Named Data Networkingにおける Interest記録数を考慮したInterest Flooding Attack対策

篠原 涼希[1] 神本 崇史[1] 大畑 百合[1] 重野 寛[1]

概要：コンテンツ名を使用して通信を行う Named Data Networking（NDN）において指摘されている攻撃の一つに，Interest Flooding Attack（IFA）がある．IFA の攻撃者は実在しないコンテンツを大量に要求し，ネットワークに負荷をかける．IFA の影響を抑制する既存手法では，通常ユーザのコンテンツ取得に影響を与えるという問題がある．そこで，本稿では，評価値と PIT エントリ数を用いて PIT に記録する Interest 情報を選別し攻撃 Interest を制限する手法である IFBRN を提案する．IFBRN では，ルータが Interest を受信している各インタフェースに対して評価値を算出する．次に，ルータは PIT を参照して，インタフェースごとの PIT エントリ数を集計する．これらの情報をもとに，ルータは攻撃 Interest が転送されているインタフェースを推定し，そのようなインタフェースに転送された Interest を制限する．シミュレーションを用いて提案手法を評価し，通常ユーザの Data 取得数が回復するという結果から IFBRN の有用性を示す．

Countermeasure against Interest Flooding Attack considering Number of Interest Records for Named Data Networking

RYOKI SHINOHARA[1] TAKASHI KAMIMOTO[1] YURI OHATA[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と言える．

NDN では，各ルータが所持している Pending Interest Table（PIT）がコンテンツ取得に大きな役割を果たしている．各ルータはコンテンツ要求パケットである Interest を受け取ると，Interest が要求しているコンテンツ名，Interest が転送されてきた方向といった情報を PIT に記録する．各ルータが応答パケットである Data を受け取ると，PIT に記録されている情報をもとに Data の転送を行い，記録されていた情報を削除する．

NDN に対する攻撃の一つとして Interest Flooding Attack（IFA） [2,3] が指摘されている．IFA とは，実在しないコンテンツを大量に要求する攻撃である．攻撃 Interest は Data が返らないため，攻撃者の Interest 情報で PIT が埋めつくされて負荷がかかる．その結果，通常ユーザの Interest 情報が PIT に残らず，通常ユーザの Data 取得が妨害される．そのため，IFA の影響を抑制する手法が必要である．IFA の対策手法として攻撃 Interest のフローを制限する Pushback [4] がある．しかし，Pushback は攻撃 Interest が転送されているリンクの Interest を一斉に制限するため，通常ユーザの Interest も制限する．

本稿では，評価値と PIT エントリ数を用いて PIT に記録する Interest 情報を選別し攻撃 Interest を制御する手法 IFBRN（Interest Flow Balancing Method Based on Reputation and the Number of Records on Named Data

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

Networking）を提案する．Pushback の問題点より，通常 Interest を制限することなく攻撃 Interest のみを完全に制限することは困難であると考えられる．そこで，攻撃 Interest を完全に制限しなくても，PIT に記録された攻撃 Interest のエントリ数と通常 Interest のエントリ数の差を小さくすれば IFA の影響を抑制できるという考えに基づき IFA の対策を行う．IFBRN は，IFA によって攻撃者の Interest 情報が大量に PIT に記録されて負荷となることに注目し，PIT への記録を制限することによって攻撃 Interest を制御する．ルータはインタフェースに対する評価値と PIT エントリ数をもとにインタフェースの状況を把握し，そのインタフェースに攻撃 Interest が転送されているか判断する．攻撃 Interest が転送されていると判断した場合，転送された Interest の情報を PIT に記録しない．したがって，通常ユーザの Interest を制限することなく，負荷の原因となる攻撃 Interest の情報のみを PIT に記録しないことが可能である．これにより，攻撃者の Interest 情報が PIT に大量に記録されて負荷となる問題への対策とする．

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 IFBRN 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

コンテンツ名を用いて通信を行う NDN では，Interest と Data と呼ばれる 2 種類のパケットが使用される．これら 2 種類のパケットはコンテンツ名を情報として含む．

パケット転送を行うために，NDN における各ルータは Content Store（CS），Forwarding Information Base（FIB），Pending Interest Table（PIT）という 3 種類のデータ構造を持つ．CS は Data がルータに転送された際に Data の複製を保存するために使用される．FIB は Interest をコンテンツサーバに向かって転送する際に転送の方向を決定するために使用される．PIT は Interest が転送された際にその Interest が転送されてきた方向，及びその Interest が要求しているコンテンツ名をエントリとして記録するための表である．Interest が流入したインタフェースを記録することにより，Interest が転送されてきた方向が保存される．PIT のエントリ数が上限に達したときの代表的な置換方式として，エントリ数が上限に達している場合は置換を行わず新たな記録を行わない Persistent と参照されていない時間が最も長いエントリを置換する LRU がある．また，PIT エントリには Lifetime があり，Interest に対応する Data が Lifetime 以上経過しても返らない場合はタイムアウトとみなされて PIT エントリが削除される．

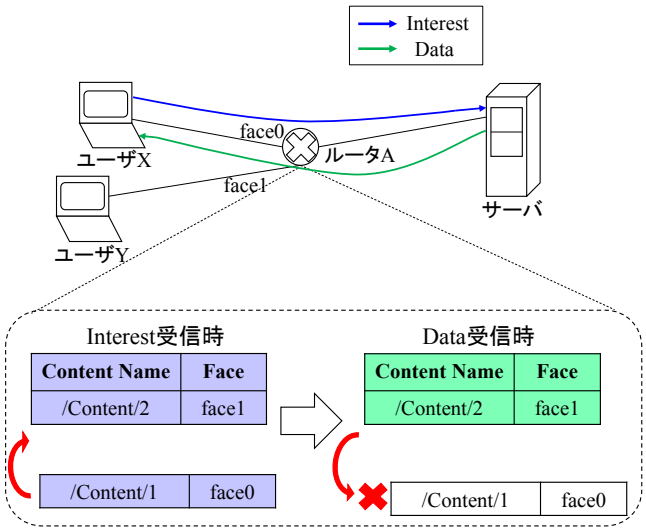


図 1　NDN における PIT の機能

図 1 はユーザが Data を取得する際の PIT の働きについて示したものである．各ルータに Interest が転送されると，ルータはその Interest の情報を PIT に記録して転送を行う．そして Data が転送されると，ルータは PIT を参照し，その情報をもとに対応する Interest が転送されてきた方向に Data を転送する．Data を転送すると，PIT は対応する Interest の情報を削除する．このように，PIT は NDN における Data の取得に重要な役割を担っている．

2.2 Interest Flooding Attack

各 Interest はコンテンツ名を所持しており，各ルータはコンテンツ名を用いて Interest の転送方向を決定する．したがって，各ユーザは Interest を送信する際に特定の宛先を指定することが出来ないため，NDN において特定のルータやサーバを対象とした攻撃を行うことは困難である [1]．

しかしながら，ネットワーク内の一定の場所に集中して負荷をかける Interest Flooding Attack（IFA） [2,5] と呼ばれる攻撃が NDN において存在する．NDN の各ルータは要求されたコンテンツが実在するか確かめることが出来ない．FIB に転送方向の情報が記録されていない Interest がルータに転送されると，ルータは Interest が要求するコンテンツ名と FIB の情報が最長一致するものを探し，その情報をもとに転送を行う．IFA は NDN におけるこれらの特徴を悪用する．IFA における攻撃者は実在しないコンテンツを要求する Interest を短期間で大量に送信する．大量の Interest がサーバに集中するとサーバに負荷がかかる．また，各ルータの PIT が攻撃 Interest の情報によって埋め尽くされるため，通常ユーザの Interest 情報の記録が妨害される．したがって，IFA によって特定のサーバに負荷が集中し，また，通常ユーザの Data 取得も妨害される．

2.3 IFA への対策手法

IFA は現在のネットワークとパケットの転送方法が異なる NDN の特徴を悪用した攻撃であるため，DoS 攻撃への既存の対策とは異なるアプローチを用いて対策を行う必要がある [6]．IFA の影響を抑制するための手法として Pushback がある [4]．Pushback は Interest の充足率に基づいて Interest の流入量を制限するフロー制御手法である．ここで，Interest 充足率とは各ルータにおいてリンクごとに到着した Interest に対する Data の返答率である．実在しないコンテンツを要求する攻撃 Interest には対応する Data が返らないため，攻撃 Interest が転送されているリンクの Interest 充足率は低くなる．各ルータは上流ルータの Interest 充足率と各ルータの Interest 充足率の積に基づいてフローを制御する．以上により，IFA が影響を及ぼす経路の Interest 流入量を削減することで，攻撃 Interest があふれることを防止する．

2.4 評価値を用いたセキュリティ対策

ネットワークに負荷をかける攻撃者への対策手法として，ユーザに対する評価値を算出して攻撃者を検知する手法が挙げられる．P2P ネットワークやモバイルアドホックネットワークなどの分散型ネットワークにおいて，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 [7–9]．その中の一つに，ノードの過去の行動を示す評価値を算出して攻撃者を検知する手法がある [10]．NDN においても，ルータにユーザが接続しているか判別できる環境において，評価値を用いることでユーザを評価し IFA の攻撃者を検知する ICRP という手法がある [11]．評価値を用いて攻撃者を検知することにより，通常ユーザに影響を及ぼさずに攻撃の影響を抑制することが可能となる．

2.5 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 Data 取得数が低下するという問題が存在する．Pushback は各ルータがリンクに対して Interest 充足率を用いることにより，IFA の影響を受けている経路を判別する手法である．Pushback はこのような IFA の影響を受けているリンク上の全ての Interest を制限するため，攻撃 Interest と同様に通常ユーザが出した Interest も制限されるという問題がある．Pushback によって制限された通常ユーザの Interest はコンテンツサーバまで到達せずに Data 取得ができなくなる．このように，Pushback は IFA によって増加するパケットの流入量を制限することを目的としているため，その結果通常ユーザの Data 取得が出来ない場合がある．したがって，攻撃 Interest のみを制限し，通常ユーザの Data 取得に影響を及ぼさない手法が必要となる．また，ICRP はルータにユーザが接続しているか判別できるという想定のうえで攻撃者を検知して攻撃 Interest のみを制限する手法であるが，提案手法ではこの想定がなくても攻撃 Interest のみを制限できることを目指す．

3. IFBRN の提案

本章では，評価値と PIT エントリ数を用いて PIT に記録する Interest 情報を選別し攻撃 Interest を制御する手法 IFBRN（Interest Flow Balancing Method Based on Reputation and the Number of Records on Named Data Networking）を提案する．

3.1 IFBRN の概要

今回提案する手法である IFBRN では PIT に記録された攻撃 Interest のエントリ数を減らすことにより，通常ユーザの Data 取得数を回復させることを目指す．Pushback は攻撃 Interest の転送を制限することにより IFA の影響を抑制する手法であった．一方で，IFBRN は攻撃 Interest を評価値と PIT エントリ数を用いて判別し PIT への記録を制限することにより IFA の影響を抑制する手法である．また，IFBRN はネットワーク上の全ルータがユーザではなくインタフェースに対して評価値を算出するため，ICRP で要求される各ルータはユーザが接続しているか判別できるという想定が不必要である．

IFBRN は大きく 2 つの段階を通して通常ユーザの Data 受信数を回復させる．

- インタフェースの状況把握
- PIT に記録する Interest 情報の選別

まず，各ルータはインタフェースの状況を把握する．ルータはインタフェースの状況をもとに攻撃 Interest が転送されているか判断する．インタフェースに攻撃 Interest が転送されていると判断した場合，ルータは PIT に Interest の情報を記録せず，Interest の転送を行わない．以下で提案手法の詳細について説明する．

3.2 インタフェースの状況把握

攻撃 Interest が転送されているインタフェースを検知するため，ルータはインタフェースごとに評価値を算出し，また，PIT のエントリ数から各インタフェースの PIT を占める量を保持することによりインタフェースの状況を把握する．NDN ルータはインタフェースを通して Interest を受け取る．攻撃 Interest を受け取っているインタフェースは転送した Interest に対する受信した Data 数の割合が低くなる．Interest が転送されるたびに，ルータはインタフェースに対する評価値を更新する．評価値を算出する式は ICRP [11] を参考にした．評価値を式 (1) で定義する．

$$R_{ij}(t) = \alpha R_{ij}(t-1) + (1-\alpha)\frac{D_{ij}(t)}{I_{ij}(t)}, \tag{1}$$

式 (1) は時刻 t においてノード i がインタフェース j に対して過去の行動を考慮したうえで算出する評価値を表す．

$D_{ij}(t)$ は時刻 t においてルータ i からインタフェース j へ転送された Data パケット数を表し，$I_{ij}(t)$ は時刻 t においてルータ i のインタフェース j に転送された Interest パケット数を表す．つまり $\frac{D_{ij}(t)}{I_{ij}(t)}$ は現在インタフェース j に転送されている Interest 数に対する返信 Data の割合を表している．評価値は過去の行動を含めて算出される．$R_{ij}(t-1)$ は時刻 $t-1$ における評価値であり，インタフェース j の過去の Interest 転送に対するルータ i の評価を表している．α は重み付け係数であり，0 から 1 の範囲の固定値である．

評価値に加えて，ルータは PIT を参照して各インタフェースごとの PIT エントリ数を保持する．IFA の攻撃者は大量の攻撃 Interest を送信する．攻撃 Interest には対応する Data が返らないため，攻撃 Interest の情報は PIT から削除されず長い間記録される．時刻 t において，ルータ i の PIT に記録されているインタフェース j に転送された Interest のエントリ数を $S_{ij}(t)$ とする．以上のように，インタフェースに Interest が転送されるごとにルータはインタフェースの状況を把握する．

3.3 PIT に記録する Interest 情報の選別

Interest が転送されると，ルータは評価値と PIT のエントリ数をもとに Interest の情報を記録して Interest の転送を行うかを決定する．以下の 3 つの条件を満たすとき，ルータは Interest の情報を PIT に記録せず，Interest の転送も行わない．

- インタフェースの評価値が低い
- 他のインタフェースと比較して評価値が低い
- 他のインタフェースと比較して PIT エントリ数が多い

攻撃 Interest が転送されているとき，インタフェースの評価値は低くなる．そこで，評価値を攻撃検知閾値 T と比較することにより攻撃 Interest が転送されているインタフェースの検知を目指す．ルータ i のインタフェース j に Interest が転送されてきたとき，ルータ i はインタフェース j に対する評価値 $R_{ij}(t)$ を更新する．$R_{ij}(t)$ が以下の式 (2) を満たすとき，インタフェース j に攻撃 Interest が転送されている可能性が高い．

$$R_{ij}(t) < T, \tag{2}$$

提案手法は攻撃 Interest が転送されているインタフェースと通常 Interest が転送されているインタフェースの PIT エントリ数の差を小さくすることにより IFA の影響を抑制する．そこで，インタフェースの評価値を比較することにより攻撃 Interest が転送されているインタフェースの検知を目指す．ルータ i はルータ i に接続している別のインタフェース k に対する評価値 $R_{ik}(t)$ を調べる．ルータ i はインタフェース j とインタフェース k の評価値を比較する．$R_{ij}(t)$ と $R_{ik}(t)$ が以下の式 (3) を満たすとき，インタフェース j に攻撃 Interest が転送されている可能性が高い．

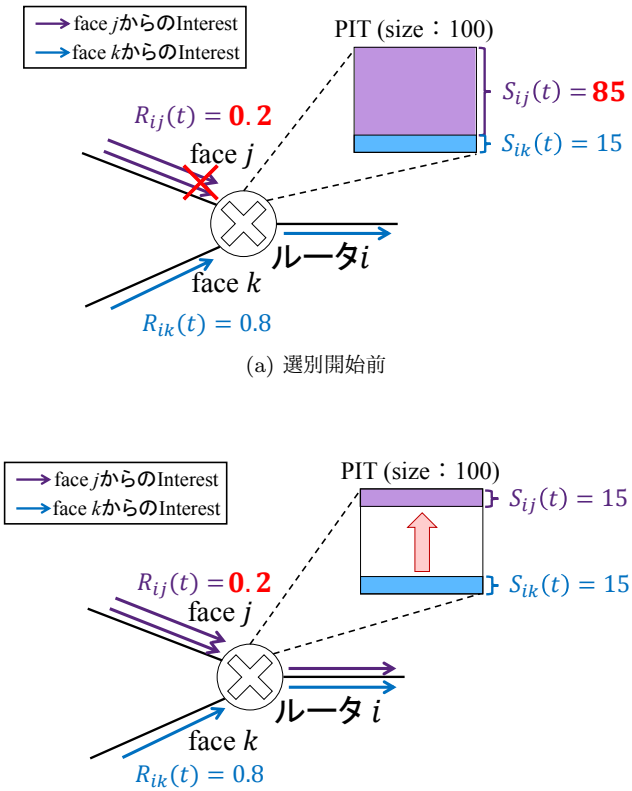


図 2 PIT に記録する Interest 情報の選別

$$R_{ij}(t) < R_{ik}(t) \times \beta, \tag{3}$$

ここで，比較係数 β は 0 から 1 の間の定数であり，$R_{ik}(t) \times \beta$ の値は $R_{ik}(t)$ よりも小さくなる．通常ユーザが送信した Interest であってもパケットロスによって Data が返らない場合があることを考慮し，β を用いることによって評価の基準を緩和する．

攻撃者は大量の攻撃 Interest を送信し，攻撃 Interest には Data が返らないため，PIT は攻撃 Interest の情報を長い間記録することになる．したがって，あるインタフェースからの PIT エントリ数が多い場合，そのようなインタフェースには攻撃 Interest が転送されていると考えられる．ルータ i は PIT を参照してインタフェース j とインタフェース k からの PIT エントリ数を $S_{ij}(t)$ と $S_{ik}(t)$ として保持する．$S_{ij}(t)$ と $S_{ik}(t)$ が以下の式 (4) を満たすとき，インタフェース j に攻撃 Interest が転送されている可能性が高い．

$$S_{ij}(t) > S_{ik}(t). \tag{4}$$

以上の情報をもとに，ルータは Interest が転送されたインタフェースを評価する．そして式 (2)(3)(4) を同時に満たすとき，ルータは Interest が転送されたインタフェースを攻撃 Interest が転送されているインタフェースと判断する．ルータはこのインタフェースから転送された Interest

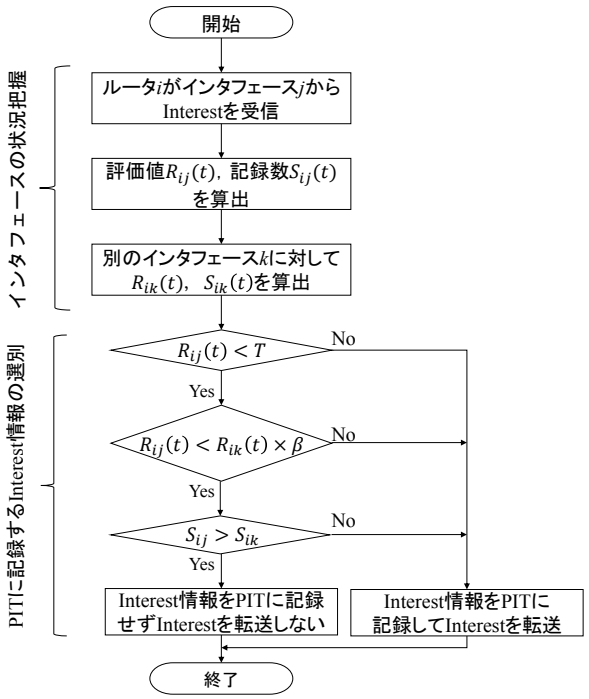


図 3　IFBRN における攻撃 Interest 制限の手順

の情報を PIT に記録せず，Interest の転送も行わない．

図 2 に PIT に記録する Interest 情報の選別を行う例を示している．図 2(a) において，ルータ i は face j と face k に対しそれぞれ 0.2，0.8 という評価値を算出している．また，ルータ i は face j と face k からの PIT エントリ数としてそれぞれ 85，15 という値を保持している．この場合，評価値 $R_{ij}(t)$ は $R_{ik}(t)$ よりも低く，PIT エントリ数 $S_{ij}(t)$ は $S_{ik}(t)$ よりも多い．もし評価値 $R_{ij}(t)$ が閾値 T よりも低い場合，ルータ i は face j に攻撃 Interest が転送されていると判断し，face j に転送された Interest 情報を PIT に記録せず Interest の転送も行わない．PIT に新たなエントリが追加されない場合，PIT エントリ数は Data の返信やタイムアウトによって減少する．したがって，Interest 情報の記録の制限を行うことにより，インタフェースごとの PIT エントリ数の差は図 2(b) で示すように IFA の対策を行う前より小さくなる．攻撃 Interest に関する PIT のエントリ数と通常 Interest に関する PIT のエントリ数の差が小さくなれば，IFA の影響は抑制され通常ユーザの Data 取得数は回復すると考えられる．PIT エントリ数が減少して式 (4) を満たさなくなった場合，IFA の影響が抑制されたと考え，ルータは Interest 情報の記録を再開する．

図 3 に提案手法のフローチャートを示す．提案手法 IFBRN はネットワーク内の全てのルータが図 3 のフローチャートに従って PIT に記録する Interest 情報の選別を行うことにより，攻撃 Interest を制限する．

4.　シミュレーション評価

提案手法 IFBRN の有用性を示すため，IFA が発生する環境を再現したシミュレーションにより評価を行った．

表 1　シミュレーション条件

ネットワークシミュレータ	ns-3.21
NDN シミュレータ	ndnSIM 1.0
シミュレーション時間	200 sec
トポロジ	二分木トポロジ
各リンクの帯域	10 [Mbps]
各リンクの最大遅延	10 [msec]
通常ユーザの要求数	1000 [/sec]
攻撃者の要求数	10000 [/sec]
攻撃開始時刻	10 [s]
各ルータの PIT サイズ	275
PIT の置換方式	LRU
Interest の Lifetime	1 [s]
攻撃検知閾値：T	0.45
重み付け係数：α	0.5
比較係数：β	0.8

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 [12] を用いた．NDN のシミュレーションを行うため，ndnSIM [13] によってネットワーク層に NDN の機能を実装した．表 1 に今回のシミュレーションで用いたパラメータを示す．シミュレーションの測定時間は 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．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．

各 NDN ルータの PIT サイズを 275，Interest の Lifetime を 1 秒とした．PIT の置換方式は，参照されていない時間が最も長いエントリを削除する LRU を選択した．攻撃者が送信する Interest の量は，通常ユーザが送信する Interest の量よりも多く設定した．評価値の算出および攻撃者の検知で用いられる重み付け係数 α と攻撃検知閾値 T は ICRP [11] で使用されている値を参考にした．IFBRN では攻撃が開始された後の 10 秒から 20 秒までの間は Interest の制限を行わず，評価値の算出のみを行う．図 4 に二分木トポロジの概形を示す．二分木トポロジの最上流にサーバを置き，最下流にユーザを置いた．

通常ユーザはサーバに蓄積されているコンテンツを Zipf の法則に従って要求する [14]．つまり，人気の高いコンテンツを高確率で要求し，人気の低いコンテンツを低確率で要求する．一方，攻撃者はサーバに蓄積されていないコンテンツを要求する．攻撃者はランダムなコンテンツ名を指定するので，毎回異なるコンテンツが要求される．

4.2　評価項目

今回のシミュレーションでは以下の 2 つの項目により提案手法の性能を評価する．比較対象は既存手法の Push-back [4] である．

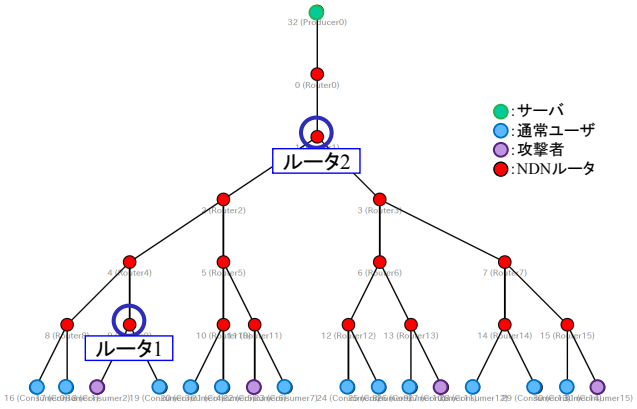


図 4　二分木トポロジ

- 通常ユーザの Interest 送信数と Data 受信数
  ネットワーク内の全ての通常ユーザが送信した Interest 数と受信した Data 数の合計を評価する．
- PIT に記録されている Interest のエントリ数
  図 4 に示される末端ルータと上流ルータを選択し，この 2 つのルータの PIT に記録されている通常ユーザと攻撃者の Interest のエントリ数を評価する．

一つ目の評価項目により，提案手法が IFA の通常ユーザへの影響を抑制できていることを示す．通常ユーザが IFA の影響を受けると，通常 Interest 情報の記録が妨害されて Data 受信数が低下する．そこで，通常ユーザの Interest 送信数と Data 受信数の時間変化の評価を行う．

二つ目の評価項目により，提案手法によって攻撃 Interest と通常 Interest のエントリ数の差が小さくなっていることを示す．提案手法は，攻撃 Interest の情報を PIT に記録せず Interest の転送を行わないことによって IFA の影響を抑制する．そこで，PIT に記録されている通常ユーザと攻撃者の Interest のエントリ数の時間変化の評価を行う．

図 4 におけるルータ 1 は通常ユーザと攻撃者の両方に接続している末端ルータであり，攻撃 Interest が多く流れ込むルータである．したがって，ルータ 1 は末端における攻撃の影響を調べることができるルータであると考えられる．また，ルータ 2 は上流ルータであり，全ての通常ユーザや攻撃者が送信した Interest が流れ込むルータである．したがって，ルータ 2 はネットワーク全体における攻撃の影響を調べることができるルータであると考えられる．

4.3　通常ユーザの Interest 送信数と Data 受信数

通常ユーザの Interest 送信数と Data 受信数の結果について確認する．図 5 に Pushback の結果を示す．表 1 より，通常ユーザが 1 秒間に送信する Interest 数は合計で 1000 パケットである．このグラフにおいて，送信 Interest 数は通常ユーザが末端ルータに送信できたパケット数を指

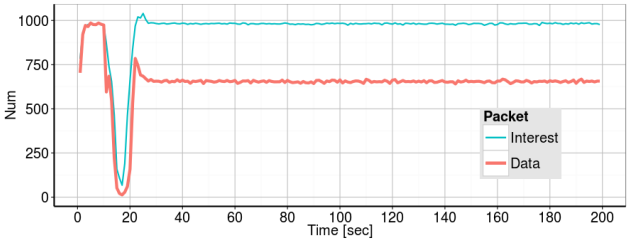


図 5　Pushback における送信 Interest 数と受信 Data 数

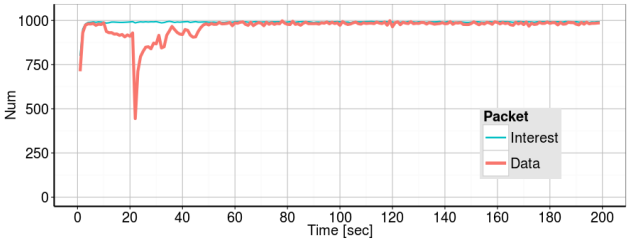
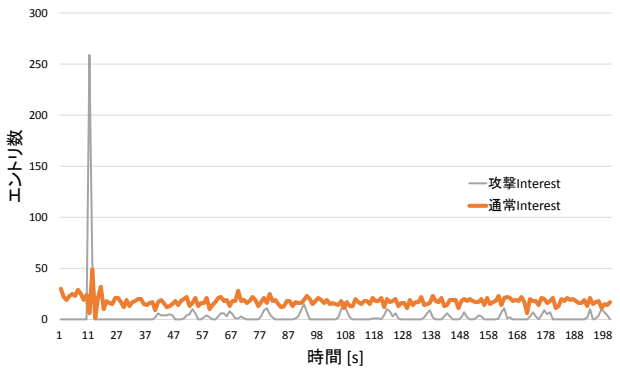


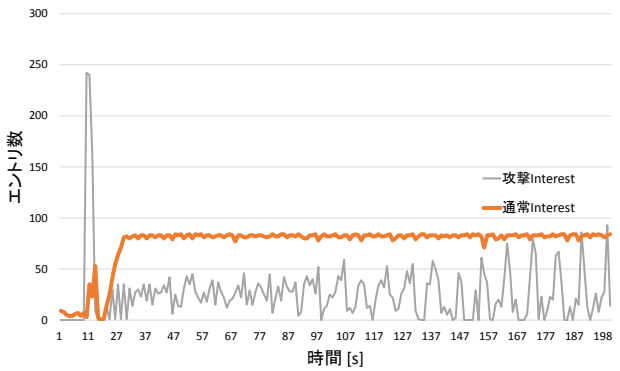
図 6　IFBRN における送信 Interest 数と受信 Data 数

しており，ルータからルータへ転送する際に制限された Interest については考慮していない．このグラフより，送信 Interest 数は IFA が開始される 10 秒で大きく減少しており，その後 15 秒ほどで 1000 パケットに回復することがわかる．しかしながら，送信 Interest 数が回復した後も受信 Data 数は 650 パケット程度にとどまり，送信 Interest 数に比べて受信 Data 数が少ないことがわかる．シミュレーション評価より，IFA の影響が抑制されて送信 Interest 数が回復した後も Data 受信率が回復しないことがわかる．通常 Interest が上流に転送されると，そのパケットは攻撃 Interest も転送されているリンクを通ることになる．そのとき，リンクの充足率が落ちて Interest が制限されるため，通常 Interest も上流ルータにおいて制限されていると考えられる．以上より，攻撃 Interest とともに通常 Interest も制限されるという Pushback の問題点が確認できた．

図 6 に IFBRN の結果を示す．まず，Interest 送信数を見ると，IFA が開始された後も一定の値を保っていることがわかる．さらに，Data 受信数を見ると，制限が開始される 20 秒以降は Data 受信数が回復し 50 秒ごろには IFA が開始される前とほぼ同じ状態まで回復していることがわかる．IFA が開始されると，攻撃者に接続しているインタフェースの評価値は通常ユーザに接続しているインタフェースの評価値に比べて低くなる．したがって，IFBRN による制限が開始されると，末端ルータは攻撃 Interest のみを制限するため，通常ユーザの Interest 送信数は減少せず Data 受信数は回復する．一方で，Data 受信数は IFA が開始される 10 秒以降減少しており，制限が開始される 20 秒直後にさらに大きく減少していることがわかる．IFBRN は 10 秒から 20 秒の間は制限を行わず評価値の算出のみを行うため，この区間は IFA によって Data 受信数が低下する．また，通常ユーザの Data 受信数が低下することにより，

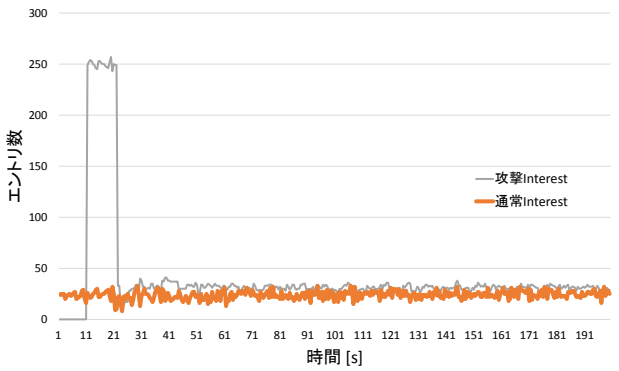


(a) ルータ 1

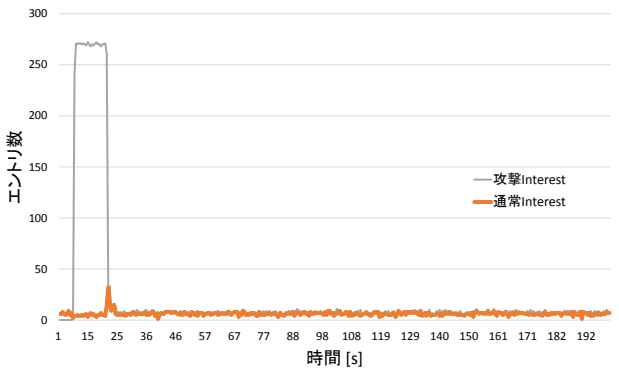


(b) ルータ 2

図 7 Pushback における PIT エントリ数



(a) ルータ 1



(b) ルータ 2

図 8 IFBRN における PIT エントリ数

攻撃 Interest を受信しているインタフェースだけでなく通常 Interest を受信しているインタフェースの評価値も低下する．したがって，IFBRN が制限を開始した直後は通常 Interest が多く転送されているインタフェースであってもルータが PIT に情報を記録せず，その結果 Data 受信数が大きく低下したと考えられる．しかしながら，Data 受信数は時間の経過に伴って回復しており，長期間ネットワークを動かす際は Data 受信数が一時的に少なくなることは問題にならないと考えられる．以上より，提案手法は通常ユーザの Interest を制限することなく攻撃を抑制できることが確認できた．

4.4 PIT に記録されている Interest のエントリ数

PIT に記録されている通常ユーザと攻撃者の Interest のエントリ数を確認する．図 7 はそれぞれ Pushback においてルータ 1，ルータ 2 の PIT に記録されている Interest のエントリ数の時間変化を示している．図 7(b) より，ルータ 2 の PIT は攻撃 Interest のエントリ数が少なく，ネットワーク全体で見ると攻撃の影響を抑制できていると言える．しかしながら，図 7(a) より，ルータ 1 の PIT には通常 Interest の情報が多く残っていることがわかる．PIT に残っているのは，まだ対応する Data が返されていない Interest の情報である．したがって，PIT に通常 Interest の情報が多く残っているということは対応する Data が返っておらず，通常ユーザの Data 受信数が少ないということを意味している．ルータ 1 の PIT に多く残っている情報は上流で制限された通常 Interest の情報であると考えられる．また，攻撃 Interest 情報の記録数に注目すると，記録数が時間によって大きく変動していることがわかる．このことより，末端ルータの攻撃 Interest 制御はその強さが時間によって変化する不安定なものであると言える．

図 8 はそれぞれ IFBRN においてルータ 1，ルータ 2 の PIT に記録されている Interest のエントリ数の時間変化を示している．図 8(a) より，制限を開始した後は PIT に記録されている通常 Interest と攻撃 Interest のエントリ数がほぼ同数になっている．IFBRN は，PIT に記録する情報を選別することによって通常 Interest と攻撃 Interest のエントリ数の差を小さくすることを目標としている．そのため，末端ルータにおいて提案手法の目標は達成されていると言える．また，図 8(b) より，攻撃 Interest 情報の記録数が通常 Interest 情報の記録数よりも多くなっていることがわかる．ルータ 2 には下流ルータの CS にヒットしなかった全ての Interest が流れ込む．そのため，ルータ 1 に比べて PIT に記録されている Interest のエントリ数は攻撃 Interest，通常 Interest ともに多くなっている．しかしながら，攻撃 Interest が CS にヒットすることはないた

め，CS にヒットして Data が返される通常 Interest に比べるとルータ 2 に流れ込む攻撃 Interest の数は多くなる．したがって，ルータ 2 の PIT には攻撃 Interest 情報が通常 Interest 情報よりも多く残っていると考えられる．また，図 8 のグラフの攻撃 Interest のエントリ数に注目すると，両方とも記録数の変動は少ない．したがって，IFBRN の攻撃 Interest 制御は Pushback に比べて安定したものであると言える．IFBRN と Pushback のルータ 2 における結果を比べると，IFBRN における攻撃 Interest のエントリ数は Pushback よりも多いことがわかる．しかし，提案手法によって攻撃 Interest のエントリ数と通常 Interest のエントリ数の差は小さくなっており，PIT に残っている Interest 情報の合計数が PIT サイズよりも小さいことを考えると問題はないと言える．以上のことから，提案手法は PIT に記録する Interest 情報を選別することで，攻撃 Interest と通常 Interest のエントリ数の差を小さくし IFA の影響を抑制できていることを確認した．

5. おわりに

本稿では，IFA による攻撃 Interest を制御する手法 IFBRN を提案した．IFBRN は，まず各ルータが接続しているインタフェースの状況を把握する．インタフェースの状況をもとに，ルータは攻撃 Interest が転送されているインタフェースを推定し，そのようなインタフェースに転送された Interest の情報を PIT に記録せず Interest の転送を行わない．これにより，PIT における攻撃 Interest の情報記録数と通常 Interest の情報記録数の差を小さくすることで攻撃の影響を抑制する．

シミュレーションによる評価を行い，提案手法を適用したときの通常ユーザの Interest 送信数と Data 受信数を調べた．その結果，提案手法では IFA が開始された後も通常ユーザの Interest 送信数は減少せず，Data 受信数についても IFA が開始される前とほぼ同程度まで回復することから，提案手法は通常 Interest を制限することなく攻撃の影響を抑制できることを確認した．また，提案手法を適用したときの PIT に記録されている Interest のエントリ数を調べた．その結果，提案手法では攻撃 Interest のエントリ数と通常 Interest のエントリ数の差が小さくなっており，提案手法によって攻撃 Interest 情報の記録を制限できることを確認した．

以上より，提案手法は PIT に記録する Interest 情報を選別することで，攻撃 Interest と通常 Interest のエントリ数の差を小さくし IFA の影響を抑制できることを確認した．

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] 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, *IEEE International Conference on Green Computing and Communications (GreenCom), IEEE Internet of Things (iThings/CPSCom) and IEEE Cyber, Physical and Social Computing*, pp. 306–310 (2013).

[4] 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).

[5] 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).

[6] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H. and Braynard, R. L.: Named Network Content, *CoNEXT*, pp. 344–350 (2009).

[7] Liu, Y., Yang, S., Guo, L., Chen, W. and Guo, L.: A Distributed Trust-based Reputation Model in P2P System, *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD)*, pp. 294–299 (2007).

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

[9] Ohata, Y., Umeda, S., Kamimoto, T. and Shigeno, H.: Secure Routing Protocol Considering Load Distribution in Mobile Ad Hoc Networks, *2015 IEEE Trustcom/BigDataSE/ISPA*, Vol. 1, pp. 840–847 (2015).

[10] 梅田沙也華，大畑百合，神本崇史，重野　寛：モバイルアドホックネットワークにおけるノードの行動に適応したトラストモデル，情報処理学会論文誌，Vol. 57, No. 2, pp. 471–479 (2016).

[11] 梅田沙也華，大畑百合，神本崇史，重野　寛：Named Data Networking におけるユーザの行動を考慮した Interest 制御手法の検討，情報処理学会マルチメディア，分散，協調とモバイル (DICOMO2015) シンポジウム，pp. 650–657 (2015).

[12] ns3: http://www.nsnam.org/ (参照 2016-05).

[13] ndnSIM: http://ndnsim.net/1.0/ (参照 2016-05).

[14] Breslau, L., Cao, P., Fan, L., Phillips, G. and Shenker, S.: Web caching and Zipf-like distributions: evidence and implications, *IEEE INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 1, pp. 126–134 vol.1 (1999).