情報処理学会論文誌 Vol.59 No.2 564–573 (Feb. 2018)

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

篠原 涼希[1,a)] 神本 崇史[1] 重野 寛[1]

受付日 2017年5月8日, 採録日 2017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，通常ユーザやネットワークに悪影響を及ぼす NDN 特有の Denial-of-Service（DoS）攻撃の存在が指摘されている．DoS 攻撃への対策手法も研究されているが，関連の攻撃対策手法では通常ユーザに対しても強力な通信の制約を課するという問題がある．また攻撃対策のために学習期間（非攻撃期間）を設けた手法が多く，データ要求が学習期間から変化した場合に対応できないという課題もある．本論文では，学習期間に依存せず，各ルータが独立的にデータ要求の影響度を算出した DoS 攻撃対策手法である IFMR を提案する．提案手法の目的は DoS 攻撃の検知・対策であり，これを実現するために各ルータがデータ要求の影響度を算出し，影響度に応じてパケット処理制御を行う．また，コンピュータシミュレーションにより様々な攻撃要求に対する提案手法の対策性能の評価を行った．

キーワード：named data networking，DoS 攻撃，cache pollution attack，interest flooding attack

Countermeasure against DoS Attacks Considering Maliciousness of Request Flow in Named Data Networking

Ryoki Shinohara[1,a)] Takashi Kamimoto[1] Hiroshi Shigeno[1]

Received: May 8, 2017, Accepted: November 7, 2017

Abstract: In Named Data Networking (NDN), which is a content-oriented network, Denial-of-Service (DoS) attacks affect normal users and networks. Countermeasures against DoS attacks have been proposed, but most of them limit requests of normal users strongly. Such countermeasures have a learning period (no attack period), and packet control is based on the information of this period. In this paper, we propose a countermeasure against DoS attacks without depending on a learning period, called IFMR. The purposes of IFMR are detection and suppression of attacks. Each router calculates maliciousness of data request and limits packet processing in proportion to the maliciousness. We evaluate suppression performance of IFMR through computer simulation.

Keywords: named data networking, DoS attack, cache pollution attack, interest flooding attack

1. はじめに

近年，主要なネットワークの使用方法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，各ルータは Data 要求パケットである Interest の転送先をそのパケットが要求する Data 名によって決定する．Interest を転送したルータはそのパケットの情報を記録し，応答パケットである 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 Data のコピーを提供することができる．NDN は現行のインターネットよりも強固なセキュリティを提供し

[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)] shinohara@mos.ics.keio.ac.jp

ている．しかし，コンテンツ指向という特徴を利用したDenial-of-Service（DoS）攻撃 [3] がNDNにおいて指摘されている．Cache Pollution Attack [4] はCSに対して作用し，通常ユーザが人気のあるデータを取得することを妨害する．攻撃者はCSに人気がないデータをキャッシュするように仕向け，人気があるデータをCSから排除する．Interest Flooding Attack（IFA）[5] において攻撃者は短期間に大量のInterestを送信し，これによりルータやサーバに負荷をかける．

Cache Pollution Attackの対策手法には大きくわけてDataを評価する手法とインタフェースを評価する手法の2つが存在する．Dataを評価する手法 [6], [7], [8], [9], [10] では攻撃者によって要求されているDataと通常ユーザによって要求されているDataを判別する．インタフェースを評価する手法 [11], [12], [13] では各インタフェースに流入するData要求に攻撃性があるかを判断する．インタフェースを評価する手法はCache Pollution AttackとIFAの両方を検知し抑制する手法として使用される．しかしながら，インタフェースを評価する手法の多くは通常ユーザのInterestを強く制限するという問題がある．また，これらの対策手法では学習期間として攻撃が行われない期間を設け，この期間の情報をもとにパケットの制御を行うが，通常ユーザの要求が学習期間から変化した場合に対応できないという課題がある．

本論文では，学習期間に依存しないDoS攻撃対策手法であるIFMR（Interest Flow Control Method Based on Maliciousness of Request）を提案する．IFMRにおいて，ルータはData要求の影響度を計算してパケットを制御する．影響度を計算するために，ルータは流入するData要求をインタフェースごとに監視する．NDNにおけるDoS攻撃の影響の大きさは攻撃パケットの量，要求するデータの種類数，そして要求頻度分布という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，通常ユーザやネットワークに影響を与えるData要求は通常の要求と異なる．IFMRではこの差を影響度と結び付け，Data要求が影響を与えると判断した場合はパケットを制限する．

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IFMR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DoS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はコンテンツ指向のネットワークアーキテクチャの1つである．NDNにおいて，各ルータはData要求パケットであるInterestの転送先をInterestが要求するData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Pending Interest Table（PIT），Forwarding Information Base（FIB），Content Store（CS）の3つのデータ構成を持つ．ルータがInterestを転送する際，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を転送する．FIBはInterestの転送方向を決定する際に使用される．CSはDataのコピー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．コピーの活用により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 NDNにおけるDoS攻撃

NDNにおいてノードは事前に通信の相手を指定する必要がない．したがって，攻撃者が位置情報を用いて特定の対象を狙うDoS攻撃に対処できる [3]．しかしながら，コンテンツ指向という特徴を悪用したCache Pollution AttackやInterest Flooding AttackといったDoS攻撃が指摘されている．これらのDoS攻撃はネットワークや発行者，通常ユーザに深刻な影響を与える．

Cache Pollution Attackは通常ユーザに対するDataのコピーの配布に影響を与える攻撃である．攻撃者はCSに人気のないコンテンツを記録させ，これにより人気のあるコンテンツをCSから追い出す．Cache Pollution Attackは攻撃者が要求するDataの種類数によってFalse-locality攻撃とLocality-disruption攻撃に分類できる．False-locality攻撃はルータに間違った局所性を持たせる攻撃である．ここでの局所性とは近接ノードにおけるコンテンツの人気度を反映したキャッシュ特性のことを指す．この攻撃において，攻撃者は数種類のDataを要求する．攻撃者によって要求されたDataは偽の人気度を持ち，人気がないDataが攻撃者によって頻繁に要求される．False-locality攻撃は要求されるDataの種類数がルータのキャッシュ容量と同数である場合に影響が大きい [6], [14]．Locality-disruption攻撃はルータの局所性を崩壊させる攻撃である．この攻撃において，攻撃者は多くの種類のDataをランダムに要求する．攻撃者は人気のないDataを要求することでキャッシュ置換を頻繁に発生させる．Locality-disruption攻撃は攻撃者が同一のDataを要求しない場合に影響が大きい．

IFAもNDNにおける主要なDoS攻撃の1つである．攻撃者は短期間に大量のInterestを送信する．これによりルータの処理が増大しData発行者の負荷が増大する．IFAの影響を最大化するために，攻撃者は重複したDataを要

求せずに多くの種類の Data を要求する必要がある．IFA は要求される Data の種類によって分類することができるが，実在しない Data 名を要求する IFA が最も影響が大きいと考えられる．

2.3 DoS 攻撃への対策とその問題点

NDN における DoS 攻撃の対策手法が提案されている．Cache Pollution Attack の影響を抑制する手法として Data を評価する方法とインタフェースを評価する方法が用いられている．Data を評価する手法では通常ユーザからの要求と攻撃者からの要求を Data 名を用いて判別する．インタフェースを評価する手法では各インタフェースに対する要求フローに影響があるかを判断する．Park らや Xu らは Interest が要求する Data 名のパターンをルータがインタフェースごとに記録し，通常ユーザの要求と比較することで攻撃を検知する手法を提案している [11], [12]．また，AbdAllah らは Data 要求の頻度やキャッシュヒット率を通常の要求と比較し，攻撃を検知したインタフェースからの Interest 転送を制御する手法を提案している [13]．これらのインタフェースを評価する手法は IFA への対策手法としても用いられる．また，Cache Pollution Attack が与える影響の大きさはルータのキャッシュ置換方式によって変動することが指摘されている [14]．キャッシュ置換方式として主に Least Recently Used（LRU）と Least Frequently Used（LFU）が用いられている．LRU は CS が一杯である場合に最も古い Data を置換する．LFU は最も人気がない Data を置換する．LFU を用いることでルータはユーザが頻繁に要求する人気のある Data を残すことができるため，LFU は Locality-disruption 攻撃の抑制に効果的である．しかし，これらのキャッシュ置換手法ではルータは正常な人気 Data と偽の人気 Data を判別しないため，False-locality 攻撃の影響を受けやすい．関連研究において，False-locality と Locality-disruption の両方に対応した対策手法 [8], [12], [14] や，Locality-disruption と IFA の両方に対応した対策手法 [13] が提案されている．一方で，DoS 攻撃全体を抑制する対策手法は提案されていない．Data 評価手法はルータが Data 名に関する大量の情報を保存できる場合に効果的であり，Data 評価手法は大量のメモリ消費を必要とする．したがって，DoS 攻撃全体を抑制するにはインタフェース評価手法が適している．

インタフェース評価手法は学習期間（非攻撃期間）を設けており，パケットの制御はこの期間の情報を基に行われる．このことは対策手法が人気度の変動に対応できないということを意味している．Data の人気度はつねに変化しており，実世界においていくつかの Data が爆発的な人気を得ることはしばしばある．したがって，通常ユーザの要求頻度分布は静的ではないため，ルータは現在の分布について再学習し，通常ユーザが要求する Data 名や要求頻度を更新する必要がある．しかし，更新期間の適切な長さについては議論されていない．そこで，ルータは学習期間を用いずにインタフェースを評価する手法を用いる必要がある．

3. IFMR の提案

本章では，インタフェース評価手法を基にした DoS 攻撃対策手法 IFMR（Interest Flow Control Method Based on Maliciousness of Request）を提案する．

3.1 IFMR の概要

IFMR は以下の 3 つの段階から構成される．

- 記録段階：ルータがインタフェース i から Interest を受け取った場合，ルータはインタフェース i の受信数を増やす．インタフェース i の受信数が一定の値に達した場合，ルータは検知段階に移行する．
- 検知段階：ルータはインタフェースごとに要求フローの影響度を計算する．ルータは各インタフェースの要求を 4 つに分類する．要求を分類した後にルータは分類を行ったインタフェースの受信数をリセットする．ルータが攻撃を検知した場合，ルータは抑制段階に移行する．
- 抑制段階：ルータは攻撃が検知されたインタフェースに対しパケットを制限することによって DoS 攻撃を抑制する．パケットを制限している間も，ルータは記録段階と検知段階を繰り返す．

検知段階において，IFMR は要求フローを False-locality 攻撃，Locality-disruption 攻撃，IFA，通常の要求の 4 種類に分類する．ルータはインタフェースごとに要求フローを監視して要求の特徴を抽出する．通常ユーザやネットワークに悪影響を及ぼす Data 要求の特徴は通常の要求とは異なるため，IFMR はこの差を影響度としている．要求フローの特徴や攻撃の影響を決定する指標は以下の 3 つである．

- Interest 量：短期間に生成された Interest の数
- Data 種類：要求された Data の種類
- 要求分布：要求頻度分布

ここで，要求頻度分布とは各 Data に対する要求頻度の分布である．Interest 量と Data 種類は Cache Pollution Attack に対する関連研究のなかで使用されている指標である．

一方で，要求分布については DoS 攻撃のフローに特徴があるにもかかわらずあまり議論されていない．そこで，提案手法では要求分布を新たに加味する．ルータは要求数を降順に並べ替える．この並べ替えられた要求数は要求分布と一致し，要求された Data の数は Data 種類と一致する．しかし，Interest は中継ルータで充足されると破棄されるため，Interest 量はルータが直接監視できない．そこで，ルータは検知の頻度を Interest 量として使用する．ルータが攻撃検知を頻繁に行う場合，ルータは攻撃要求を強く制

限する．連続的な攻撃はとても影響があるが，攻撃が検知されたときにそれが一時的な攻撃なのか連続的な攻撃なのかは判断できない．したがって，IFMR は受信数をリセットして繰り返し検知段階において要求の分類を行うことにより，攻撃と判断されていた要求フローが通常の要求と判断された際に抑制されないようにする．

3.2 IFMR におけるパケット処理

図 1 はルータにおける DoS 攻撃の検知およびパケット処理の流れについて示している．はじめに，ルータは False-locality 攻撃を判別する．その後，ルータは Locality-disruption 攻撃と通常の要求を分別する．IFMR では IFA を Locality-disruption 攻撃の一種として扱う．

ルータがインタフェース i に対して False-locality 攻撃を検知すると，ルータは CS を参照する前に処理率 $P_i(t)$ に基づいてインタフェース i の Interest を破棄する．Interest を破棄しなかった場合，ルータは CS に保存されている Data が Interest に返信できるかを確認する．キャッシュヒットが起こらなかった場合は，ルータは PIT を参照する前に処理率 $P_i(t)$ に基づいて Interest を破棄する．また，ルータが IFA を検知した場合は破棄率 $1 - IR_i(t)$ に基づいて Interest を破棄する．ルータが Locality-disruption 攻撃を検知した場合，ルータは Data を転送した後キャッシュ率 $C_i(t)$ に基づいて Data を CS に保存せずに破棄する．

各 DoS 攻撃の検知や抑制の方法およびそこで使用する変数について以下で詳しく説明する．

3.3 False-locality 攻撃の検知と抑制

False-locality 攻撃の検知を行うために，提案手法では要求分布に FalseZone を導入する．ルータは各インタフェースに対して FalseZone における要求フローの特徴から False-Reputation FR_i を算出する．FR_i の値が閾値よりも大きい場合，ルータは False-locality 攻撃を受けていると判断して要求フローを制限する．False-locality 攻撃を効率的に抑制するため，提案手法は 2 段階の制限を導入している．攻撃の検知と抑制の流れについて以下で詳しく説明する．

提案手法では要求分布の中に FalseZone を導入する．False-locality 攻撃は攻撃者によって要求される Data の種類が CS の大きさと同じであるときに強力になることが指摘されている [6], [14]．さらに，強力な False-locality 攻撃の要求分布は均一分布となる．つまり，攻撃フローが均一分布で Data の種類数が CS の大きさと同じになるとき，False-locality 攻撃の影響は最大になる．FalseZone は要求分布において False-locality の攻撃者による要求の割合が通常ユーザの要求よりも高くなる領域を指す．IFMR は FalseZone に含まれる要求率の合計を用いて False-locality 攻撃を検知する．ここで，要求率とは全 Data の要求数に対する各 Data の要求数の割合である．要求率の合計は影響度を数値化したものとなる．ここで，FalseZone の始点を制御するためのパラメータ α を導入する．要求分布における FalseZone の終点は CS サイズとなる．α は CS サイズの割合として示され，FalseZone を CS サイズの 10 パーセントから始める場合 α は 0.1 となる．図 2 は FalseZone と要求分布の関係を示している．通常ユーザの要求は Zipf の法則 [15] に従うといわれている．この場合，図 2 で示すように通常ユーザの FalseZone における要求率の合計は攻撃者よりも小さくなる．したがって，IFMR は Data 種類と要求分布から通常の要求と False-localty 攻撃の要求を分別することが可能である．

検知段階において，ルータは各インタフェースに対して FalseReputation FR_i を算出する．FR_i とはキャッシュを汚染しようとしているインタフェースの要求フローの影響度を示すものである．FR_i は式 (1) によって示される．

$$FR_i = HitRatio_i \cdot \frac{1}{1-\alpha} \sum_{j=(CSsize)\times\alpha}^{CSsize} r_{ij}, \quad (0 \le FR_i \le 1) \tag{1}$$

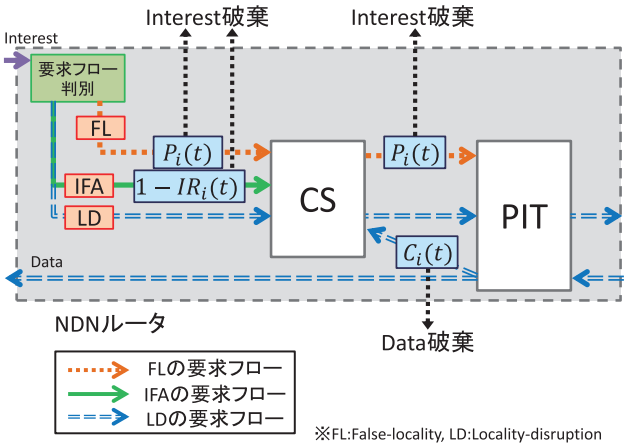

図 1 攻撃検知時のパケット処理
Fig. 1 Timing of drop interest or data for alleviating DoS.

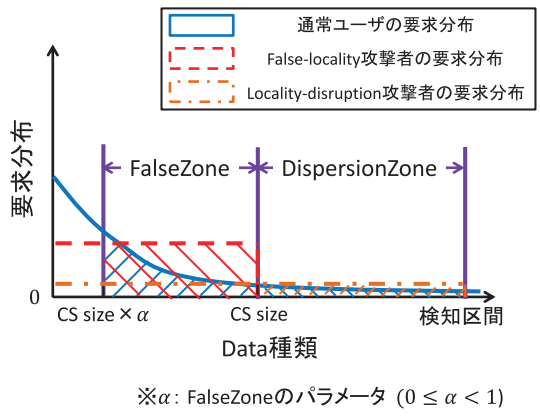

図 2 FalseZone と DispersionZone の概形
Fig. 2 Overview of FalseZone and DispersionZone.

ここで，$HitRatio_i$ はインタフェース i のキャッシュヒット率を示し，r_{ij} はインタフェース i における Data$j$ の要求率を示す．$HitRatio_i$ は False-locality 攻撃の実際の影響度を示す．攻撃によりキャッシュが汚染されている場合，キャッシュヒット率は大きくなる．要求率の合計は Data 種類と要求分布を基にした要求フローの影響度を示す．合計値は FalseZone の幅によって正規化される．式 (1) より，要求フローの影響度および実際の影響度が大きくなると FR_i の値も大きくなる．

FR_i が式 (2) を満たすとき，ルータは攻撃を検知する．

$$FR_i > T_F, \quad (0 \leq T_F \leq 1) \tag{2}$$

ここで，T_F は FR_i の閾値である．算出の頻度は受信した Interest 数を基に決定するため，FR_i の算出の頻度は要求フローの強度を示している．攻撃要求の強度が大きい場合，検知段階は頻繁に実行される．この検知の頻度は攻撃の抑制に重要である．

ルータが False-locality 攻撃を検知すると，ルータは攻撃を検知したインタフェースの影響度が更新されるまで要求フローを制限する．False-locality 攻撃を抑制するために，提案手法では攻撃 Data と攻撃 Interest の両方を制限する．攻撃 Data を制限する方法として，即座に攻撃 Data を除外する方法と徐々に除外する方法の 2 種類がある．ルータが即座に攻撃 Data を除外する方法において，攻撃 Data はキャッシュから強制的に置換されるか削除される．この方法では CS の Data に人気がない状態をすぐに修復することが可能であるが，除外すべき Data を決定するために，ルータは Data の評価を行う必要がある．攻撃 Data を徐々に除外する方法において，ルータは Interest を段階的に制限し，Interest で要求されない Data は自然に除外される．この方法において，ルータは CS に保存されている Data を評価する必要がない．したがって，この手法はインタフェース評価手法に適しており，キャッシュの有効活用と攻撃抑制の両面において効果的である．False-locality 攻撃を抑制するためには攻撃 Data の制限に加えて攻撃 Interest の転送制御を行う必要がある．攻撃 Data を除外した結果，攻撃 Interest はルータで返信できずネットワークへ流れていく．したがって，通信量の増加を抑制するために攻撃 Interest を制限する仕組みが必要である．

攻撃 Data と攻撃 Interest の両方を制限するために，IFMR は攻撃を検知したインタフェースに対して CS を参照する前後で 2 段階の制限を導入している．最初の制限ではルータが CS を参照する前に Interest を破棄する．この制限により CS 内の攻撃 Data が参照される回数が減るため，攻撃 Data は徐々に除外される．このように，提案手法では攻撃 Interest を制限することで間接的に攻撃 Data の制限も行う．2 段階目の制限ではルータが CS を参照した後に Interest を転送せずに破棄する．この制限により発行者の通信負荷が削減される．これらの制限は処理率 P_i に基づく．P_i は攻撃を検知したインタフェースから転送される Interest に対して処理を続けるか決定する確率である．ルータがインタフェース i の要求フローを False-locality 攻撃と判断した場合，ルータはインタフェース i の Interest を $1 - P_i$ の確率で破棄する．P_i は式 (3) で示される．

$$P_i(t) = P_i(t-1) \cdot (1 - FR_i), \quad (0 \leq P_i(t) \leq 1) \tag{3}$$

ここで，$P_i(t-1)$ は過去の処理率を表す．

式 (3) より，ルータは FR_i が大きいときに高い確率で Interest を破棄する．さらに，IFMR は処理率を過去の処理率を基にして計算するため，連続的な False-locality 攻撃に対して Interest 処理を強く制限する．

3.4 Locality-disruption 攻撃の検知と抑制

Locality-disruption 攻撃の検知を行うために，提案手法では False-locality 攻撃の検知と同様に要求分布に DispersionZone を導入し，各インタフェースに対して DisruptionReputation DR_i を算出する．DR_i の値が閾値よりも大きい場合，ルータは Locality-disruption 攻撃を受けていると判断して要求フローを制限する．False-locality 攻撃の抑制とは違い，提案手法では攻撃 Data のみを制限することで Locality-disurption 攻撃を抑制する．以下で検知と抑制の詳細を説明する．

提案手法では要求分布に DispersionZone を導入する．図 2 に DispersionZone と要求分布の関係を示す．Locality-disruption 攻撃の特徴として要求の種類が CS サイズよりも大幅に多いことと要求フローのヒット率が低いことがあげられる．したがって，DispersionZone における Locality-disruption 攻撃者の Data 要求率は通常ユーザの要求率よりも高くなる．IFMR は DispersionZone における要求率の合計を用いて Locality-disruption 攻撃の検知を行う．

検知段階において，ルータは各インタフェースに対して DisruptionReputation DR_i を算出する．DR_i は局所性を崩壊させようとしている要求フローの影響度を意味する．DR_i は式 (4) で算出される．

$$DR_i = (1 - HitRatio_i) \cdot \frac{1}{\beta - 1} \frac{1 - \sum_{j=1}^{CSsize} r_{ij}}{\sum_{j=1}^{CSsize} r_{ij}}, \quad (0 \leq DR_i \leq 1) \tag{4}$$

$1 - HitRatio_i$ は Locality-disruption 攻撃の実際の影響度を示しており，β（$\beta \geq 1$）は CS サイズに対する検知区間の比を示している．

ルータが検知区間と同数の Interest を受信すると記録段階から検知段階に移行する．検知区間が長くなるほど Interest 情報が多くなるため，ルータは正確に Locality-disruption 攻撃と通常の要求を分別できる．しかし，検知区間が長くなると検知の間隔が長くなるため，攻撃検

知は遅くなる．正確性を確保しつつすばやく攻撃検知を行うためには，DR_i の値がフローの変化に対して鋭敏に変化する必要がある．DR_i を鋭敏に変化させるために，DispersionZone に含まれる要求率の合計に対するそれ以外の要求率の合計の割合を利用する．この割合は Data 種類と要求分布の両面から見た要求フローの影響度を示す．式 (4) より，要求フローの影響度およびの実際の影響度が大きくなると DR_i の値も大きくなる．

DR_i が式 (5) を満たすとき，ルータは攻撃を検知する．

$$DR_i > T_D, \quad (0 \leq T_D \leq 1) \tag{5}$$

ここで，T_D は DR_i の閾値を表す．

通常ユーザが大量の Data からなるコンテンツを要求している場合，ルータは通常の要求を Locality-disruption として検知する．この場合，通常ユーザはルータの局所性を崩壊させようとしているわけではないが，要求フローは Locality-disruption の攻撃者と同様のものになっている．悪意のない Locality-disruption はしばしば発生する．したがって，IFMR は頻繁に Locality-disruption 攻撃を検知するため，攻撃の抑制に検知の頻度は使用しない．

Locality-disruption 攻撃の抑制段階も攻撃が検知されたインタフェースの影響度が更新されるまで継続される．IFMR は容易に Locality-disruption 攻撃を検知しうるため，Locality-disruption に対する制限は軽量なものにする．Locality-disruption 攻撃を軽量に抑制するために提案手法では攻撃 Data のみを制限する．攻撃 Data を制限する方法として，CS に保存されている攻撃 Data を即座に除外する方法と攻撃 Data が CS に保存される前に除外する方法の 2 つがある．CS に保存されている攻撃 Data を除外する方法は除外すべき Data を評価する必要がある．一方で，攻撃 Data が CS に保存される前に除外する方法はルータが各 Data の人気度を算出する必要がないため，インタフェース評価手法に適している．

IFMR ではキャッシュ置換が発生する前に Data を破棄する．IFMR はすべての受信した Data を転送する．IFMR はルータが Data を下流に転送した後に Data を破棄することでルータに人気のない Data を保存させないようにする．ルータが Locality-disruption 攻撃を検知すると，ルータは攻撃を検知したインタフェースから要求された Data を CS に保存するか判断する．この判断はキャッシュ率 C_i を基に行われる．C_i は攻撃によって要求された Data をルータに保存する確率である．C_i は式 (6) で示される．

$$C_i(t) = 1 - DR_i. \quad (0 \leq C_i(t) \leq 1) \tag{6}$$

式 (6) より，DR_i の値が高い場合にルータは高い確率で CS に Data を保存しない．

3.5 IFA の検知と抑制

IFA を検知するために，IFMR は Locality-disruption 攻撃の検知手法を使用する．IFMR では IFA を Locality-disruption 攻撃の一種として扱う．IFA は強力な Locality-disruption 攻撃と同様であり，IFA の攻撃者は非常に多くの種類の Data を要求する．IFMR は IFA と Locality-disruption 攻撃を要求の量によって分別する．IFA を抑制するために，提案手法では攻撃 Interest を制限する．以下で検知と抑制の詳細を説明する．

提案手法ではインタフェースごとの正常度を示す変数 InterestfloodingReputation IR_i を導入する．インタフェースの要求が Locality-disruption 攻撃として判断されると，インタフェースの IR_i が減少する．通常の要求フローが IFA として判断されることを防ぐために，IR_i は時間経過にともない回復する．回復量は IR_i の比率として定義される．このことは IR_i が小さいときは回復が遅くなるということを意味する．IR_i は式 (7) で定義される．

$$IR_i(t) = IR_i(t-1)\frac{\sum_{j=1}^{CSsize} r_{ij}}{1 - \sum_{j=1}^{CSsize} r_{ij}}, \quad (0 \leq IR_i(t) \leq 1) \tag{7}$$

ここで，$IR_i(t-1)$ は IR_i の過去の値である．

Locality-disruption 攻撃の強度が大きい場合は IR_i の減少率が回復率を上回るため，攻撃フローの評価値は減少し続ける．

IR_i が式 (8) を満たすとき，ルータは IFA を検知する．

$$IR_i < T_I, \quad (0 \leq T_I \leq 1) \tag{8}$$

ここで，T_I は閾値である．

抑制段階において，ルータは攻撃を検知したインタフェースからの Interest を CS を参照する前に破棄する．Interest を破棄する確率は $1 - IR_i$ である．この確率は IFA の閾値 T_I に依存する．IFA を強く制限するために閾値は低い値に設定する．

4. シミュレーション評価

提案手法 IFMR の有用性を示す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 XC トポロジ [7], [14] を使用した．XC トポロジは Cache Pollution Attack の対策手法の効果を評価する際にしばしば用いられる．**図 3** に XC トポロジの概形を示す．通常ユーザや攻撃者は一定の割合で Data を要求する．通常ユーザはシミュレーション時間いっぱいに Data を要求するが，攻撃者はシミュレーションの後半において Data を要求する．すべての発行者は同じ Data のセットを所持している．今回のシミュレーショ

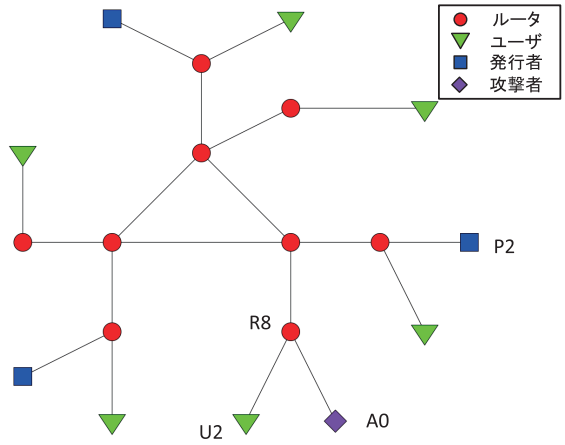

図 3 XC トポロジの概形
Fig. 3 Overview of XC topology.

表 1 通常ユーザと攻撃者のパラメータ
Table 1 User and attacker parameters.

パラメータ	通常ユーザ	攻撃者	
		FL[1]	LD[2] IFA
要求時間	0〜1,800 [sec]	900〜1,800 [sec]	
Data の種類数 θ	10,000	100	10,000
要求の強度	10 [pkt/sec]	—	
攻撃の強度 γ	—	10〜1,000 [pkt/sec]	

[1] FL: False-locality
[2] LD: Locality-disruption

ンでは発行者が所持する Data セットを半分にわけ，一方を通常ユーザが要求する人気のある Data セット，もう一方を攻撃者が要求する人気のない Data セットとする．この要求モデルは人気のない Data が人気のある Data と重複しないため，攻撃の影響が最も大きくなるモデルであるといえる．通常ユーザは Zipf の法則 [15] に従いコンテンツを要求する．攻撃者は各攻撃に基づいて Data を連続的に要求する．提案手法では，攻撃者が CS サイズと同数の Data の種類を要求するフローを False-locality 攻撃と定義する．Locality-disruption 攻撃に関しては攻撃者が可能な限り同じ Data を再度要求しないフローと定義する．IFA の要求フローは大量に異なる Data を要求するフローと定義する．

表 1 に通常ユーザと攻撃者の基本的なパラメータについて示す．各攻撃において使用される Data の種類は θ で表し，攻撃の強度は γ で表す．各通常ユーザは 10,000 種類の Data を要求する．各攻撃者は False-locality 攻撃において CS の容量と同じ 100 種類の Data を要求する．一方で，攻撃者が Locality-disruption 攻撃や IFA を実行する場合は 10,000 種類の Data を要求する．攻撃の強度はすべてのユーザの要求率の合計から設定する．攻撃者 1 人あたりの要求率がすべてのユーザの要求率と同じ場合，攻撃者の強度はユーザの強度と同等になる．XC トポロジ上では 6 人の通常ユーザが存在するものとし，攻撃者の要求率は各ユーザの要求率の 6 倍とした．

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 [16]
NDN モジュール	ndnSIM 1.0 [17]
シミュレーション時間	1,800 [sec]
キャッシュ置換アルゴリズム	LRU，LFU
ルータの CS サイズ	100 [pkt]
ルータの PIT サイズ	100 [pkt]
Data サイズ	1,024 [byte]
リンクの帯域	10 [Mbps]
リンクの遅延	10 [ms]

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 LRU または LFU を用いた．ルータの CS の大きさは通常ユーザによって要求される Data 全体の 1%に設定した [7], [9], [14]．PIT サイズは各ルータで 100 である．固定値である α，T_F，T_D，T_I と $IR_i(t)$ の回復率，検知区間の値は予備実験を基に決定した．予備実験では通常ユーザの幅広い要求パターンに対応するため，Zipf の法則のパラメータを変動させたうえで通常ユーザの評価値を算出し固定値を決定した．そのため，提案手法では改めて通常ユーザの要求を学習する必要はない．固定値の具体的な値については次節以降に記載している．

DoS 攻撃の影響と IFMR の性能を評価するために，以下の評価項目を設けた．

- ユーザキャッシュヒット率
  ユーザが生成した Interest 数に対してキャッシュから返信された Data 数の割合である．ユーザがすべての要求 Data をルータから入手して Interest が発行者に到達しなかった場合値は 1 になる．
- 通信負荷
  データ発行者における受信した Interest のサイズと送信した Data のサイズの合計である．

ユーザキャッシュヒット率は R8 で観察し，通信負荷は P2 で観察する．R8 において，通常ユーザ U2 と攻撃者 A0 の要求は異なるインタフェースから入力される．NDN では 1 ホップのパケット送信者を判別できるため，ユーザに近いルータの中には通常ユーザと攻撃者の要求フローをインタフェースごとに分離できるルータが存在すると考えられる．以上の仮定に基づき，今回のシミュレーションではインタフェースごとに通常ユーザと攻撃者の要求フローを分離できる末端ルータでの観測を行った．

4.2 攻撃の抑制性能の評価

図 4 と**図 5** は False-locality 攻撃の抑制結果について示している．実線が IFMR を用いた場合の結果であり，破線が対策手法を使用しない場合の結果である．通常ユーザおよび攻撃者の系列はユーザキャッシュヒット率に対応し，

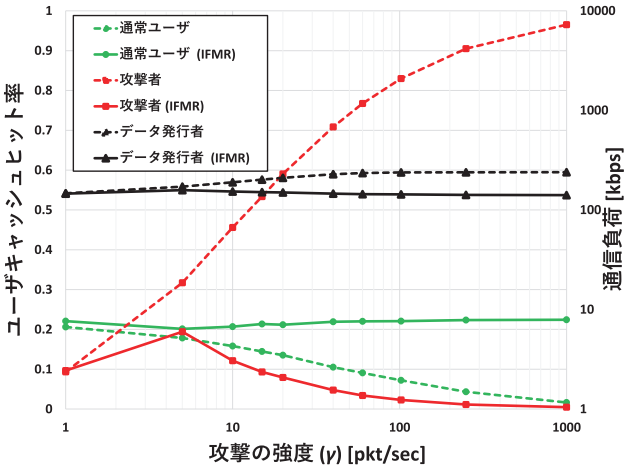

図 4 False-locality 攻撃の抑制（LRU）
Fig. 4 Alleviation of False-locality attack (LRU).

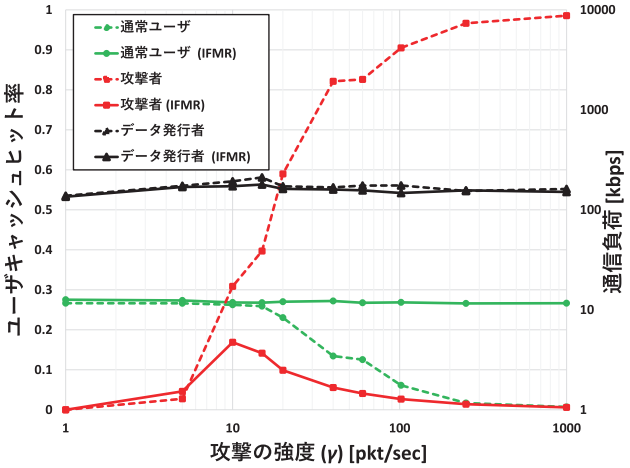

図 5 False-locality 攻撃の抑制（LFU）
Fig. 5 Alleviation of False-locality attack (LFU).

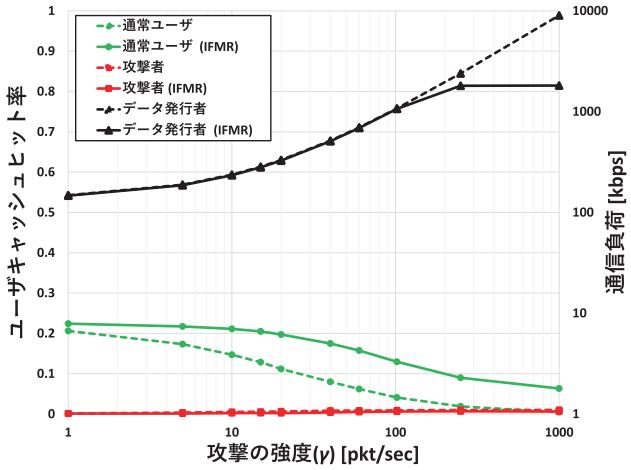

図 6 Locality-disruption 攻撃と IFA の抑制（LRU）
Fig. 6 Alleviation of Locality-disruption and IFA (LRU).

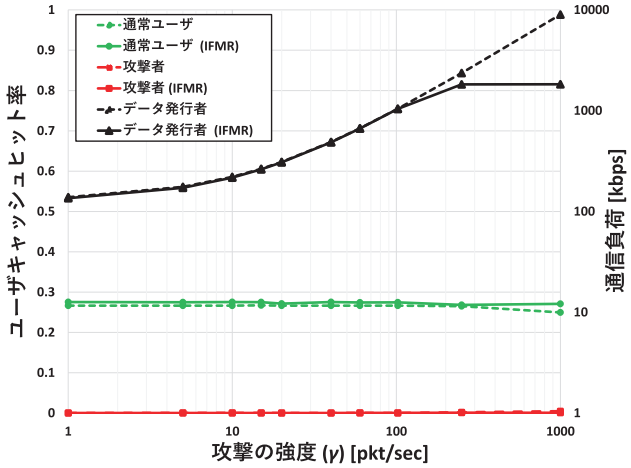

図 7 Locality-disruption 攻撃と IFA の抑制（LFU）
Fig. 7 Alleviation of Locality-disruption and IFA (LFU).

データ発行者の系列は通信負荷に対応している．LRU 時は α の値として 0.1 を，LFU 時は 0.3 を使用している．T_F の値は 0.3 である．図 4 より，IFMR を適用している場合は通常ユーザは攻撃の強度の増加にかかわらず一定のヒット率を保つ．一方で，攻撃者のヒット率は強度が大きくなるほど低下している．また，サーバの通信負荷は増加しない．評価項目のこれらの傾向は図 5 の LFU 時も同様である．ルータが False-locality 攻撃を検知すると，ルータは攻撃の要求フローを強力に制限する．攻撃の強度の増加にともない制限の強さと反応速度は増加する．また，IFMR が攻撃パケットを破棄することで通信負荷の増加が抑えられる．以上より，提案手法は False-locality 攻撃と通信負荷の増加を同時に抑制できることが確かめられた．

次に，Locality-disruption 攻撃と IFA に対する抑制性能について評価する．これらの攻撃は同一の手順を経て検知され，異なる方法によって抑制される．T_D の値は 0.6，T_I の値は 0.01，IR_i の回復率は 1 秒あたり 5% ，検知区間は 500 パケットである．CS サイズが 100 であるため，検知区間の比 β は 5 となる．**図 6** と**図 7** に Locality-disruption 攻撃と IFA の抑制結果を示す．図 6 で示すように，LRU 時において IFMR は通常ユーザのヒット率の減少を抑制するが，攻撃の強度の増加にともないヒット率は減少する．一方で，LFU は Locality-disruption 攻撃を抑制できるため，IFMR を使用した場合と対策手法を使用しない場合の結果に差はない．通信負荷に注目すると，IFMR は各キャッシュ置換手法において P2 の通信負荷の爆発的増加を抑制できている．通常ユーザが長期間にわたって異なる Data を要求することがしばしば起こりうるため，IFMR は Locality-disruption 攻撃の影響を強く制限しない．このため，ヒット率の減少が見られる．DR_i は攻撃者のヒット率にも依存する．DR_i においてヒット率は Locality-disruption 攻撃の影響を反映させるために使用される．しかし，Locality-disruption 攻撃者のヒット率は攻撃の強度に依存しない．そのため，DR_i は攻撃の強度が増加した場合もほぼ一定の値をとる．したがって，Locality-disruption に対する提案手法は強力な Locality-disruption の抑制には不十分である．IFMR に

おいて，通信負荷の爆発的増加は抑制されるが，負荷は一定の割合を保持する．Data の人気度が爆発的に上昇した場合，バーストトラフィックが通常ユーザによってしばしば起こされる．このような状況においてユーザにある程度 Data の取得を許可するためには要求を過度に抑制しないことが望ましい．したがって，IFMR は IFA の要求を完全には抑制せず，攻撃者を含むすべてのユーザにある程度のネットワーク利用を許容している．

5. おわりに

本論文では，NDN における DoS 攻撃の対策手法である IFMR を提案した．攻撃を検知するために，IFMR は要求フローから Interest 量，Data 種類，要求分布の 3 つの特徴を抽出して要求を 4 つのクラスに分類する．ルータが False-locality 攻撃を検知した場合は Interest の制限処理を 2 回に分けて実行する．また，ルータが Locality-disruption を検知した場合は攻撃フローによって要求された Data を CS に保存しないようにする．IFMR は IFA を Locality-disruption の一種と考え，IFA のフローは強力に制限する．これらの攻撃検知は要求フローから得られる現在の情報によって実行されるため，ルータは学習期間を設ける必要がない．

シミュレーションを用いて IFMR の攻撃抑制の性能を評価した．シミュレーション結果より，提案手法では False-locality 攻撃を抑制し通信負荷の増加を抑制できることを確認した．提案手法では Locality-disruption を検知することで過剰な要求フローを見張っている．そして過剰な要求を制限することにより，IFMR は IFA を抑制できていることを確認した．

以上より，提案手法は DoS 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] 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).

[4] Deng, L., Gao, Y., Chen, Y. and Kuzmanovic, A.: Pollution Attacks and Defenses for Internet Caching Systems, *Comput. Netw.*, Vol.52, No.5, pp.935–956 (2008).

[5] Choi, S., Kim, K., Kim, S. and Roh, B.H.: Threat of DoS by interest flooding attack in content-centric networking, *The International Conference on Information Networking 2013* (*ICOIN*), pp.315–319 (2013).

[6] Guo, H., Wang, X., Chang, K. and Tian, Y.: Exploiting Path Diversity for Thwarting Pollution Attacks in Named Data Networking, *IEEE Trans. Information Forensics and Security*, Vol.11, No.9, pp.2077–2090 (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] Kamimoto, T., Mori, K., Umeda, S., Ohata, Y. and Shigeno, H.: Cache protection method based on prefix hierarchy for content-oriented network, *2016 13th IEEE Annual Consumer Communications Networking Conference* (*CCNC*), pp.417–422 (2016).

[10] Adithya, S., Gowtham, K.G., Hariharan, H. and Vetriselvi, V.: Assuaging Cache based attacks in Named Data Network, *2016 International Conference on Wireless Communications, Signal Processing and Networking* (*WiSPNET*), pp.872–876 (2016).

[11] Park, H., Widjaja, I. and Lee, H.: Detection of cache pollution attacks using randomness checks, *IEEE International Conference on Communications* (*ICC*), pp.1096–1100 (2012).

[12] Xu, Z., Chen, B., Wang, N., Zhang, Y. and Li, Z.: ELDA: Towards efficient and lightweight detection of cache pollution attacks in NDN, *2015 IEEE 40th Conference on Local Computer Networks* (*LCN*), pp.82–90 (2015).

[13] AbdAllah, E.G., Zulkernine, M. and Hassanein, H.S.: Detection and Prevention of Malicious Requests in ICN Routing and Caching, *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp.1741–1748 (2015).

[14] Conti, M., Gasti, P. and Teoli, M.: A lightweight mechanism for detection of cache pollution attacks in Named Data Networking, *Computer Networks*, Vol.57, No.16, pp.3178–3191 (2013).

[15] Breslau, L., Cao, P., Fan, L., Phillips, G. and Shenker, S.: Web caching and Zipf-like distributions: Evidence and implications, *Proc. 18th Annual Joint Conference of the IEEE Computer and Communications Societies*, *INFOCOM '99*, Vol.1, pp.126–134, IEEE (1999).

[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).

篠原 涼希 （学生会員）

2016 年慶應義塾大学理工学部卒業．現在，同大学大学院理工学研究科前期博士課程在学中．

神本 崇史

2015 年慶應義塾大学理工学部卒業．2017 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，同高度交通システム研究会幹事，電子情報通信学会英文論文誌 B 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，Secretary of IEEE ComSoc APB．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．