら，トラストモデルにおいて，攻撃ノードが虚偽報告を流すことで，通常ノードのトラスト値を低下させる BMA [12] が指摘されている．CFCM において，攻撃ユーザが正しいコンテンツを受信した際にフラグを付けて Interest を再送することにより，ルータに正しいコンテンツを不正なコンテンツと判断させる BMA を行うことが可能である．CFCM では情報の集計を行うため，ある程度の虚偽報告は対処可能であると考えられるが，虚偽報告が通常の報告と同程度の量になるとルータが誤った判断を行う可能性がある．

BMA を行う攻撃ユーザが増加するにつれて，正しいコンテンツの不信度が増加する．そして，BMA を行う攻撃ユーザの割合が 50%になると，正しいコンテンツと不正なコンテンツの不信度はほぼ同程度となる．あるコンテンツについて同程度の不信度が算出される場合は BMA の影響を受けていると考えられるが，その中でも不信度が最も大きいコンテンツは不正コンテンツである可能性が高く，そのコンテンツを制限することで BMA に対処可能であると考えられる．

以上のことをふまえ，提案手法における不正なコンテンツの判定を以下のように行う．提案手法では不正なコンテンツの判定を 2 段階で実行する．

不正コンテンツ判定

まずルータはコンテンツ i の不信度を閾値 T_F と比較し，以下の条件を満たす場合には不正なコンテンツと判定する．

$$R_i > T_F \tag{3}$$

この判定は式 (2) の説明で述べたとおりである．この判定により，まずルータは通常ユーザによって情報が送信され不信度が高くなっているコンテンツを不正コンテンツと判定する．

BMA 判定

不正コンテンツ判定で式 (3) を満たさなかったコンテンツに対し，ルータはさらなる判定を行う．まずルータはコンテンツ i の不信度を新たな閾値 T_B と比較する．そして以下の式を満たす場合にはルータはさらなる判定を行う．

$$R_i > T_B \tag{4}$$

ここで，閾値 T_B とは BMA の判定用に新たに設定した閾値である（$T_B < T_F$）．R_i が式 (4) を満たしている場合，ルータは CS に記録されている他のコンテンツの不信度を確認する．そしてコンテンツ i とは異なるコンテンツ j が以下の条件を満たす場合，ルータはさらなる判定を行う．

$$R_j > T_B \quad (j \neq i) \tag{5}$$

最後にルータは R_i と R_j を比較し，以下の条件を満たす場合にコンテンツ i を不正なコンテンツと判定する．

$$R_i > R_j \tag{6}$$

これら 3 つの条件式は，ルータが BMA の影響を受けていると考えられる場合に最も不正なコンテンツである可能性が高いものを判定するものである．不信度が T_B 以上のコンテンツが 1 つしかない場合は不正なコンテンツとは見なされず不正コンテンツ判定の閾値が大きくなる．しかし，不信度が T_B 以上のコンテンツが複数存在していた場合は，そのコンテンツの不信度が最も大きい場合にキャッシュが置換される．NDN の特性上，キャッシュはつねに置換される可能性があり，それによって不正コンテンツ判定の閾値もつねに変動する．このように，提案手法では不正なコンテンツの判定を 2 段階で実行することで，不正なコンテンツと判定する閾値が T_B 以上 T_F 以下の間で動的となり，ユーザからの情報の信頼度を向上させ BMA への耐性を向上させている．

4. シミュレーション評価

提案手法 CFCM 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

今回のシミュレーションでは評価環境として DFN トポロジを使用した．DFN トポロジは現実のネットワークをモデル化したトポロジである．**図 3** に DFN トポロジの概形を示す．CFCM ユーザや非 CFCM ユーザは一定の割合で Data を要求する．一方で非 CFCM ユーザはコンテン

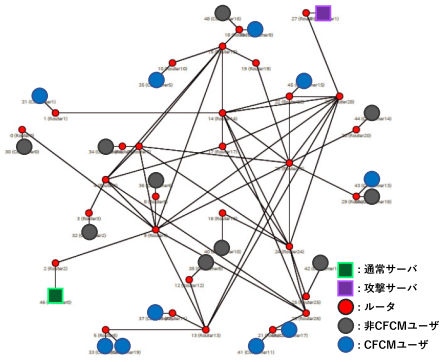

図 3 DFN トポロジ
Fig. 3 DFN topology.

表 1 ユーザパラメータ
Table 1 User parameters.

パラメータ	値
要求時間	200 [sec]
Data の種類数	10,000
1 ユーザあたりの要求頻度	50 [pkt/sec]

表 2 シミュレーションパラメータ
Table 2 Basic simulation parameters.

パラメータ	値
ネットワークシミュレータ	ns-3 [16]
NDN モジュール	ndnSIM 1.0 [17]
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	1,000 [pkt]
ルータの PIT サイズ	15,000 [pkt]
Data サイズ	1,100 [byte]
リンクの帯域	10 [Mbps]
リンクの遅延	10 [ms]

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 CFCM 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を要求した際にどれだけ不正なコンテンツが返信されるかを調べる．

各ユーザは毎秒 50 個のコンテンツを要求する．要求するコンテンツはランダムとなっており，その確率分布は一定となっている．BMA ユーザは CFCM ユーザのなかから一定の割合で設定し，CFCM ユーザとは正反対の行動をとるものとした．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する．コンテンツの署名が無効である偽コンテンツを不正なコンテンツとする．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．CFCM ユーザ数と非 CFCM ユーザ数は同数とした．また，BMA に対する CFCM の効果を確かめるために，CFCM ユーザ中の BMA ユーザの割合を 0%から 100%まで変動させた．

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．DFN トポロジ使用時のパラメータは関連研究 [11] の値を参考にした．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．

表 3 は CFCM に関するパラメータを示している．本論文において，固定値である T_F，T_B の値は予備実験を基に決定した．さらに，BMA ユーザの割合を変動させたうえでの不信度の評価値を算出し固定値を決定した．この予備実験については次の項で詳しく説明する．

表 3 CFCM パラメータ
Table 3 CFCM parameters.

パラメータ	値
T_F	0.6
T_B	0.3

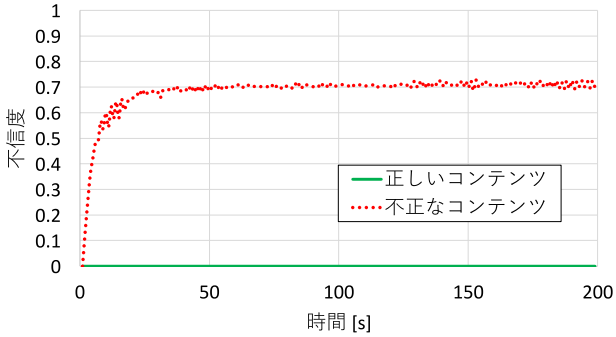

図 4 コンテンツの不信度
Fig. 4 Disrust value of contents.

CPA の影響と CFCM 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 CFCM 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
- 正しいコンテンツの取得率
  非 CFCM ユーザが取得した全コンテンツにおける正しいコンテンツの割合をシミュレーション時間内での平均値

4.2 不信度の算出

今回のシミュレーションパラメータとネットワークトポロジにおいてコンテンツの不信度がどの程度の値となるかを確認するために予備実験を行った．予備実験ではすべてのユーザを CFCM ユーザとした．**図 4** はその実験においてのコンテンツの不信度を表している．正しいコンテンツの不信度は 0 である一方，不正なコンテンツの不信度はおよそ 0.7 程度で収束していることを確認した．ほかに二分木トポロジにおいて予備実験を行ったところ，不信度は 0.45 程度で収束した．このことから不信度はトポロジに依存することが分かった．

また，BMA ユーザが存在する場合の不正なコンテンツの不信度を確認する．**図 5** は BMA ユーザが 50%のときの不正なコンテンツの不信度を表している．不信度は正しいコンテンツ，不正なコンテンツともに BMA ユーザが 50%であることから，どちらが正しいコンテンツであるかを判断することは難しく，正しいコンテンツ，不正なコンテンツともに 0.25 程度で収束していることを確認した．正

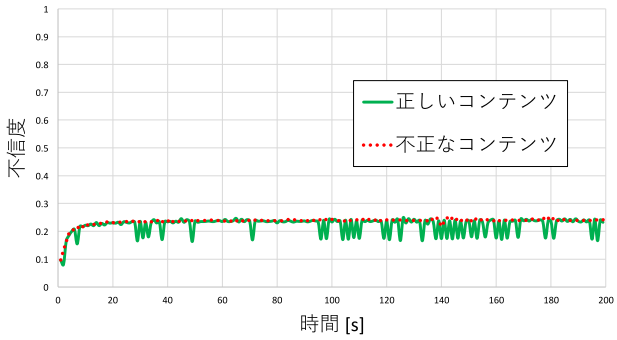

図 5 BMA ユーザが 50%のときのコンテンツの不信度
Fig. 5 Disrust value of contents when BMA users are 50%.

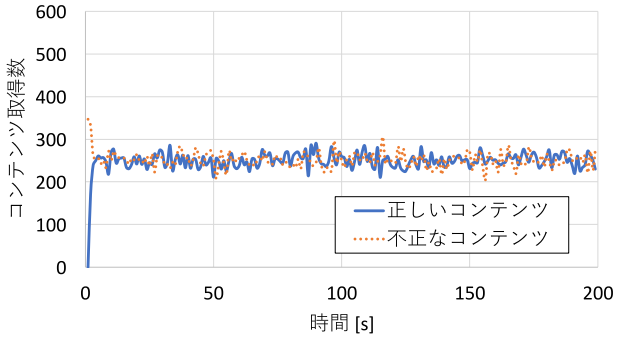

図 6 CFCM 非動作時のコンテンツ取得数
Fig. 6 Number of retrieved Data without CFCM.

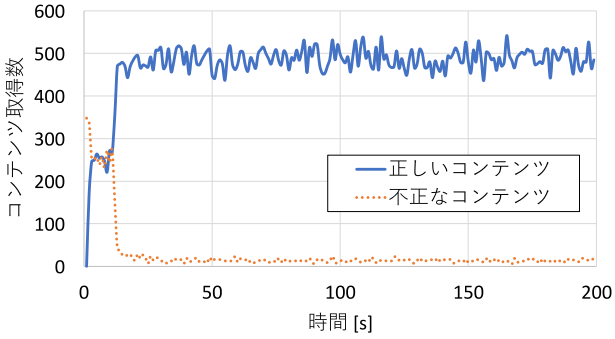

図 7 CFCM 動作時のコンテンツ取得数
Fig. 7 Number of retrieved Data with CFCM.

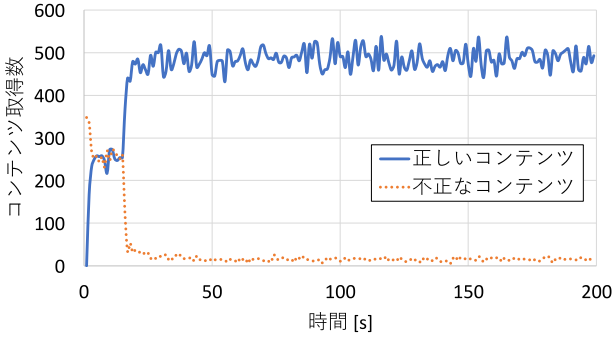

図 8 BMA ユーザが 50%のときのコンテンツ取得数
Fig. 8 Number of retrieved Data when BMA users are 50%.

しいコンテンツの不信度が時折低くなることがあるが，これは実際のネットワークトポロジを模倣した DFN トポロジを利用しているため，ユーザとルータの距離が通常ユーザと BMA ユーザで異なることが原因として考えられる．これらのことから不正なコンテンツと判定する不信度 T_F を 0.6 に，BMA ユーザが半分以上であることは考えにくいことから，BMA を受けていると判定する不信度 T_B を 0.3 に設定する．しかし，閾値の値については検討する余地がある．

4.3 Content Poisoning Attack の抑制性能の評価

コンテンツの確認を行わない非 CFCM 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 6 は非 CFCM 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，ユーザが取得するコンテンツの約半数は不正なコンテンツとなっており，CPA の影響を受けていることが確認できる．同様に二分木トポロジで行った場合には，ユーザが取得したコンテンツのほぼ 100%が不正なコンテンツとなり，ユーザが取得する不正なコンテンツの割合はネットワークのトポロジや，ユーザのアクセスモデルに依存することを確認した．

図 7 は CFCM 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 6 において約半数となっていた正しいコンテンツの取得数が，約 10 秒後には速やかに増加したことが確認できる．CFCM では不正報告が一定数となるまではキャッシュを置換しないことから，最初の約 10 秒間は非 CFCM 環境と同程度の正しいコンテンツ取得数となった．

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．

4.4 Bad-Mouthing Attack の抑制性能の評価

DFN トポロジ上における BMA の影響について確認する．**図 8** は CFCM ユーザ内における BMA ユーザの割合が 50%のときのコンテンツ取得数の時間経過を示している．この図より，BMA の影響が大きくなる BMA ユーザの割合が 50%の場合でも，図 7 と同程度の正しいコンテンツ取得数となっていることを確認した．実際に BMA ユーザの割合を 10%，30%，60%と変化させた場合でも正しいコンテンツの取得数は同程度であった．BMA ユーザと通常ユーザのデータ要求モデルが異なっているため，BMA ユーザの割合が 60%でも不正なコンテンツを判別することが可能となった．このことより提案手法は BMA の影響を抑制できることを確認した．

また，2 段階の判定を行うことの有用性を確かめるために，不正コンテンツ判定のみを行った場合と BMA 判定を加えた場合の，全動作期間での正しいコンテンツの取得率を**図 9** に示した．図 9 より，不正コンテンツ判定のみの

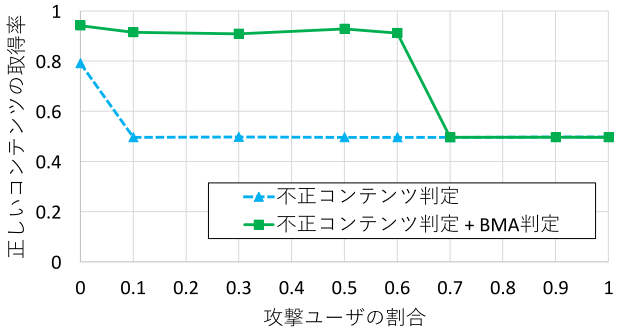

図 9 正しいコンテンツの取得割合の比較
Fig. 9 Rate of retrieved normal Data.

場合では，BMA ユーザの割合を 10%にすると正しいコンテン取得率が 30%低下したが，不正コンテンツと BMA の 2 段階の判定において正しいコンテンツ取得率はほとんど変化しなかった．不正コンテンツ判定のみを実行した場合と比較し，BMA 判定を加えた場合のほうが正しいコンテンツの取得率が向上したことを確認した．

5. おわりに

本論文では，NDN における CPA の対策手法である CFCM を提案した．

CFCM では各ユーザが判定した不正なコンテンツの情報を収集する．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．また，CFCM ではユーザが虚偽報告をすることで正しいコンテンツを除外しようとする BMA が実行される可能性が想定されるが，2 段階の判定を行うことでユーザからの虚偽報告に対応している．

シミュレーションを用いて，DFN トポロジ上で CFCM 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，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．また，2 段階の判定を行うことにより，BMA を実行するユーザが増加した場合でもある程度の正しいコンテンツの取得率を維持することができることを確認した．

以上より，提案手法は CPA 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] Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H. and Braynard, R.L.: Networking Named Content, *Proc. 5th International Conference on Emerging Networking Experiments and Technologies, CoNEXT '09*, pp.1–12 (2009).

[2] 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).

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

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

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

[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, *Proc. 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, *Proc. 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (*IEEE TRUSTCOM-16*), pp.481–488 (2016).

[12] Sun, Y., Han, Z. and Liu, K.R.: Defense of trust management vulnerabilities in distributed networks, *IEEE Communications Magazine*, Vol.46, No.2, pp.112–119 (2008).

[13] NAMED DATA NETWORKING (2018), available from ⟨http://named-data.net/doc/NDN-packet-spec/current/interest.html⟩.

[14] Umeda, S., Takeda, S. and Shigeno, H.: Trust evaluation method adapted to node behavior for secure routing in mobile ad hoc networks, *Proc. 2015 8th International Conference on Mobile Computing and Ubiquitous Networking* (*ICMU*), pp.143–148 (2015).

[15] Ohata, Y., Kamimoto, T., Shinohara, R. and Shigeno, H.: Cooperation Incentive System Balancing Virtual Credit in Mobile Ad hoc Networks, *Proc. 13th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (*MobiQuitous 2016*), pp.218–226 (2016).

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

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

小林 諒二郎

2017 年専修大学ネットワーク情報学部卒業．現在，慶應義塾大学大学院理工学研究科前期博士課程在学中．

篠原 涼希

2016 年慶應義塾大学理工学部卒業．2018 年同大学大学院理工学研究科前期博士課程修了．

重野 寛 （正会員）

1990 年慶應義塾大学理工学部計測工学科卒業．1997 年同大学大学院理工学研究科博士課程修了．現在，同大学理工学部教授．博士（工学）．情報処理学会学論文誌編集委員，同 DPS 研究会主査，Secretary of IEEE ComSoc APB 等を歴任．現在，情報処理学会理事，同 ITS 研究会主査，Co-Chair of IEEE ComSoc APB ISC．ネットワーク・プロトコル，ITS 等の研究に従事．著書『ユビキタスコンピューティング』（オーム社），『情報学基礎第 2 版』（共立出版）等．電子情報通信学会，IEEE，ACM 各会員．