情報処理学会論文誌 Vol.57 No.8 1816–1825 (Aug. 2016)

推薦論文

Named Data Networkingにおけるユーザへの影響を考慮したInterest Flooding Attack対策手法

梅田 沙也華[1,a)] 神本 崇史[1] 大畑 百合[1] 重野 寛[1]

受付日 2015年11月10日, 採録日 2016年5月17日

概要：コンテンツ指向型ネットワークである Named Data Networking（NDN）は，Interest Flooding Attack（IFA）と呼ばれる攻撃によってネットワーク上にパケットが溢れるという影響を受ける．IFA への対策として，リンクごとにパケットの流入を制限する Pushback がある．しかし，Pushback では，通常ユーザの Interest パケットも制限されるという問題が存在する．そこで，本論文では，通常ユーザへの影響を考慮した IFA 対策手法 ICRP を提案する．ICRP では末端ルータにおいて攻撃ユーザと攻撃に使用されるコンテンツのプレフィックスを特定する．この結果に基づいて Interest を制限することで，通常ユーザのデータ取得を維持しながらパケットの量を制御する．提案手法の評価はシミュレーションにより行い，通常ユーザのデータ取得が安定しているという結果から ICRP の有用性を示す．

キーワード：Named Data Networking，Interest Flooding Attack，DoS 攻撃，行動変化

Countermeasure against Interest Flooding Attack Considering Influence on Users in Named Data Networking

Sayaka Umeda[1,a)] Takashi Kamimoto[1] Yuri Ohata[1] Hiroshi Shigeno[1]

Received: November 10, 2015, Accepted: May 17, 2016

Abstract: In Named Data Networking (NDN), which is a content-oriented network, Interest Flooding Attack (IFA) overloads networks. Pushback mechanism is a countermeasure against IFA to control the flow of packets at each link. However, it also limits Interests from normal users. In this paper, we propose a countermeasure against IFA considering influence on normal users, called ICRP. In ICRP, each edge router detects attackers and content name prefixes requested by detected attackers. As it limits Interests based on such detection, it controls the flow of packets and normal users can acquire data. We evaluate ICRP through the computer simulation. The results show ICRP alleviates the influence on normal users and they can acquire data normally.

Keywords: Named Data Networking, Interest Flooding Attack, DoS attack, changing behavior

1. はじめに

近年，コンテンツを名前で指定するネットワークとして Named Data Networking（NDN）が研究されている [1]．NDN では，要求パケットである Interest と応答パケットである Data の 2 種類のパケットがコンテンツ名に基づいて転送される．コンテンツのある場所を指定する現在のインターネットに比べて，NDN では多くのセキュリティに関する問題が解決するといわれている [1]．しかし，NDN において Interest Flooding Attack（IFA）と呼ばれる攻撃が指摘されている [2], [3], [4]．IFA は，攻撃者のユーザが，実在しないコンテンツを要求する Interest パケットを大量に送信することで，ネットワークを混乱させる攻撃である．

そこで，NDN における IFA への対策手法の 1 つとして

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

本論文の内容は 2015 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO2015）シンポジウムにて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

Pushbackがある [4], [5]．Pushbackは，各ルータがリンクごとに到着したInterestに対するDataの返答率から算出されるInterest充足率に基づいてパケットの流入を制限する手法である．これにより，Dataの返答率が低くIFAの影響を強く受けているルータでInterest量を制限できる．

しかし，Pushbackでは通常ユーザのデータ取得に影響を与えるという問題が存在する．それは，攻撃者を特定しない制御であることと，IFAの影響を受けるたびに行う制御であることが原因である．まず，IFAの影響を受けるすべてのルータが全Interestを攻撃かどうかによらず制御する．そのため，通常ユーザのInterest量も制限されて，データを正常に取得できない可能性がある．また，既存研究ではIFAを続ける単純な攻撃モデルを想定しており，インターネットにおいてネットワークを乱すとされているような，複雑に行動を変化させる攻撃モデル [6] を考慮していない．そのため，行動変化が起こるたびにInterest制御を繰り返し，通常ユーザのデータ取得が不安定になる．

そこで，本論文では，通常ユーザへの影響を考慮したIFA対策手法ICRP（Interest Flow Control Method Based on User Reputation and Content Name Prefixes）[7] を提案する．ICRPは，攻撃者やコンテンツ名の先頭部分として攻撃に使用されるプレフィックスを特定してInterest制御を行うことで，通常ユーザのデータ取得を維持することを目的とする．まず，ユーザと直接接続された末端ルータが，ユーザの行動から算出される評価値によって攻撃者を検知する．そして，評価値が低いほどIFAを行う攻撃者である可能性が高いと考え，そのユーザからのInterestを制限する．さらに，過去の行動も考慮した評価値を用いることで，行動を変化させる攻撃にも対応する．また，末端ルータは，検知した攻撃者が要求するInterestの数から攻撃に利用されているプレフィックスを推測し，このプレフィックスを名前に含むコンテンツを要求するInterestを制限することで，行動変化によって一時的に検知から外れる攻撃者に対応する．

以下本論文では，2章において関連研究について述べ，3章でICRP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やIFA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

コンテンツ指向型のネットワークであるNDNでは，Interestパケットによってデータの要求が行われ，それに対してDataパケットによる応答が返ることで通信ができる．これらのパケットは，コンテンツ名に基づいて転送される．NDNで用いられるコンテンツ名は，‘/’を境界として複数の名前を組み合わせた階層構造をとる [1]．このコンテンツ名の先頭部分をプレフィックスと呼び，プレフィックスの最長一致でルーティングが行われる．このようなコンテンツ名によるパケット転送を実現するために，各ルータはForwarding Information Base（FIB）とPending Interest Table（PIT）という2種類の表を管理する．FIBはコンテンツサーバへの方向を保持し，PITはDataが返されていないInterestの情報を蓄積する．ルータがInterestを受け取ったとき，PITに情報を蓄積してからFIBに基づいて転送を続ける．そして，そのルータにDataが返ってきたとき，PITに含まれる情報からInterestが送られてきた経路と逆向きにDataパケットを転送し，さらにその情報をPITから削除する．また，各PITの情報にはLifetimeが決められており，この期間内に返答がないInterestの情報はPITから削除する．

2.2 NDNにおけるセキュリティ

NDNでは，現在のインターネットに比べて多くのセキュリティに関する問題を解決するといわれている [1]．たとえば，コンテンツに対する署名や暗号化によってコンテンツを保護することや，コンテンツ名の階層化によって上位の認証に対して下位のコンテンツを自動的に認証できるといった仕組みがある．しかし，NDNにおけるルータ特有の機能を利用した攻撃が新たに発生する．それがInterest Flooding Attack（IFA）であり，この攻撃によってPITが機能しなくなり，ネットワークが正常に使えなくなる [2], [4], [8]．次節においてIFAの詳細を説明する．

2.3 Interest Flooding Attack

IFAとは，攻撃者となるユーザが，実在しないコンテンツを要求するInterestパケットを大量に送信することで，ネットワークを混乱させる攻撃である．NDNでは，ルータにおいて受け取ったInterestの要求するコンテンツが実在するか判断できずにInterestを転送する．さらに，各ルータではDataが返るまでPITにInterestの情報を保持するためにリソースが消耗される．そのため，実在しないコンテンツを要求するInterestが多く流れた場合，中継ルータで応答となるDataが確認できないInterestが溢れる．さらに，ルータのPITが埋められる場合，置換方式に基づいて通常ユーザのInterest情報がPITから削除され，ネットワークが正常に機能しない．また，PITの置換が発生しない場合でも，ネットワークの負荷が増加することで，通常ユーザのInterestへの応答Dataの到着遅延がLifetimeを超え，PITから削除される．ここで，NDNでは中継ルータや目的地を指定できないため，特定のルータやホストを狙った攻撃はない．しかし，特定のプレフィックスを攻撃できるので，一部のルータに負荷が偏りIFAが発生する．

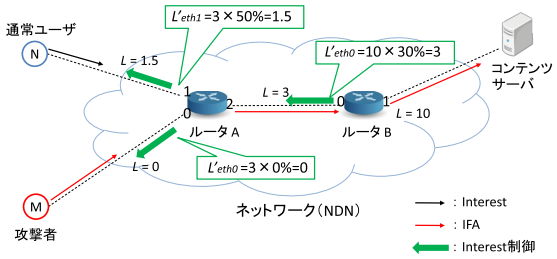

図 1 Pushback の動作例
Fig. 1 Example of Pushback mechanism.

2.4 IFA への対策手法

IFA は NDN の特徴に基づいた攻撃であるため，インターネットにおける DoS 攻撃の対策とは異なる独自のアプローチが必要である．そこで，IFA の影響を軽減する手法として Pushback がある [5]．Pushback は，各ルータがリンクごとの Interest 充足率に基づいてパケットの流入を制限するフロー制御手法である．Interest 充足率とは，到着した Interest に対する Data の返答率である．具体的には，Interest 充足率の値が小さいリンクに流入するパケットを転送しないことでパケット量を制限できる．つまり，Data が返らない Interest が多いリンクは，IFA の影響を受けていると考えて強くフローを制御する．以上により，IFA が影響を及ぼす経路の Interest 流入量を削減し，IFA により Interest が溢れることを防止する．

図 1 に Pushback の動作例を示す．上流ルータから受け取る制限値 L に各リンクの Interest 充足率を掛け合わせて新たな制限値を算出する．ここで，上流ルータにおいて制限値 L は正規化遅延から算出される．そのため，制限値 L と実際の遅延を比較してパケットの転送を決定することで，IFA により溢れる Interest を上流ルータから制限する．

2.5 評価値を用いたセキュリティ対策

分散型のネットワークにおける攻撃対策として，P2P やモバイルアドホックネットワークに見られるような，評価値を用いたセキュリティ対策手法が研究されている [9], [10]．その 1 つに，過去の行動から算出する評価値によってノード間で互いに攻撃者を検知する手法がある [11]．また，評価値によって必要とされていないコンテンツを見つけ，トラフィック制御を行う手法もある [12]．このように，分散型のネットワークを維持するため，ノードやコンテンツの動きを数値化した評価値による手法が使われている．

2.6 攻撃者の行動モデル

IFA として想定されている攻撃者の行動モデルは，単純に攻撃を続けるモデルのみである．一方で，インターネットでは攻撃者が通常の行動も混ぜることで攻撃者として検知されずに，ネットワークを混乱させるといわれている [6]．また，その他の分散型のネットワークにおいても，通常のノードが一時的に攻撃をするような行動変化モデルへの対応策が研究されている [13]．そのため，NDN における IFA の攻撃としてもより現実的で複雑なモデルを想定して対策を行うべきである [5]．

2.7 既存手法の問題点

IFA への対策である既存手法の Pushback では，通常ユーザのデータ取得に影響を与えるという問題がある．つまり，Pushback は IFA によって増加する Interest 量の制限を目的とするため，通常ユーザがデータ取得可能であるかを考慮していない．これは，Pushback が攻撃者を特定していない制御であることと，IFA の影響を受けるたびに行う制御であることが原因として考えられる．

まず，NDN では受信したパケットの送信元ユーザが分からないため，Pushback においてルータは攻撃者を特定できない．そこで，IFA の経路上にあたるすべてのルータにおいて全 Interest を攻撃かどうかによらず制御する．そのため，通常ユーザの Interest も要求するコンテンツに到達せずに制限され，正常なデータ取得ができなくなる．そこで，通常ユーザの Interest 送信数を制限せずに，IFA を行う攻撃者に限定した制御手法が必要となる．

また，既存の研究では IFA を続ける単純な攻撃モデルを想定しており，他のネットワークにおいて検知できずに混乱を招くとされているような，複雑に行動を変化させる攻撃モデルを考慮していない．具体的には，Pushback で制御に用いられる Interest 充足率は時間変化にともなって変動する値であるため，行動を変化をさせる攻撃者が発生した場合，行動変化が起こるたびに Interest 制御を繰り返す．そのため，Pushback の制御に合わせて通常ユーザのデータ取得も変動するような不安定な状態になる．そこで，行動変化を含む攻撃モデルを考慮し，通常ユーザのデータ取得の変動を抑制する手法が必要となる．

3. ICRP の提案

本章では，通常ユーザへの影響を考慮した IFA 対策手法 ICRP（Interest Flow Control Method Based on User Reputation and Content Name Prefixes）を提案する．

3.1 ICRP の概要

提案手法では，IFA に対して攻撃者の Interest に限定した制御を行うことで通常ユーザのデータ取得を維持することを目的とする．ICRP は，末端ルータでユーザの行動とコンテンツに対して評価を行うことで，攻撃者や攻撃に使用されるプレフィックスを特定して Interest 制御を行う．**図 2** に ICRP による Interest 制御の例を示す．

まず，ユーザと直接接続された末端ルータが，ユーザの評価値によって攻撃者を検知する．評価値とは，各ユーザの送信する Interest の中で実在するコンテンツを要求する

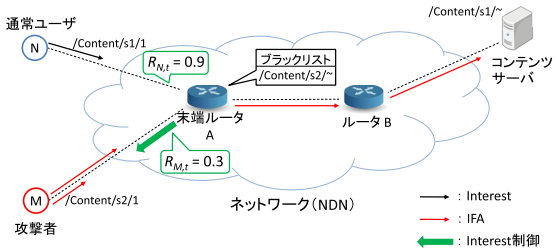

図 2 ICRP の動作例
Fig. 2 Example of ICRP.

Interest の割合を表した値であり，各末端ルータが接続するユーザに対して算出する．そのため，評価値が低いほど IFA を行う攻撃者である可能性が高いと考え，Interest を制限する．次に，末端ルータは検知した攻撃者が要求する Interest からコンテンツに対する評価を行う．ルータは，攻撃者が要求するプレフィックスを保持して集約することで，実在しないコンテンツ名のプレフィックスを推定し，ブラックリストに追加する．そして，ブラックリスト内のプレフィックスを名前に含むコンテンツを要求する Interest を制限する．

3.2 ICRP における想定環境

ICRP を利用する際に前提とするネットワーク環境と想定する IFA の攻撃の仕方について述べる．

3.2.1 ネットワーク環境

NDN では，パケットの情報として送信元のユーザを含まない．そのため，ルータは受信したパケットから，その送信元が攻撃者であるか判断できない．そこで，本研究ではユーザから直接パケットを受け取り，ユーザを特定できる末端ルータに着目する．そして，ICRP は末端ルータで攻撃者を検知して攻撃に利用される Interest を制御することで，IFA によって溢れる Interest を抑制する．

3.2.2 攻撃モデル

IFA に利用される実在しないコンテンツ名の決定方法は複数あるといわれている [3]．本研究では，ランダムなプレフィックスではなく，ある程度同様のプレフィックスを用いたうえで異なるコンテンツを要求する Interest を送信すると想定する．IFA による各ルータの PIT を図 3 に示す．まず，IFA は異なるコンテンツを大量に要求することで，ルータの PIT を埋めることができる．さらに，同じプレフィックス（e.g. /Content/t1/）を含む異なるコンテンツを要求したとき，Interest は同じルータを通過し，そのルータの PIT が多く埋まる．そこで，攻撃者は特定のプレフィックスを攻撃することで一部のルータにパケットを集中させ，IFA の影響を強めると想定する．また，攻撃者の行動モデルは，既存研究でも考慮されているようなつねに攻撃を続けるモデルと，時間経過にともない通常ユーザのような行動を混ぜた行動変化モデルを想定する．この想定

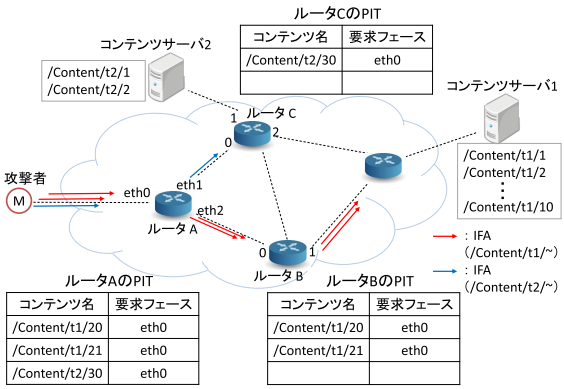

図 3 IFA とルータの PIT
Fig. 3 IFA and PIT of each router.

に基づき，提案手法 ICRP でのコンテンツに対する評価を行う．

3.3 ユーザの行動評価

Pushback は攻撃者を特定しない制御手法であったため，通常ユーザのデータ取得に影響を与えた．そこで，提案手法はユーザの行動から算出される評価値によって攻撃者を検知した後，Interest を制御する．ICRP はユーザを特定できる末端ルータのみが制御を行う．これにより，特に多くのパケットが通過する上流ルータでの制限から多くの通常ユーザに与えるデータ取得の影響を軽減させる．

時刻 t におけるユーザ i に対する評価値 $R_{i,t}$ を式 (1) によって定義する．

$$R_{i,t} = \alpha R_{i,t-1} + (1-\alpha)\frac{D_{i,t}}{I_{i,t}} \qquad (0 \le \alpha \le 1) \qquad (1)$$

ここで，$D_{i,t}$ は時刻 t におけるユーザ i への返信 Data パケット数，$I_{i,t}$ は時刻 t における上流ルータに転送したユーザ i からの Interest パケット数を表す．α は重み付け係数であり，定数とする．

つまり，ユーザの評価値 $R_{i,t}$ はユーザ i が送信する Interest のうち Data の返答があるコンテンツを要求する Interest の割合を表す．IFA の原因である実在しないコンテンツを要求する Interest を含め，Data の返答がないことでネットワークに負荷を与える Interest を送信するユーザの評価値が低下する．そのため，提案手法では評価値が低いユーザほど攻撃者である可能性が高いと考える．つまり，本論文では意図的であるかにかかわらず，Data が返らないことで IFA を引き起こす原因となる Interest を送信するユーザを攻撃者として判断する．さらに，時刻 t の評価値に $R_{i,t-1}$ の項を含めることで，過去の評価を利用した平均的な評価値を算出する．$R_{i,t-1}$ の項を含む評価値によって，過去のすべての評価が考慮されるため，各ルータは過去のすべての評価値を保持せずに，直前の評価値，直前の評価値算出以降の返信 Data パケット数と転送 Interest パケット数の 3 つの変数を保持しておくことで評価値を算出

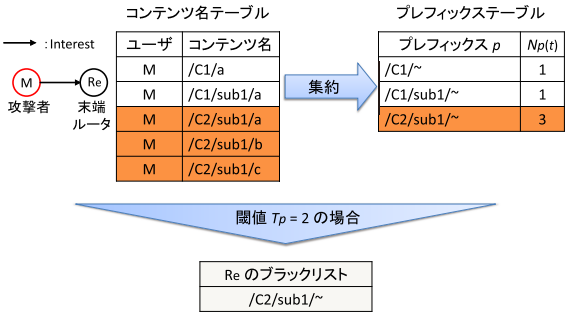

図 4 ブラックリスト作成例
Fig. 4 Example of making a blacklist.

できる．本論文では，行動を変化させる攻撃者は一時的に攻撃をやめて正常な Interest を送信している場合であっても，再びネットワークを乱す危険性があると見なす．そこで，過去の評価を含む評価値によって，行動変化に対して評価値の変動が緩やかになる仕組みとする．

3.4 コンテンツの評価

Pushback は，IFA によって Interest がネットワーク上に溢れるたびに Interest を制限するため，攻撃者が行動を変化した場合に通常ユーザのデータ取得が不安定になる．そこで，提案手法では 3.3 節で述べた制御に加えて，攻撃者の評価とは別に，攻撃に使用されるプレフィックスを特定した制御を行うことで，行動変化を行う攻撃者に対応する．

末端ルータは攻撃者として検知したユーザの Interest に含まれるコンテンツ名を管理し，プレフィックスごとの表としてまとめる．そして，プレフィックス p の要求回数 $N_p(t)$ を数える．この要求回数 $N_p(t)$ が大きい値となるプレフィックス p は，攻撃者が要求するコンテンツに頻繁に含まれるプレフィックスであり，攻撃に利用されている可能性が高いと考えてブラックリストに追加する．なお，ブラックリストに追加されたプレフィックスを名前に含むコンテンツは Interest の転送を制限されるため，このままではそのルータが時間経過にともなうコンテンツ取得の回復を知る機会はない．そのため，実際にはブラックリスト内のプレフィックスを一定期間で解除することや Interest を一定間隔で送信することで，各ルータはコンテンツ取得の回復を知ることが必要である．本論文では，特定の方式を指定しないこととする．

図 4 にブラックリスト作成の例を示す．ここで，コンテンツ名 “/C1/sub1/a” に対して最後のデータ名を除いた “/C1/sub1/” を集約のプレフィックスとする．末端ルータ R_e は攻撃者 M からの Interest が要求するコンテンツ名を表にする．これをプレフィックスごとに集約して要求回数 $N_p(t)$ を算出する．プレフィックス閾値 T_p が 2 の場合，ルータ R_e はプレフィックス “/C2/sub1/” を攻撃に使用されるプレフィックスと判断してブラックリストに加える．

Algorithm 1 Interest forwarding algorithm

```
1: Edge router A receives Interest I from user i.
2:
3: A calculates reputation R_{i,t} for user i in eq.1.
4: if R_{i,t} ≤ T then
5:    distinguish that the user i is an attacker.
6:    calculate drop rate P_{i,t} in eq.3.
7:    if P_{i,t} > uniform_rand(0,1) then
8:       drop Interest I.
9:    else
10:      N_p(t) ⟵ N_p(t) + 1
11:      if Prefix p of Interest I is stored in A's blacklist then
12:         drop Interest I.
13:      else if N_p(t) ≥ T_p then
14:         add prefix p in A's blacklist.
15:         drop Interest I.
16:      else
17:         forward Interest I.
18:      end if
19:   end if
20: else if Prefix p of Interest I is stored in A's blacklist then
21:   drop Interest I.
22: else
23:   forward Interest I.
24: end if
```

ここで，IFA によってブラックリストの作成にルータのリソースが多く使われることが考えられる．そのため，提案手法 ICRP ではユーザの行動評価に基づいて Interest の量を制限した後に残る IFA の影響に対してブラックリストを作成する．このような手順によってルータの負荷を軽減する．以上により，行動変化を行うユーザが一時的に攻撃者として検知されていない状況であっても，IFA に使用される実在しないコンテンツを特定できる．

3.5 Interest 制御

ICRP は，ユーザの行動とコンテンツに対する評価を用いて Interest を制御する．Algorithm 1 に提案手法を用いたときの Interest パケットの転送決定のアルゴリズムを示す．

Algorithm 1 の 8 行目までは，ユーザの行動評価に基づく制御の手順を表す．末端ルータはユーザから Interest を受信したとき，式 (1) に従って評価値を算出する．ここで算出される評価値 $R_{i,t}$ が以下の式 (2) の条件を満たすとき，ルータはユーザ i が攻撃者であると検知する．

$$R_{i,t} \leq T \qquad (0 \leq T \leq 1) \tag{2}$$

T は攻撃検知閾値であり，定数とする．

そして，末端ルータは攻撃者と検知したユーザ i からの Interest のみ破棄率 $P_{i,t}$ に基づいて破棄することで攻撃者の Interest を制限する．Algorithm 1 の 7 行目で，0 以上 1 以下の乱数と破棄数を比較して Interest の転送を決定する．ここで時刻 t にユーザ i に対して用いられる破棄率 $P_{i,t}$

は式 (3) で表す．

$$P_{i,t} = 1 - R_{i,t} \tag{3}$$

つまり，評価値の低いユーザに対して強く Interest の制限をかけて，攻撃検知閾値付近のユーザには弱い制限をかける．ここで，攻撃者の Interest をすべて破棄せずに，破棄率に基づいて一部のパケットのみを転送するのは，閾値の設定によって攻撃者として誤検知される通常ユーザの可能性を考慮したためである．

Algorithm 1 の 9 行目以降は，コンテンツ評価に基づく制御の手順を表す．末端ルータは，ユーザの行動評価に基づく制御によって破棄されなかった Interest に対して，要求するコンテンツのプレフィックスが自身のブラックリスト内に存在するか確認して，転送の判断を行う．さらに，攻撃者として検知されたユーザから Interest を受信した場合，更新した要求回数 $N_p(t)$ がプレフィックス閾値 T_p に対して以下の式 (4) の条件を満たすとき，プレフィックス p は攻撃に使用されていると判断し，自身の保持するブラックリストに追加する．

$$N_p(t) \geq T_p \tag{4}$$

これは，攻撃者が負荷を集中させてネットワークを乱すことを目的とするため，通常の Interest 以上に攻撃となる Interest を多く送信し，さらにある程度同様のプレフィックスを用いた異なるコンテンツを要求するという特徴を利用している．また，プレフィックス閾値 T_p は各ルータが検知した攻撃者ごとに決定する．これは，攻撃者によって攻撃に用いる Interest 量が異なることを考慮し，その攻撃者が相対的に多く要求することでネットワークへの負荷を与えるような，攻撃に使用されるプレフィックスを特定して制限することを目的とする．そのため，本論文では攻撃者はネットワークを乱すためにある程度 Interest を送信しており，T_p が極端に小さな値にならない状況に適応するといえる．このように作られたブラックリスト内にあるプレフィックスを名前に含むコンテンツを要求する Interest を上流ルータに転送せずに破棄する．以上により，攻撃の Interest を特定した制御を行うことで，IFA への対策による通常ユーザへの影響を軽減できる．

4. シミュレーション評価

提案手法 ICRP の有用性を示すため，IFA が発生する環境における通常ユーザのデータ取得に関して，シミュレーションにより評価を行った．

4.1 シミュレーションモデル

攻撃者のモデルから 2 種類のシナリオを用いてシミュレーションを行った．1 つは単純な攻撃モデルであり，シミュレーション時刻 10 秒から IFA を開始して最後まで攻撃を続けるモデルである．もう 1 つは行動変化を含む攻撃モデルであり，同様に IFA を開始した後，10 秒ごとに攻撃と通常の行動を交互に続けるモデルである．さらに，シミュレーションのトポロジとして二分木とより現実的で大規模な AT&T トポロジ [14] の 2 種類を用いた．各トポロジのパラメータを**表 1** に示す．

表 1 各トポロジのパラメータ
Table 1 Simulation parameters of each topology.

トポロジ	二分木	AT&T
全ユーザ数：N_u	16	296
末端ルータの数：N_e	8	109
その他のルータの数：N_b	8	109
リンクの帯域	最大 10 [Mbps]	1 - 3 [Mbps]
リンクの最大遅延	最大 10 [ms]	10 - 70 [ms]
通常ユーザの要求数	1000 [/sec]	100 [/sec]
攻撃者の要求数	10000 [/sec]	1000 [/sec]

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

ネットワークシミュレータ	ns-3.20
NDN モジュール	ndnSIM 1.0 [15]
シミュレーション時間	200 [sec]
データパケットサイズ	1100 [byte]
PIT の置換方式	LRU
Interest の生存時間	1.0 [sec]
評価値算出間隔	1.0 [sec]
重み付け係数：α	0.5
攻撃検知閾値：T	0.45
プレフィックス閾値：T_p	最大 $N_p(t)$ の 80%
攻撃者の割合	25%

また，シミュレーションのパラメータを**表 2** に示す．ここで，各ルータの PIT 容量は無限とした．このことは，本評価が PIT の容量制限でなく，強い IFA によって Lifetime の期間内に返らない通常ユーザの Interest の情報が PIT から削除される場合の評価であることを意味する．提案手法で用いるパラメータ α，T，T_p は予備実験により決定した．α は 1 に近い値であるほど過去の評価が反映されて評価値の変化が緩やかになる．一方で，0 に近い値になると行動変化に対して急激な変動を受ける．そこで，予備実験から通常ユーザと攻撃者への評価値の変化を確認して，通常ユーザは高く，攻撃者は低く評価値が収束するように α と攻撃検知閾値 T を決定した．また，プレフィックス閾値 T_p は，誤検知によって通常の Interest を制限しないような大きい値に設定した．予備実験では，提案手法におけるユーザの行動評価による Interest 制御のみを行った状態で，行動変化をともなう攻撃者が攻撃に利用する Interest がまだ制御されずに残っていることを確認した．そこで，攻撃に使用される実在しないコンテンツを要求する Interest 数を基準として通常の Interest 数は 3 割程度であった．このこ

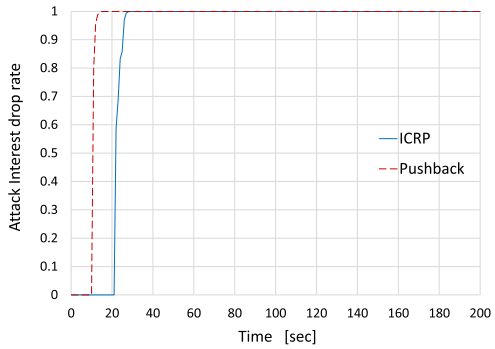

図 5 攻撃 Interest の破棄率
Fig. 5 Attack Interest drop rate.

とから，T_p は十分大きな値としてユーザと接続するルータで設定した．具体的には，この予備実験からユーザごとの最大要求回数 N_p の 80%をプレフィックス閾値とした．本来は過去の結果から各ルータが学習するという過程を想定するが，今回は予備実験による決定で簡略化した．

提案手法によって通常ユーザのデータ取得への影響が軽減できることを示すため，以下の 3 つの項目により提案手法の性能を評価する．比較対象は Pushback [5] である．

- 攻撃 Interest の破棄率
  攻撃者の Interest 送信数に対するルータで制限された Interest 破棄数の割合を表す．
- 通常ユーザの Interest 送信数と Data 取得数
  通常ユーザの Interest の制限とそれにともなうデータ取得の変化を確認する．
- 通常ユーザのデータ取得率
  通常ユーザの Interest 送信数に対するデータ取得数の割合を表す．ICRP と Pushback での比較を行う．

4.2 攻撃 Interest の制限

IFA の影響を軽減できることを調べるため，攻撃 Interest の破棄率を比較する．ここでは，各手法の基本動作の特徴を確認するため，二分木トポロジにおいて単純な攻撃モデルを用いたシミュレーション評価を行う．

図 5 に IFA 開始後の時間経過にともなう攻撃 Interest の破棄率の変化を示す．ここで，攻撃は時刻 10 秒から開始する．図より，提案手法は攻撃開始後 20 秒程度（時刻 30 秒）で攻撃 Interest を制限できることが確認できる．反応が遅れるのは，攻撃者や攻撃に使用されるプレフィックスを特定した後に Interest を制御する提案手法では，検知に時間がかかるためである．一方で，Pushback は攻撃開始 10 秒程度（時刻 20 秒）で攻撃 Interest を制限できることが確認できる．これは，Pushback が IFA による Interest の増加に対して制御を開始するためである．以上により，提案手法 ICRP は Pushback より制限が遅れるが，異なるアプローチによって IFA の影響を軽減できることが分かる．

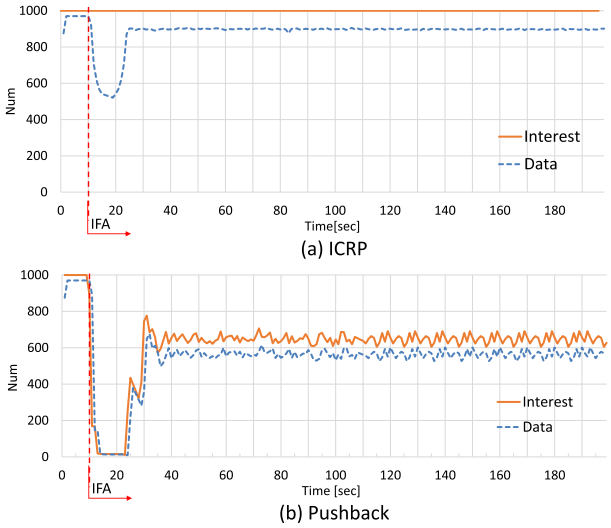

図 6 通常ユーザの Interest 送信数と Data 取得数
Fig. 6 Number of Interest and Data acquisitions.

4.3 単純な攻撃モデルによる通常ユーザへの影響

通常ユーザへの影響を調べるため，Interest 送信数と Data 取得数を比較する．ここでは，Pushback の通常ユーザに対する制限を確認するため，二分木トポロジにおいて単純な攻撃モデルを用いたシミュレーション評価を行う．

図 6 に時間経過にともなう通常ユーザの Interest 送信数と Data 取得数の変化示す．(a) は提案手法の結果，(b) は Pushback の結果を表す．図より，提案手法では IFA が開始した後でも Interest 送信数は制限されず，Data 取得数も攻撃開始直後に一時的に低下するが，15 秒程度で回復して 90%を維持することが確認できる．一方で，Pushback では IFA の開始とともに Interest 送信数が大きく制限され，一部回復した後でも 70%程度の送信数になることで Data 取得数も低下することが確認できる．どちらの手法でも，攻撃開始直後に比べて，一定時間経過後には IFA の影響を軽減したデータ取得の回復を実現できる．しかし，Pushback では攻撃者を特定していないため，通常ユーザの Interest 送信数にも制限が見られた．この問題に対して，提案手法では通常ユーザの Interest 送信数を制御せずに攻撃への対策を行うことで，攻撃者を特定した後には高いデータ取得に回復することが可能になった．以上により，提案手法 ICRP は通常ユーザの Interest 送信数を制限せずに，IFA を行う攻撃者に限定した制御手法といえる．

4.4 行動変化の攻撃モデルによる通常ユーザへの影響

行動変化をともなう IFA による通常ユーザへの影響を調べるため，二分木トポロジにおいて行動変化を含む攻撃モデルを用いた場合のデータ取得率を比較する．**図 7** に時間経過にともなう通常ユーザのデータ取得率の変化を示す．図より，提案手法では IFA 開始直後に一時的にデータ取得率が低下するが，攻撃者が行動変化した場合にも，

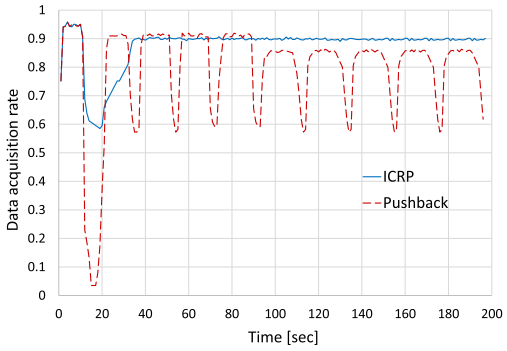

図 7 通常ユーザのデータ取得率
Fig. 7 Data acquisition rate of normal users.

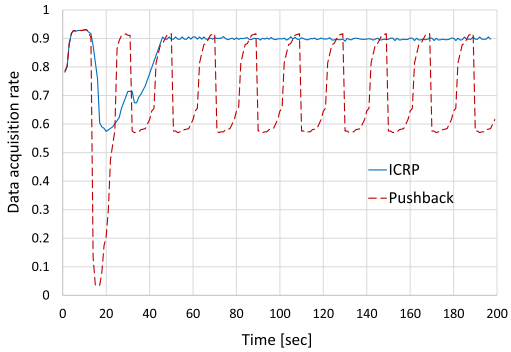

図 8 AT&T トポロジにおける通常ユーザのデータ取得率
Fig. 8 Data acquisition rate on AT&T topology.

表 3 平均データ取得率
Table 3 Average data acquisition rate.

対策なし	ユーザの行動評価に基づく制御のみ	提案手法
33.5%	76.2%	87.7%

90%のデータ取得率を維持することが確認できる．一方で，Pushback では行動変化のたびにデータ取得率が変動しており，不安定な状態が確認できる．提案手法は過去の行動も考慮してユーザに対する評価値を算出することで，行動変化の影響を低減させる．さらに行動変化によって一時的に攻撃者としての検知もれがあっても，攻撃に使用されるプレフィックスを含む Interest を制限できる．

また，**表 3** に図 7 と同じ条件時の平均データ取得率を示す．表より，提案手法の一部であるユーザの行動評価に基づく制御手法と，それにコンテンツの評価に基づく制御を加えた手法（提案手法）を比較する．この結果から，行動評価に基づく制御は IFA の影響を抑制できるが，提案手法と比較するとまだ IFA の影響を受けることが分かる．これは，行動変化による攻撃の Interest が残っているからである．以上より，提案手法 ICRP は 2 種類の制御によって，行動変化を含む攻撃モデルを考慮して通常ユーザのデータ取得の変動を抑制する手法といえる．

4.5 大規模なトポロジへの適応

より現実に近い大規模な環境で提案手法が有効であることを調べるため，AT& T トポロジで行動変化を含む攻撃モデルを用いた場合のデータ取得率を比較する．**図 8** に時間経過にともなう通常ユーザのデータ取得率の変化を示す．図より，提案手法は大規模なトポロジで IFA の影響を軽減させてデータ取得率を回復し，行動変化の影響として Pushback に見られるデータ取得の変動も軽減できる．さらに，提案手法は末端ルータのみが制御を行う手法であり，規模の拡大に対して制御を行うルータ数の増加は小さい．また，各ルータはローカルな処理だけを行うため，規模の拡大にともなうオーバヘッドの増加は発生しない．したがって，提案手法は大規模なトポロジでも適応できると考えられる．

また，図 7 と 8 を比較すると，大規模なトポロジでは両方の手法でデータ取得の回復が緩やかであることが分かる．これは，多くのルータからなる大きなネットワークでは IFA の影響も強く，制御までの時間がかかるためだと考えられる．提案手法は，このように IFA の影響を強く受けるような大規模なトポロジにも適応可能だといえる．

4.6 考察

シミュレーションの結果より，提案手法では通常の Interest に比べて多くの攻撃となる Interest を送信する攻撃者を検知し，通常ユーザの Interest 送信数を制限せずに IFA の対策ができることを確認した．評価値は，ユーザが意図した攻撃の Interest 量だけでなく，上流ルータの状況に依存して変動する．そのため，提案手法において攻撃者として検知されない程度に攻撃となる Interest の量を調整した攻撃は難しいと考えた．しかし，攻撃量を調整することにより，検知されない攻撃者が複数存在できた場合，末端ルータでの制限がなく，上流ルータでは大きな影響が発生する．このような状況で末端ルータに影響がでない場合，ICRP より上流ルータでも制限を行う Pushback が有効であると考えられる．したがって，Pushback は全ルータにおいて IFA により増加した Interest を制限する手法であるのに対して，提案手法 ICRP は末端ルータで受ける IFA の影響のみに注目することで，通常ユーザのデータ取得への影響も軽減できる手法であるといえる．

5. おわりに

本論文では，Named Data Netwoking における通常ユーザへの影響を考慮した IFA 対策手法 ICRP を提案した．

ICRP は，まずユーザと直接接続された末端ルータが，ユーザに対する評価値によって攻撃者を検知する．そして，攻撃者の Interest から攻撃に使用されるプレフィックスを特定する．ここから攻撃に関わる Interest に限定した制御を行う．提案手法をシミュレーションにより比較評価し，通常ユーザの Interest 送信数を制限しない制御手法で

あることを確認した．そして，単純な攻撃モデルと行動変化を含む攻撃モデルにおいて，通常ユーザの安定した高いデータ取得率を維持できた．また，より現実に近い大規模なトポロジでも，提案手法が適応できることを確認した．

以上より，提案手法はIFAに対してInterest制御を行いながらも，通常ユーザのデータ取得への影響を軽減でき，有用性があることを示した．

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] Choi, S., Kim, K., Kim, S. and Hee Roh, B.: Threat of DoS by Interest Flooding Attack in Content-Centric Networking, *International Conference on Information Networking* (*ICOIN*), pp.315–319 (2013).

[3] Tang, J., Zhang, Z., Liu, Y. and Zhang, H.: Identifying Interest Flooding in Named Data Networking, *Green Computing and Communications* (*GreenCom*), *IEEE and Internet of Things* (*iThings/CPSCom*), *IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pp.306–310 (2013).

[4] Compagno, A., Conti, M., Gasti, P. and Tsudik, G.: Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking, *38th Annual IEEE Conference on Local Computer Networks*, pp.630–638 (2013).

[5] Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E. and Zhang, L.: Interest flooding attack and countermeasures in Named Data Networking, *IFIP Networking Conference*, pp.1–9 (2013).

[6] Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B. and Cukier, M.: Characterizing Attackers and Attacks: An Empirical Study, *IEEE 17th Pacific Rim International Symposium on Dependable Computing* (*PRDC*), pp.174–183 (2011).

[7] Umeda, S., Takashi, K., Ohata, Y. and Shigeno, H.: Interest Flow Control Method Based on User Reputation and Content Name Prefixes in Named Data Networking, *The 2015 IEEE International Symposium on Recent Advances of Trust, Security and Privacy in Computing and Communications* (*RATSP*), pp.710–717 (2015).

[8] Gasti, P., Tsudik, G., Uzun, E. and Zhang, L.: DoS and DDoS in named-data networking, *22nd International Conference on Computer Communications and Networks* (*ICCCN*), pp.1–7 (2013).

[9] 武田苑子，梅田沙也華，重野　寛：ピアの参加離脱を考慮したインセンティブベースのピース拡散手法，情報処理学会論文誌，Vol.56, No.2, pp.421–429 (2015).

[10] Banerjee, A., Neogy, S. and Chowdhury, C.: Reputation based trust management system for MANET, *3rd International Conference on Emerging Applications of Information Technology* (*EAIT*), pp.376–381 (2012).

[11] 牛窪洋貴，武田苑子，重野　寛：モバイルアドホックネットワークにおけるトラストを利用した効率的セキュアルーティング，情報処理学会論文誌，Vol.55, No.2, pp.649–658 (2014).

[12] Yan, Z., Kantola, R., Shi, G. and Zhang, P.: Unwanted Content Control via Trust Management in Pervasive Social Networking, *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), pp.202–209 (2013).

[13] Umeda, S., Takeda, S. and Shigeno, H.: Trust Evaluation Method Adapted to Node Behavior for Secure Routing in Mobile Ad hoc Networks, *8th International Conference on Mobile Computing and Ubiquitous Networking* (*ICMU*), pp.143–148 (2015).

[14] Spring, N., Mahajan, R., Wetherall, D. and Anderson, T.: Measuring ISP topologies with Rocketfuel, *IEEE/ACM Trans. Networking*, Vol.12, No.1, pp.2–16 (2004).

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

推薦文

本提案は，Named Data Networking（NDN）におけるInterest Flooding Attack（IFA）攻撃に対する対策として，ユーザの行動を考慮したInterest制御手法ICRPを提案している．従来手法では，リンクごとにパケット流入を制限しているが，本提案は，攻撃者の行動の変化を考慮することにより，攻撃ユーザを高い精度で特定する一方，通常ユーザが攻撃ユーザであるとの誤検知を防いでいる．また，論文は簡潔かつ明瞭に書かれており，問題提起も含めて読者に有用な情報を与える論文である．

（DICOMO2015プログラム委員長　藤田　悟）

梅田 沙也華　（正会員）

2014年慶應義塾大学理工学部情報工学科卒業．2016年同大学大学院理工学研究科修士課程修了．

神本 崇史　（学生会員）

2015年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．

大畑 百合　（学生会員）

2015年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．

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，等を歴任．現在，情報処理学会マルチメディア通信と分散処理研究会主査，Vice Chair of IEEE ComSoc APB TAC．ネットワーク・プロトコル，ITS 等の研究に従事．著書『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．