「マルチメディア，分散，協調とモバイル
(DICOMO2019) シンポジウム」 令和元年7月

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

髙橋 佑太[1]　稲村 浩[2]　中村 嘉隆[2]

概要：インターネット通信において広く使われている TCP は，低量分散型サービス妨害（LDDoS: Low-rate Distributed Denial of Service) 攻撃によって継続的な通信妨害が可能であることが理論上と単純な環境における検証により明らかになっているが，現実のインターネットにおける実行可能性は不明である．そこで本研究では，上記のネットワークの特性について現実性の高いシミュレーションを実行することで，現実のネットワークにおいて効果的な LDDoS 攻撃に必要な条件・制約を明らかにし，現実のインターネットにおける LDDoS 攻撃の潜在的な標的の発見や有効な検知・緩和手法の確立を目指す．本稿では，インターネットトポロジの特性に着目し，家庭用ブロードバンドを提供している ISP ネットワークに見られる特徴を反映したトポロジを生成した．さらに生成したトポロジにおいて LDDoS 攻撃のシミュレーションを実行し，標的ボトルネックリンク帯域幅が 100Mbps の場合に TCP スループットを大きく低減させることが可能な攻撃フローの大きさを示し，今後に向けた課題を整理した．

A Feasibility Study on Low-rate DDoS Attack in Realistic Topology

YUTA TAKAHASHI[1]　HIROSHI INAMURA[2]　YOSHITAKA NAKAMURA[2]

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．CDNetworks の調査では，2018 年度に同社が対処した DDoS 攻撃のうち，UDP フラッドや SYN フラッド等のフラッド型と呼ばれるネットワーク帯域幅攻撃が全体の半分以上の割合を占めていた [1]．この手法は，ボットネットから大量の攻撃トラフィックを送信することによって，標的周辺のネットワーク帯域幅や標的の CPU，メモリなどの資源を可能な限り消費し，サービスの提供を停止させるという特徴をもつ．単純で強力な攻撃効果を生むことが可能であるが，大量の攻撃トラフィックを用いて負荷を与えるため，検知や緩和が容易である．

Kuzmanovic らは，低量分散型サービス妨害 (LDDoS: Low-rate Distributed Denial of Service) 攻撃によって，TCP 通信を継続的に妨害可能であることを明らかにした [2]．LDDoS 攻撃は TCP 再送信タイムアウトの仕様を利用して低い平均通信量で TCP 通信を妨害することが可能であり，攻撃が完全に成功した場合，標的 TCP は継続してタイムアウトを引き起こし，スループットはほぼ 0 まで低下する．長さが短く高レートな矩形波のバーストトラフィックを用いて攻撃することで，攻撃トラフィックの平均通信量が一般的なフラッド型 DDoS 攻撃のものと比較して低量となるため，既存の DDoS 攻撃トラフィックの検知手法で LDDoS 攻撃トラフィックを検知することは困難である．攻撃者によって LDDoS 攻撃が正確に実行された場合の脅威は大きいため，攻撃の検知についてさまざまなアプローチ [3][4][5] が検討されているが，誤検知率が高いことや，評価実験が不十分であるということが課題となっており，現在効果的な検知手法は確立されていない．一方で，これまでに LDDoS 攻撃の実例は確認されていない．理由として，LDDoS 攻撃は複数の低量トラフィックを合成して瞬時にボトルネックリンクのバッファを溢れさせる必要があるため，複雑な実ネットワークにおいては実行難易度が高く，一般的なフラッド型 DDoS 攻撃の方が容易に大きな効果を得られるためであることが考えられる．しかし，

[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

DDoS 攻撃はこれからも複雑化・高度化されることが予想されているため [1]，現在最も使用されている通信プロトコルである TCP に対しステルス性の高い LDDoS 攻撃が今後実行される可能性も考えられる．

効果的な LDDoS 攻撃は，単純なダンベル型トポロジ（図 2）上では実行可能であることが確認されている（詳細は 2 章で説明）．しかし，単純なダンベル型トポロジを現実的なネットワークに照らし合わせて考えた場合，送信ノードと攻撃ノードが同一ネットワーク内に接続されているという状況に限定されるため，LDDoS 攻撃が実ネットワークにおいて真に脅威となる攻撃手法であるかは定かでない．加えて現実のネットワークでは，以下のような様々なネットワークの特性によってパケットの損失率や遅延，ジッタが大きく変動し，正確な LDDoS 攻撃フローの合成を困難にする可能性が考えられる．

- ネットワークトポロジの特性
- ネットワークトポロジの規模
- 外乱トラフィックによるネットワークのリンク品質の変動
- ルータのキュー制御アルゴリズム

そこで本研究では，上記のネットワークの特性について現実性の高いシミュレーションを実行することで，現実のネットワークにおいて効果的な LDDoS 攻撃に必要な条件・制約を明らかにし，現実のインターネットにおける LDDoS 攻撃の潜在的な標的の発見や有効な検知・緩和手法の確立を目指す．

本稿では，ネットワークトポロジの特性に着目し，以下の構成のもと，家庭用ブロードバンドにおいて LDDoS 攻撃を実行する場合に必要な攻撃条件と制約を明らかにする．2 章で，背景の TCP 再送信タイムアウトと LDDoS 攻撃の詳細を説明する．3 章で，現実的な特性をもったトポロジで LDDoS 攻撃をシミュレーションするために，家庭用ブロードバンドを提供している ISP ネットワークに見られる特徴を反映したトポロジを生成する．4 章で，生成したトポロジを用いてシミュレーションを実行し，効果の高い LDDoS 攻撃に必要なトラフィックの条件とその際に発生する制約について考察と議論をする．5 章で，関連研究をまとめ，さらに現実的なシミュレーションの実行のために必要な事柄と本研究の立ち位置について確認する．6 章で，まとめと今後の展望を述べる．

2. 背景

本章では，LDDoS 攻撃の原因である TCP 再送信タイムアウトと，それを利用した LDDoS 攻撃の詳細に加え，実ネットワーク環境下における LDDoS 攻撃の実行可能性について述べる．

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:Retransmisson Time Out）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 の初期値は RFC6298[6] により，次の式で設定される．

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

ここで $minRTO$ は RTO の最小値，$SRTT$ は平滑化したラウンドトリップタイム（RTT: Round Trip Time），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[6] 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

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

が成り立つため，これ以降 RTO の初期値は $minRTO$ に設定され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．

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

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．攻撃者は $minRTO$ の間隔で標的コネクションを輻輳させることにより，低い平均通信量で標的の TCP 通信は継続してタイムアウトを引き起こし，スループットを低下させることが可能である．

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状の LDDoS 攻撃フロー（図 1）を複数の攻撃ノードから送信し，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，低い平均通信量で TCP 通信を妨害することが可能な攻撃手法である [2].

2.2.1 LDDoS 攻撃フローのモデル化

1 つの攻撃ノードが送信する LDDoS 攻撃フローをバースト間隔 T_a，バースト幅 T_b，バーストレート R_b，攻撃開始時間 s により定義する（図 1）.

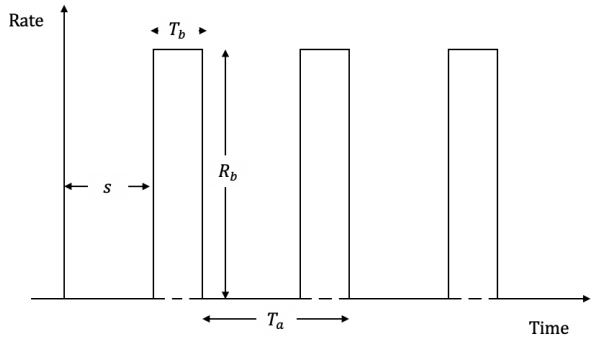

図 1 LDDoS 攻撃の単一フロー　複数のフローを合成することによりボトルネックリンクのバッファを溢れさせる

複数のフローがボトルネックリンク上で合成された LDDoS 攻撃フローのバースト間隔を T_a^+，バースト幅を T_b^+，バーストレートを R_b^+ と定義する（図 3）．文献 [3] では，更に詳細にモデル化されている.

2.2.2 効果的な LDDoS 攻撃

LDDoS 攻撃は，T_a^+ を minRTO と等しい長さ，T_b^+ を 200ms から 300ms の長さ，R_b^+ をボトルネックリンクのバッファを十分に満たす大きさに設定した場合に最も大きな効果を生み，標的の TCP スループットをほぼ 0 まで低下可能であることが示されている [2][7].

ボトルネックリンク上で上記パラメータを満たす LDDoS 攻撃フローを生成できた場合，1 回目の合成バーストトラフィックにより，ボトルネックリンクのバッファが溢れ，標的の TCP のパケットが喪失する．次に，標的 TCP は（3）式により，minRTO だけ再送信タイムアウトを待ったあと喪失したパケットを再送信する．このとき，タイミングを合わせて攻撃フローを繰り返し送信し，合成バーストトラフィックを生成して攻撃を継続することで，再びボトルネックリンクのバッファが溢れるため標的 TCP のパケットが喪失する．その後も標的 TCP の minRTO と同じバースト間隔でバーストトラフィックを送信を続けることで，標的 TCP の送信ノードの RTO が（4）式により，minRTO の倍数の値を取り続けるため，バーストトラフィックと再送信のタイミングが重なり，通信が抑止された状態が継続される.

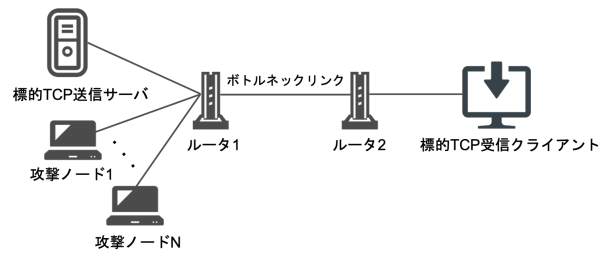

図 2 効果的な LDDoS 攻撃が可能なダンベル型トポロジ　標的 TCP の送信ノードとすべての攻撃ノードがルータ 1 に接続されており，ルータ 1 のバッファを溢れさせることにより，送信ノードから受信ノードに向けた TCP パケットを妨害する.

効果的な LDDoS 攻撃を検証している多くの研究（シミュレーション [2][4][8]，実証実験 [9]）では，単純なダンベル型トポロジ（図 2）を用いており，現実のインターネットのように複雑な環境においても同様に実行可能であるかは明らかではない.

3. シミュレーション環境の設定

本章では，家庭用ブロードバンドを提供している ISP ネットワークに見られる特徴を反映したシミュレーション環境の設定について説明する．シミュレーションにはネットワークシミュレータ ns-3[10] を使用する．以下の特性を設定し，図 4 のトポロジを生成した．図 4 中のノードの説明を表 1 に示す.

表 1 ノードの説明

ノード	説明
$R_0 \cdots R_9$	バックボーンルータ 0$\cdots$ バックボーンルータ 9
TCP_{Tx}	標的 TCP 送信サーバ
TCP_{Rx}	標的 TCP 受信クライアント
$Attacker_1 \cdots Attacker_{40}$	攻撃ノード 1$\cdots$ 攻撃ノード 40
$M_{TCP_{Tx}}$	標的 TCP 送信サーバのモデム
$M_{TCP_{Rx}}$	標的 TCP 受信クライアントのモデム
$M_{A1} \cdots M_{A40}$	攻撃ノード 1$\cdots$ 攻撃ノード 40 それぞれのモデム

3.1 トポロジの構成

Barabasi と Albert によって現実のバックボーンネットワークにはスケールフリー性（次数分布のべき乗則）が見出されており，BA モデルとして知られている [11]．Kong らは数多く存在する DDoS 攻撃検知手法の現実的な有効性を実証するためには，BA モデルのトポロジを用いた DDoS 攻撃のシミュレーションが有効であると提案している [12].

そこで，上記を参考に ns-3 でサポートされているトポロジジェネレータ BRITE[13] を用いて BA モデルのトポロジを生成し，シミュレーションを実行する．表 2 にトポロジの生成使用する BRITE の設定パラメータを示す．現実の ISP は複数の AS によって構成されている [14] が，複雑性を徐々に上げていくため今回は複数の AS を考慮せず，すべてのノードを 1 つの AS 内に配置する Router BA モデルで生成した．今回のシミュレーションでは，BRITE で生成した 10 個のノード（$R_0 \cdots R_9$）を ISP の AS トポロジ一つを構成するバックボーンルータと想定

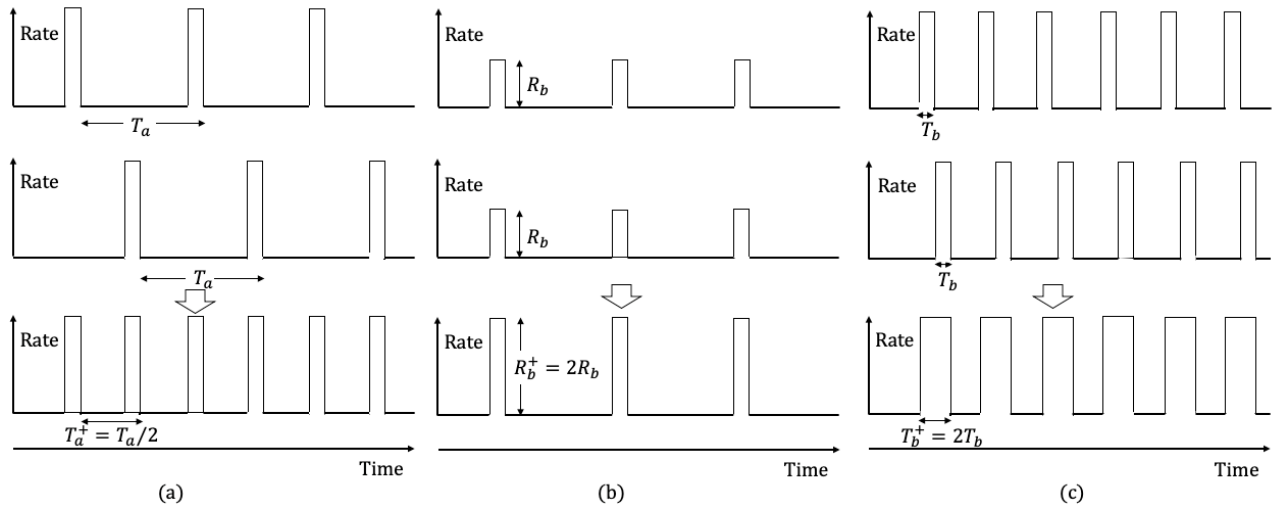

図 3　LDDoS 攻撃フローの合成（a）バースト間隔，（b）バーストレート (c) バースト幅　（文献 [3] 図 3 を参考に作成）

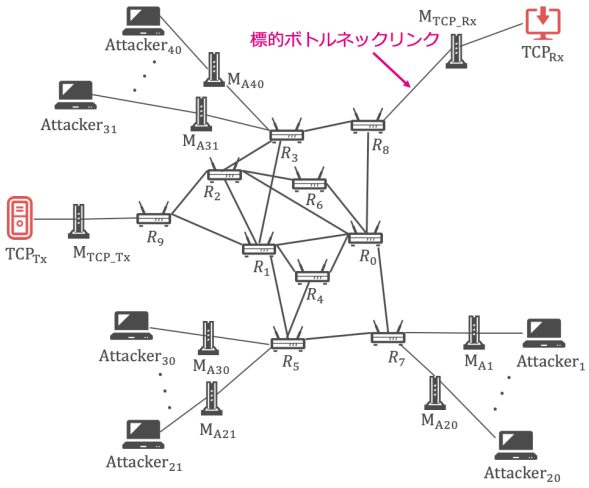

図 4　生成したトポロジ

する．次に標的 TCP 送信サーバ（TCP_{Tx} ）1 台，標的 TCP 受信クライアント（TCP_{Rx}）1 台，攻撃ノード 40 台（$Attacker_1 \cdots Attacker_{40}$）をそれぞれの各モデムノード（$M_{TCP_{Tx}}$, $M_{TCP_{Rx}}$, $M_{A1} \cdots M_{A40}$）と接続し，モデムノードをバックボーンルータに接続した．

表 2　BRITE 設定パラメータ

パラメータ（意味）	設定値	備考
Name (モデル)	2	Router BA model
N (ノード数)	10	
HS (主平面の大きさ)	1,000	デフォルト値
LS (内面の大きさ)	100	デフォルト値
NodePlacement (ノード配置方法)	1	ランダム
m (link/node)	2	
BWDist (帯域幅の割当分布)	1	一定（すべて BWMin に固定）
BWMin (最小帯域幅)	2,500	2.5Gbps
BWMax (最大帯域幅)	2,500	BWDist が一定のため無効

3.2　リンクパラメータ・ボトルネックリンクの位置

北米とヨーロッパの主要 ISP を対象にした Dischinger らの家庭用ブロードバンドネットワークの調査によって，住宅ネットワークのバックボーンルータと家庭に設置されたモデムを繋ぐブロードバンドリンク（ラストマイル）がボトルネックリンクになっていることが明らかとなった [15]．これを参考に，インターネットトポロジと攻撃ノードが接続されたモデムノードを繋ぐリンクがボトルネックとなるように帯域幅と RTT を設定する．

$R_0 \cdots R_9$ を結ぶ各リンクの帯域幅は，文献 [16] を参考に 2.5Gbps，バックボーントポロジの RTT はごく僅かな値として 0.75ms を設定した．その他のリンクの帯域幅と RTT は表 3 の値を設定した．標的 TCP 受信クライアントと攻撃ノードは家庭用ブロードバンドに接続されていると仮定し，それらが接続されているモデムのブロードバンドリンクの下り帯域幅を 100Mbps，上り帯域幅を 10Mbps に設定した．文献 [9] において我々は IoT 端末の Raspberry Pi を用いて R_b =10Mbps の LDDoS 攻撃フローを生成できたことから，上り帯域幅の設定は現実的な値として考えられる数値であるといえる．標的 TCP 送信サーバは他 ISP のサービス事業者用のネットワークから接続されていると仮定し，帯域幅を 1,000Mbps に設定した．RTT の現実性は今回のシミュレーションで考慮せず，すべての攻撃ノードが適切に攻撃フローを合成できるようにボトルネックリンクルータ R_8 までの RTT をほぼ等しく設定した．

3.3　ルータバッファ

$R_0 \cdots R_9$ の各リンクのネットワークデバイスには BRITE の初期値である 100pkts のドロップテールキューを設定した．

表 3　リンクパラメータ

リンク	帯域幅（Mbps）	RTT (ms)
TCP_{Tx} to $M_{TCP_{Tx}}$	1,000	1
$M_{TCP_{Tx}}$ to R_9	100	10
TCP_{Rx} to $M_{TCP_{Rx}}$	1,000	1
$M_{TCP_{Rx}}$ to R_8 (標的ボトルネックリンク)	100	5
$Attacker_i$ to $M_{Ai}(i=1,2,\cdots,40)$	1,000	1
$M_{A1}\cdots M_{A20}$ to R_7	10	10
$M_{A21}\cdots M_{A30}$ to R_5	10	10
$M_{A31}\cdots M_{A40}$ to R_3	10	10

3.4　LDDoS 攻撃に必要な前提条件

図 4 のトポロジで LDDoS 攻撃を実行するために必要な前提条件を整理する．

(1) 攻撃者は $Attacker_1\cdots Attacker_{40}$ を自由に操作可能である．

(2) 攻撃者は $Attacker_1\cdots Attacker_{40}$ と R_8 間の RTT を計測し，それぞれの攻撃開始時間を指定できる．

(3) $Attacker_1\cdots Attacker_{40}$ と R_8 間の RTT が安定しており大きなジッタは発生しない．

(4) $M_{A1}\cdots M_{A40}$ に $Attacker_1\cdots Attacker_{40}$ 以外のノードが接続されていた場合，それらのノードは攻撃フローを送信している間は通信を行わない．

(5) 攻撃者は TCP_{Tx} の minRTO を特定している．（今回は 1 秒に設定）

以上が満たされたと仮定してシミュレーションを実行する．

4.　シミュレーション実験

4.1　効果的な LDDoS 攻撃に必要なバーストレートと攻撃ノード数の推定

3 章で生成した家庭用ブロードバンドネットワークの特性を設定したトポロジにおいて，効果的な LDDoS 攻撃に必要なバーストレートと攻撃ノード数をシミュレーションにより検証する．標的 TCP スループットを 1 割未満に妨害することが可能なバーストレートの大きさを明らかにするために，ボトルネックリンクルータである R_8 のバッファを 100pkts と 1,000pkts に設定したそれぞれの場合について，以下のシミュレーションを実行する．

TCP_{Tx} は TCP_{Rx} へ 200MB のデータを 60 秒間可能な限り Bulk Send で送信し，その平均正規化スループットを計測する．攻撃ノード 1 台当たり $T_a = 1.0s$，$T_b = 250ms$，$R_b = 10Mbps$ の攻撃フローを TCP_{Rx} に送信し，TCP_{Tx} の TCP を妨害する．シミュレーションは計 40 回実行する．1 回のシミュレーションごとに，$Attacker_1$ から $Attacker_{40}$ を 1 台ずつ参加させ，攻撃に参加するノードはすべて同時刻に攻撃を開始する．今回はすべての攻撃ノードからボトルネックリンクルータ R_8 までの RTT がほぼ等しくなるように設定したため，R_8 で合成された攻撃フローの合計パラメータは $T_a^+ = 1.0s$，$T_b^+ = 250ms$，$R_b^+ = 10, 20, \cdots, 400Mbps$ となる．

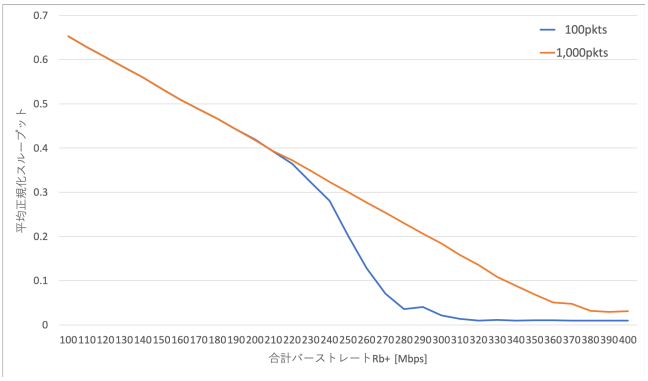

図 5　ボトルネックリンクルータ R_8 のバッファとバーストレート R_b^+ の増加による標的 TCP の平均正規化スループットの推移

4.2　実験結果

シミュレーションの結果を図 5 に示す．標的 TCP の平均正規化スループットを 1 割未満に低下させるために最低限必要な合計バーストレート R_b^+ は，ボトルネックリンクルータ R_8 のバッファが 100pkts の場合は約 270Mbps，1,000pkts の場合は約 340Mbps という結果が得られた．よって，家庭用ブロードバンドの特性を設定したトポロジにおいて，攻撃者が 3.4 節の前提条件を満たすことができた場合，効果的な LDDoS 攻撃が実行可能であることが明らかになった．

4.3　考察

本節では，効果的な LDDoS 攻撃に必要な条件と制約，現実性について考察する．

4.3.1　攻撃に必要な条件と制約

攻撃ノードの配置に関する制約と現実性について考察する．一般的なバックボーンリンクの使用率は 10%から 30%であると文献 [17] で述べられている．今回のトポロジでバックボーンリンク全体の帯域幅が他の一定的なトラフィックによって 30%使用された場合，残りの使用可能帯域幅は 1.75Gbps となる．よって R_b^+ が 1.75Gbps 未満の場合，すべての攻撃フローが同じリンク経路を流れたとしてもリンクが溢れることはないため，攻撃フローが損失されないことから，攻撃ノードの配置を考慮しなくても効果的な攻撃を実現できるといえる．したがって，今回のシミュレーションにおいて効果的な LDDoS 攻撃を実行するために必要な条件は，ボットネット環境を構築する際に最低限 340Mbps の帯域幅を確保することであるといえる．このときに攻撃ノードの配置に関する制約はない．一方で，標的ボトルネックリンクの帯域幅が高く，必要なバーストレート R_b^+ が 1.75Gbps 以上必要となる場合に攻撃フローが一部のリンクに集中してしまうとロスが発生するため，

攻撃ノードの配置に制約が生まれることが考えられる．この制約について一般化し，明らかにすることは今後の課題となる．

攻撃ノードの配置については，標的ボトルネックリンクと同じ AS 内にすべての攻撃ノードを構築することは現実的ではない．より現実的なシミュレーションにするために複数の AS トポロジを考慮し，トポロジの規模拡大と攻撃ノードを複数の AS トポロジに分散した際に発生する制約を明らかにすることが課題として挙げられる．

4.3.2 ボトルネックリンクルータのバッファによる攻撃効果の低減

図 5 の結果から，標的ボトルネックリンク帯域幅の 2 倍から 3 倍のバーストレートの攻撃フローに対して，ルータのバッファが大きいほど，スループットの損失率を大きく低減できることがわかった．バーストレートが標的ボトルネックリンクの 4 倍以上の大きさである $R_b^+ = 400Mbps$ の場合，ルータのバッファサイズによる平均正規化スループットに変化はほとんど見られないため，リンクに対して過剰なバーストレートに対する検知精度を高め，検知が難しいそれ以下のバーストレートに対してはルータのバッファサイズを多く確保することにより，攻撃の検知と緩和を両立できる可能性があると考える．

5. 関連研究

Heckmann らはネットワークトポロジを比較するための類似性メトリクスを提示し，それに基づいて現実の ISP（DFN，AT&T）に類似性が高いトポロジを BRITE などのトポロジジェネレータで生成するために必要なパラメータを導き出した [14]．これを使用することで現実性の高いトポロジを生成できるため，今後これらのパラメータを活用していく．

Feng らはデータセンターネットワーク（DCN: Data Center Network）における LDDoS 攻撃の実行可能を検証した [18]．DCN は高帯域幅，低遅延で安定しており，トポロジの特性も限られているいるため，悪意のあるテナントが LDDoS 攻撃によって同じネットワークリソースを共有している他のテナントの TCP 通信を妨害できる危険性があった．24 台の物理サーバに 48 台の VM を構築して再現した DCN のテスト環境を用いて LDDoS 攻撃を検証した結果，TCP スループット損失率が最大 83%まで上昇したことから DCN において LDDoS 攻撃が有効であることが示された．この研究は LDDoS 攻撃の実行可能性を議論している点で関連しているが，本研究はさらに一般的なインターネット上における実行可能性を明らかにすることが目的である．

6. おわりに

6.1 まとめ

本稿では，家庭用ブロードバンドの特徴を設定したトポロジを用いて LDDoS 攻撃をシミュレーションし，ボトルネックリンクの帯域幅が 100Mbps の場合，合計バーストレートが 270Mbps から 340Mbps の LDDoS 攻撃フローを生成することで，標的 TCP スループットを 1 割以下に低減させることが可能であることを確認した．さらに，攻撃に必要な条件と制約やボトルネックリンクルータのバッファによる攻撃効果の低減から LDDoS 攻撃の検知・緩和について考察した．

6.2 今後の展望

現実のインターネットにおける LDDoS 攻撃を実行可能性をさらに詳しく検討するために，今回のシミュレーションの課題とアプローチについてまとめる．1 つ目はトポロジのモデルである．今回のシミュレーションでは AS トポロジについて考慮できなかったため，AS トポロジと Router トポロジを組み合わせ，遅延や帯域幅について現実のトポロジに近似したトポロジモデルを構築する必要がある．2 つ目はトラフィックモデルである．文献 [12] のように，統計的モデルを使用した現実的なバックグラウンドトラフィックを生成し，ジッタによる RTT の変動が大きい環境における LDDoS 攻撃の実行可能性について検証する必要がある．3 つ目はルータのキュー制御アルゴリズムである．今回のシミュレーションではすべてのルータに Droptail を設定したが，RED などのキュー制御アルゴリズムもトポロジモデルやトラフィックモデルと同時に考慮する必要がある．これらの他に，攻撃者が実ネットワークにおいて，3.4 節で設定した LDDoS 攻撃に必要な前提条件を満たすことができるのかについても検証する必要がある．

参考文献

[1] 株式会社シーディーネットワークス・ジャパン：2018 年度、DDoS 攻撃の動向と今後の見通し，CDNetworks セキュリティレポート (オンライン)，入手先 ⟨https://engage.cdnetworks.co.jp/LP_WP36⟩（参照 2019-04-19）

[2] 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).

[3] Zhang,C.,Cai,Z.,Chen,W.,et al:Flow level detection and filtering of low-rate DDoS,Computer Networks,Vol.56,No.15,pp.3417-3431(2012).

[4] Kieu,M. V.,Nguyen,D. T.,and Nguyen,T. T.:Using CPR Metric to Detect and Filter Low-Rate DDoS Flows,Proceedings of the Eighth International Symposium on Information and Communication Technology. ACM,pp.325-332(2017).

[5] Jadhav,P. N.,and Patil,B. M.:Low-rate DDOS At-

tack Detection using Optimal Objective Entropy Method,International Journal of Computer Applications,Vol.78,No.3,pp.33–38(2013).
[6] Paxson,V.,Allman,M.,Chu,J.,et al:Computing TCP's Retransmission Timer,Internet RFC 6298(オンライン), 入手先 ⟨https://tools.ietf.org/html/rfc6298⟩（参照 2019-05-01）.
[7] Efstathopoulos,P.:Practical study of a defense against low-rate TCP-targeted DoS attack,2009 International Conference for Internet Technology and Secured Transactions,(ICITST). IEEE,pp.1-6(2009).
[8] Zhijun,W.,Lan,M.,Minghua,W.,et al: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).
[9] 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).
[10] ns-3 — a discrete-event network simulator for internet systems, 入手先 ⟨https://www.nsnam.org/⟩（参照 2019-05-01）.
[11] Barabási,A.L. and Albert,R.:Emergence of scaling in random networks,science,Vol.286,No.5439,pp.509-512(1999).
[12] Kong,J.,Mirza,M.,Shu,J.,et al:Random flow network modeling and simulations for DDoS attack mitigation,IEEE International Conference on Communications,2003. ICC'03.. IEEE,Vol.1,pp.487-491(2003).
[13] Medina,A.,Lakhina,A.,Matta,I.,et al:BRITE:An approach to universal topology generation,MASCOTS 2001,Proceedings Ninth International Symposium on Modeling,Analysis and Simulation of Computer and Telecommunication Systems. IEEE,pp.346-353(2001).
[14] Heckmann,O.,Piringer,M.,Schmitt,J.,et al:On realistic network topologies for simulation,Proceedings of the ACM SIGCOMM workshop on Models,methods and tools for reproducible network research. ACM,pp.28-32(2003).
[15] Dischinger,M.,Haeberlen,A.,Gummadi,K. P.,et al:Characterizing residential broadband networks,Internet measurement conference,Vol.7,pp.43-56(2007).
[16] Fraleigh,C. J.:Provisioning Internet Backbone Networks to Support Latency Sensitive Applications. PhD thesis,Stanford University(2002).
[17] Appenzeller,G.,Keslassy,I.,and McKeown,N.:Sizing router buffers,ACM,Vol.34,No.4,pp.281-292(2004).
[18] Feng,Z.,Bai,B.,Zhao,B.,et al:Shrew Attack in Cloud Data Center Networks,2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks. IEEE,pp.441–445(2011).