Vol.2020-DPS-182 No.63
Vol.2020-CSEC-88 No.63
2020/3/13

TCPを標的としたLow-rate DDoS攻撃における正常トラフィックを用いた攻撃レート削減の検討

髙橋 佑太[1]　稲村 浩[2]　中村 嘉隆[2]

概要：TCP を標的とした低量分散型サービス妨害 (LDDoS: Low-rate Distributed Denial of Service) 攻撃は，定期的なバーストトラフィックをボトルネックリンクに送信してネットワークに輻輳を発生させることにより，低い平均通信量で TCP スループットを妨害することが可能かつ検知が困難な攻撃手法である．これまでの LDDoS 攻撃に関する既存研究では，数多くの検知手法の提案，並びに数学的モデルによる攻撃効果について議論されているが，インターネットにおける現実的な攻撃効果，及び実行可能性に関する議論は少ない．最近はルータバッファの大容量化が進んでいるため，LDDoS 攻撃で十分な攻撃効果を得るためにはより大きな攻撃レートが必要になっている．本稿では，クラウド環境における大容量バッファを備えたルータを標的とした LDDoS 攻撃の実行可能性について明らかにするために，正常トラフィックを用いた攻撃レート削減手法を検討する．ns-3 を使ったシミュレーションにより，攻撃ノードの一部が標的サーバに対して正常な通信を装って TCP 通信でルータバッファを消費させることによって，攻撃レートを削減可能なことを示した．

キーワード：ネットワークセキュリティ，Low-rate DDoS 攻撃，TCP 輻輳制御

Study of Attack Rate Reduction using Normal Traffic in TCP-targeted Low-rate DDoS Attack

1. はじめに

分散型サービス妨害（DDoS: Distributed Denial of Service）攻撃は，インターネットを代表する脅威のひとつである．代表的な事例として，2016 年 10 月に米国の DNS プロバイダである Dyn 社を標的とした攻撃が挙げられる [1]．大規模なボットネットから 620Gbps に上る DDoS 攻撃を受けたことにより，Twitter や Spotify をはじめとした様々なサービスへの接続が困難になる問題が発生した事例 [1] のように，ネットワーク帯域幅やコンピュータリソースを使い果たすフラッド（ブルートフォース）型 DDoS 攻撃は，攻撃トラフィックの割合が高いため容易に検出が可能である．上記を示す印象的な事例として，2018 年に GitHub に対して最大レート 1.8Tbps に上る DDoS 攻撃が発生したが，Akamai 社によってわずか 10 分で復旧された [2] ことが挙げられる．このような背景から，攻撃者は低レート DDoS (LDDoS: Low-rate DDoS) 攻撃によって検知を回避しながら，サービスの品質を低下させることに注目している [3]．

LDDoS 攻撃には様々な手法が存在することが既存研究により明らかにされている [3]．本稿で対象とする LDDoS 攻撃は TCP を標的とした LDDoS 攻撃（別名，Shrew 攻撃）[4] である．TCP を標的とした LDDoS 攻撃（以下，LDDoS 攻撃）は，標的 TCP の再送タイムアウト (RTO: Retransmission Time Out) の間隔に合わせて，矩形波の攻撃トラフィックによってボトルネックリンクに輻輳を発生させることで，低い平均通信量で標的 TCP のスループットを妨害することが可能である [4]．

インターネット上に流れているトラフィックのほとんどが TCP であることから [5]，LDDoS 攻撃が容易に実行可能な場合，インターネットにとって重大な脅威となる．しかし，我々の知る限りでは LDDoS 攻撃の事例は報告されていない．そのため，インターネットにおける LDDoS 攻撃の実行可能性は大変興味深い研究課題である．さらに，

[1] 公立はこだて未来大学大学院 システム情報科学研究科
[2] 公立はこだて未来大学 システム情報科学部

LDDoS 攻撃の実行可能性を明らかにすることは，脅威となり得るネットワークとサービスおよび攻撃トラフィックの特性を明らかにすることに繋がるため重要である．これまで我々は，LDDoS 攻撃の実行可能性を明らかにするための研究を続けてきた [6][7].

本稿では，現実のインターネットにおける LDDoS 攻撃の実行可能性の観点から，正常トラフィックを用いた LDDoS 攻撃トラフィックの削減によって検知を回避する可能性，並びに攻撃効果を最大化する可能性について検討する．

本稿の貢献は以下の 3 点である．

i. 既存研究により明らかとなっている LDDoS 攻撃の知見とネットワークの特性に着目し，LDDoS 攻撃の構成における障壁について議論した．
ii. LDDoS 攻撃の脅威を明らかにすることを目的として，LDDoS 攻撃トラフィックのレートを削減することで，検知を回避する可能性について検討した．検知を回避しながら TCP スループットを十分に低下させるために，攻撃ノードの一部が標的サービスと通信している正規ユーザと同等の通信でボトルネックルータのバッファ容量を消費することで，攻撃レートを削減する．
iii. 上記の手法を現実的に実行可能と考えられるクラウドのストレージサービスの TCP 通信を標的とした攻撃シナリオを検討した．攻撃シナリオに沿って攻撃レート削減手法の実証実験をネットワークシミュレータ上で行い，攻撃効果の向上と検知を回避する可能性を示した．

本稿は以下のように構成される．2 章では，LDDoS 攻撃の詳細について説明し，LDDoS 攻撃が TCP スループットを妨害する原理を確認する．3 章では，既存研究の結果とネットワークの特性から，LDDoS 攻撃の構成における障壁について議論する．4 章では，正常トラフィックを用いた LDDoS 攻撃トラフィックのレート削減手法を検討する．5 章では，4 章で検討した攻撃レート削減手法が実行され得る攻撃シナリオを検討する．6 章では，攻撃レート削減手法の概念検証のためのシミュレーション実験を行い，結果から手法の有効性について考察する．7 章では，LDDoS 攻撃の実行可能性，現実的なルータのバッファ容量，最新の LDDoS 攻撃手法に関する関連研究をまとめる．最後に 8 章では，本稿のまとめと今後の課題について述べる．

2. 背景

本章では，LDDoS 攻撃に利用されている TCP 再送信タイムアウト機構と，LDDoS 攻撃トラフィックのモデルの詳細について説明する．

2.1 TCP 再送信タイムアウト

TCP 通信においてパケットが送信されると，再送信タイマーがスタートする．再送信タイマーの最大待ち時間を再送信タイムアウト（RTO）と呼び，RTO 以内に送信したパケットの応答が返ってこない場合，TCP は当該パケットが廃棄されたと判断し再送信する．RTO の初期値 RTO_1 は RFC6298[8] により，次の式で設定される．

$$RTO_1 = max\{minRTO, SRTT + max(G, 4 \times RTTAVR)\} \quad (1)$$

ここで $minRTO$ は RTO の最小値，$SRTT$ は平滑化した RTT，G はオペレーティングシステムに設定されているクロック粒度，$RTTAVR$ は RTT の平均偏差である．$minRTO$ は RFC6298[8] により，1 秒に設定することが推奨されている．多くの場合で（1）式の右辺では

$$minRTO > SRTT + max(G, 4 \times RTTAVR) \quad (2)$$

が成り立つ [4] ため，RTO の初期値は $minRTO$ に設定されるとする．よって，これ以降（1）式は，以下の（3）式であるものとして議論を進める．

$$RTO_1 = minRTO \quad (3)$$

TCP 通信において，2 回以上連続して同じパケットがタイムアウトした場合，当該パケットが再送なく正常に応答を返すまでタイムアウトごとに RTO の値を 2 倍ずつ増加させていく．i 回連続でタイムアウトしたパケットの RTO の値を RTO_i と表すとこの値は以下の（4）式により設定される．ただし，RTO の値は 60 秒以上の上限値を持つように制限されている [8].

$$RTO_i = 2RTO_{i-1} \quad (4)$$

当該パケットの送信と応答が成功した場合，（3）式により RTO は $minRTO$ に再設定される．このアルゴリズムは Karn のアルゴリズムと呼ばれ，ほとんどの TCP で実装されているが，RTO_i が $minRTO$ に依存して一意に決定される単純な仕様が，LDDoS 攻撃に利用される．

2.2 LDDoS 攻撃

LDDoS 攻撃は，短いバーストトラフィックと無通信が一定の周期で繰り返される矩形波の LDDoS 攻撃フローを複数の攻撃ノードから送信する．標的 TCP パケットがボトルネックリンクを流れるわずかな時間のみ輻輳を繰り返し発生させることで，低い平均通信量で TCP 通信を妨害する [4].

LDDoS 攻撃を N 台のノードで構成した攻撃モデルを図 1 に示す．LDDoS 攻撃モデルはバースト間隔 T，バースト幅 L，バーストレート R により定義される矩形波パルスである．最も基本的な LDDoS 攻撃は，N 台の攻撃ノードからバースト間隔 T，バースト幅 L，バーストレート R/N の攻撃トラフィックを送信する．攻撃ノード N 台分の攻撃

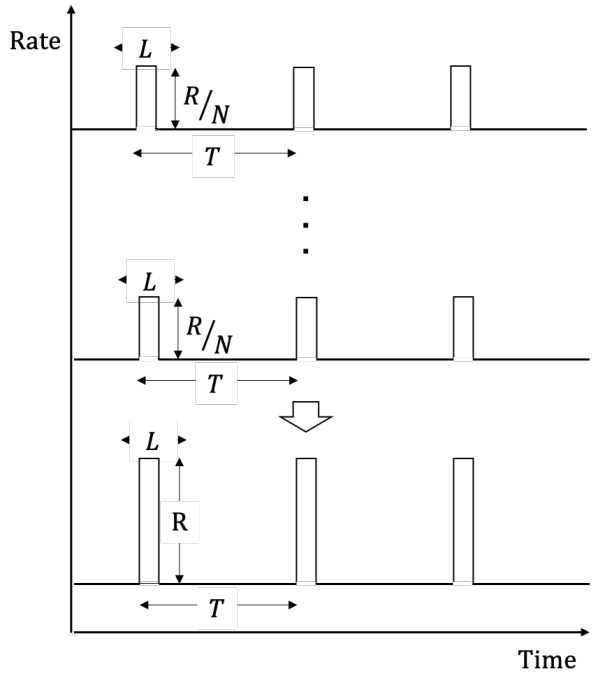

図 1 LDDoS 攻撃モデル N 台の攻撃ノードによるバーストレート R の集約

トラフィックをボトルネックリンクで適切に集約できた場合，集約トラフィックのバーストレートは R となる．このように攻撃トラフィックを分割することにより，個々の攻撃トラフィックの平均通信量がさらに低くなるため，検知が困難になる．

LDDoS 攻撃のモデルは文献 [4] で示され，文献 [9] は攻撃効果が最大となる攻撃パラメータの各値について明らかにしている．それによれば，T は $minRTO$ 以上（1 秒以上），L はボトルネックリンクルータのバッファ容量を埋めるに十分な時間または RTT 以上（RTT の 2〜3 倍の範囲），R はボトルネックリンク帯域幅と等しい値であることが理想とされている [9]．

3. LDDoS 攻撃の構成における障壁

LDDoS 攻撃は実行可能であればインターネットにとって脅威である．一方，LDDoS 攻撃は通常の DDoS 攻撃と比較して，技術的な側面において実現することが難しい．

本章では，高度な攻撃者によって実行される可能性がある LDDoS 攻撃手法を検討するために，既存研究とネットワークの特性から LDDoS 攻撃の構成における障壁について議論する．

3.1 バッファ容量の増加による攻撃効果の低下と攻撃トラフィックの DoS 化

近年，ルータのバッファ容量は増加傾向にある．一方で，ルータのバッファ容量 B が大きいほど，LDDoS 攻撃の効果が低下することが明らかになっている [10]．B が十分に大きい状況において，攻撃者が高い攻撃効果を得るためには，バースト長 L を長く保つ必要がある．しかし，L が長いほどパルス状の攻撃トラフィックの矩形波は DoS に見られる形状に類似するため，LDDoS 攻撃の重要な特性の 1 つであるステルス性を損なってしまう [10]．

3.2 既存検知手法による検知

LDDoS 攻撃の平均トラフィック量は通常のトラフィックと同様，もしくはそれ以下のため，時間領域の検知手法では検知が困難である．

文献 [11] において，LDDoS 攻撃トラフィックのパワースペクトル密度が 0Hz〜50Hz の低周波数帯域で強い特徴を示すことが明らかにされて以降．多くの既存研究で周波数領域のアプローチを利用した LDDoS 攻撃の検知が試みられている [3]．文献 [12] では，バックボーンルータ間の協調検出アプローチが提案された．この手法では，あらかじめ Autonomous System 内を流れる攻撃トラフィックの平均スペクトルをテンプレートとして算出し，テンプレートスペクトルとリアルタイムトラフィックのスペクトルの差から LDDoS 攻撃を検出する．文献 [13] では，様々な攻撃シナリオにおいて，スペクトル解析による LDDoS 攻撃の検出効果を評価した．評価の結果，攻撃者がバースト間隔をランダム化した場合，日常的なトラフィックデータから攻撃トラフィックを検出することは困難であると結論づけた．文献 [14] では，ローカルシーケンスアラインメントの Smith-Waterman アルゴリズムを使用して正常な TCP トラフィックの中に隠れた LDDoS 攻撃トラフィックを検知する手法が提案された．この手法では，あらかじめ推定された攻撃パラメータ T, L, R から検出シーケンスを構築する．検出シーケンスと 100ms ごとにサンプリングしたトラフィックのシーケンス（トラフィックレートが値として構成された配列）を比較して，閾値で設定された回数だけ一致すると攻撃が検知される．

既存の検知手法はパラメータが固定された攻撃に対しては有効である．そのため，将来は単調なトラフィックによる LDDoS 攻撃は検知される可能性が高いと予想する．

3.3 ネットワーク遅延による攻撃トラフィック集約誤差の発生

LDDoS 攻撃は短い長さの攻撃トラフィックをボトルネックリンクで適切に集約する必要があるため，通常の DDoS 攻撃と比較すると攻撃難易度が高い．通常のネットワークの RTT が 10ms から 100ms であると考えると，バースト長 L は 100ms から 300ms であると予測できる [4]．このように長さの短いトラフィックを，複数の異なるネットワークエッジに存在する攻撃ノードをから送信した場合，攻撃ノードから標的ボトルネックリンクまでの RTT の違いや

ジッタによって，集約後のバーストレート R がボトルネックリンクの帯域幅 C に満たず，十分な攻撃効果が得られない可能性が予想される．

4. 正常トラフィックを用いた攻撃レートの削減

本章では，LDDoS 攻撃の標的ボトルネックリンクルータのバッファ容量に応じて正常（良性）トラフィックを併用することで，攻撃効果の向上とバーストレートを削減する手法について検討する．

3 章では，現実のインターネットにおいて，単調なトラフィックによる LDDoS 攻撃の構成には障壁があることを述べた．しかし，高度な攻撃者はあらゆる手段を用いて検知を回避しつつ，最大の攻撃効果を得る努力を続けている．その例として，文献 [15] では，DeNy（検出不能）攻撃と呼ばれる新たな攻撃手法が今後利用されると予想されている．DeNy 攻撃は良性かつ可変な正常トラフィックのみで攻撃を構成し，コスト駆動型のクラウドサービスを標的とする．DeNy 攻撃で使用されるトラフィックはボリューム型であり，LDDoS 攻撃のように低レートではない．攻撃者はリソースの価格設定，アプリケーション機能，および良性ユーザのアクセスパターンを利用して，標的ごとにトラフィックパターンを変更するため，DeNy 攻撃はトラフィックベースの検出方法でパターンを検出できた場合でも，常に誤検知を引き起こす可能性がある [15]．

DeNy 攻撃を参考に，LDDoS 攻撃においても検出が困難な正常トラフィックを使うことで攻撃効果の向上や，バーストレートの削減が可能であるかを検討する．図 2 に正常トラフィックを使用した LDDoS 攻撃（以下，検討手法）の簡易的なモデルを示す．正常トラフィックによる攻撃はボトルネックリンクルータのバッファ容量を消費するために開始される．正常トラフィックの攻撃レートは $R_{normal}(\leq B)$ とし，ボトルネックリンクルータのバッファ容量を消費するために開始される．標的サービスは TCP のバルク転送で通信することを想定する．すなわち，正常トラフィックは TCP で通信する．LDDoS 攻撃は多くの既存研究で用いられている UDP で通信する．

検討手法によって，攻撃効果の向上や，バーストレートの削減が期待できる．3.1 節で述べた標的ボトルネックリンクルータのバッファ容量が十分に大きい場合，$R_{LDDoS} = C$ では攻撃効果が減衰してしまう．しかし，R_{normal} がバッファ容量を消費することで帯域幅の利用率が高くなり，より多くの正規トラフィックを妨害することが期待できる．さらに，R_{normal} で消費されたバッファ分だけ，R_{LDDoS} を削減できることが期待できる．

検討手法と DeNy 攻撃の違いは，正常トラフィックを使用する目的と使用するトラフィック量である．両手法は，

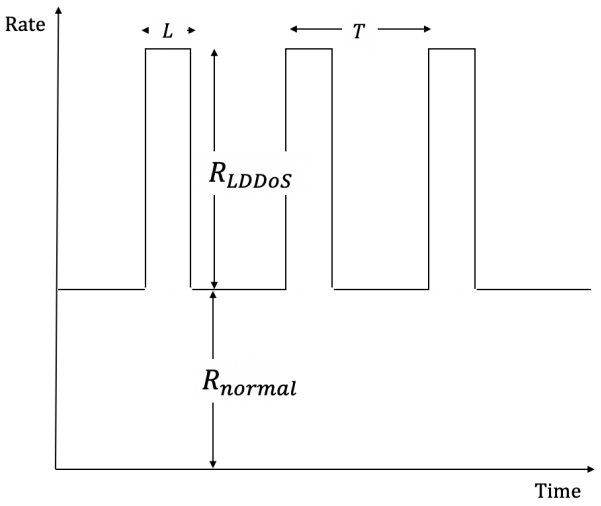

図 2　正常トラフィックを用いた LDDoS 攻撃モデル

検出が困難な正常トラフィックを使用している点で類似しているが，DeNy 攻撃は大量の正常トラフィックのみで検出を回避しながらクラウドサービスのスケーリング機能を悪用することを目的としており，検討手法は LDDoS 攻撃の攻撃効果を向上させるために，正常トラフィックによってバッファを消費する点が異なる．そのため攻撃に使用するトラフィック量も異なる．DeNy 攻撃ではクラウドサービスをスケーリングさせるために悪意のある多くの正常トラフィックを使用するが，検討手法ではボトルネックリンクのバッファを消費可能な量のトラフィックが必要となる．バッファを消費させる割合は攻撃者が任意に決定できるが，適切なバッファ容量を消費するためには攻撃者が標的バッファの容量を把握する必要がある．現実的なバッファ容量に関しては 7.2 節で関連研究を参考に議論する．

5. 攻撃シナリオの検討

本章では，正常トラフィックを用いた LDDoS 攻撃が有効な攻撃シナリオを検討する．

攻撃シナリオは，文献 [16] で提案されている Eucalyptus [*1] を軸に設計されたクラウドセキュリティモデルを参考に検討する．図 3 に攻撃シナリオを示す．

標的サービスは長期間のバルク転送を行うクラウドストレージサービスとする．長期間コネクションを張り続けるバルク転送は，LDDoS 攻撃の被害を受けやすい．

クラウド環境は内部の遅延が非常に小さいため LDDoS 攻撃トラフィックの集約に適している．文献 [18] の調査によって，Amazon Web Services や Google Cloud を始めとしたパブリッククラウド内部の遅延は 1ms 未満であることが明らかになっている．LDDoS 攻撃のバーストトラフィックはクラウド内部の Virtual Machine から標的スト

[*1] Amazon Web Services 互換のプライベートおよびハイブリッドクラウドコンピューティング環境を構築するためのオープンソースソフトウェア [17]

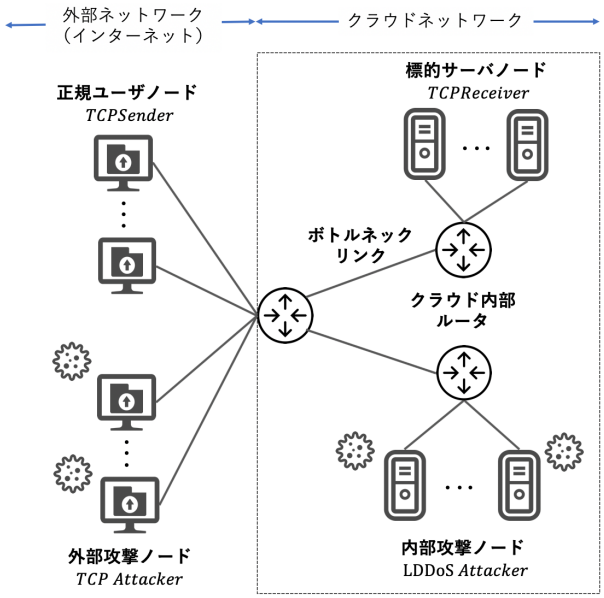

図 3　攻撃シナリオ

レージサーバに向けて送信する．クラウド内部からバーストトラフィックを送信することにより，3.3 節で議論したネットワーク遅延による集約誤差を解決することが可能である．攻撃に用いる正常トラフィックは正規ユーザを装い，同等の TCP バルク転送で通信する．

文献 [16] のセキュリティモデルにはボトルネックリンクの明確な記述は無かったが，本稿の議論ではクラウド内部ルータ間を相互接続するリンクがボトルネックリンクであると仮定する．

以上の攻撃によって，正規ユーザが標的サーバに向けて送信する TCP トラフィックが妨害される．

6. 実証実験と考察

本章では，以下の仮説 A，仮説 B を明らかにするために実証実験を行う．

仮説 A).攻撃者が 3.1 節で述べた攻撃レートの不足を解決するために，LDDoS 攻撃に正常トラフィックを併用することで，ボトルネックリンクルータバッファの容量が大きい場合においても攻撃効果を得られること

仮説 B).攻撃者が 3.2 節で述べた検知手法を回避するために，LDDoS 攻撃に正常トラフィックを併用することで，攻撃効果を維持したまま LDDoS 攻撃トラフィックのバーストレートを削減可能なこと

6.1 実験環境

実験は離散イベントネットワークシミュレータ ns-3[19] を用いたシミュレーション環境で行う．実験ネットワークは 5 章で検討した攻撃シナリオをもとに，ダンベル型を拡張したトポロジを構成する（図 4）．

$TCPSender$ は $TCPReceiver$ に向けてバルク転送で TCP トラフィックを送信するホストである．$TCPAttacker_{1\cdots M}$ は $TCPSender$ と同様に $TCPReceiver$ に向けてバルク転送を行う M 台の攻撃ノードである．$LDDoSAttacker_{1\cdots5}$ は $TCPReceiver$ に向けて，UDP 通信でバーストトラフィックを送信する．$LDDoSAttacker$ は 1 ノードあたり $T = 1000ms$，$L = 200ms$，$R = 10Mbps$ のバーストレートで送信する．攻撃は全ノードが同じ時刻に開始される．したがって，5 ノードによる集約トラフィックの最大パラメータは，$T = 1000ms$，$L = 200ms$，$R = 50Mbps$ である．UDP パケットは 1 パケット 542Byte である．

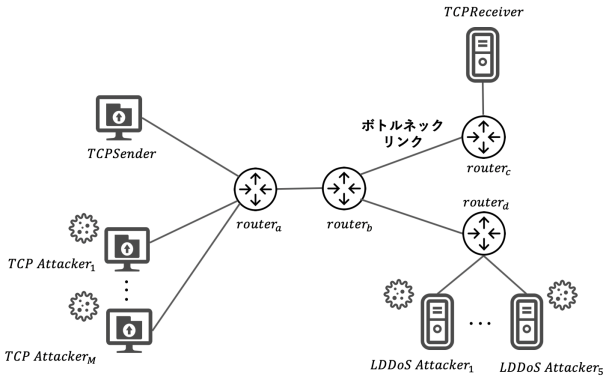

図 4　実験ネットワークトポロジ

表 1　リンクパラメータ

Link	帯域幅（Mbps）	伝搬遅延 (ms)
$TCPSender$ to $router_a$	100	50
$TCPAttacker_{1\cdots M}$ to $router_a$	100	50
$router_a$ to $router_b$	1000	10
$router_b$ to $router_c$, $router_d$	50	0.1
$router_c$ to $TCPReceiver$	100	0.1
$router_d$ to $LDDoSAttacker_{1\cdots5}$	100	0.1

各リンクの帯域幅と伝搬遅延は表 1 の値を設定する．$router_b$ と $router_c$ を接続するリンクがボトルネックリンクであり，LDDoS 攻撃によって輻輳が発生する．

TCP ソケットバッファは送受信バッファそれぞれを 4MB とする．各ルータのリンクごとのバッファ容量は 10,000 パケットとする．ただし，$router_b$ と $router_c$ 間は大容量バッファを想定し，入力・出力ともに 500,000 パケットとする．

TCP 輻輳制御アルゴリズムは TCPNewReno を使用する．さらに，文献 [4] にて LDDoS 攻撃の耐性が明らかになっている，TCP の選択確認応答（SACK）機能 [20] を有効にする．

6.2 実験と結果

合計 3 回のシミュレーションを実行した．使用した集約バーストレート R と $TCPAttacker$ のノード数 M の値を表 2 に示す．各シミュレーションは 60 秒間行った．時刻 0 か

表 2　実験パラメータ

シミュレーション	R (Mbps)	M (nodes)
1	50	0
2	50	5
3	50	10

表 3　実験結果：$TCPSender$ の正規化スループット

シミュレーション	正規化スループット
1	0.148
2	0.05
3	0.03

ら $TCPSender$, $TCPAttacker_{1\cdots M}$, $LDDoSAttacker_{1\cdots 5}$ が同時に通信を開始した．評価指標として，$TCPSender$ の正規化スループットを計測した．

各試行における 60 秒間の $TCPSender$ の正規化スループットを表 3 にまとめる．この結果から，LDDoS 攻撃に正常トラフィックを組み合わせることによって，攻撃効果の向上が確認できた．

6.3　考察

表 3 から $TCPAttacker$ のノード数 M が増加するにしたがって，スループットは低下している．このことから，LDDoS 攻撃に正常トラフィックを併用することで，ボトルネックリンクルータバッファの容量が大きい場合においても攻撃効果を得られることが示された．

この結果を応用することで，UDP のバーストトラフィックレートを削減可能であると考える．これまで提案されてきたテンプレートマッチングの検知手法 [14] は攻撃レートに変動があった場合，検知が困難となる．そのため，正常 TCP トラフィックを使用してバーストレートを削減または変動することによって，検知を回避できる可能性が考えられる．今後，本手法の数学モデルを確立した後，検知回避の効果について明らかにする．

さらに，攻撃に使用する正常トラフィックの量と LDDoS バーストトラフィック量を動的に変化することによって，固定長の LDDoS 攻撃を検知する既存手法を回避する可能性も考えられる．これについても，数学モデルから攻撃手法の詳細を検討し，現実に実行可能であるかを検討することが課題である．

今回のシミュレーションは簡易的であったため，トポロジの現実性や攻撃に加担しているノード数の割合が現実的ではない．本手法の実行可能性を明らかにするためには攻撃シナリオをさらに詳細化し，同時アクセス可能なユーザ数を推定した上でシミュレーションする必要がある．

7.　関連研究

7.1　LDDoS 攻撃トラフィックの正確な集約

ネットワークの遅延やジッタにより，数百ミリ秒単位で LDDoS 攻撃トラフィックを正確に集約することは難しい (3.3 節)．この障壁を攻撃者が解決する可能性として，文献 [21] では，ネットワーク遅延による攻撃トラフィック集約誤差の調整が検討された．この手法では異なるネットワーク遅延のノードから攻撃トラフィックを送信し，標的で発生した集約誤差を相互相関アルゴリズムを利用して理想的な集約となるように送信時刻のフィードバックを各攻撃ノードに行う．ただし，実際に攻撃者は攻撃トラフィック送信先の標的ネットワークに，フィードバックするボットノードの設置が必要となる制限がある．

7.2　現実的なルータバッファ容量

4 章では，通常トラフィックによって消費するバッファ容量を攻撃者が把握する必要について述べた．現実的なルータのバッファ容量の適切な値はネットワーク運用の分野において未解決の課題であり，長い間議論されている．ルータのバッファ容量は経験則として，帯域遅延積 $B = \overline{RTT} \cdot C$ だけ必要とされていたが，文献 [22] にて，フロー数の増加にしたがって，はるかに小さいバッファ容量で同等の性能を発揮できると主張された．この研究では，リンク流れるフローの数を n とした場合，バッファ容量は $B = \frac{\overline{RTT} \cdot C}{\sqrt{n}}$ で十分であり，この値にバッファ容量を減少した場合においてもネットワークの使用率に変化が現れず，性能に影響が出ないことがシミュレーションによって示されている [22]．このように，理論上ルータのバッファ容量を削減しても問題ないことは示されているが，実際の運用にあたって n を推定することは困難であるため，商用ルータのバッファ容量は増加傾向にある．

近年は一般企業も適切なバッファ容量について研究を進めている．文献 [23] では，Facebook 社が同社のバックボーンルータのバッファ容量を標準の 50 万パケットから最小 200 パケットまで減らした場合のネットワークパフォーマンスを計測した．計測の結果，バッファ容量が非常に小さな値になると，RTT が大幅に小さくなり，リンクの使用率がわずかに減少し，パケット廃棄率が許容可能な範囲で増加することが明らかになった．文献 [24] では，Netflix 社が同社のネットワークルータの仮想出力キューを調整して，ユーザへ提供する動画ストリームの品質の変化を調査した．調査の結果，輻輳制御アルゴリズムが TCPNewReno の場合は，バッファが縮小するにつれてパケット損失が増加し，RTT が減少する結果となった．加えて，動画ストリーム通信におけるバッファ容量にはスイートスポットが存在し，小さすぎても大きすぎても再バッファの数を増加させ，ビデオ品質の低下に繋がることが明らかになった．

これらの調査から，バッファ容量はサービスごとに適切な大きさが存在するため，LDDoS 攻撃の実行可能性を検討する上では，標的サービスを明確にした上で適切な実験

環境の構築が必要である．

7.3 新たな LDDoS 攻撃モデル

本稿ではバッファ容量について焦点をおいて LDDoS 攻撃の実行可能性について議論した．これに関連する研究として，Full-buffer Shrew（FB-Shrew）攻撃と呼ばれる TCP を標的とした LDDoS 攻撃の変形が明らかになている [25][26]．FB-Shrew 攻撃では，攻撃者はボトルネックリンクルータのバッファがバックグラウンドトラフィックによる TCP パケットで満たされた後にのみ，バーストトラフィックを送信する．これにより，ルーターは正当なパケットを廃棄し，TCP パケットの再送信を強制する．

本稿で検討した正常トラフィックを用いた LDDoS 攻撃は，RTO 間隔の典型的な Shrew 攻撃をベースにしており，攻撃者がバーストトラフィックに加えて，正常トラフィックを合わせて送信する点で FB-shrew 攻撃と異なる．

8. おわりに

本稿では，正規ユーザを装った攻撃ノードが正常トラフィックでバッファを消費することで，LDDoS 攻撃のバーストレートを削減する手法を検討した．シミュレーションによる実験から，正常トラフィックを使うことで，大容量バッファを備えたルータに対して攻撃効果が向上することを示し，攻撃トラフィックのバーストレートを削減する可能性について考察した．

今後改善するべき課題を二つ整理する．一つ目は，シミュレーション環境の現実性の向上である．今回のシミュレーションではクラウドストレージサービスを標的と仮定したが，ネットワーク帯域幅，ルータのバッファ容量，トポロジの構成について，現実の値や構成にすることができなかった．これは，我々の調査不足により，現実の値を推定できなかったためである．今後，標的となる環境をさらに詳細に定めて，上記の値と構成について現実的なシミュレーションを行うことで，インターネットにおける LDDoS 攻撃の実行可能性について明らかにする．加えて，シミュレーションに留まらず実機を用いた環境で検証を行うことで，現実的な実行可能性を示すことが可能であると考える．二つ目は．本稿にて検討した正常トラフィックを用いた LDDoS 攻撃の数学モデルの確立である．本稿では数学モデルを検討できなかったことから，攻撃効果について詳細な議論ができなかった．今後，数学モデルを確立することによって，特定のシミュレーション環境だけでなく，様々な環境における攻撃効果の適切な議論を可能にする．

謝辞　本研究は JSPS 科研費 JP17K00127 の助成を受けたものです．

参考文献

[1] Etherington, D. and Conger, K.: Large DDoS attacks cause outages at Twitter, Spotify, and other sites, TechCrunch (online), available from ⟨https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/⟩ (accessed 2020-02-18).

[2] Kottler, S.: February 28th DDoS incident report, COMPUTERWORLD (online), available from ⟨https://github.blog/2018-03-01-ddos-incident-report/⟩ (accessed 2020-02-18).

[3] Agrawal, N. and Tapaswi, S.: Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges, *IEEE Communications Surveys & Tutorials*, Vol. 21, No. 4, pp. 3769–3795 (2019).

[4] Kuzmanovic, A. and Knightly, E. W.: Low-rate TCP-targeted denial of service attacks and counter strategies, *IEEE/acm transactions on networking*, Vol. 14, No. 4, pp. 683–696 (2006).

[5] John, W. and Tafvelin, S.: Analysis of internet backbone traffic and header anomalies observed, *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pp. 111–116 (2007).

[6] 髙橋佑太, 稲村　浩, 中村嘉隆：実ネットワーク環境下における LDDoS 攻撃の検証, 研究報告モバイルコンピューティングとパーベイシブシステム (MBL)，Vol. 2018-MBL-89, No. 8, pp. 1–7 (2018).

[7] 髙橋佑太，稲村　浩，中村嘉隆：実行可能性の検討を目的とした現実的なトポロジにおける Low-rate DDoS 攻撃のシミュレーション，マルチメディア, 分散協調とモバイルシンポジウム 2019 論文集，Vol. 2019, pp. 57–63 (2019).

[8] Paxson, V., Allman, M. and Sargent, M.: Computing TCP's Retransmission Timer, Internet RFC 6298 (online), available from ⟨https://tools.ietf.org/html/rfc6298⟩ (accessed 2020-02-18).

[9] Luo, J., Yang, X., Wang, J., Xu, J., Sun, J. and Long, K.: On a mathematical model for low-rate shrew DDoS, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 7, pp. 1069–1083 (2014).

[10] Sarat, S. and Terzis, A.: On the effect of router buffer sizes on low-rate denial of service attacks, *Proceedings. 14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005.*, IEEE, pp. 281–286 (2005).

[11] Chen, Y., Hwang, K. and Kwok, Y.-K.: Filtering of shrew DDoS attacks in frequency domain, *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) l*, IEEE, pp. 1–8 (2005).

[12] Chen, Y. and Hwang, K.: Collaborative detection and filtering of shrew DDoS attacks using spectral analysis, *Journal of Parallel and Distributed Computing*, Vol. 66, No. 9, pp. 1137–1151 (2006).

[13] Brynielsson, J. and Sharma, R.: Detectability of low-rate HTTP server DoS attacks using spectral analysis, *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, IEEE, pp. 954–961 (2015).

[14] Wu, Z., Pan, Q., Yue, M. and Liu, L.: Sequence alignment detection of TCP-targeted synchronous low-rate DoS attacks, *Computer Networks*, Vol. 152, pp. 64–77 (2019).

[15] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M. and Buyya, R.: Combating DDoS attacks in the

cloud: requirements, trends, and future directions, *IEEE Cloud Computing*, Vol. 4, No. 1, pp. 22–32 (2017).

[16] Agrawal, N. and Tapaswi, S.: A lightweight approach to detect the low/high rate IP spoofed cloud DDoS attacks, *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, IEEE, pp. 118–123 (2017).

[17] Eucalyptus Cloud-computing Platform, GitHub (online), available from ⟨https://github.com/eucalyptus/eucalyptus⟩ (accessed 2020-02-18).

[18] Cloud Performance Benchmark 2019 – 2020 v1.1, ThousandEyes, Inc (online), available from ⟨https://www.thousandeyes.com/resources/cloud-performance-benchmark-report-november-2019⟩ (accessed 2020-02-18).

[19] ns-3 — a discrete-event network simulator for internet systems, nsnam.org (online), available from ⟨https://www.nsnam.org/⟩ (accessed 2020-02-18).

[20] Mathis, M., Mahdavi, J., Floyd, S. and Romanow, A.: TCP selective acknowledgment options, RFC 2018 (online), available from ⟨http://www.hjp.at/doc/rfc/rfc2018.html⟩ (accessed 2020-02-18).

[21] Zhijun, W., Lan, M., Minghua, W., Meng, Y. and Lu, W.: Research on time synchronization and flow aggregation in LDDoS attack based on cross-correlation, *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, pp. 25–32 (2012).

[22] Appenzeller, G., Keslassy, I. and McKeown, N.: Sizing router buffers, *ACM SIGCOMM Computer Communication Review*, Vol. 34, No. 4, pp. 281–292 (2004).

[23] Beheshti, N., Lapukhov, P. and Ganjali, Y.: Buffer Sizing Experiments at Facebook, *Proceedings of the 2019 Workshop on Buffer Sizing*, pp. 1–6 (2019).

[24] Spang, B., Walsh, B., Huang, T.-Y., Rusnock, T., Lawrence, J. and McKeown, N.: Buffer sizing and Video QoE Measurements at Netflix, *Proceedings of the 2019 Workshop on Buffer Sizing*, pp. 1–7 (2019).

[25] Yue, M., Wu, Z. and Wang, M.: A new exploration of FB-shrew attack, *IEEE Communications Letters*, Vol. 20, No. 10, pp. 1987–1990 (2016).

[26] Yue, M., Wang, M. and Wu, Z.: Low-High Burst: A Double Potency Varying-RTT Based Full-Buffer Shrew Attack Model, *IEEE Transactions on Dependable and Secure Computing* (2019).