情報処理学会論文誌 Vol.63 No.9 1410–1418 (Sep. 2022)

拡散型フロー制御を用いるDDoS攻撃緩和方式の有効性評価

奥田 尚樹[1,a)] 前田 香織[1] 高野 知佐[1] 市原 英行[1]

受付日 2021年12月8日, 採録日 2022年6月14日

概要：サイバー空間に脅威を与えるサイバー攻撃の１つ，DDoS（Distributed Denial of Service）攻撃は，攻撃トラヒックサイズが増幅する傾向にあり，その規模は数テラ bps に到達している．これに対して DDoS 攻撃の被害を抑える DDoS 攻撃緩和システムが提案されている．特に，サービス継続のために緩和期間中に攻撃外の正常通信のパケット損失を防ぐことが重要である．本稿では，サービス継続を目的として拡散型フロー制御を用いる DDoS 攻撃緩和方式を提案し，その有効性を示す．この方式は，DDoS 攻撃元から攻撃対象までのルータ等をオーバレイネットワークで構成し，ノードのバッファあふれまでの時間（緩和時間）を拡散型フロー制御により，伸ばすものである．このとき攻撃トラヒックの転送レートの算出が必要となるが，本稿では既存の算出式を改良することにより，従来できてなかった各ノードのバッファ容量のばらつきがある実ネットワークに近い場合の緩和時間を伸ばすことができることを示す．また，DDoS 攻撃の攻撃規模が増大した場合についても，攻撃規模に応じた適切なネットワーク資源の配分を行うことで，十分に緩和の効果を発揮できることを示す．

キーワード：ネットワークセキュリティ，DDoS 攻撃，DDoS 攻撃緩和，拡散フロー制御

An Effectiveness Evaluation the DDoS Mitigation Method Based on Diffusion Flow Control

Naoki Okuda[1,a)] Kaori Maeda[1] Chisa Takano[1] Hideyuki Ichihara[1]

Received: December 8, 2021, Accepted: June 14, 2022

Abstract: DDoS (Distributed Denial of Service) attacks, which are one of the cyber attacks that pose a threat to cyberspace, tend to increase the attack traffic size, and the scale has reached several Tera bps. On the other hand, a DDoS attack mitigation system that suppresses the damage of DDoS attacks has been proposed. In particular, it is important to prevent packet loss of normal communication outside the attack during the mitigation period in order to continue the service. In this paper, we propose a DDoS attack mitigation method that uses diffuse flow control for the purpose of service continuity, and show its effectiveness. In this method, routers from the DDoS attack source to the attack target are configured with an overlay network, and the time (mitigation time) until the node buffer overflows is extended by diffuse flow control. At this time, it is necessary to calculate the transfer rate of the attack traffic. The proposed calculation method in this paper by improving in the existing one can extend the mitigation time in the case of actual networks of which the buffer capacity of each node varies. This case is not focused in the existing method. Shows that can be stretched. The paper also shows that even when the attack scale of a DDoS attack increases, tour proposed method is useful the paper by allocating appropriate network resources according to the attack scale.

Keywords: network security, distributed denial of service attack, DDoS mitigation, diffusion flow control

1. まえがき

サイバー空間に脅威を与えるサイバー攻撃の１つ，DDoS（Distributed Denial of Service）攻撃は，攻撃トラフィッ

[1] 広島市立大学
Hiroshima City University, Hiroshima 731–3194, Japan
[a)] okuda@v6.netsci.info.hiroshima-cu.ac.jp

クサイズが増幅する傾向にあり，その規模は数テラ bps に到達している．たとえば，Amazon Web Services は 2020 年 2 月に 2.3 Tbps の DDoS 攻撃を受けたことを報告している [1]．また，コロナ禍によるオンラインサービスの需要の増加により，標的が増えたことから DDoS 攻撃の件数が 2020 年第 1 四半期は前年同期比で 25%増加という報告も出ている [2]．さらに，国内においても，攻撃者が標的とする組織宛に DDoS 攻撃を示唆するメールを送り，仮想通貨による送金を要求する事案が発生しており，この攻撃では，攻撃能力を示すためとして，数十 Gbps から 100 Gbps 程度の規模で標的に対して DDoS 攻撃を行ったことが報告されている [3]．DDoS 攻撃は，その頻度や影響度も大きくなっており，引き続き，DDoS 攻撃の脅威に対する対策が必要である．

DDoS 攻撃の緩和のために，事前に防御すべき（標的の可能性となる）サーバやネットワークの定常的なトラフィックパターンを調査し，それに基づいて事前に緩和対応策を実施する事前対応型と攻撃を確認した後に緩和対応をする事後対応型がある．事前対応型には Akamai 社のサービスとして提供されているものもある．事後対応型は一定時間トラフィックの観察や，緩和できるまでの時間がかかるものの，事前対応型のような事前準備は不要である．事後対応型では，攻撃の検知，攻撃元から標的までの複数の経路で攻撃トラフィックを排除や分散する等して，標的への攻撃が及ぶまでの時間の短縮が重要となる．そのために，ルーティングアルゴリズム，ブロックチェーン，機械学習等を適用した様々な緩和手法が提案されている [4], [5], [6]．

著者らも物理現象である拡散現象を指導原理とした自律分散制御を用いて DDoS 攻撃トラフィックの集中を緩和する，事後対応型の手法を提案している [7]（以下，既存方式と呼ぶ）．既存方式 [7] では，標的までの経路上に大量の攻撃トラフィックを緩和するための装置をおき，標的そのものへのトラフィックを緩和する方式である．この方式による緩和により，標的が攻撃の被害を受ける（サービス妨害が発生する）まで時間に猶予をもたせ，その間に攻撃元の特定とフィルタリング等の対策を講じることを想定している．そのため，緩和可能な時間（以降，緩和時間）が長い方がよいが，既存方式 [7] では緩和装置におけるトラフィックの分散パターンやバッファ容量が固定した限定的な制御をしていることから，緩和すべき対象のネットワークのトポロジの構成によっては，経路上での緩和装置のバッファのあふれが早期に起こる．すなわち緩和時間が極端に短くなる．この限定的な制御は，実際の緩和装置や動的なトラフィック変化に即しておらず，より柔軟な制御が必要である．

そこで，本稿では偏りのあるトポロジ（たとえば，完全 2 分木のような子ノード数や葉ノードの深さがすべて揃っているものではなく，子ノード数や葉ノードの深さに違いがあるようなもの）やバッファ容量のばらつきがある場合にも，より長い緩和時間を確保することを目的として，既存方式 [7] を改良する．具体的には，バッファリングノードで形成するオーバレイネットワークのトポロジのタイプやバッファ容量等の偏りのあるトポロジやバッファ容量のばらつき等，ネットワーク状態が不均衡である場合にも，より安定した性能を確保することを目的として，ノード間のパケットの転送を制御している転送レート算出式を改良することで，より長時間パケット損失を防ぐことを可能とする．また，既存方式 [7] と本稿で提案する方式について，シミュレーションを実施し，その結果を比較することで提案方式の有効性を評価する．

本稿の構成は，以下のとおりである．2 章で関連研究について，3 章で提案方式について述べる．4 章で改良方式を用いた DDoS 攻撃緩和システムについて，5 章でシミュレーションの評価について説明を行う．6 章でシミュレーション結果より考察を行い，最後に 7 章で本稿のまとめと今後の課題について述べる．

2. 関連研究

2.1 DDoS 攻撃の検知・対策

最近の DDoS 攻撃緩和（ミチゲーション）に関する研究は，以下のようなものがある．

文献 [4] では，攻撃を受けている疑いのある宛先への通信について，DDoS ミチゲーション装置を経由させることで，不正なトラフィックを検知し排除することを目的とし，ルーティングにより，「ミチゲーション装置」への経由をより効率的に実施するアルゴリズムが提案されている．また，文献 [5] では，分散された緩和装置間でブロックチェーンを用いたスマートコントラクトによるブラックリストやホワイトリストの制御情報を自動化し，共有することで攻撃を検知する手法が提案されている．さらに，文献 [6] で提案されている手法は，トラフィックの監視を行い攻撃検知するもので，その検知方法に過去のデータから，決定木アルゴリズム等の機械学習を用いて学習を行うことであり，誤検知を減らすとともに，未知の攻撃の検知も試みるものである．

これらの研究は，主に攻撃の検知を効果的に行うことに焦点をあてて，標的への攻撃を回避する提案で，本研究や本研究の先行研究である文献 [7] のように DDoS 攻撃の緩和により検知から対策までの緩和時間を確保して，標的の攻撃を回避するというアプローチとは異なる．

文献 [7] では，攻撃対象の拡散型フロー制御 [8] を用いて，隣接するノードとの相互作用のみで自律分散的に転送レートの制御を行い，DDoS 攻撃検知後から攻撃対象となる標的サーバ側に近い下流でのネットワーク負荷を回避しながら，正規パケットの損失を防ぐことを可能とする手法が提案されている．

2.2 拡散型フロー制御の DDoS 攻撃緩和への適応

拡散型フロー制御 [8] とは，物理学における拡散現象を指導原理とし，ネットワークの輻輳回避を目的とした自律分散型フロー制御である．エンドホスト間で経由されるネットワーク機器（以下，ノード）が隣接するノードとの相互作用のみで自律分散的に転送レートの制御を行い，転送パケットのネットワーク機器間での平滑化を実現する．

既存方式 [7] では，DDoS 攻撃の標的となるサーバに向かう DDoS 攻撃トラフィックの経路上のノード（ルータ等）が，攻撃トラフィックの転送レートを制御するための大きなバッファを持つノード（緩和装置）となることを前提とする．転送レートを制御してバッファ使用率の平滑化することで，標的サーバに向かう DDoS 攻撃トラフィックの緩和をする手法である．各ノードのバッファ容量の平滑化に前述の拡散型フロー制御 [8] による自律分散的な転送レート制御を用いる．

ノードの動作モデルを**図 1** に示す．図 1 では，ネットワークに存在する n 個のノードの識別子を $i\,(=0,1,2,\ldots,n-1)$ とし，ノード i の下流ノードを $suc(i)$，上流ノードの集合を $pre(i)$ と定義している．このモデルでは DDoS 攻撃の攻撃トラフィックは上流ノードから流入し，最下流ノードの先にある標的サーバに向かっていくことを表す．攻撃元は複数あることから拡散型フロー制御 [8] の動作モデルで想定されているノードが直列につながったトポロジのモデルではなく，木構造のトポロジを採用している既存方式 [7] では，各ノードで構成されるオーバレイネットワークとなるため木構造のトポロジである．このトポロジ上において，上流ノード向きにフィードバック情報（自ノードのバッファ使用率とパケットの転送レート）が送信される．また，フィードバック情報は，各ノードで一定時間ごと（フィードバック情報送信間隔）に送信しており，かつ各ノード間の伝搬遅延の時間に連動してフィードバック情報を同期している．

各ノードは，下流からの全フィードバック情報をもとに転送レートを計算して，それに応じて上流ノードからのパケットを自ノードでバッファリングするとともに必要量を下流へ転送する．ノード i に流れるフローの時刻 t の転送レート $J_i(t)$ は式 (1) のように算出する．

$$J_i(t) = D_i' J_{suc(i)}(t-d_i) - D_i S_i(u_{suc(i)}(t-d_i) - u_i(t)) \quad (1)$$

ただし，$0 \le J_i(t) \le L_i$

$$D_i' = \frac{1}{|pre(suc(i))|} \quad (2)$$

$$D_i = \frac{1}{|pre(suc(i))|+1} \quad (3)$$

ただし

$suc(k)$：ノード k の下流ノード

$pre(k)$：ノード k の上流ノードの集合

（$|pre(k)|$ は，$pre(k)$ の要素数を示す）

ここで，式 (1) の右辺第 1 項をドリフト項，第 2 項を拡散項とよぶ．d_i はノード i とノード i+1 の間の伝送遅延時間（ただし，上り下りとも同じ値），D_i' が分散係数，D_i が拡散係数，S_i はスケール係数である．$J_i(t)$ は，下流ノードから送られてきた転送レート $J_{suc(i)}(t-d_i)$，バッファ使用率 $u_i(t)$，下流ノードから送られてきたバッファ使用率 $u_{suc(i)}(t-d_i)$，各ノード間の使用可能帯域 L_i より算出される．ただし，スケール係数 S_i はノード i のバッファ容量とする．

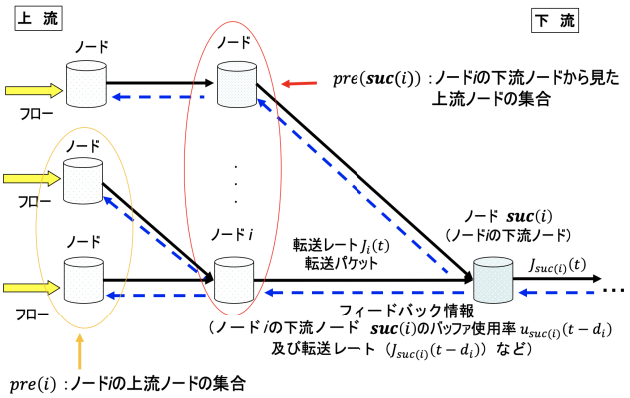


図 1 ノードの動作モデル

Fig. 1 Node behavior model.

3. 提案方式

既存方式 [7] では，分散係数 (2) の算出式のように，各ノードの下流向け転送レートの決定時に上流ノードの数で均等割を行っている．しかし，実際の DDoS 攻撃緩和システムで動作するノードの接続構成も様々なため上流ノード向けのリンク数も様々である．また，各ノードのバッファ容量も均一でない場合もある．これらが考慮されてないため，特定ノードでのバッファのあふれが早期に起るという問題点がある．以降でこの問題を詳述し，転送レートの算出式の見直しについて述べる．

3.1 容量のばらつきを考慮した拡散項の改良

既存方式 [7] では，バッファ使用率を平滑化することを目的として，式 (1) を定義している．しかし，各ノードのバッファ容量が異なるとき，式 (1) はバッファ使用率の平滑化を行うため，各ノードのバッファ容量の違いによる残容量の平滑化が達成されない場合がある．たとえば，自身のノードとその下流のノードのバッファ容量がそれぞれ 10 GB と 20 GB で，どちらもバッファ使用率が 0.5 の場合，それぞれのバッファ使用量は，5 GB と 10 GB である．この場合，既存方式 [7] では自身のノードの式 (1) の拡散項のスケール係数 × (バッファ使用率の差) は 10 GB × (0.5 − 0.5) = 0 GB となり，実際のバッファ使

用量のノード間の差 $20\,\mathrm{GB} \times 0.5 - 10\,\mathrm{GB} \times 0.5 = 5\,\mathrm{GB}$ を示せない．これにより，本来の目的である，各ノードの偏りを解消することができないという問題が生じる．

このことを解決するため，既存方式 [7] で使用しているバッファ使用率 $u_i(t)$ を，ノードの利用可能な残りのバッファ容量をスケールとするバッファ残容量 $\tilde{U}_i(t)$ に変更する．これにより，各ノードのバッファ容量に対する残りの容量を平滑化するように，拡散現象が起こるため，より効率的に，バッファを使用できる．つまり，各ノードのバッファ容量の違いによる既存方式の問題点を解決する．

改良方式として，各ノードのバッファ容量のばらつきを考慮した転送レート算出を式 (1) の拡散項を式 (4) のとおり変更する．

$$\begin{aligned} J_i(t) = {} & D'_i J_{suc(i)}(t - d_i) \\ & + D_i(\tilde{U}_{suc(i)}(t - d_i) - \tilde{U}_i(t)) \end{aligned} \tag{4}$$

なお，各ノードのバッファ容量が同一の場合，改良方式と既存方式 [7] は同値となる．

3.2 トポロジ分岐を考慮したドリフト項の改良

本節では，式 (1) で定義されているドリフト項にかかる分散係数の修正を行う．

分散係数 $D'_{f,i}$ は，下流ノードから上流ノードに送られてくる転送レートを分配するための係数である．既存方式 [7] は，DDoS 攻撃の送信元は図 1 のモデルのように木構造になっており，下流ノードに対して上流ノードは 1 対多となる場合がある．そのため，既存方式 [7] では，下流ノードに対する上流ノードの数を均等割し，下流ノードから送られてくる転送レートを式 (2) の分散係数で分配する．

しかし，ノードによって各上流ノードからのパケットの流入量が異なるので，既存方式 [7] のように均等割した場合，パケットの流出量の多い上流ノードでは，パケットを下流ノードに転送できず早期にバッファあふれが発生することが予想される．そこで，分散係数 D'_i の定義である式 (2) について，時点 t での，上流ノードからの下流ノードに流入するパケットの流入量を各上流ノードの流入量で分配して重み付けする手法に変更することで前述の問題の発生の改良をする．この改良により，各上流ノードからのパケットの流入量の違いを吸収する．

具体的には，式 (2) を式 (5) に変更する．

$$\begin{aligned} & D'_i(t) \\ & = (\text{ノード } i \text{ から下流ノード } suc(i) \text{ への流入量}) \div \\ & \quad (\text{下流ノード } suc(i) \text{ への総流入量}) \\ & = \begin{cases} \dfrac{J_i(t-2d_i)}{\sum_{k \in pre(suc(i))} J_k(t-2d_i)} & (\text{分母} > 0 \text{ の場合}) \\ 0 & (\text{分母} = 0 \text{ の場合}) \end{cases} \end{aligned} \tag{5}$$

式 (5) では，流入量を単位時間あたりの流入量，つまり，転送レート $J_i(t)$ としている．また，$t - 2d_i$ となっているのは，ノード間で遅延が往復分となるためである．

このドリフト項の改良にともないフィードバック情報に新たに定義した分散係数 $D'_i(t)$ を追加する．これにより，上流ノードに対して，下流ノードから新たな分散係数が定期的に伝えられ，順次上流ノードの転送レート算出式のドリフト項が更新される．これにより各上流ノードのパケットの流入量の変化に対して柔軟に対応できる．

4. 改良方式による DDoS 攻撃緩和システム

3 章で述べた改良方式を用いた DDoS 攻撃緩和システムの構成は文献 [7] と同様に**図 2** になる．DDoS 攻撃緩和の対象となるネットワーク（以降，緩和ネットワーク）内のノードは，パケットが蓄積できるバッファリングノード（以下，bn）であるとともに，ミチゲーションを行う．システムとしては，「常時ネットワークを監視し DDoS 攻撃を検知するネットワーク監視機器」，「bn と連携してトラフィックを学習しフィルタリングルールを生成する緩和装置」から構成される．各緩和ネットワークの bn どうしはオーバレイネットワークを構成し，このノードが図 1 のノードに対応する．bn のうち送信元からのパケットを受信するノードを流入 bn，最下流に位置する標的サーバにパケットを転送するノードを流出 bn，それ以外のノードを中間 bn と呼ぶ．ネットワーク監視機器が異常トラフィックを検知することで DDoS 攻撃を検知し，流出 bn にミチゲーションを要求する．ミチゲーションが始まると，隣接 bn 間が連携して転送レートを制御し，下流にパケットを転送やバッファリングを行う．動作の詳細は以下となる．

① 各 bn は，自ノードのバッファ残容量，転送レートおよび分散係数をフィードバック情報として上流ノードに送信する．

② 下流ノードから送られてきたフィードバック情報と自ノードのバッファ残容量をもとにパケットの転送レー

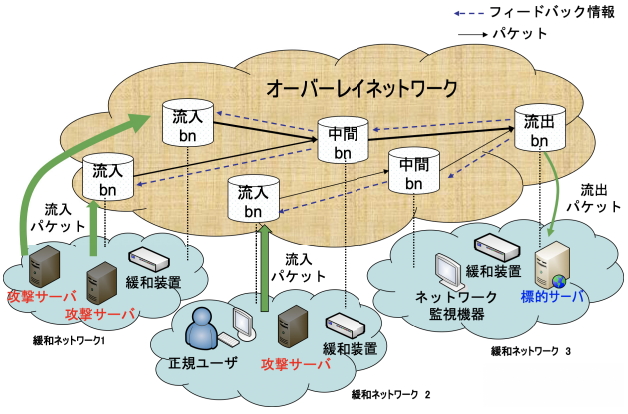


図 2 システムの全体構成

Fig. 2 Overall configuration of the system.

表 1 シミュレーションのパラメータ
Table 1 Simulation parameters.

パラメータの種類		変 数 値				
① bn 数		60				
② 流入 bn 数		20				
シナリオ		(a)	(b)	(c)	(d)	(e)
	転送レートパターン	固 定	固 定	ランダム	ランダム	ランダム
	バッファ容量パターン	固 定	ランダム	固 定	ランダム	ランダム
③ 流出 bn 送信レート[pps]		1.0×10^4				1.0×10^6
④ 流入トラフィック送信レート[pps]		1.0×10^5		$0.5\sim1.5\times10^5$		$0.5\sim1.5\times10^7$
⑤ bn のバッファ容量[packet]		2.0×10^6	$1.0\sim3.0\times10^6$	2.0×10^6	$1.0\sim3.0\times10^6$	$1.0\sim3.0\times10^8$
⑥ bn 間使用可能帯域[pps]		1.0×10^6				1.0×10^8
⑦ bn 間の伝搬遅延時間[ms]		10				
⑧ フィードバック情報送信間隔[ms]		10				

トを計算する．

③ 下流ノードへ自ノードの転送レートに従って宛先宛パケットの転送を行うとともに，上流ノードから送られてきた宛先宛のパケットを受け取りバッファリングする．

④ ミチゲーション終了の通知が届くまでは，新たなフィードバック情報を受け取った場合は，上記を再度①～③を実施する．

上記の動作と同時に，攻撃パケットの解析を行い，フィルタリングルールを生成し，緩和装置が生成したフィルタリングルールを用いて bn が攻撃パケットを遮断する（バッファにある攻撃パケットは廃棄する）．

5. シミュレーションによる評価

5.1 提案方式の評価方法について

改良方式を評価するため，標的サーバ宛の DDoS 攻撃を開始した後，各方式で用いる転送レートの算出式を用いて緩和をするシミュレーションを行う．シミュレータは文献 [7] のシミュレータを一部変更して用いた．そのため，シミュレーションで使用するパラメータや bn で構成されるオーバレイネットワークのトポロジも文献 [7] で使用したものを用いた．パラメータの一覧を**表 1** に示す．

bn 数を 60 とした理由は，以下のような想定による．bn 数は，提案システムの適用するオーバレイネットワークを構成するノード数であり，言い換えると連携して提案システムを用いる緩和ネットワーク数に相当する．本研究では，連携して提案システムを用いる集まりを IX（Internet Exchange Point）に接続するもの（ISP 事業者，CDN 事業者，クラウド事業者，データセンタ事業者等）と想定し，実際に存在する IX にどれくらいの接続があるかを調べた．2021 年 10 月現在，世界中に存在する IX への接続情報を共有するデータベースである Peering DB [9] には，約 900 の IX が登録されており，国内の登録数は 14 である．また，国内の各 IX に接続されているネットワーク数は，1～230 程度である．たとえば，IX に接続されたネットワークのうち DDoS 攻撃緩和システムに参加するネットワーク数を 4 分の 1 程度と仮定すると最大で 60 程度の緩和ネットワーク数が見込まれる．これにより bn 数を 60 とした．また，各 bn で構成されるオーバレイネットワークのトポロジの木の深さについては 7 から 10 としている．この深さについては，既存研究 [7] と差異を比較するため同じ深さとした．

他のパラメータは，②緩和ネットワークよりパケットが流れ込む bn の数である流入 bn 数，③オーバレイネットワークより標的サーバへの流れ込む流出パケットである流出 bn 送信レート，④標的サーバ宛に緩和するネットワークよりオーバレイネットワークに流れ込む流入パケット（正規および攻撃）の流入トラフィック送信レート，⑤各 bn のバッファ容量，⑥各ノード間の使用可能帯である bn 間使用可能帯域，⑦ノード間の伝送遅延時間である bn 間の伝搬遅延時間，⑧ノード間のフィードバック情報の送信間隔となるフィードバック情報送信間隔である．

評価基準としては，文献 [7] の評価基準でもある，トポロジを構成するいずれかの bn のバッファからパケットがあふれ出す最初の時刻（パケット損失発生時刻）までの時間とする．これを緩和時間（mitigation time）と呼ぶ．

5.2 実験方法

前述の評価方法に基づき，以下の 4 方式に対して，トポロジや各種パラメータが緩和時間に与える影響を調べるシミュレーション実験を実施した．

- 既存)：既存方式

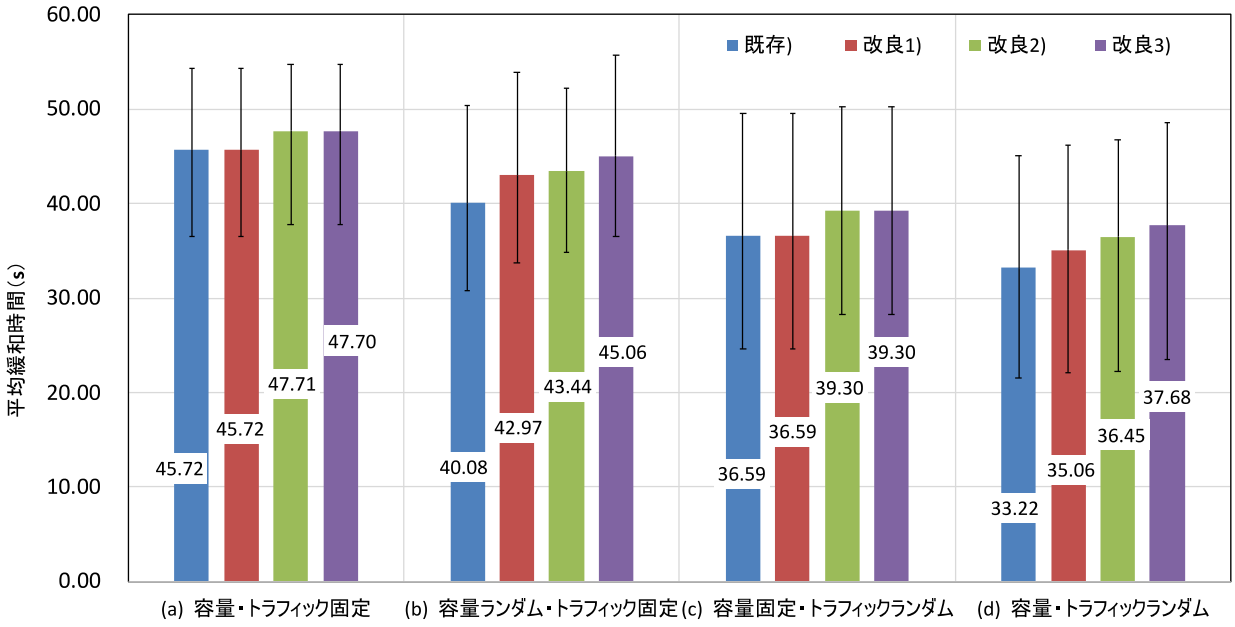


図 3 平均の緩和時間の変化（s）
Fig. 3 Average mitigation time (s).

- 改良 1)：拡散項改良方式（3.1 節）
- 改良 2)：ドリフト項改良方式（3.2 節）
- 改良 3)：拡散項・ドリフト項改良方式（3.1，3.2 節）

5.2.1 既存方式との比較に関する実験

シミュレーション実験では表 1 のシナリオ (a) から (d) のように各パラメータの値を設定し，トラフィック送信レートとバッファ容量がそれぞれ固定とランダムの 4 つの組合せで，50 パターンのトポロジを用いてシミュレーションを実施した．また，以下に変数値のシナリオを記述する．

(a) バッファ容量および宛先トラフィック一定
(b) バッファ容量ランダム・宛先トラフィック一定
(c) バッファ容量一定・宛先トラフィックランダム
(d) バッファ容量および宛先トラフィックランダム

ただし，各トポロジで使うランダムな値について，同じトポロジでは同一とした．

5.2.2 攻撃規模の増大の影響に関する実験

DDoS 攻撃の規模は年々増加傾向にあり，たとえば，Amazon Web Services は 2020 年 2 月に 2.3 Tbps の DDoS 攻撃を受けたことが報告されている [1]．そこで，攻撃規模の増大による本システムへの影響について考察する．表 1 の攻撃トラフィックに相当する流入トラフィック送信レートが増加した場合についての実験を実施する．具体的には，表 1 のシナリオ (d) における流入トラフィック送信レート，流出 bn 送信レートおよび，bn のバッファ容量を 100 倍としたシナリオ (e) を作成し，攻撃規模を増大させた変数について，改良 3) で 5 パターンのトポロジを用いて，各トポロジでの緩和時間および緩和時間を超える直前の全ノードのバッファ容量に対してどれくらいバッファリングしているかを示すバッファ使用率を確認する．

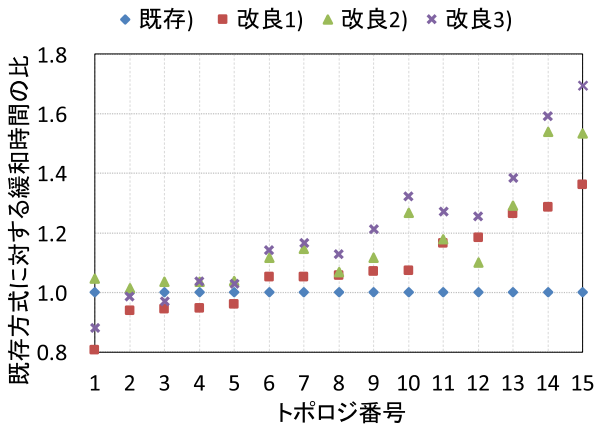


図 4 シナリオ (d) のトポロジによる各提案方式
Fig. 4 Results of each proposed method for each topology in scenario (d).

6. 結果と考察

6.1 改良方式の有効性

5.2.1 項の実験における 50 パターンのトポロジの結果の平均緩和時間（s）を図 **3** に示す．また，図 **4** にシナリオ (d) 転送レートとバッファ容量がどちらもランダムに変わる場合，トポロジによって既存方式 [7] に比べて，3 つの改良方式の緩和時間がどう変化するかを示す．横軸は既存方式 [7] の緩和時間を 1 としたときの改良方式の緩和時間の比率を示す．縦軸の 1～15 の番号に相当するトポロジは，50 パターンのトポロジのうちから，既存方式 [7] と改良 3) の緩和時間の差が最小となるもの（番号 1～5），緩和時間の差が中央値付近のもの（番号 6～10），緩和時間の差が最大のもの（番号 11～15）である．

図 3 のとおり，平均緩和時間は，既存) と比較した場合，すべてのシナリオで改良 3) が上回る結果となった．また，パラメータやトポロジのタイプによっては，図 4 の番号 15 のように，約 1.7 倍の緩和時間を延ばすことができている．加えて，最大と最小の緩和時間も (a) から (d) のすべてのシナリオにおいて改良 3) が既存) を上回る．シナリオ (a) と (c) のようなバッファ容量一定の場合には，既存) と改良 1) または改良 2) と改良 3) のような組合せで，各トポロジでの緩和時間がおおむね一致した．これは，理論的にもバッファ容量が一定の場合，3.1 節で提案方式と既存方式 [7] は同じ値となるためであり，実験と理論が一致した結果を示している．

既存と改良 1) でバッファ残容量が緩和時間に与える影響を比較するために，シナリオ (b) において，「緩和時間」，「バッファ残容量の各 bn の分散の時間変化」および「最小 bn のバッファ残容量の時間変化」についての追加検証を実施した．結果として**図 5** のとおり，改良 1) は既存に比べ，バッファ残容量の各 bn の分散が小さくなることが分かった．このことは，各 bn のバッファ残容量の平滑化を実現していると考えることができ，各 bn のバッファ残容量を平滑化することで，バッファからパケットがあふれる緩和時間を引き伸ばすことができる（図 5 では，既存が 38.47 s に対して改良 1) が 43.64 s となった）．また，bn のバッファ残容量が少なくなると，拡散の効果が小さくなるため，たとえば，図 5 において 15 秒経過以降のように拡散効果が機能しなくなり，最終的に bn からのバッファあふれを引き起こしていることも分かる．これらの現象ついては，他のトポロジでも同様の結果であることを確認している．

各シミュレーション単位で観察すると，改良 2) は既存) に対して，シナリオ (a) から (d) のパターンのすべてのトポロジで，緩和時間が上回る結果となった．これは，ドリフト項改良手法（3.2 節）がパラメータやトポロジの違いを柔軟に吸収し，拡散効果を発揮している結果だと考えられる．しかし，改良 1) については，シナリオ (b) および (d) で，少数ではあるが緩和時間が既存方式 [7] を下回る場合も確認した．

本研究では拡散現象を利用したものであり，各 bn の状態の情報が遅れるとその効果が発揮できなくなる．そのため，本研究では，既存研究の想定と同じ 10 ms としている．また，送信間隔について考察するために，フィードバック情報送信間隔を 100，1,000 ms という長い間隔とし，シミュレーションを実施した結果，送信間隔が長くなると拡散効果が効きにくくなることも確認した．ただし，10 ms と 100 ms では大きな違いはなかった．

以上より，改良 3) の方式がトポロジや複雑なパラメータ設定に対して，より柔軟に拡散効果を発揮し，既存方式 [7] の改良として効果が大きいことが分かる．一方，(a) から (d) のすべてのシナリオにおいて，トポロジの違いによる緩和時間が異なることが観測できた．このことは，既存方式 [7] においても指摘されたことである．これらについては，トポロジおよびバッファ容量，宛先パケット等のパラメータの設定に要因があると推測されるが，現時点で解析できておらず今後の課題とする．

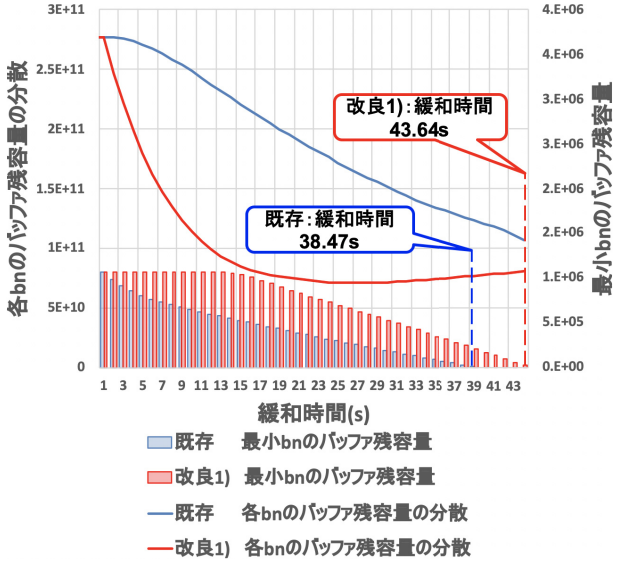


図 5 バッファ残容量および分散の時間変化と緩和時間

Fig. 5 Transition of buffer remaining capacity and variance, and mitigation time.

6.2 攻撃規模の増大による影響

5.2.2 項の実験結果を**表 2** に示す．パラメータについて，1 パケット 1,450 byte と仮定した場合，(d) のシナリオでは，流入トラフィック送信レートが $0.5 \sim 1.5 \times 10^5$（pps），送信元（流入 bn 数）が 20 なので，総流入トラフィックレートは $0.5 \sim 1.5 \times 10^5 \times 1{,}450 \times 8 \times 20 \fallingdotseq 23$ Gbps である．ま

表 2 攻撃規模の増大による影響

Table 2 Impact of increased attack scale.

シナリオ		(d)	(e)
トポロジ 1	緩和時間	38.75	36.76
	使用率	0.705	0.580
トポロジ 2	緩和時間	39.71	37.96
	使用率	0.623	0.679
トポロジ 3	緩和時間	48.53	42.94
	使用率	0.818	0.735
トポロジ 4	緩和時間	34.99	29.77
	使用率	0.544	0.634
トポロジ 5	緩和時間	41.50	36.74
	使用率	0.652	0.694
平 均	緩和時間	40.70	36.83
	使用率	0.668	0.664

た，各 bn のバッファ容量は 20×10^6 パケット分なので，$1.0 \sim 3.0 \times 10^6 \times 1{,}450 \fallingdotseq 2.9$ GB となる．一方，(e) のシナリオでは，流入トラフィック送信レート $0.5 \sim 1.5 \times 10^7$ (pps)，送信元は 20，総流入トラフィックレートは $0.5 \sim 1.5 \times 10^7 \times 1{,}450 \times 8 \times 20 \fallingdotseq 2.3$ Tbps である．また，各 bn のバッファ容量は 20×10^8 パケット分であるため，$1.0 \sim 3.0 \times 10^8 \times 1{,}450 \fallingdotseq 290$ GB となる．

表 2 のとおり，平均緩和時間については，10%程度下回る結果となり，各トポロジにおいても (e) が (d) を下回る結果となった．だだし，バッファ使用率については，トポロジ 2，4，5 で (e) が (d) を上回る結果となった．なぜ，このような逆転現象が起きたのかは解明できなかった．しかしながら，オーバレイネットワークに流入するトラフィック総量を 100 倍にしても，適切にネットワーク資源を増やすことで，十分に緩和の効果を発揮した結果となった．また，必要なネットワーク資源は，流入量=流出量+蓄えられる量となるため，本システムでは「流出量」が少ないため「流入量 $\fallingdotseq$ 蓄えられた量」の比例関係になる．すなわち，DDoS の攻撃量が増えても，それに比例してバッファ容量や bn 数を増やすことで，オーバレイネットワーク全体の総バッファ容量を攻撃規模に比例させることで，十分に緩和の効果を発揮することが可能となる．

また，本実験では，文献 [1] で報告された，2.3 Tbps の DDoS 攻撃を受けた事例を想定し，攻撃規模を約 2.3 Tbps とした．さらに，各 bn のバッファ容量についても，平均で約 290 GB と現実的な設定とし，実験を実施した．結果として，十分な効果が発揮できており，想定した緩和が可能であると考える．

ただし，本システムで確保する緩和時間が攻撃パケットを検知し，フィルタリングルール適用・排除までに十分かどうかの判断は，標的となるサーバのサービス品質やオーバレイネットワークの構成形態によって異なる．これらのことを考慮したうえで，緩和時間を延ばすための方法は今後の課題とする

7. まとめと今後の課題

本稿では，バッファリングノードで形成するオーバレイネットワークのトポロジのタイプやバッファ容量等の偏りのあるトポロジやバッファ容量のばらつきがある場合にも，より安定した性能を確保することを目的として，ノード間のパケットの転送を制御している転送レート算出式を改良し，より長時間パケット損失を防ぐことを可能とした．また，シミュレーションにより既存方式 [7] と提案方式の緩和性能を評価した．実験の結果，本稿の提案方式が既存方式 [7] に対して，平均緩和時間がすべて上回る結果となった．加えて，バッファ容量等のパラメータを複雑に設定したものほど，本稿の提案方式が既存方式 [7] に対して，緩和時間を引き延ばすことも確認した．これらのことから本稿提案方式がトポロジや複雑なパラメータの設定に対して，柔軟に拡散効果を発揮し，バッファあふれによる緩和時間が延長されたと考えられる．ただし，トポロジおよびバッファ容量等のパラメータの設定によっては，本稿の提案方式が既存方式 [7] に対して下回る結果も観測されており，これら要因について解明できなかった．今後，パラメータとトポロジとの関係を類型化することでその原因を究明し，多様なネットワーク状況に対して性能を維持できる方式を検討する予定である．

また，DDoS 攻撃の規模は年々増加傾向にあり，DDoS 攻撃の攻撃規模が増大した場合について，本システムへの影響を考察した．結果として，攻撃規模に応じた適切なネットワーク資源の配分を行うことで，攻撃規模が増大した場合でも，十分にミチゲーションの効果を発揮できるという結果となった．

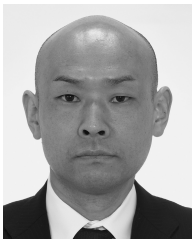
今後の課題としては，ミチゲーションの効果を最大限発揮するためのオーバレイネットワークのトポロジ構築方法およびバッファ容量等の各種パラメータの設定方法の検討，DDoS 攻撃の検知，ミチゲーションおよびフィルタリングルールの適用による攻撃の回避を包括したシステムの設計・評価がある．

謝辞 本研究の一部は JSPS 科研費 19K11929，19K11882，20H04179 および 21H03432 の支援を受けて実施しました．

参考文献

[1] AWS Shieled, Treat Landscape Report-Q1 2020, available from ⟨https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf⟩ (accessed 2021-05-19).
[2] DDoS attacks in Q1 2020, Kaspersky DDoS REPORTS, 06 May 2020, available from ⟨https://securelist.com/ddos-attacks-in-q1-2020/96837/⟩ (accessed 2021-05-19).
[3] DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為（DDoS 脅迫）について，CyberNewsFlash，JPCERT/CC，入手先 ⟨https://www.jpcert.or.jp/newsflash/2020090701.html⟩（参照 2021-05-19）．
[4] 増田絢斗，今堀慎治，小原泰弘：DDoS ミティゲーションを可能にするネットワークルーティングアルゴリズム，信学技報，Vol.118, No.268, COMP2018-25, 電子情報通信学会，pp.33–39 (2018).
[5] Abubakar, R., Aldegheishem, A., Majeed, M.F. et al.: Open Access: An Effective Mechanism to Mitigate Real-Time DDoS Attack, *IEEE Access*, Vol.8, pp.126215–126227 (2020).
[6] Novaes, M.P., Carvalho, L.F., Lloret, J. and Proença, M.L.: Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment, *IEEE Access*, Vol.8, pp.83765–83781 (2020).
[7] 平 空也，高野知佐，前田香織：拡散型フロー制御を用いる DDoS 攻撃緩和システム，情報処理学会論文誌，Vol.59, No.9, pp.1656–1665 (2018).
[8] 住 達郎，高野知佐，会田雅樹，石田賢治：拡散方程式に基づく自律分散的輻輳制御技術の実証実験，電子情報通信学会論文誌 D，Vol.J95-D, No.12, pp.2048–2058 (2012).

[9] Peering DB. available from ⟨https://www.peeringdb.com/⟩ (accessed 2021-10-19).



奥田 尚樹

2006 年広島市立大学情報科学部卒業．2010 年防衛大学校理工学研究科修了．2020 年広島市立大大学院情報科学研究科博士後期課程入学．現在，広島県職員として勤務．

前田 香織 （正会員）

1982 年広島大学総合科学部卒業．同大学工学部助手，(財) 放射線影響研究所技術員，広島市立大学情報科学部助手，情報処理センター助教授を経て，現在，同大学大学院情報科学研究科教授．博士（情報工学）．コンピュータネットワーク，モバイル通信に関する研究に従事．電子情報通信学会，IEEE 各会員．

高野 知佐 （正会員）

2000 年阪大学工学部電子通信工学科卒業．2008 年首都大学東京大学院博士後期課程修了，博士（工学）．2000 年 NTT アドバンステクノロジ（株）入社．2008 年広島市立大学大学院情報科学研究科准教授．2020 年同大学院教授．通信トラフィック制御，社会ネットワーク分析の研究に従事．IEEE，電子情報通信学会各会員．

市原 英行 （正会員）

1995 年大阪大学工学部応用物理学科卒業．1999 年同大学大学院工学研究科応用物理学専攻博士後期課程修了．博士（工学）．同年広島市立大学情報科学部情報機械システム工学科助手．2021 年より同大学教授．フォールトトレラントシステム，エラートレランス，ストカスティックコンピューティングの研究に従事．IEEE，電子情報通信学会各会員．