Vol.2018-DPS-173 No.7
2018/1/19

キャッシュ参照回数を基準とした NDNにおける共謀型IFA対策手法の提案

園田 彩香[1,a)]　重安 哲也[1,b)]

概要：NDNでは，コンテンツルータのキャッシュを有効利用することによりトラフィックやコンテンツ取得遅延を短縮する．しかしながら，コンテンツ要求の転送情報を記録するPITエントリをネットワーク上のサーバと共謀してオーバフローさせることで，コンテンツ配信を阻害する共謀型IFAによってNDNの性能が大きく低下することが指摘されている．本論文では，共謀型IFAでコンテンツルータ上に蓄積されたキャッシュがその後に再利用されないことに着目し，これを参照することで共謀型IFAの検知ならびに，対策を行う手法を提案する．

A Proposal for Coping with Collusive IFA According to Frequency of Cache Reference on NDN

Ayaka Sonoda[1,a)]　Shigeyasu Tetsuya[1,b)]

Abstract: NDN can reduce amount of traffic and contents acquisition delay by utilizing the cached contents on Contents Router (CR). The NDN, however, can not effectively work when the malicious user attacks to the CR by collusive with the illegal provider on the network. In this paper, the authors propose to detect such CIFA attack by referring frequency of cache usage on CR, and clarify the proposal well works for reducing effect of CIFA on NDN.

1. はじめに

近年，ネットワークは写真や動画，テキストなどのコンテンツ配信に主に利用されており，トラフィック量は膨大となっている [1]．そのため，これらの通信の実施はネットワーク帯域を圧迫し，遅延や輻輳を発生させてしまう．しかしながら，コンテンツ配信の観点からは，ユーザは要求するコンテンツを取得できれば問題ないため，コンテンツを「どこから」取得するかではなく，「何を」取得するかが今後のトラフィック急増対策を検討する上での重要な視点である．

そこで，現在のIPネットワークに代わるネットワークアーキテクチャとしてNDN (Named Data Networking) が注目を集めている [1][2]．NDNは，IPネットワークにおける位置識別子にあたるIPアドレスに代えて，コンテンツそのものを指し示す識別子であるコンテンツ名を用いて通信を行う．また，これに加えて，コンテンツプロバイダだけでなく，中継ルータからもユーザは，要求するコンテンツを取得することができる．そのため，NDNではコンテンツプロバイダへの負荷集中を避けることができ，ユーザの要求に対する応答時間を大幅に短縮できる可能性を有する [3]．また，ユーザのコンテンツ要求を伝達するパケットであるInterestの履歴を中継ルータのPIT (Pending Interest Table) に記録することで，NDNは従来ネットワークの位置依存から完全に脱却して確実なコンテンツ配信を実現する．

しかし，NDNでは，その実運用を想定する上で，現在，様々なセキュリティ攻撃に対する対策が検討されている [4]．一般的に，攻撃者がネットワーク機器や回線に対して負荷をかけ，通常ユーザのサービス利用を妨害する攻撃をDoS

[1] 県立広島大学経営情報学科
Department of Management and Information System, Prefectural University of Hiroshima , Japan
[a)] q404019fw@ed.pu-hiroshima.ac.jp
[b)] sigeyasu@pu-hiroshima.ac.jp

(Denial of Service) 攻撃と呼ぶ [5]．NDN では，DoS 攻撃と同種の効果を狙った攻撃として，IFA (Interest Flooding Attack) 攻撃の危険性が指摘されている [6]．IFA は，攻撃者が実在しないコンテンツを要求する Interest を大量にネットワークに送出することで，中継ルータの PIT をオーバフローさせ，通常ユーザのコンテンツ取得を妨害する攻撃である [7]．しかしながら，この種の IFA では攻撃者に対して Data が返送されないため，攻撃者からの Interest を中継するコンテンツルータにおいて実在しないコンテンツに対する Interest の送信を検査することで，IFA 対策は十分に可能であることが報告されている [9][10]．本稿では，この IFA を通常型 IFA と呼ぶ．

さて，通常型 IFA の発展型として共謀型 IFA 攻撃の危険性も指摘されている．この共謀型 IFA は，通常型 IFA と同様に中継ルータの PIT オーバフローを目的とするが，攻撃者であるエンドホストと悪意のあるコンテンツプロバイダが共謀することで，攻撃者に対しても Data が返送されることが通常型 IFA と大きく異なる．そのため，通常ユーザと攻撃者の区別が曖昧なため，攻撃対策が困難とされている．

そこで本稿では，各ルータが保持するキャッシュの参照回数を基準とし，共謀型 IFA を緩和する手法を提案し，計算機シミュレーションによって，通常ユーザのコンテンツ取得率への影響を大きく軽減できることを明らかにする．

2. NDN

NDN は，コンテンツ要求パケットである Interest と，コンテンツ応答パケットである Data の二種類のパケットを使用する [8]．コンテンツ名は，’/’ で区切られた階層構造を持ち，プレフィックスとサフィックスという部分に分けられる．’/’ で区切られた先頭部分はプレフィックスと呼ばれ，コンテンツがどのプロバイダに格納されているかを示す．プレフィックス以降の部分はサフィックスと呼ばれ，プレフィックスとサフィックスを組み合わせたものが各コンテンツを識別するための ID の役割を果たす．

各ルータは，コンテンツをキャッシュする CS (Content Store)，Interest を受信したインタフェースと要求コンテンツ名を保持する PIT，Interest の転送先を記録する FIB (Forwarding Information Base) の三つのテーブルを保持する．

図 1 に NDN の概要を示す．Interest を受信したルータは，まず，要求コンテンツが自身の CS にキャッシュされているか確認する．ここで，要求コンテンツがキャッシュされていれば対応するコンテンツを Data として返信し，そうでなければ PIT を確認する．既に同じ名前のコンテンツが要求された記録があれば，Interest の到着インタフェースをその記録に追加し，その Interest を破棄する．記録がなければ，PIT に Interest の情報と到着インタフェースを記録し，FIB を参照した後，Interest を自身の上流ルータに転送する．その後，返信された Data を受信したルータは，自身の PIT を参照し，対応する Interest の到着インターフェースに Data を転送し，その PIT エントリを削除する．また，自身の CS にその Data に含まれるコンテンツがキャッシュされていなければ，そのコンテンツを自身の CS にキャッシュする．

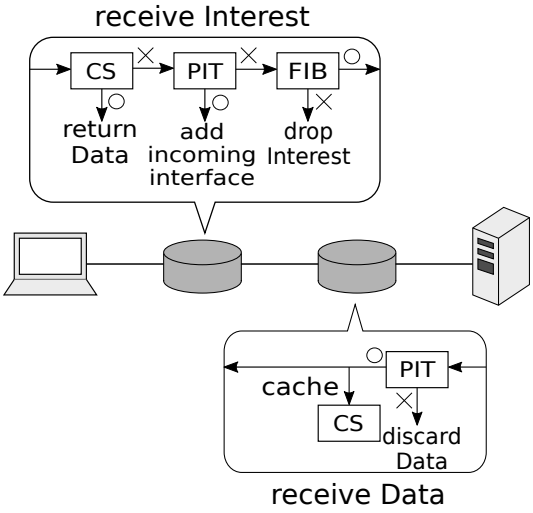

図 1 NDN の概要
Fig. 1 Overview of NDN.

3. 関連研究

3.1 Interest Flooding Attack

Interest Flooding Attack（IFA）は，実在しないコンテンツを要求する Interest を攻撃者が大量にネットワーク中に送信し，中継ルータ上の PIT をオーバフローさせることで，Data の返信を不可能にする．攻撃者の Interest は，重複したコンテンツを要求しないために，ランダムなサフィックスが付与されている．これは，中継ルータに同一にコンテンツが要求された履歴がある場合，そのコンテンツを要求すると PIT に受信インタフェースの情報だけが追加され，Interest そのものが破棄されてしまい，攻撃の影響が弱まるのを防ぐためである．以降本稿では，これを通常型 IFA と呼ぶことにする．

図 2 に，通常型 IFA の概要を示す．ここで，通常ユーザが”/*host*0/0”というコンテンツを要求する Interest を送信すると，中継ルータの PIT に Interest 履歴が記録される．しかし，悪意のあるユーザ（攻撃者）からの IFA 攻撃が開始されると，攻撃者は”/*host*0/”というプレフィックスの後に，ランダムなサフィックスを付与した Interest を大量に送信し，実在しないコンテンツを要求する．そうすると，中継ルータの PIT は攻撃者の PIT エントリで埋め尽くされ，先に記録されていた通常ユーザの PIT エントリがオーバフローする．コンテンツプロバイダが送信した Data は，これを受信した中継ルータの参照する PIT エントリに対

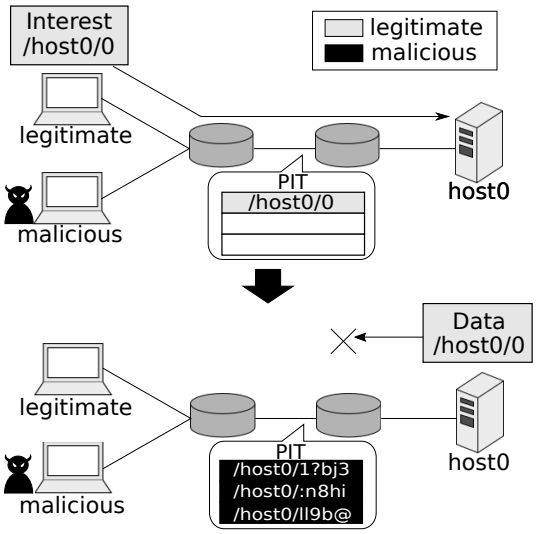

図 2　IFA の概要
Fig. 2　Overview of IFA.

応するものが存在しなければ，転送不能と判断され，破棄されるため，通常ユーザの元まで Data は返送されない．

ここで，攻撃者は実在しないコンテンツを要求するため，対応する Data は返信されない．そのため，各プレフィックス毎の Interest に対する Data の返信率（Interest 充足率）を中継ルータが算出することで，通常ユーザの Interest 充足率は高く，攻撃者の Interest 充足率は低くされるために，攻撃の有無を容易に検出できる．

通常型 IFA 対策の既存手法として，文献 [9] の ICRP や文献 [10] の IFBRN がある．ICRP は，ユーザと隣接するルータがユーザに対して，Interest 充足率やコンテンツの要求回数を算出し，評価を行う．攻撃者の Interest と特定されたプレフィックスの Interest は，転送を制限される．

また，IFBRN は，中継ルータが各インタフェースに対して，Interest 充足率や PIT エントリ数を算出し，他のインタフェースと比較することで評価を行う．攻撃者の Interest が自身に流入していると判断した場合，中継ルータはそのインタフェースからの Interest を PIT に記録せず，転送も行わない．

これらの手法は，通常型 IFA には有効であるが，Interest 充足率を用いる点から，攻撃者に対して Data の返送がある共謀型 IFA には適用できない．

3.2　共謀型 IFA

共謀型 IFA では，攻撃者がコンテンツプロバイダと共謀して，攻撃者の Interest に対して意味のない Data を返信する．そのため，前節で述べた通常型 IFA の対応策である Interest 充足率の算出手法では，中継ルータでの攻撃検出はできなくなる．

共謀型 IFA 対策の既存研究として，パケットホップ数を用いた手法 [11] やドメインコントローラを用いた手法 [12]

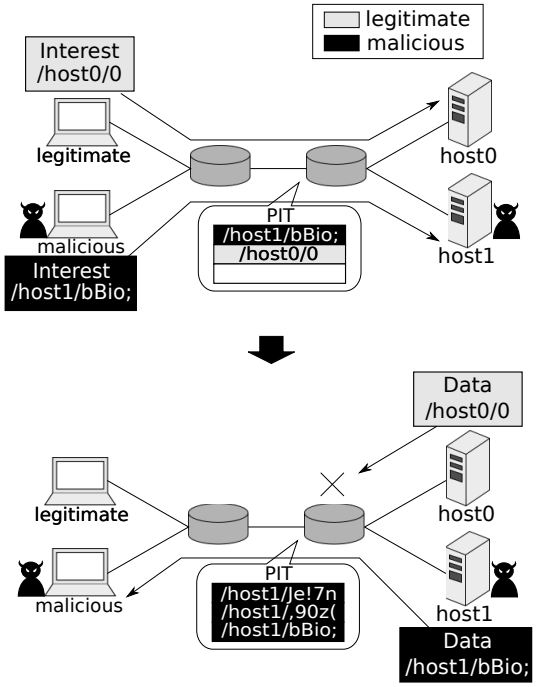

図 3　共謀型 IFA の概要
Fig. 3　Overview of Collusive IFA.

がある．パケットホップ数を用いた手法は，Data のホップ数の平均値及び分散を比較し通常ユーザと攻撃者を分別する．ここで，同手法ではパケットホップ数の平均値が小さく，分散が大きいものを通常ユーザ，平均値が大きく，分散が小さいものを攻撃者と判定する．しかし，同手法は通常ユーザが多くの人気のないコンテンツを要求した場合，キャッシュヒットせずにコンテンツプロバイダから Data が返送される可能性が高くなるため，通常ユーザが攻撃者と誤検知されてしまう危険性がある．

一方，ドメインコントローラを用いた手法は，自身の PIT 情報をドメインコントローラに送信するモニタリングルータと，受信した PIT 情報を収集し攻撃検知を行うドメインコントローラを利用する．ドメインコントローラは収集した情報を分析し，攻撃の有無を判断した結果をモニタリングルータに通知する．モニタリングルータは受信した結果を元に，攻撃を緩和する．しかし，同手法はドメインコントローラを攻撃の対象にされた場合に，攻撃の有無を正常に判断できない可能性がある．

これらから，共謀型 IFA の対策には，通常ユーザを攻撃者と誤検知することなく，攻撃の対象が分散されるよう各ルータで攻撃検知，また攻撃緩和を行う必要があると考えられる．

4.　提案手法

4.1　提案手法の概要

本節では，中継ルータのキャッシュが参照された回数（以下，参照回数）をプレフィックス毎に算出した値を基準

として，攻撃に使用されるプレフィックスを特定し，攻撃者の Interest の流入を制限する手法を提案する．

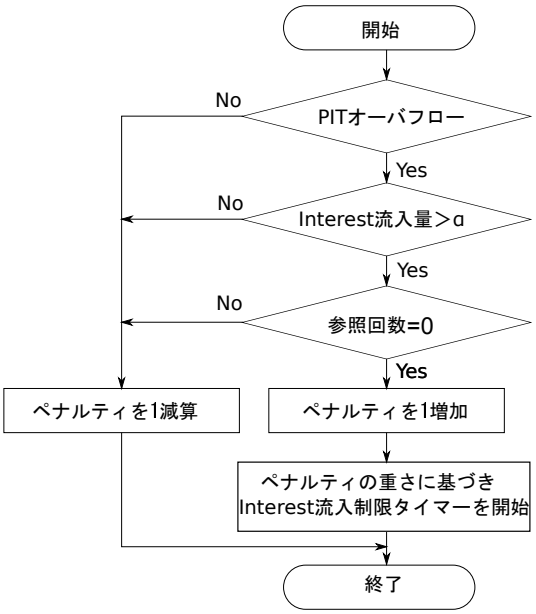

図 4　攻撃検知の動作手順
Fig. 4　A prediction procedure for Collusive IFA.

提案手法は，三段階の判別条件を全て満たしたプレフィックスを攻撃に使用されるプレフィックスとみなし，ペナルティの重さに応じて Interest の流入を制限する時間を設定する．同手法では，全ての中継ルータは一定時間毎に攻撃者判定を行う．ここで同手法で三段階の判別を行う際に着目する点は，PIT オーバフロー，Interest 流入量，参照回数である．

図 4 に，攻撃検知の動作手順を示す．まず，中継ルータに自身の PIT サイズを超える Interest 量が到着し，PIT の置換が起きている場合，PIT オーバフローが生じていると判断する．これは，PIT エントリが溢れると，通常ユーザが要求した Data が返送されなくなるためである．

PIT オーバフローが生じていると判断された場合，次は，プレフィックス毎の Interest 流入量を検査する．共謀型 IFA において，攻撃者は共謀するコンテンツプロバイダまで，自身の Interest を配送するために同一のプレフィックスの Interest を大量に使用する．そのため，流入数が多いプレフィックスの Interest は攻撃者の可能性があると考える．ここで閾値 α は，リンクの速度や遅延を考慮し，決定する．

Interest 流入量が過多であると判断された場合，提案手法では次に参照回数に着目する．攻撃者の Interest は，重複したコンテンツを要求しないため，中継ルータ上に蓄積されたキャッシュを再利用しない．したがって，参照回数は 0 回であると考えられる．そのため，この三段目の判定で参照回数が 0 回であると判明した場合，そのプレフィックスは攻撃に使用されているものだと判断する．

三段階の判別条件を全て満たしたプレフィックスを攻撃に使用されているものと判断する，

4.2　ペナルティの導入

通常ユーザが人気のないコンテンツを大量に要求した場合，通常のコンテンツのプレフィックスが誤検知される可能性があるため，制限を解除する必要がある．しかし，検知時間毎にプレフィックスの判定・制限を行うとすると，攻撃プレフィックスの Interest の制限が開始されたタイマー期間では，前節の三つの条件を満たさないため，直後には制限が解除される．そのため，前節の判別条件を全て満たしたプレフィックスには，その都度ペナルティを付与し，ペナルティの値が大きいプレフィックスほど，Interest の流入の制限時間を長く設定する．ペナルティを付与することで，通常のコンテンツのプレフィックスが誤検知され，制限されたとしても，制限時間が短いため，すぐに制限が解除される．

反対に，攻撃プレフィックスの Interest は，前節の判別条件を満たす回数が多いために，ペナルティの値が大きくなり，攻撃検知される毎に制限時間が長く設定される．そうすると，ペナルティを導入しない場合と比較して攻撃プレフィックスの Interest を制限する時間が長くなるため，より攻撃の影響を抑制することができる．

実際に導入するペナルティの概要について述べる．ペナルティの値の初期値は 0 であり，攻撃に使用されていると判断されたプレフィックスは，ペナルティが 1 増加する．反対に，いずれか一つの条件でも当てはまらない場合，ペナルティを 1 減算する．ペナルティの値は，Interest の流入を制限する時間の長さに反映する．なお，本稿の性能評価の際は，ペナルティが 3 である場合，そのプレフィックスの Interest の流入を 3 秒制限するタイマを設定した．さて，Interest の流入が制限されている間は，一定時間毎にタイマを 1 ずつ減算していく．その後タイマが 0 になると，制限が解除され，この Interest の受信・転送を再開するとともに，検知対象としての監視を再開する．

5.　性能評価

5.1　シミュレーション環境

提案手法により通常ユーザのコンテンツ取得率が改善できることを示すために，コンテンツ取得率を算出した．シミュレーションに用いたトポロジを図 5 に，シミュレーション条件を表 1 にそれぞれ示す．ノード 0 が通常のコンテンツプロバイダで，n をサフィックスの最大値とすると”$/host0/0$”～”$/host0/n$”の $n+1$ 種類のコンテンツを保持しており，ノード 1 は攻撃者の共謀コンテンツプロバイダで，攻撃者に対して意味のないコンテンツを返信する．ノード 8，10 は通常ユーザで，”$/host0/0$”～”$/host0/n$”の $n+1$ 種類のコンテンツを Zipf 則に従って要求し，ノード

7，9，11 は攻撃者で，”/*host*1/”というプレフィックスの後に意味のないランダムなサフィックスを付与し，要求する．Interest 生成レートは，通常ユーザは 10[pkt/sec] で，攻撃者は 320-3020[pkt/sec] と変化させる．CS と PIT の置換方式はどちらも，先に記録されたものから破棄する FIFO とする．攻撃検知は，1 秒毎に実行する．閾値 α はシミュレーションに使用するリンクが 1 秒間に約 110[pkt] 転送できるとして，110 に設定する．

比較対象は，攻撃緩和手法が導入されていない場合と，ペナルティを導入しない場合とした．

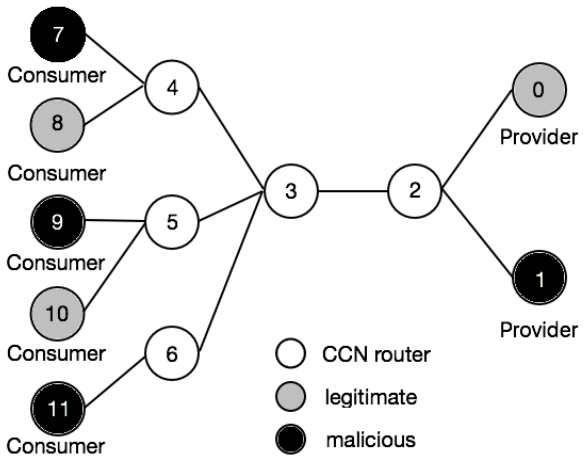

図 5　シミュレーショントポロジ
Fig. 5　Simulation topology.

表 1　シミュレーション条件
Table 1　Simulation conditions.

Parameter	Value
legitimate provider ID	0
malicious provider ID	1
legitimate consumer ID	8, 10
malicious consumer ID	7, 9, 11
NDN router ID	2, 3, 4, 5, 6
Interest generation rate (legitimate)	10 [pkt/sec]
Interest generation rate (malicious)	320-3020 [pkt/sec]
Interest Packet	1024 [bytes]
Data Packet	1024 [bytes]
CS size	10
PIT size	50
link rate	1[Mbps]
link delay	1[msec]
α	110
simulation period	100 [sec]

5.2　シミュレーション結果

図 6 は，攻撃緩和手法が導入されていない場合のコンテンツ取得率である．同図より，Interest 生成レートが 1,020[pkt/sec] 付近で通常ユーザと攻撃者のコンテンツ取得率が急激に 10 %以下まで低下していることがわかる．これは，中継ルータの PIT エントリが大量に到着した Interest によりオーバフローするために，Data の返信経路が消失したためと考えられる．

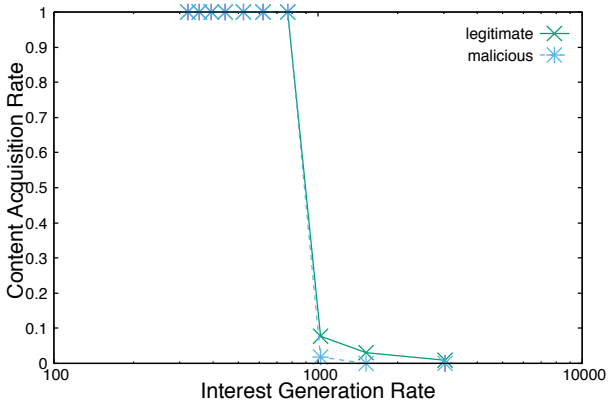

図 6　攻撃緩和手法を導入していない場合のコンテンツ取得率
Fig. 6　Content acquisition rate without mitigation.

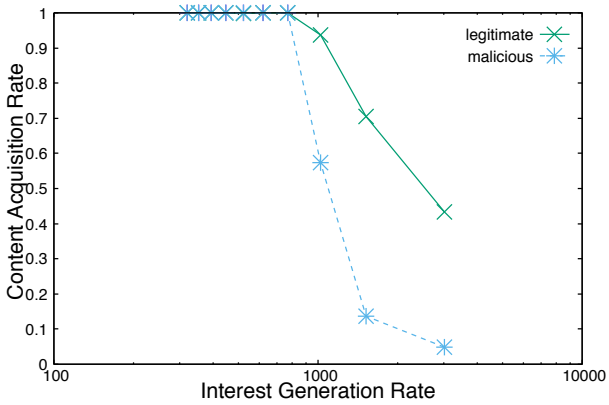

図 7　ペナルティを導入しない場合のコンテンツ取得率
Fig. 7　Content acquisition rate without penalty.

図 7，図 8 は提案手法を実装した時のコンテンツ取得率であり，図 7 はペナルティを導入しない場合，図 8 はペナルティを導入した場合である．図 7 より，図 6 と比較すると，通常ユーザのコンテンツ取得率が少し改善していることがわかるが，攻撃の影響を大きく受けたままである．これは，攻撃者の Interest のプレフィックスに対して，流入の制限と解除を交互に繰り返しており，Interest の流入制限時間はシミュレーション時間の半分ほどしかないためと考えられる．

図 8 より，図 6 と比較すると，攻撃の影響が現れ始めた Interest 生成レートが 1,020[pkt/sec] 以降，コンテンツ取得率が約 85 %改善していることがわかる．また，図 7 と比較しても，攻撃の影響が現れてはいるものの，コンテンツ取得率の低下が大幅に改善されていることがわかる．したがって，ペナルティを導入することにより，攻撃者の Interest の影響をより抑制できていると考えられる．

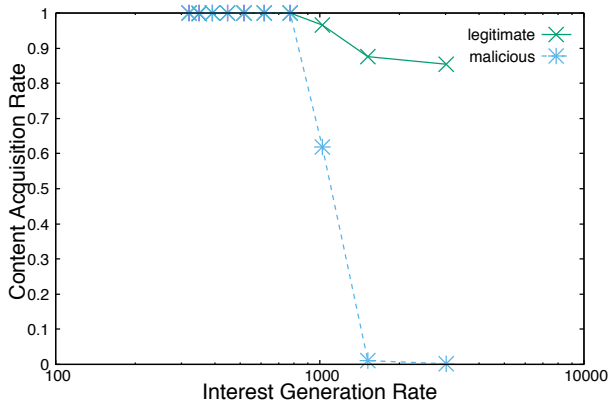

図 8　ペナルティを導入した場合のコンテンツ取得率
Fig. 8　Content acquisition rate with penalty.

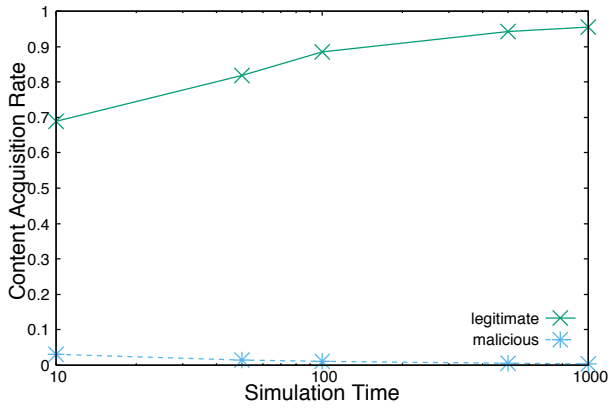

図 9　Interest 生成レート 1,250[pkt/sec] の時のコンテンツ取得率
Fig. 9　Content acquisition rate when Interest generation rate is 1,250 [pkt / sec].

図 9 に，Interest 生成レートが 1,020pkt/sec] の時にシミュレーション時間を変化させた場合のコンテンツ取得率を示す．シミュレーション時間が長くなるにつれ，通常ユーザのコンテンツ取得率が上昇し，攻撃者のコンテンツ取得率が低下していることがわかる．これは，シミュレーション開始から時間が経過するとペナルティが長くなり，攻撃者の Interest が制限される時間が長くなるためである．攻撃の影響が軽減されるため，通常ユーザのコンテンツ取得率は改善される．

6. おわりに

本稿では，共謀型 Interest Flooding Attack 対策として，CS のコンテンツの参照回数をプレフィックス毎に算出した値を基準とし，攻撃プレフィックスを特定する手法を提案した．計算機シミュレーションにより，提案手法は通常ユーザのコンテンツ取得率を攻撃緩和手法がない場合と比較して，コンテンツ取得率を約 85 %改善することを明らかにした．また，共謀型 IFA 攻撃として判定された Interest に対する転送制限時間長にペナルティを導入することにより，攻撃プレフィックスの Interest を制限する時間をその影響度合いに応じ，適応的に設定可能にすることで，攻撃の影響をより抑制できることを確認した．そして，シミュレーション時間が長くなるほど，攻撃プレフィックスのペナルティの値が大きくなるため，攻撃緩和の効果が大きくなることを確認した．したがって，提案手法は共謀型 Interest Flooding Attack に対して有用性があることが示された．

参考文献

[1] 山本幹, “コンテンツオリエンテッドネットワーク,” 電子情報通信学会誌, vol. 95, no. 4, pp. 341-346, 2012.
[2] 中里秀則, “コンテンツ指向型ネットワーク,” 映像情報メディア学会誌, vol. 69, no. 3, pp. 253-255, 2015
[3] 朝枝仁, “情報指向ネットワークがもたらす可能性と研究課題,” 情報通信研究機構研究報告, vol. 61, no. 2, pp. 113-117, 2015
[4] 永井翔平, 水野修, “コンテンツセントリックネットワークのユーザプライバシ保護のためのコンテンツ取得方式,” 電子情報通信学会技術研究報告, IN, vol. 116, no. 485, pp. 109-114, 2017-02-23
[5] 武藤展敬, 佐藤直, “帯域制御を利用した Dos 攻撃対策,” 情報処理学会研究報告, CSEC, vol. 2008, no. 122, pp. 7-12, 2008-11-28
[6] 篠原涼希, 神本崇史, 重野寛, “Named Data Networking における要求フローに特徴を使用した 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, vol. 2017, pp. 85-91, 2017-10-04
[7] 篠原涼希, 神本崇史, 梅田沙也華, 重野寛, “Interest Flooding Attack によるルータへの負荷集中と対策,” 第 78 回全国大会講演論文集, vol. 2016, no. 1, pp. 161-162, 2016.
[8] 朴容震, “情報指向ネットワーキングの研究動向,” GITS, GITI research bulletin 2012-2013, pp. 8-13, 2014-04-29
[9] 梅田沙也華, 神本崇史, 大畑百合, 重野寛, “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,” 情報処理学会論文誌, vol. 57, pp. 1816-1825, 2016-08-15
[10] 篠原涼希, 神本崇史, 梅田沙也華, 重野寛, “Named Data Networking における Interest 記録数を考慮した Interest Flooding Attack 対策,” マルチメディア，分散協調とモバイルシンポジウム 2016 論文集, vol. 2016, pp. 336-343, 2016-07-06
[11] 中塚義道, 西宏章, “Named Data Networking におけるパケットホップ数を用いた Interest Flooding Attack の検知及び緩和手法,” 電子情報通信学会技術研究報告, CPSY, vol. 116, pp. 327-332, 2017-03-02
[12] H. Sarah and T. Strufe, “Evaluating and mitigating a Collusive version of the Interest Flooding Attack in NDN,” Proc. of 2016 IEEE Symposium on Computers and Communication (ISCC) , pp. 938-945, 2016.