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

篠原 涼希[1,a)]　神本 崇史　重野 寛[1,b)]

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．NDN における DoS 攻撃にはいくつか種類があり，それぞれの攻撃に応じた適切な対策が提案されている．したがって，攻撃を対策するためには攻撃を検知する際に攻撃の種類を正しく分類する必要がある．従来の攻撃対策手法には対応できる攻撃の種類が限定されるという課題がある．また攻撃検知のために学習期間（非攻撃期間）を設けた手法が多く，Data 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．本稿では，ルータが学習期間に依存せずに DoS 攻撃の種類を分類できる検知手法 ICEM を提案する．提案手法の目的は DoS 攻撃の検知と分類であり，これを実現するために各ルータが Data 要求の影響度を算出し攻撃の検知を行う．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攻撃検知分類性能の評価を行った．

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伴い，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一つに 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 Data を取得することを妨害する．攻撃者は CS に人気がない Data をキャッシュするように仕向け，人気がある Data 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．

DoS 攻撃の適切な対策は攻撃の種類によって異なるため，対策を行うためには攻撃の検知に加えて分類を行うことが重要である．Cache Pollution Attack の検知手法には Data を評価する手法 [6], [7] とインタフェースを評価する手法 [8], [9] の二つが存在する．インタフェースを評価する手法は Cache Pollution Attack と IFA の両方を検知する手法として使用される．したがって，DoS 攻撃の検知と分類を行うためにはインタフェースを評価する手法が適していると考えられる．しかしながら，Cache Pollution Attack にはいくつかの種類があり，インタフェースを評価する手法においてすべての Cache Pollution Attack を検知できる手法は存在しない．また，これらの検知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攻撃の検知を行うが，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．

本稿では，学習期間に依存しない DoS 攻撃検知分類手法である ICEM（Interest Flow Classification Method Evaluating Maliciousness of Request）を提案する．ICEM において，ルータは Data 要求の影響度を計算することで攻撃を検知分類する．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 における要求フローの特徴は要求パケットの量，要求す

[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
[b)] shigeno@mos.ics.keio.ac.jp

る Data の種類数，そして要求頻度分布という三つの指標によって決定される．これらの指標で評価した際に，通常ユーザやネットワークに影響を与える Data 要求の特徴は通常の要求の特徴と異なる．また，Cache Pollution Attack に分類される攻撃や IFA といった攻撃の種類ごとにも要求の特徴に差が出る．ICEM ではこの差を影響度と結びつけ，Data 要求が影響を与えると判断した場合は攻撃として検知し分類を行う．

以下本稿では，2 章において関連手法について述べ，3 章で ICEM 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，その検知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一つである．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）の三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], [10]．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 攻撃の一つである．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 がもっとも影響が大きいと考えられる．

2.3 DoS 攻撃の検知とその問題点

NDN における DoS 攻撃の検知手法が提案されている．Cache Pollution Attack を検知する手法として 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．このインタフェースを評価する手法は IFA の検知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 [10]．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もっとも古い Data を置換する．LFU はもっとも人気がない 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，あるいは Locality-disruption と IFA の両方に対応した検知手法が提案されている．一

方で，DoS 攻撃全体を検知する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 攻撃全体を検知分類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，攻撃の検知はこの期間の情報を基に行われる．このことは検知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 の人気度は常に変化しており，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. ICEM の提案

本章では，インタフェース評価手法を基にした DoS 攻撃検知分類手法 ICEM（Interest Flow Classification Method Evaluating Maliciousness of Request）を提案する．

3.1 ICEM の概要

ICEM は以下の二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四つに分類する．

検知段階において，ICEM は要求フローを False-locality 攻撃，Locality-disruption 攻撃，IFA，通常の要求の四種類に分類する．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，ICEM 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三つである．

- 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

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関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び替える．この並び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．

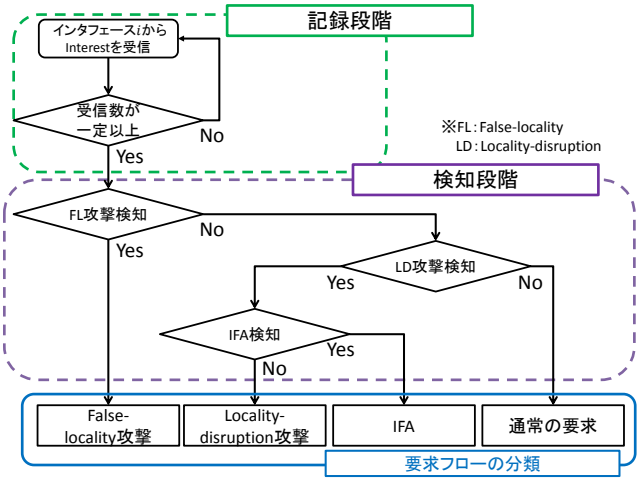


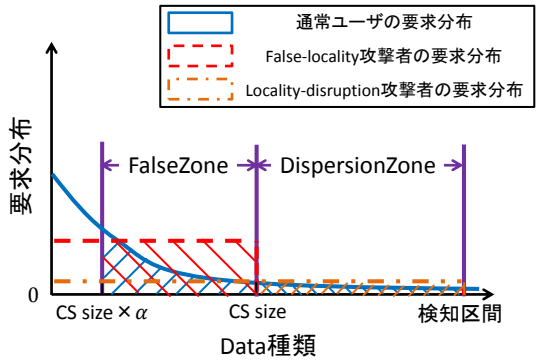
図 1　DoS 攻撃の検知と分類

図 1 はルータにおける DoS 攻撃の検知分類の流れについて示している．記録段階から検知段階に移行したルータははじめに 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．ICEM では IFA を Locality-disruption 攻撃の一種として扱う．

各 DoS 攻撃の検知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．

3.2 False-locality 攻撃の検知

False-locality 攻撃の検知を行うために，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], [10]．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，False-locality の攻撃フローは均一分布で Data の種類数は CS の大きさと同じになる．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．ICEM 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．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 [11] 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，ICEM 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．



※α: FalseZoneのパラメータ $(0 \leq \alpha < 1)$

図 2　FalseZone と DispersionZone の概形

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．

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

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，FR_i の値が大きくなると要求の影響度も大きくなる．

FR_i が式 (2) を満たすとき，ルータは攻撃を検知する．

$$FR_i > T_F, \qquad (0 \leq T_F \leq 1) \qquad (2)$$

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．

3.3　Locality-disruption 攻撃の検知

Locality-disruption 攻撃の検知を行うために，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．ICEM 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 (3) で算出される．

$$DR_i = (1 - HitRatio_i) \cdot \frac{1}{\beta - 1} \frac{1 - \sum_{j=1}^{CSsize} r_{ij}}{\sum_{j=1}^{CSsize} r_{ij}}, \quad (3)$$
$$(0 \leq DR_i \leq 1)$$

ここで，$\beta(\beta \geq 1)$ は CS サイズに対する検知区間の比である．検知区間が長くなるほど，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攻撃検知は遅くなる．$1 - HitRatio_i$ は Locality-disruption 攻撃の影響を示している．DR_i を急激に大きくさせるために，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影響度を示す．式 (3) より，DR_i が大きくなると要求の影響度も高くなる．

DR_i が式 (4) を満たすとき，ルータは攻撃を検知する．

$$DR_i > T_D, \qquad (0 \leq T_D \leq 1) \qquad (4)$$

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．

3.4　IFA の検知

IFA を検知するために，ICEM は Locality-disruption 攻撃の検知手法を使用する．ICEM 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．ICEM は IFA と Locality-disruption 攻撃を要求の量によって分別する．以下で検知の詳細を説明する．

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 は時間経過に伴い回復する．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 (5) で定義される．

$$IR_i(t) = IR_i(t-1) \frac{\sum_{j=1}^{CSsize} r_{ij}}{1 - \sum_{j=1}^{CSsize} r_{ij}}, (0 \leq IR_i(t) \leq 1) \quad (5)$$

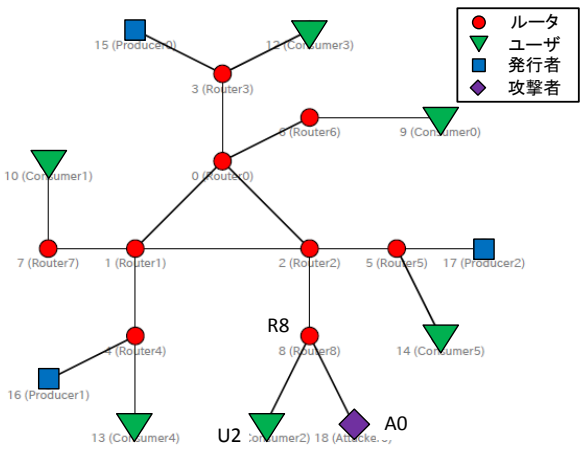


図 3　XC トポロジの概形

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 (6) を満たすとき，ルータは IFA を検知する．

$$IR_i < T_I, \qquad (0 \leq T_I \leq 1) \tag{6}$$

ここで，T_I は閾値である．

4. シミュレーション評価

提案手法 ICEM 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], [10] 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．この要求時間の差が関連研究における学習期間となる．しかし，ICEM は学習期間に依存しない手法であるため，攻撃がない期間とある期間の差を観察する目的で要求時間の差を設けている．通常ユーザは Zipf の法則 [11] 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．各ユーザが要求する Data の種類数は θ で表し，要求の強度は γ で表す．各通常ユーザは 10000 種類の Data を要求する．False-locality 攻撃または Locality-disruption

表 1　通常ユーザと攻撃者のパラメータ

パラメータ	通常ユーザ	攻撃者		
		FL[1]	LD[2]	IFA
要求時間	0 ～ 1800[sec]	900 ～ 1800[sec]		
Data の種類数 θ	10000	0 ～ 10000		10000
要求の強度 γ	10[pkt/sec]	10 ～ 1000[pkt/sec]		

[1] FL:False-locality

[2] LD:Locality-disruption

表 2　シミュレーションパラメータ

ネットワークシミュレータ	ns-3[12]
NDN モジュール	ndnSIM 1.0[13]
シミュレーション時間	1800[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	1024[byte]
リンクの帯域	10[Mbps]
リンクの遅延	10[ms]
α	0.1(LRU), 0.3(LFU)
$IR_i(t)$ の回復率	0.1 秒ごとに 5%
検知区間	500[pkt]

攻撃において攻撃者は要求する Data の種類数を 0 から 10000 で変動させる．一方で，攻撃者が IFA を実行する場合は 10000 種類の Data を要求する．各通常ユーザは一秒あたり 10 パケットを要求する．各攻撃者は攻撃の種類やキャッシュ置換方式に応じて要求の強度を変動させる．

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], [10]．PIT サイズは各ルータで 100 である．固定値である α，$IR_i(t)$ の回復率，検知区間の値は予備実験を基に決定した．通常ユーザの要求モデルが判明している場合，シミュレーションにより要求フローの特徴を抽出し固定値を決定することが可能である．

ICEM の攻撃検知分類性能を評価するために，以下の評価項目を設けた．

- ICEM における評価値
  提案手法のふるまいを確かめるために FR_i，DR_i，$IR_i(t)$ を使用する．これらの値は式 (1)，式 (3)，式 (5) で算出される．

4.2 攻撃の検知分類性能の評価

図 4 は LRU および LFU における FR_i と攻撃者の Data の種類数の関係について示したものである．実線は LRU を用いた場合の結果であり，破線は LFU を用いた場合の結果である．攻撃の強度は LRU が一秒あたり 10 パケット，LFU が一秒あたり 102 パケットとなる．LFU は要求が少ないコンテンツのキャッシュが置換されるため，攻撃者の強度を高くすることで攻撃者の Data がキャッシュされ続けるようにしている．この結果は R8 の観測結果であ

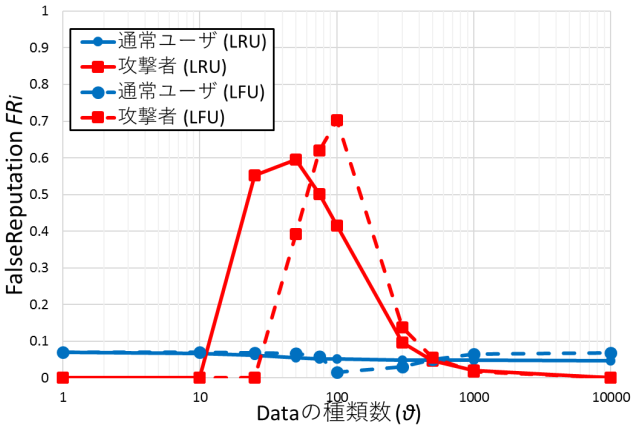


図 4　FR_i の値と Data の種類数の関係

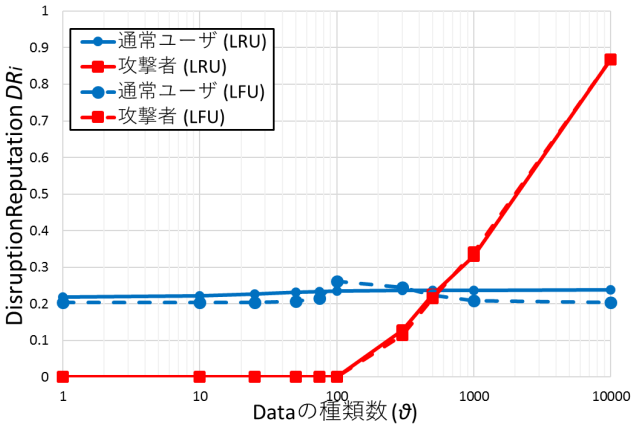


図 5　DR_i の値と Data の種類数の関係

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，今回のシミュレータ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ルータでの観測を行った．横軸が False-locality 攻撃者の Data の種類数を表している．通常ユーザは U2 に接続しているインタフェースの FR_i を表し，攻撃者は A0 に接続しているインタフェースの FR_i を表している．FR_i の値は攻撃期間の平均を取っている．この図より，LFU における FR_i の値は Data の種類数が CS サイズに近づくほど大きくなることがわかる．また，LRU における FR_i の値は Data の種類数が 50 のときに最大となり，以後 Data の種類数の増加に伴い値は減少しているが，全体として Data の種類数が CS サイズ以下であるときに大きな値となっていることがわかる．LFU は弱い False-locality 攻撃に強いため，LFU における FR_i の値の変動は LRU よりも大きい．以上の結果は ICEM が FR_i を算出することで通常ユーザと False-locality 攻撃者の要求フローを区別できることを示している．ICEM は閾値 T_F の値を 0.3 に設定することで False-locality 攻撃を検知する．

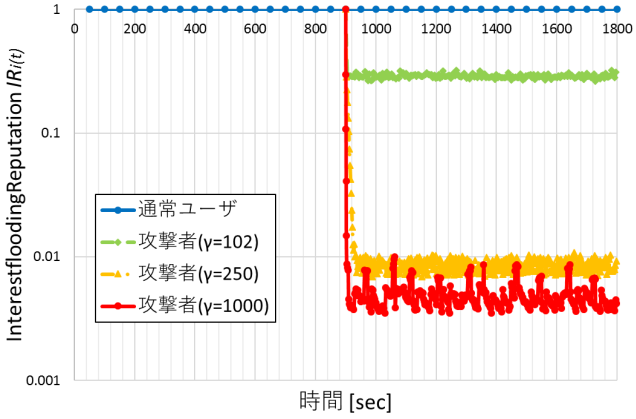


図 6　攻撃の強度による $IR_i(t)$ の値の変動

図 5 は LRU および LFU における DR_i と攻撃者の Data の種類数の関係について示したものである．攻撃の強度および評価値の観測場所については False-locality の実験と同様である．この図で示したように，攻撃者の DR_i の値は Data の種類数の増加に伴い急激に増加する．攻撃の強度は異なるが，結果の値は LRU の場合も LFU の場合もほぼ同じである．これは Locality-disruption 攻撃の検知は攻撃の強度にあまり依存しないためである．以上の結果は ICEM が DR_i を算出することにより通常ユーザと Locality-disruption 攻撃者の要求フローを区別できることを示している．通常の要求がしばしば Locality-disruption と同様になることを踏まえ，ICEM は閾値 T_D の値を 0.6 に設定することで Locality-disruption 攻撃を検知する．

図 6 は LRU における $IR_i(t)$ の時間変動を示している．LRU を用いる場合と LFU を用いる場合の結果はほぼ変わらないため，LRU 時の結果のみを示している．攻撃の強度は一秒あたり 102 パケット，250 パケット，1000 パケットで変動させている．評価値の観測場所については False-locality および Locality-disruption の実験と同様である．インタフェース i の要求フローが Locality-disruption 攻撃であると判断されたとき，$IR_i(t)$ の値は減少する．通常ユーザの要求は Locality-disruption 攻撃と判断されていない．したがって，通常ユーザの $IR_i(t)$ の値は初期値である最大値を維持する．$IR_i(t)$ の値が減少するとき，その評価値は時間経過に伴い回復する．評価値の回復率が減少率を上回った場合，評価値は最大値とはならないが高い値を維持する．減少率は検知の頻度と DR_i の値に依存する．IFA と同義である強力な Locality-disruption 攻撃は攻撃者が頻繁に Data を要求して検知が多く行われるため減少率は高くなる．結果として，攻撃の強度に応じて評価値の大小が決定する．今回のシミュレーションにおいては，攻撃者の要求が一秒間に 250 パケットを超えるものを IFA とする．ICEM は閾値 T_I の値を 0.01 に設定することで IFA を影響が大きい Locality-disruption として区別する．

5. おわりに

本稿では，NDN における DoS 攻撃の検知分類手法である ICEM を提案した．ICEM は要求フローから Interest 量，Data 種類，要求分布の三つの特徴を抽出して要求を四つに分類する．ICEM においてルータはインタフェースに対し評価値 FR_i，DR_i，$IR_i(t)$ を算出し，これらの評価値を閾値と比較することにより攻撃の検知分類を行う．これらの検知分類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 ICEM の攻撃検知分類の性能を評価した．シミュレーション結果より，提案手法の評価値は攻撃者と通常ユーザにおいて差があり，通常ユーザの要求と攻撃者の要求を区別できることを確認した．また，攻撃の要求フローの違いによって FR_i，DR_i，$IR_i(t)$ の値の変動に差が出ることを確認し，DoS 攻撃を攻撃の種類によって分類できることを確認した．

以上より，提案手法は DoS 攻撃を検知分類することが可能であり，DoS 攻撃の種類に応じた対策を行う際に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, *Proceedings of the 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 h. Roh, B.: 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 Transactions on 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, *INFOCOM, 2012 Proceedings IEEE*, pp. 2426–2434 (2012).

[8] 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).

[9] 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).

[10] 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).

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

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

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