平成 30 年度 公立はこだて未来大学卒業論文

実ネットワーク環境下における Low-rate DDoS 攻撃の研究

髙橋 佑太

システム情報科学部　情報アーキテクチャ学科　　学籍番号 1015143

指導教員　　(主) 稲村 浩　　(副) 中村 嘉隆

提出日 平成 31 年 1 月 29 日

Empirical Study on Low-rate DDoS Attack in Practical Network Environment

by

Yuta TAKAHASHI

BA Thesis at Future University Hakodate, 2019

Advisor: Hiroshi INAMURA, Coadvisor: Yoshitaka NAKAMURA

Department of Media Architecture, School of Systems Information Science
Future University Hakodate

January 29, 2019

Abstract− Existing research has revealed that TCP which is widely used in Internet communication is capable of continuous communication interference by Low-rate Distributed Denial of Service (LDDoS) attack. However, since the cases where LDDoS attacks have actually been done have not been confirmed, the effect of LDDoS attacks under the network environment is not clear. We aim to establish and evaluate LDDoS attacks under the network environment and to establish means for effective detection and deterrence of LDDoS attacks using the findings. In this paper, we investigated and discussed on LDDoS attacks on servers in small networks assumed for general households and small business offices under a real network environment. We investigate whether effective LDDoS attacks are possible when IoT equipment is used as an attack node, when the transmission queue capacity of routers making bottleneck links is realistic values and when attack traffic is generated from attack nodes connected via wireless LAN. Furthermore, we verified whether the attacker acquired the minimum RTO (Retransmisson Time Out) of the target server, which is important for setting the attack parameters, and it is possible to generate the attack traffic with realistically effective attack parameters. Through these verifications, we showed that LDDoS attacks can pose a threat in small networks.

Keywords: Network Security, Low-rate DDoS Attack, TCP Congestion Control, IoT Device

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既存研究により明らかにされつつある．しかし，これまで実際に LDDoS 攻撃が行われた事例は確認されていないため，実ネットワーク環境下における LDDoS 攻撃の効果は明らかではない．そこで我々は，実ネットワーク環境下において LDDoS 攻撃を構成・評価し，その知見を用いて LDDoS 攻撃の効果的な検知・抑止の手段を確立することを目指している．本稿では，一般家庭や小規模事業所を想定した小規模ネットワーク内のサーバに対して LDDoS 攻撃が有効な手法であるかについて実ネットワーク環境下で検証し議論した．IoT 機器を攻撃ノードに用いた場合，ボトルネックリンクを構成するルータの送信キュー容量が現実的な値の場合，無線 LAN で接続された攻撃ノードから攻撃トラフィックを生成した場合において効果的な LDDoS 攻撃が可能であるのかを検証した．さらに，攻撃パラメータの設定に重要な標的サーバの最小 RTO（Retransmisson Time Out）を攻撃者が取得し，現実的に効果的な攻撃パラメータで攻撃トラフィックを生成することが可能であるかについて検証した．これらの検証を通して，小規模ネットワークにおいて LDDoS 攻撃が現実的に脅威となり得ることを示した．

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, IoT 機器

目 次

第1章　序論

1.1　背景

サービス妨害（DoS:Denial of Service）攻撃や分散型 DoS（DDoS:Distributed DoS）攻撃は，インターネットを代表する脅威のひとつである．近年，セキュリティ対策が不十分な IoT（Internet of Things）機器を踏み台とした大規模な DDoS 攻撃が引き起こされていることが問題となっている．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 社が 620Gbps にも達する大規模な DDoS 攻撃を受けたことにより，Twitter や Amazon.com をはじめとした様々なサイトに一時的にアクセスしにくくなる問題が発生した [1]．この DDoS 攻撃の原因は，Dyn 社の調査によって Mirai と呼ばれるマルウェアに感染した IoT 機器によって構築されたボットネットによって引き起こされたものであり，攻撃に関与した機器は 10 万台に及ぶことが明らかとなった [2]．

インターネットに接続する IoT 機器の台数は年々増加しており，2020 年には 200 億台を超えると予測されている [3]．これに伴い，IoT 機器を標的としたマルウェアの数も増加の傾向にある．図 1.1 は Kaspersky 社が 2016 年から 2018 年上半期までに IoT 機器を対象としたマルウェアの修正数である [4]．2018 年上半期の修正数が 2017 年全体の修正数よりも 3 倍以上多いという結果を示していることから，今後も IoT 機器を対象としたマルウェアの数は増加していくと考えられる．

トレンドマイクロ社は 2019 年セキュリティ脅威予測において，ホームネットワークに接続する IoT 機器の増加に従い，サイバー犯罪者同士がより規模の大きいボットネット構築のため IoT 機器をめぐる「ワーム戦争」が勃発するという予測を行っている [5]．インターネット上ではサイバー犯罪者が DDoS 攻撃請負プラットフォームを構築し，DDoS 攻撃を第三者にビジネスとして提供しているため [6]，大規模な DDoS 攻撃が容易になりつつある．

これらの背景から，今後も IoT 機器を踏み台とした DDoS 攻撃が引き起こされる可能性が大いに懸念される．一方で，このような一般的な DDoS 攻撃は大量であるという点で攻撃トラフィックの特徴が捉えやすいため，単純な手法の特性はよく知られている．そのため，近年では様々な企業が DDoS 攻撃の対策ソリューションを提供している [7][8]．

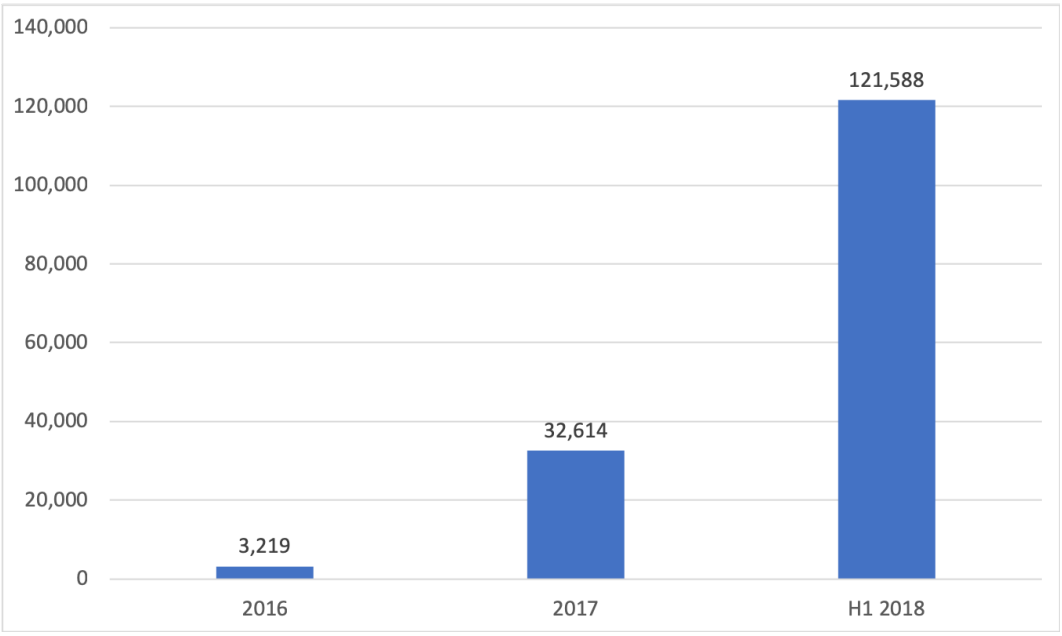


図 1.1: Kaspersky 社が 2016 年から 2018 年上半期までに IoT 機器を対象としたマルウェアの修正数（出典：文献 [4]）

1.2 低量なサービス妨害攻撃の手法

一般的な DDoS 攻撃の対策が進んできている一方で，低量 DoS(LDoS:Low-rate DoS) 攻撃 [9] と呼ばれる手法により，低い平均攻撃通信量で TCP 通信の妨害が可能であることが既存研究により明らかにされている．LDoS 攻撃は TCP の再送信タイムアウトの仕様を利用し，再送信が行われる短い時間の間に対象のボトルネックリンクに輻輳を発生させることで正規の通信を妨害する手法である．さらに，LDoS 攻撃を複数の攻撃ノードから分散して行う LDDoS 攻撃も可能であることが明らかになりつつあり [10][11][12][13]，一般的な DDoS 攻撃の防御手段を回避するよう企図されていることから脅威となり得ることが指摘されている．しかし，これまでに LDDoS 攻撃による被害は確認されていないため，複雑な実ネットワーク環境下において正確に低量な攻撃トラフィックを集約して任意の標的に対して効果的な LDDoS 攻撃を構成できるのかについては明らかになっていない．既存研究では，LDDoS 攻撃の検知や対策として，標的のボトルネックリンクルータ上で攻撃トラフィックを分析して LDDoS 攻撃を検知する手法が提案されているが，誤検知率が高いことや評価実験が不十分であるという課題があるため，効果的な検知手法は現在確立されていない．

1.3 本研究の目的

本研究は実ネットワーク環境下にて効果的な LDDoS 攻撃を構成する際に必要な条件を明らかにし，その条件を用いて LDDoS 攻撃の効果的な検知・抑止の手段を確立することを最終目的とする．そのための第一段階として，本稿では実ネットワーク環境下において効果的な LDDoS 攻撃を構成するために必要な条件を明らかにすることに焦点をおき，実ネットワーク環境下で LDDoS 攻撃を検証することで，LDDoS 攻撃の実現性について議論をおこなう．

1.4 論文の構成

本稿は全 9 章から構成されている．第 1 章は本研究の背景と研究目的について述べる．第 2 章では LDoS 攻撃と LDDoS 攻撃について詳細に説明する．第 3 章では関連研究とその課題について述べる．第 4 章では本稿で検証する LDDoS 攻撃の想定環境と実践的な検証のアプローチについて述べる．第 5 章では IoT 機器を用いた LDDoS 攻撃の検証とその結果と考察について述べる．第 6 章では標的ルータの送信キュー容量を現実的な値に近づけた環境で LDDoS 攻撃を検証しその結果と考察について述べる．第 7 章では無線環境下における LDDoS 攻撃の検証とその結果と考察について述べる．第 8 章では標的サーバの minRTO の値を攻撃者が取得し，実践的な LDDoS 攻撃が可能であることの指摘と，その有効性を検証するための実験について述べる．最後に，第 9 章でまとめと今後の課題について述べる．

第2章　関連技術

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[17] により，次の式で設定される．

$$RTO = max\{minRTO, SRTT + max(G, 4 \times \ RTTAVR)\} \tag{2.1}$$

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[17] 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（2.1）式の右辺では

$$minRTO > SRTT + max(G, 4 \times \ RTTAVR) \tag{2.2}$$

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．

$$RTO_1 = minRTO \tag{2.3}$$

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（2.4）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．

$$RTO_i = 2RTO_{i-1} \tag{2.4}$$

当該パケットの送信と応答が成功した場合，(2.3) 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という単純な仕様が LDoS/LDDoS 攻撃に利用されている．

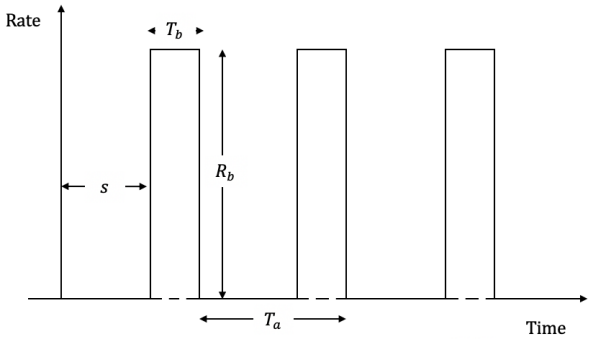


図 2.1: LDoS 攻撃フロー

2.2 LDoS 攻撃

LDoS 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 LDoS 攻撃フローを連続して送信することで，TCP で通信をしている標的サーバが喪失したパケットを再送信するわずかな時間の間のみ，対象の TCP コネクションのボトルネックリンクに輻輳を発生させてクライアントとの通信を妨害する攻撃手法である [9]．LDoS 攻撃フローは図 2.1 のようにバースト間隔 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 の 4 つのパラメータにより定義される．ここで，T_a を minRTO と等しい長さ，T_b を RTT 程度の長さ，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得ることが可能であり，標的サーバの TCP コネクションのスループットを完全に抑止することができる．このときの攻撃について説明する．

はじめに，攻撃者による 1 回目の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枯渇し正規の送信トラフィックにパケット喪失が発生する．次に，標的サーバは（2.3）式により，minRTO だけ再送信タイムアウトを待ったあと通信に失敗したパケットを再送信する．このとき，攻撃者が繰り返しバーストトラフィックを送信することで，再びボトルネックリンクのバッファが枯渇するため標的サーバの通信が再び失敗する．攻撃者はその後も標的サーバの 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，標的サーバの RTO が（2.4）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．このときの正規化回線容量は文献 [9] により以下の（2.5）式で表せる．

$$\rho = \frac{T_a - minRTO}{T_a} (for T_a \geq minRTO) \tag{2.5}$$

正規化回線容量は 0 以上 1 以下の値となり，1 との差がサービス妨害の被害になる．バースト間隔 T_a が minRTO と等しい場合，正規化回線容量は 0 となるため通信が完全に抑止される．

2.3 LDDoS 攻撃

LDDoS 攻撃は LDoS 攻撃フローを複数の攻撃ノードから分散して送信し，標的のボトルネックリンク上で LDDoS 攻撃フローとして集約することで LDoS 攻撃と同様に通信を妨害する攻撃手法である．バーストトラフィックを複数の攻撃ノードから分散して送信することで，攻撃ノード一台から送信されるトラフィックの大きさが LDoS 攻撃の場合と比較してさらに低量になるため，攻撃の検知をより困難にすることや，より強力な攻撃フローを生成することが可能になる．そのため，LDDoS 攻撃はインターネットの新たな脅威となる可能性があるが，今までに LDDoS 攻撃が実際に行われた事例は確認されていないため，実ネットワーク環境下でどの程度の攻撃効果を及ぼすのかは明らかになっていない．

LDDoS 攻撃フローは Zhang らによって詳細にモデル化されている [10]．このモデルでは，LDDoS 攻撃フローを複数の LDoS 攻撃フローの集合と定義し，T_a，T_b，R_b，s がすべて等しい LDoS 攻撃フローの集合を 1 つの LDDoS 攻撃フローとしてグループ化する．図 2.2 はこの定義に従い LDDoS 攻撃フローをグループ化した様子を示したものである．ここで，LDDoS 攻撃フローを 4 つのパラメータ（n，g，m，σ）で定義する．n は攻撃ノード数，g は攻撃グループ数，m は 1 つの攻撃グループを構成している攻撃ノード数，σ は連続したグループ間の攻撃開始時間の差を表す．ここで，σ は一定に保たれると仮定する．すなわち，図 2.1 において $sg_1 = sg_2$ である．m はすべてのグループで等しいものと仮定する．

これらの定義と仮定に基づき，Zhang らは LDDoS 攻撃フローを生成することを LDoS フローを強化するとみて，LDDoS 攻撃フローがバースト間隔（T_a）について強化されているものを「攻撃頻度強化（AFI:Attack Frequency Intensification）」，バースト幅（T_b）について強化されているものを「攻撃バースト幅強化（AWI : Attack burst Width Intensification）」，バーストレート（R_b）について強化されているものを「攻撃バーストレート強化（ARI : Attack burst Rate Intensification）」，これら 3 つの内 2 つ以上を組み合わせたものを「混合強化（MI : Mixed Intensification）」として分類した（図 2.3）．

これ以降，本稿では LDDoS 攻撃フローを Zhang らが定義したモデルを用いて表す．

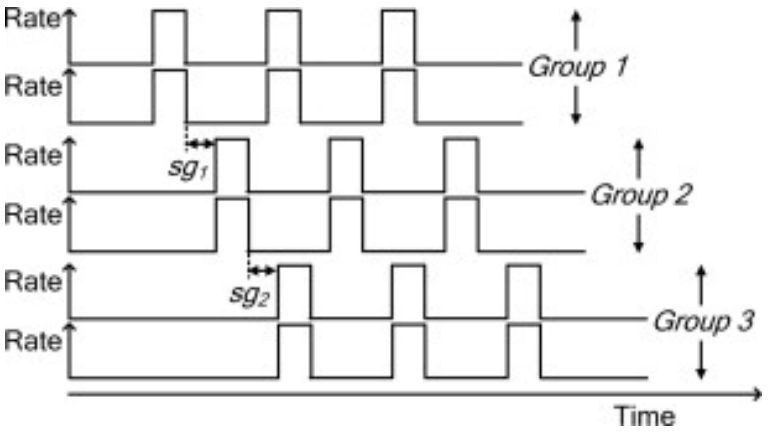


図 2.2: LDDoS 攻撃フローのグループ化（出典：文献 [10]）

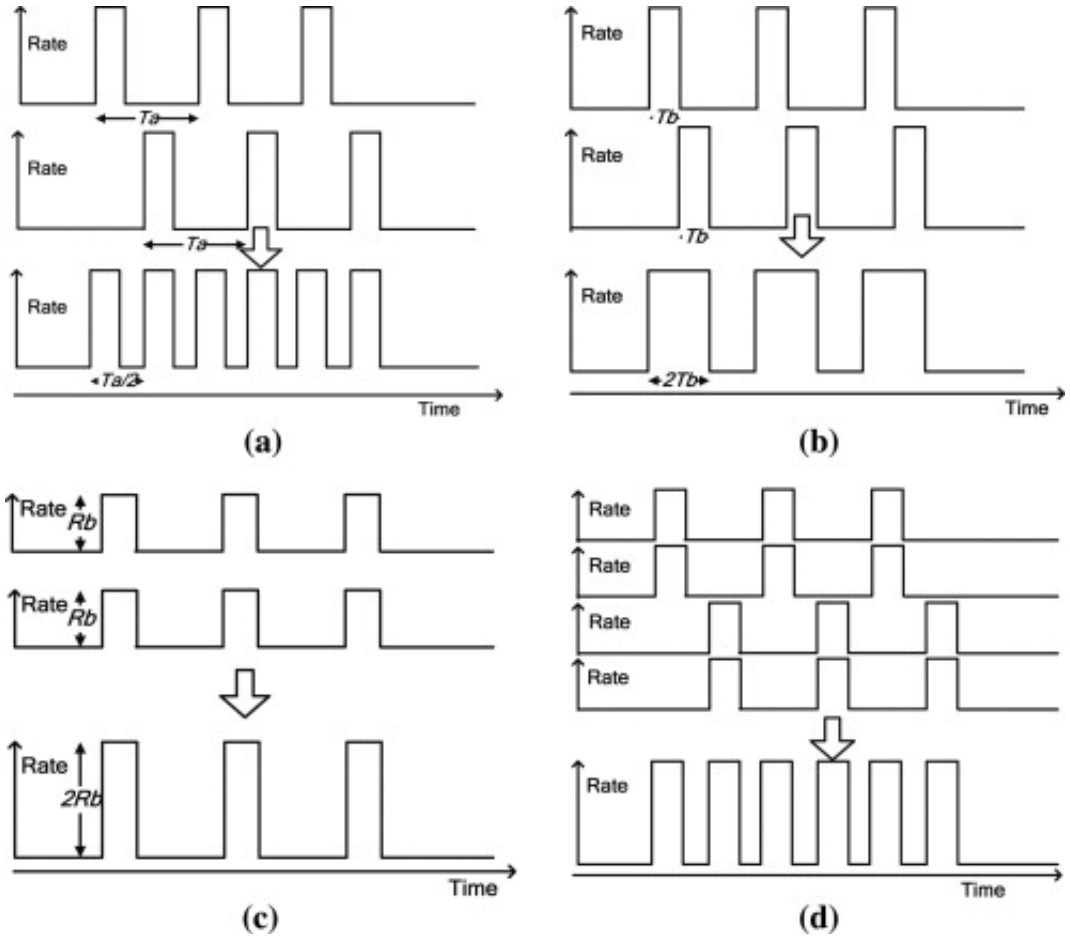


図 2.3: LDDoS 攻撃フローの分類（a）攻撃頻度強化（AFI），（b）攻撃バースト幅強化（AWI），(c) 攻撃バーストレート強化（ARI），(d) 混合強化（MI）（出典：文献 [10]）

第3章　関連研究

3.1　LDDoS 攻撃の検知

LDDoS 攻撃は平均通信量の低いトラフィックの集合で形成されるため，一般的な DDoS 攻撃による防御手段では対策することが困難である．そのため，トラフィックの輻輳参加率をもとに LDDoS 攻撃を検出する手法 [10][11] や様々なエントロピーベースの検知手法 [12][13] が提案されている．

Zhang らは LDDoS 攻撃トラフィックが積極的に輻輳を引き起こすのに対し，通常の TCP トラフィックは積極的に輻輳を回避するという特徴からトラフィックの輻輳参加率をもとに LDDoS 攻撃フローを検出手法を提案したが，有効性を示すためにさらに多様なバーストトラフィックに対する実験や分析が必要であった [10]．Kieu らは Zhang らのアプローチを使用する場合，攻撃を受けている間に TCP スループットを最大化することと通常時に新しい TCP フローに公平性を提供することとの間にトレードオフがあることを示した [11]．

Jadhav らは，最適客観エントロピー法を用いた LDDoS 攻撃の検出手法を提案した [12]．実験の結果，検知精度は従来のエントロピーを用いた検知手法よりも大幅に上回った結果となったが，通常のトラフィックと攻撃トラフィックの間の距離値が 0.000019 と非常に小さいため，誤検知率が高いことが課題としてあげられる．

このように，現状 LDDoS 攻撃の最適な対策手法は確立されていないため，より正確な分析と安定した検知手法の検討の確立が求められている．

3.2　実践的な LDDoS 攻撃の検証

Feng らはクラウドデータセンターネットワークが複数のテナント間で同じネットワークリソースを共有していることと，その帯域幅が安定しており遅延もごくわずかであるという特徴が LDDoS 攻撃に適していると着目し，クラウドデータセンターネットワーク内で現実的に LDDoS 攻撃が可能であるか検証した [14]．検証の結果，標的となったバーチャルマシンのダウンリンクの TCP スループット損失率が最大 83%まで上昇したことから，クラウドデータセンターネットワークにおいて LDDoS 攻撃が有効な攻撃手法であることが示された．

この他に実践的な LDDoS 攻撃について議論されている事例はなく，現在実ネットワーク環境下において攻撃効果の高い LDDoS 攻撃を行うために必要な条件は明らかではない．適切な LDDoS 攻撃の対策手法確立のために，実ネットワーク環境下において LDDoS 攻撃を構成するために必要な条件と現実的な攻撃効果について検証し議論する必要がある．

3.3 TCP 再送信タイマの管理の変更による LDoS/LDDoS 攻撃の緩和

第 2.1.2 項で解説したとおり，LDoS/LDDoS 攻撃はバーストトラフィックの送信間隔が再送信タイムアウトに同期している場合（$T_a = minRTO$）に大きなサービス妨害効果が発生する，これは TCP が連続して再送信を続ける場合に，(2.3) 式と (2.4) 式により RTO が minRTO の整数倍を取り続けることに起因してる．

この問題を解決するため，Kuzmanovic らは minRTO の値を一定の幅の範囲からランダムに選ぶことで LDoS 攻撃の被害を緩和する手法を提案した [9]．しかし，TCP 輻輳制御を正常に動作させるためにはこの幅を大きくとることができないため，大きな被害低減効果は得ることができなかった．

細井らは (2.4) 式による RTO の増加方法を以下の (3.1) 式に変更する手法を提案した [16]．

$$RTO_i = (1+u)RTO_{i-1}(for 0 > u > 1) \tag{3.1}$$

この手法を用いると，連続した再送信における RTO は

$$RTO_i = (1+u)^{i-1} minRTO \tag{3.2}$$

となり，minRTO の整数倍にはならない系列が得られる．この手法を用いた場合の $T_a = minRTO$ における正規化回線容量は以下の (3.3) 式のようになるため，既存の再送タイマ管理に比べて LDoS 攻撃の被害を緩和することが可能である．

$$\rho' = \frac{1-u}{3} \tag{3.3}$$

第4章　アプローチ

4.1　一般家庭や小規模事業所を標的としたLDDoS攻撃

既存研究 [10][11] における LDDoS 攻撃の実験は攻撃効果の高い LDDoS 攻撃を構成しやすい環境で行われているため，現実的なネットワークに近い環境で検証を行い，LDDoS 攻撃を現実的に構成するために必要な条件について明らかにする必要がある．そこで，本稿では以下の 4 つの観点において，一般家庭や小規模事業所を想定した小規模なネットワークで LDDoS 攻撃を構成し，小規模ネットワークにおいて LDDoS 攻撃が現実的に可能であるのかを検証する．

1 つ目は，IoT 機器を用いた LDDoS 攻撃の検証である．IoT 機器の普及拡大 [3] にともなって，事例 [1] のように一般家庭や事業所に導入した IoT 機器を不正に操作され LDDoS 攻撃が行われる可能性が考えられる．しかし，IoT 機器を攻撃ノードとして LDDoS 攻撃を構成した関連研究や事例がないため，IoT 機器のようなリソースの限られているコンピュータでネットワークシミュレータや PC と同様にバーストトラフィックを生成できるのかは不明である．そのため，IoT 機器を用いて LDDoS 攻撃フローを生成した際の正確性と IoT 機器にかかる負荷の観点から現実的に LDDoS 攻撃が可能であるかについて検証する．

2 つ目は，標的ルータの送信キュー容量に着目した LDDoS 攻撃の検証である．関連研究 [10][11] では，ボトルネックリンクルータの送信キュー容量を 50 パケットに設定して実験を行っているが，Linux の送信キュー容量の初期設定が 1,000 パケットであることや，家庭用ルータの送信キュー容量が約 1,000 パケットであると考えられるため，関連研究 [10][11] で設定している送信キュー容量は，現実的な値と比べて小さいと考える．そこで，ボトルネックリンクルータの送信キュー容量を実ネットワーク環境下に近い値に設定した場合に，LDDoS 攻撃の及ぼす効果がどのように変化するか検証する．

3 つ目は，無線環境下における LDoS 攻撃の検証である．LDDoS 攻撃の踏み台として利用される機器は無線 LAN によって接続されていることが考えられるが，現在までに無線 LAN でネットワークに接続された機器から LDDoS 攻撃を検証した事例が確認されていないため，基礎実験として無線 LAN で接続された攻撃ノード一台から LDoS 攻撃を行い，無線環境下において LDoS/LDDoS 攻撃が可能であるか検証する．

4 つ目は標的サーバの minRTO が未知の場合における効果的な LDDoS 攻撃の可能性についての検討である．関連研究や本稿の第 5 章から第 7 章の実験では，標的サーバの minRTO が RFC6298[17] で推奨されている 1 秒に設定されていると仮定した上で送信するバーストトラフィックの間隔も 1 秒に設定し，検証する．しかし，この 1 秒という値はあくまで推奨値であるため，実際にすべての標的サーバで minRTO の値が 1 秒に設定されているという保証はなく，実際に Linux の初期設定では 0.8 秒に設定されている．この

ことから，攻撃者が標的サーバの再送信間隔と等しいバースト間隔のバーストトラフィックを生成することが難しいと期待されるが，minRTO の値の取得が容易であれば可能であると考えられる．そこで，正規の通信を装って標的サーバの minRTO の値を取得することが可能であることを指摘し，本手法が有効であるかを検証する．

4.2 一般家庭や小規模事業所を想定した小規模ネットワーク

本稿の実験では，LDDoS 攻撃の標的ネットワークとして，図 4.1 のような一般家庭や小規模事業所を想定した小規模ネットワークにおいて効果的な LDDoS 攻撃が可能であるか検証する．標的ネットワーク内には，TCP でデータを送信するサーバ（以下：標的サーバ）が 1 台，IoT 機器が 3 台，ルータが 1 台あり，ルータを通してインターネットに接続されている．3 台の IoT 機器は攻撃者のマルウェアの制御下に置かれて（ボット化されて）おり，攻撃者は外部ネットワークに存在する C&C（Command & Control）サーバから自由な命令をボット化した IoT 機器（以下：攻撃ノード）に実行させることが可能である．このとき発生する C&C サーバから攻撃ノードへのネットワークの遅延は考慮しないものとする．インターネットを通じて正規ユーザネットワーク内のクライアントは標的サーバからデータを受信し，攻撃者は標的サーバがクライアントに送信するデータトラフィックを 3 台の攻撃ノードから送出されるトラフィックで構成される LDDoS 攻撃によって妨害する．

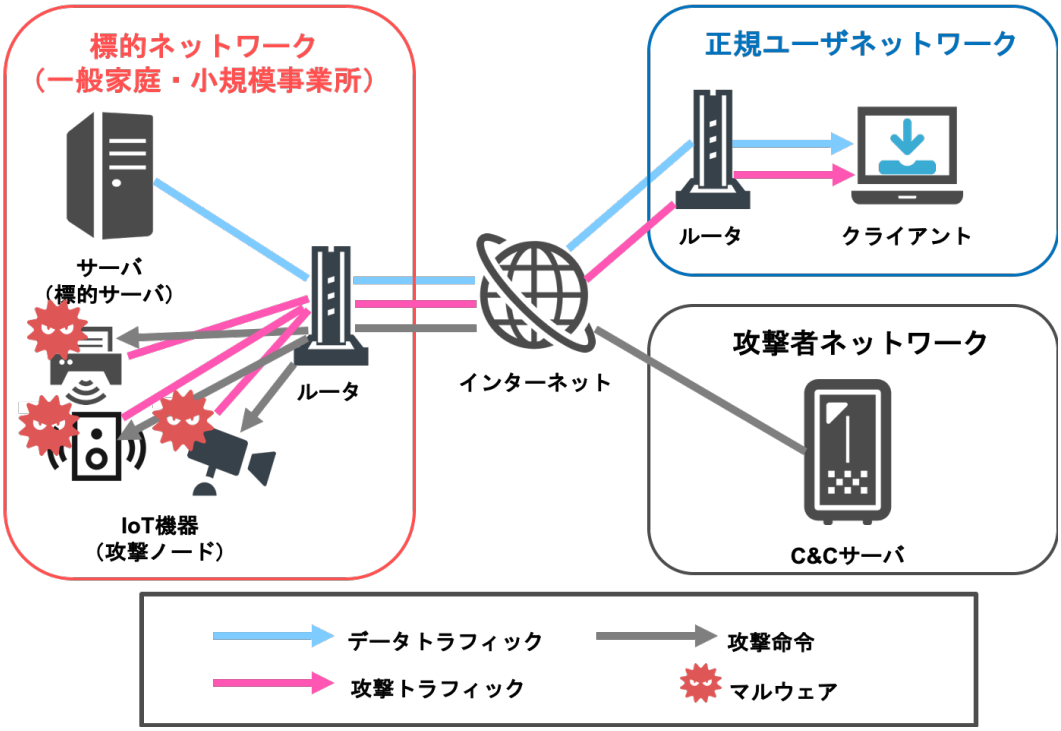


図 4.1: 本稿の検証で想定するネットワーク

第5章　IoT機器を用いたLDDoS攻撃の検証

5.1　実験概要

本章では，近年 DDoS 攻撃の踏み台として多く利用されている IoT 機器を用いて LDDoS 攻撃フローを生成した際の正確性と IoT 機器にかかる負荷の観点から現実的に LDDoS 攻撃が可能であるか検証する．

5.2　実験環境

実験環境は図 5.1 に示す，2 台のルータ（ルータ 1，ルータ 2）と 1 台の標的サーバと 3 台の攻撃ノード（攻撃ノード 1, 2, 3）と 1 台のクライアントからなるダンベル型トポロジである．すべてのリンクは有線 LAN で接続した．2 つのルータをつなぐリンクは Linux のトラフィックコントロールの Token Bucket Filter[18] を利用し，帯域幅が 10Mbps，RTT が 20ms のボトルネックリンクとし，その他のリンクは帯域幅を 100Mbps，RTT を 1ms に設定した．ルータ 1 の送信キューのサイズは文献 [10] と文献 [11] の実験を参考に 50 パケットに設定した．標的サーバの minRTO の値は RFC6298[17] で推奨値とされている 1 秒に設定し，輻輳制御アルゴリズムは CUBIC を用いた．TCP パケット 1 つの大きさは 1514Byte である．攻撃ノード 1, 2, 3 は Raspberry Pi 3 Model B，その他の機器は PC を用いて環境を構築した．実験に使用した機器の詳細を表 5.1 に示す．

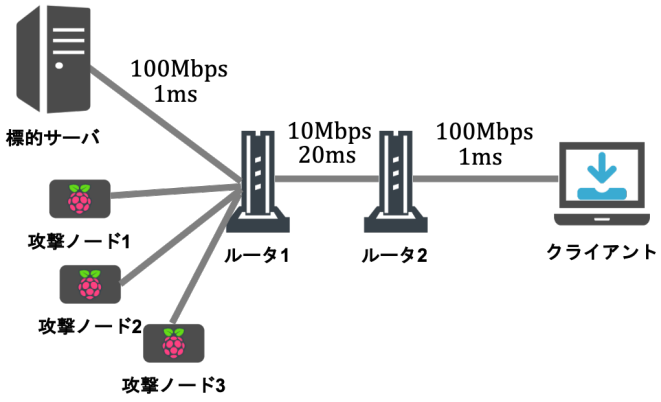


図 5.1: 実験環境

表 5.1: 実験に使用した機器

機器名	OS	CPU	メモリ
クライアント	Ubuntu 18.04	Intel(R) Core(TM) i5 @3.60GHz	8.00GB
標的サーバ	Ubuntu 16.04	Intel(R) Core(TM) i5 @3.60GHz	8.00GB
ルータ 1，2	Ubuntu 16.04	Intel(R) Core(TM) i5 @3.60GHz	8.00GB
攻撃ノード 1，2，3	Ubuntu Mate 16.04	ARMv7 Processor rev4	1.00GB

表 5.2: LDDoS 攻撃パラメータ

分類	LDDoS 攻撃				単体 LDoS 攻撃フロー			集約後の LDDoS 攻撃フロー		
	n	g	m	σ	$T_a(s)$	$T_b(ms)$	$R_b(Mbps)$	$T_a^+(s)$	$T_b^+(ms)$	$R_b^+(Mbps)$
AFI	3	3	1	$T_a/3$	3	300	10	1	300	10
ARI	3	1	3	0	1	300	3.4	1	300	10.2

5.3 実験手順

実験は時刻 0 から 60 秒間，標的サーバはクライアントに対し iPerf[19] を用いて TCP 通信でデータパケットを帯域幅の速度 10Mbps で送り続け，攻撃ノード 1，2，3 は Kuzmanovic が開発した LDoS 攻撃フロー生成プログラム [21] の linuxps と linuxSend を用いて，クライアントに対し UDP で LDoS 攻撃フローを送り続けた．linuxSend は引数として（T_a，T_b，R_b，1 パケットの長さ（50Byte））を受け取り LDoS 攻撃フローのトラフィックを生成し，linuxps は宛先の IP アドレスとポート番号を引数で受け取り，linuxSend によって生成されたトラフィックを宛先に送信するプログラムである．LDDoS 攻撃フローは AFI と ARI で生成した 2 種類を使用した．攻撃に用いたパラメータを表 5.2 に示す．標的サーバと攻撃ノード 1，2，3 の通信開始時刻を正確に同期するため，これらの機器の時刻を Linux の ntpdate コマンドを用いてルータ 1 の時刻と同期させた後，Linux の at コマンドを用いて同時刻に通信を開始した．通信中は，ルータ 1 でパケットキャプチャツールの Wireshark[20] を用いて攻撃ノード 1，2，3 が生成した攻撃フローのパケットキャプチャデータを取得した．さらに，ARI を用いた LDDoS 攻撃フローの生成時における linuxps と linuxSend の CPU とメモリ使用率を 1 秒ごとに Linux の ps コマンドを用いて計測した．

5.4 評価

正確に LDDoS 攻撃フローを生成できるかについて，平均バースト間隔と平均バースト幅を評価項目として評価する．LDDoS 攻撃フローのバーストトラフィックを先頭から$< B_1, B_2, \cdots, B_n >$としたとき，隣接するバーストトラフィック B_i, B_{i+1} のバースト間隔を Ta_i，B_i のバースト幅を Tb_i とすると，平均バースト間隔 $\bar{Ta}$ は（5.1）式，平均バースト

幅 $\bar{Tb}$ は（5.2）式で計算できる．

$$\bar{Ta} = \sum_{i=1}^{n-1} Ta_i \tag{5.1}$$

$$\bar{Tb} = \sum_{i=1}^{n} Tb_i \tag{5.2}$$

AFI と ARI で生成した LDDoS 攻撃フローそれぞれについて，60 秒間に生成された 60 個のバーストトラフィック$< B_1, B_2, \cdots, B_{60} >$を対象に $\bar{Ta}$，$\bar{Tb}$ を求める．

5.5 実験結果と考察

LDDoS 攻撃フローごとの $\bar{Ta}$ と $\bar{Tb}$ を計測した結果を表 5.3 に示す．AFI と ARI ともに平均バースト間隔，平均バースト幅ともに誤差がないことがわかった．

次に，ルータ 1 で取得したパケットキャプチャデータからプロットした攻撃フローの外形についての結果と考察を述べる．図 5.2 は，AFI で生成した LDDoS 攻撃フロー全体の外形である．この図からは，攻撃期間全体において各攻撃ノードがパラメータで設定した一定のバースト間隔とバースト幅を保って攻撃フローを生成できていることが読み取れる．図 5.3 は，図 5.2 の時刻 0 から 3.2 について縦軸方向に一部抜粋し拡大したものである．この図からは，各攻撃ノードのバースト幅が 300ms，隣接したバーストトラフィックのバースト間隔が 1s であることが読み取れる．図 5.4 は，ARI で生成した LDDoS 攻撃フロー全体の外形である．この図からは，35 秒付近のバーストトラフィックが欠損しているが，その他は AFI と同様に正確に攻撃フローを生成できていることが読み取れる．図 5.5 は，図 5.4 の時刻 0 から 3.2 について縦軸方向に一部抜粋し拡大したものである．この図からは，各攻撃ノードのバースト幅が 300ms，隣接したバーストトラフィックのバースト間隔が 1s であることが読み取れる．

表 5.3: 平均バースト間隔と平均バースト幅の計測結果

	$\bar{Ta}(s)$	$\bar{Tb}(s)$
AFI	1.00	0.30
ARI	1.00	0.30

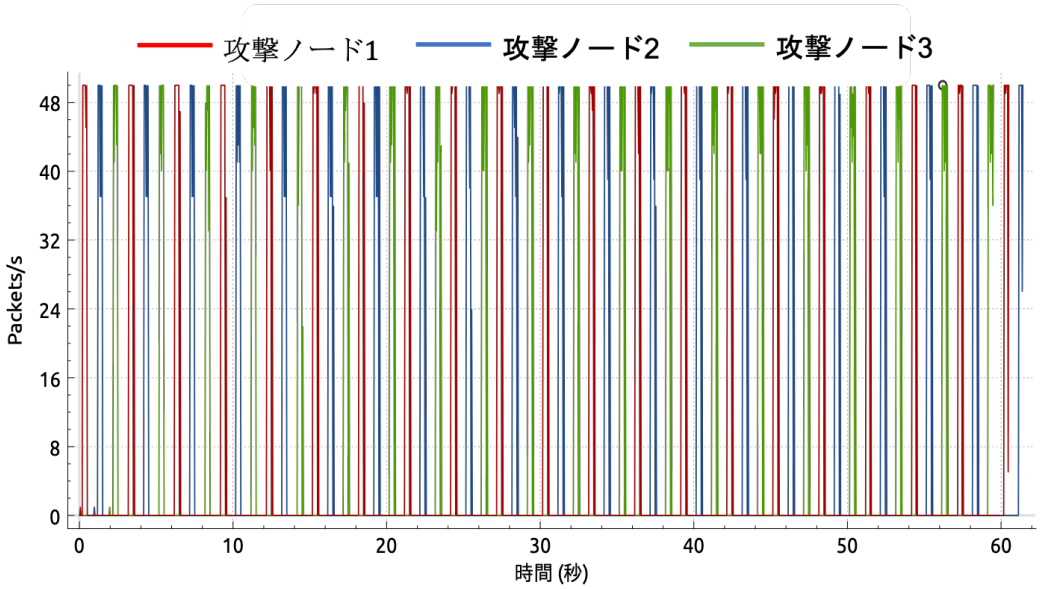


図 5.2: パケットキャプチャデータからプロットした AFI LDDoS 攻撃フローの外形

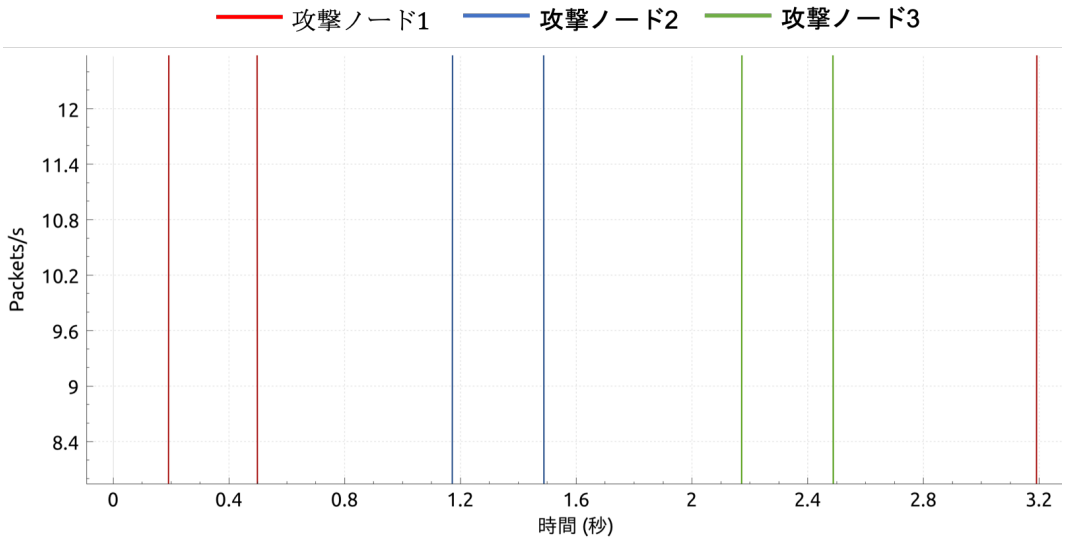


図 5.3: AFI LDDoS 攻撃フローの外形 図 5.2 の時刻 0 から 3.2 について縦軸方向に一部抜粋し拡大した

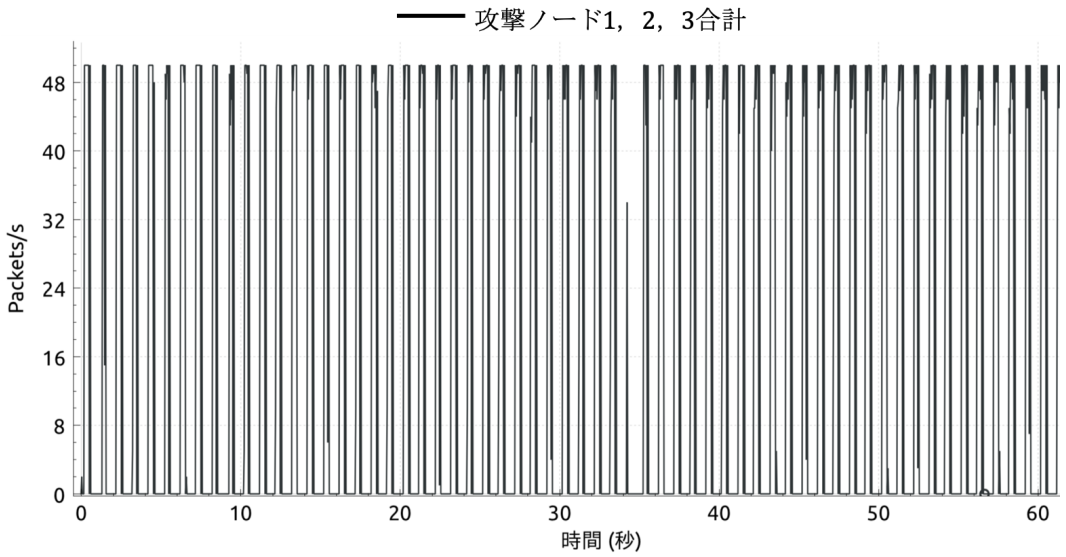


図 5.4: パケットキャプチャデータからプロットした ARI LDDoS 攻撃フローの外形

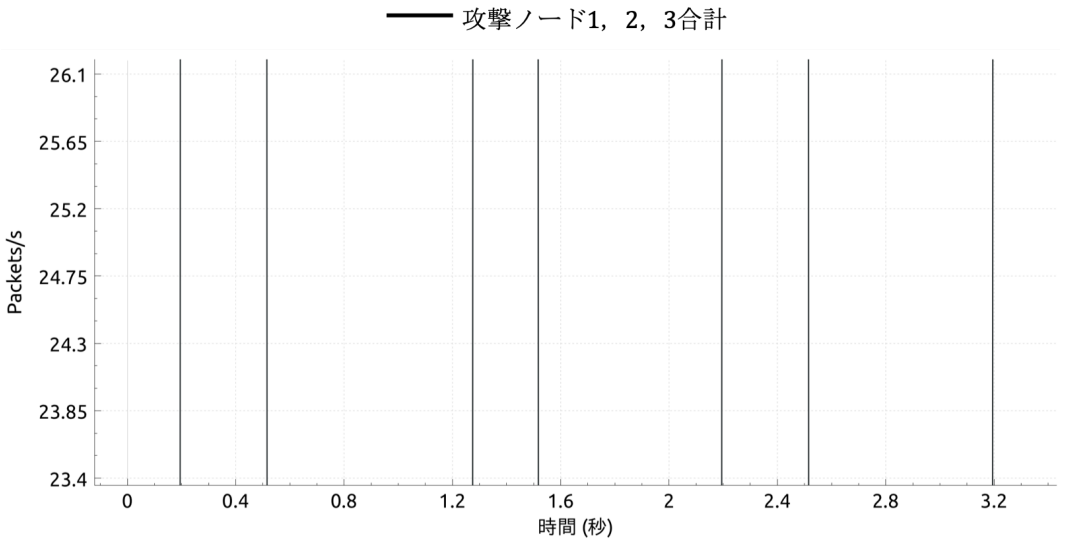


図 5.5: ARI LDDoS 攻撃フローの外形　図 5.4 の時刻 0 から 3.2 について縦軸方向に一部抜粋し拡大した

AFI を用いた攻撃中における標的サーバの正規化スループットの遷移を図 5.6，ARI を用いた攻撃中における標的サーバの正規化スループットの遷移を図 5.7 に示す．これらの図から攻撃中における標的サーバの正規化スループットを 9 割以上抑止しており，十分な攻撃効果が得られていることがわかる．

以上の結果から，攻撃ノードに IoT 機器を使った場合においても，ほぼ正確に LDDoS 攻撃フローを生成し，効果的な LDDoS 攻撃が可能であると考える．

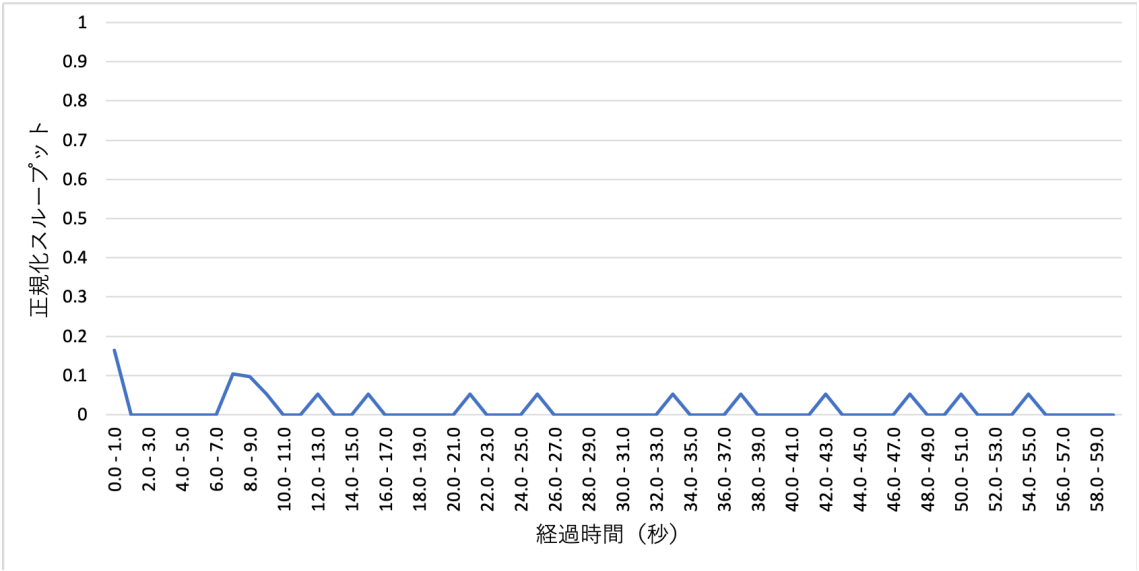


図 5.6: AFI を用いた攻撃中における標的サーバの正規化スループットの遷移

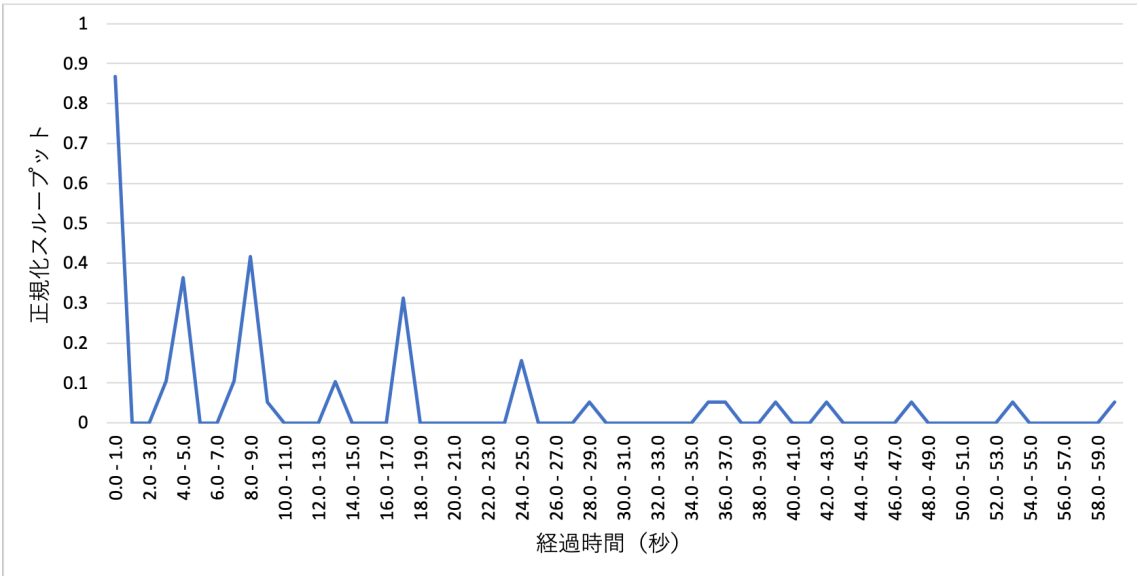


図 5.7: ARI を用いた攻撃中における標的サーバの正規化スループットの遷移

ARI を用いた攻撃中における linuxps のリソース使用率を図 5.8，linuxSend のリソース使用率を図 5.9 に示す．攻撃フローを生成する際に IoT 機器に与える負荷については，メモリの使用率はごくわずかであったが，linuxps の CPU 使用率が常時 100 %であったことから，通常の動作に影響を及ぼす可能性があると考える．このことから，今後多くの IoT 機器を踏み台とした LDDoS 攻撃が発生する可能性があるため，さらに複雑なネットワーク環境において複数のネットワークに分散した攻撃ノードから効果の高い LDDoS 攻撃が可能であるかを検証する必要がある．今回攻撃ノードとして使用した Raspberry Pi 3 Model B は IoT 機器としては性能が高いため，低い性能や一般的な性能の IoT 機器でバーストトラフィックを生成した際の負荷についても検証する必要がある．

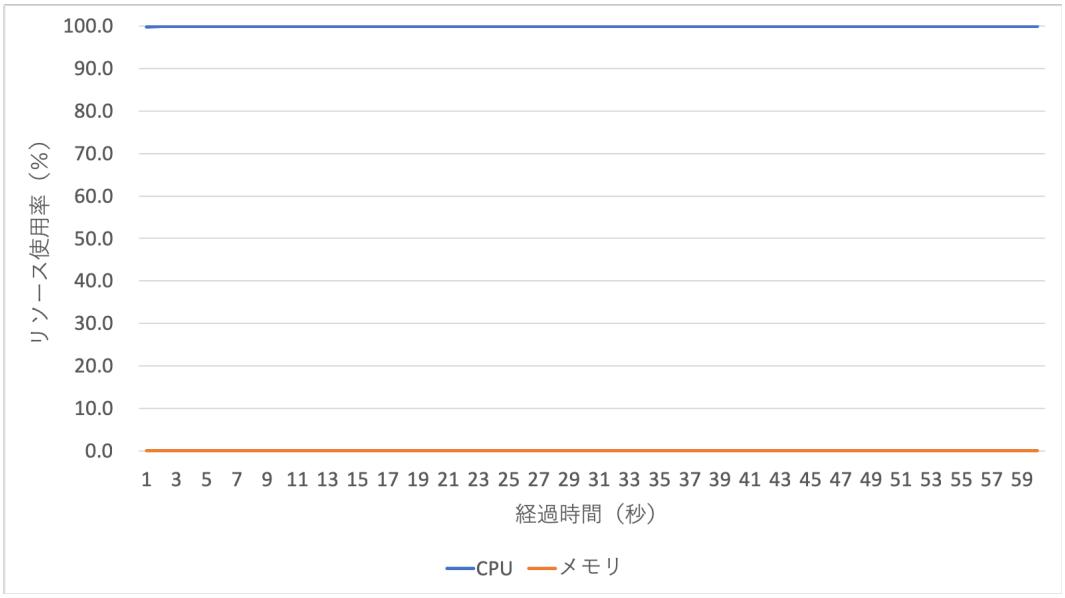


図 5.8: ARI を用いた攻撃中における linuxps のリソース使用率

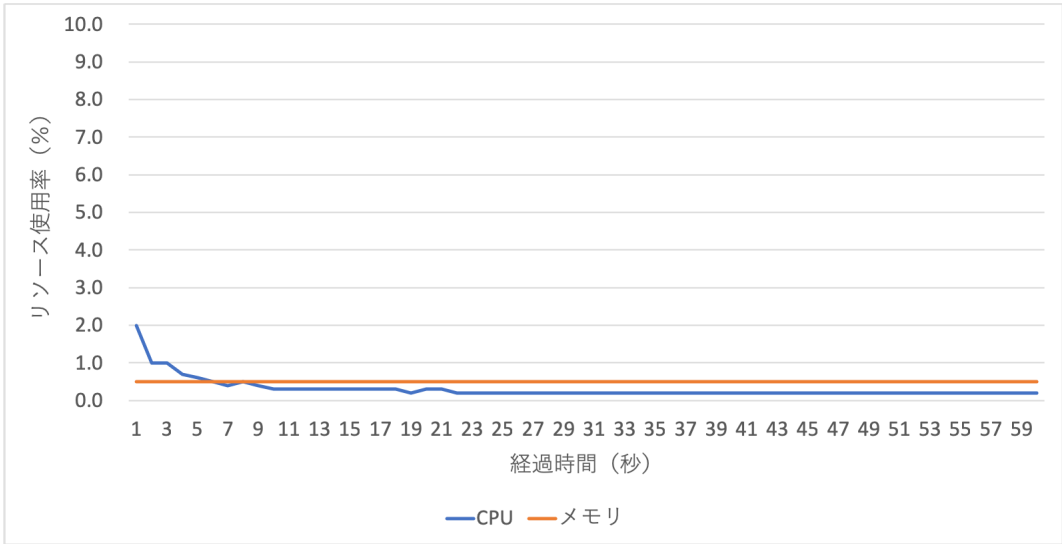


図 5.9: ARI を用いた攻撃中における linuxSend のリソース使用率

第6章　標的ルータの送信キュー容量に着目したLDDoS攻撃の検証

6.1　一般的な家庭用ルータの送信キュー容量

山本らは文献 [15] において，無線 LAN パケットの輻輳を深層学習を用いて予測するための正解データを検討するために，5 台の Android 端末から市販の無線 LAN ルータ MZK-MF300N[23] を経由したサーバに対して一斉にパケットを送信し，各 Android 端末の輻輳ウィンドウ（CWND）の振る舞いを測定した．図 6.1 は 5 台の Android 端末の CWND の推移を計測した結果である．この図から 20 秒付近以降，輻輳を検知した TCP が CWND の値を制御しており，5 台の端末の CWND 合計が最も大きい 30 秒における各端末の CWND のパケット数を合計すると約 1,000 パケットであることがわかる．このことから，この実験で使用していた市販の無線 LAN ルータの送信キュー容量は約 1,000 パケットであると考える．そのため，本稿では一般家庭や小規模事業所で使用されている市販のルータの送信キュー容量が約 1,000 パケットであると仮定して議論を進める．

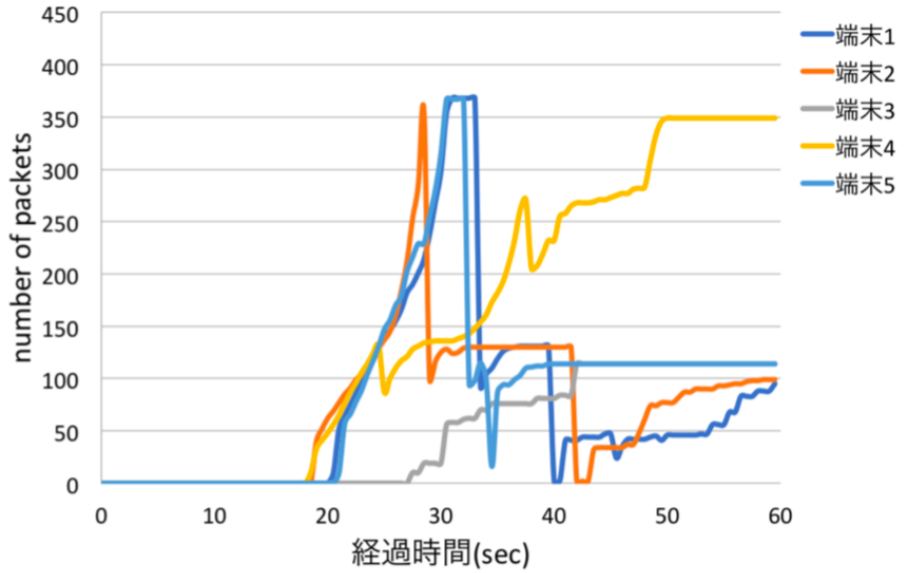


図 6.1: 5 台同時通信における Android 端末の CWND の推移（出典：文献 [15]）

6.2 ルータの送信キュー容量が LDDoS 攻撃の効果へ及ぼす影響

6.2.1 実験概要

本節では，既存研究 [10][11] と比較して，ボトルネックリンクを構成するルータの送信キュー容量がより現実的な値の場合において，LDDoS 攻撃の効果にどのような変化が発生するのかについて検証する．

6.2.2 実験環境

実験環境は，第 5 章で使用した実験環境と同じ環境を用いた．

6.2.3 実験手順

実験は，ルータ 1 の送信キューの大きさを 50 パケットから 1,000 パケットまで 50 パケットずつ増加させて，第 5 章と同じ手順で LDDoS 攻撃を行った．

6.2.4 評価

評価は，標的サーバがクライアントにデータトラフィックを送信した際の平均正規化スループットの変化を観察して評価した．

6.2.5 実験結果と考察

図 6.2 に結果を示す．500 パケットまでは平均正規化スループットが約 0.6 まで大きく上昇しているが，500 パケットから 1,000 パケットの間は約 0.6 を維持したまま，上昇しないという結果が得られた．1,000 パケットでの平均正規化スループットは約 7 割で，この状態ではパケットロスは発生するが，問題なく通信はできていること考えられる．3.1 節で述べたとおり，一般的なルータは送信キュー容量が 1,000 パケットほどの大きさであると考えられるため，一般的なルータがボトルネックリンクを構成している場合において，ボトルネックリンクの帯域幅と同程度の速度の LDDoS 攻撃フローでは高い攻撃効果を得られないと考えられる．このことから，現実的な場合においても，送信キューの容量が 50 パケット程度と場合と同様に平均正規化スループットを 1 割未満に抑えることができる攻撃を行うためには，さらに複数の攻撃ノードを増やして，生成する LDDoS 攻撃フローの強さを増幅する必要があると考える．

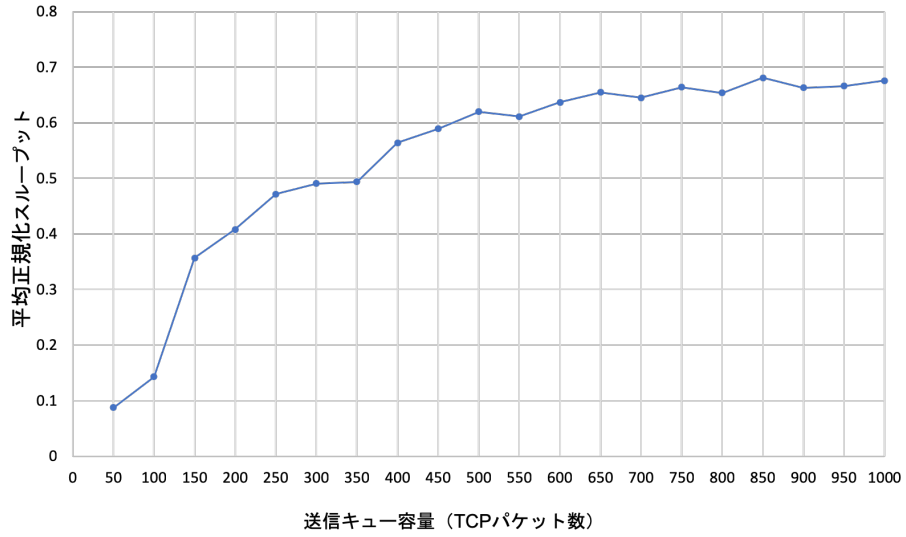


図 6.2: ルータ 1 の送信キューの大きさとサーバの平均正規化スループット

6.3 一般家庭用ルータに対する効果的な攻撃に必要な攻撃ノード数の見積もり

6.3.1 実験概要

前節の実験と評価により，送信キュー容量が 1,000 パケットのボトルネックリンクルータに対して，平均正規化スループットを 1 割未満に抑える効果的な LDDoS 攻撃を構成するためには，攻撃ノードを増やし，生成する LDDoS 攻撃フローの強さを増幅させる必要があることがわかった．

生成する LDDoS 攻撃フローの強さを増幅させる方法は 2 つ存在する．一つは，攻撃ノード 1 台当りから送信する LDoS 攻撃フローを大きくする方法である．もう一つは，さらに多くの攻撃ノードを用いて LDDoS 攻撃フローを生成する方法である．しかし，前者の方法ではバーストトラフィックが一般的な DDoS 攻撃のように検知されてしまうリスクがあるため，このリスクを回避するために 1 台あたりのバーストトラフィックの大きさは変更せずに後者の方法で増幅するほうが妥当である．

そのため本実験では，平均正規化スループットを 1 割未満に抑えるために必要な攻撃ノード数を検証する．ただし，4 台以上の攻撃ノードを実ネットワーク環境下で構成することが難しいため，混合強化を用いて生成した LDDoS 攻撃フローを再現した巨大な攻撃フロー（以下：見積もり用攻撃フロー）を 1 台の攻撃ノード攻撃から送信し，見積もり用攻撃フローの送信に必要な攻撃ノード数を外挿で推定する．

6.3.2 実験手順

見積もり用攻撃フローには，表 6.1 に示す F_1 から F_5 の 5 つを用いた．これらは，前節で表 5.2 のパラメータを用いて生成した AFI の LDDoS 攻撃フローを AWI を用いてさら

表 6.1: 見積もり用攻撃フローのパラメータ

見積もり用攻撃フロー	$T_a^+(s)$	$T_b^+(ms)$	$R_b^+(Mbps)$
F_1	1	600	10
F_2	1	700	10
F_3	1	800	10
F_4	1	900	10
F_5	1	1,000	10

にバースト幅を 600ms から 1,000ms まで増幅したと想定したものである．見積もり用攻撃用トラフィック $F_1 \cdots F_5$ をそれぞれ用いて DoS 攻撃を行い，前節と同様の方法で標的サーバの平均正規化スループットを計測した．

6.3.3 評価

$F_1 \cdots F_5$ の中から計測した平均正規化スループットが 0.1 以下になるために必要十分な攻撃フローを F とし，F を生成するために必要な攻撃ノード数 n を以下の（6.1）式により算出する．

$$n = Round(T_b^+/T_b) * m * g \tag{6.1}$$

$Round()$ は括弧の中の式の小数点以下を切り上げるものとする．T_b^+ は F のパラメータ，T_b，m，g は第 5 章で用いた AFI のパラメータ（表 5.2）を使用する．既知の値を代入すると（6.1）式は以下の（6.2）式になる．

$$n = Round(T_b^+/300) * 1 * 3 \tag{6.2}$$

6.3.4 実験結果と考察

T_b^+ の増幅による標的サーバのスループットの変化を 6.3 に示す．この結果から，$T_b^+ = 900ms$ であれば平均正規化スループットを 1 割以下に抑えることが可能であることから $F = F_4$ となった．よって，$T_b^+ = 900$ となるため，（6.2）式から n を算出すると値は 9 となり，必要な攻撃ノード数は 9 台の攻撃ノードが必要になると推測できる．

今回の実験では十分な攻撃ノードの台数を確保できなかったことから実際に 9 台の攻撃ノードで増幅した実験を行えなかったが，第 5 章の実験結果で LDDoS 攻撃フローを正確に生成できることは示したため，実際に 9 台の攻撃ノードから生成させた場合にも同等の効果が期待できると考えられる．

以上の結果から，既存研究 [10][11] ではボトルネックリンクのバッファの大きさに対して最小限の大きさの LDDoS 攻撃フローを検知する試みが行われているが，攻撃効果が高い LDDoS 攻撃フローに着目した検知手法を検討することで，既存の検知手法の精度をさらに向上できる可能性があると考える．

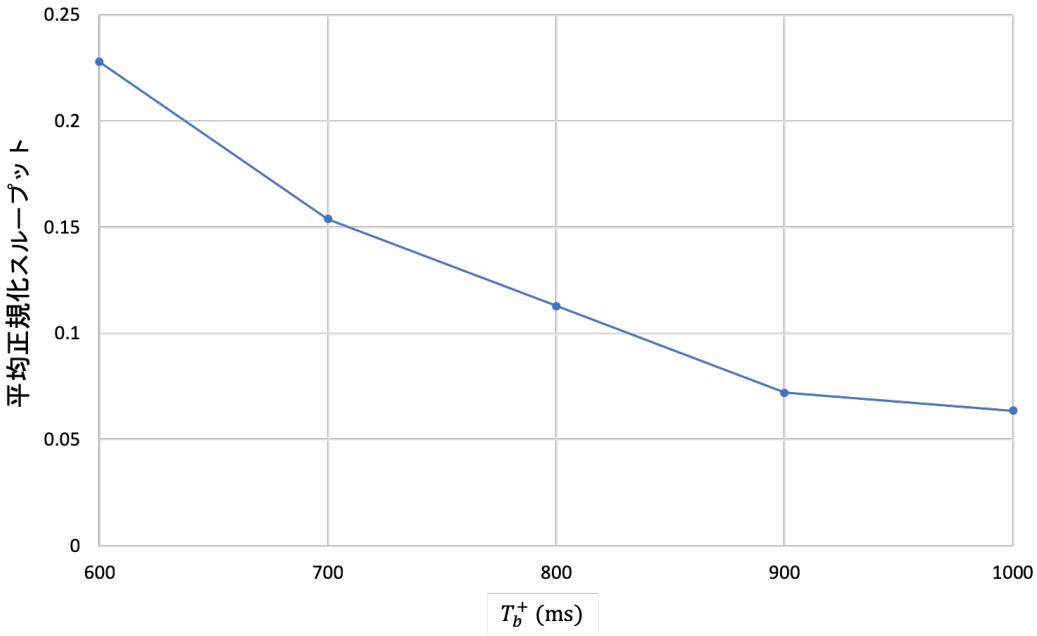


図 6.3: バースト長 T_b^+ の増幅によるサーバの平均正規化スループットの変化

第7章　無線環境下におけるLDoS攻撃の検証

7.1　実験概要

LDDoS 攻撃の踏み台として利用される機器は無線 LAN で接続されていることが考えられる．しかし，現在までに無線 LAN で接続された攻撃ノードから LDoS/LDDoS 攻撃を検証した事例はない．そのため．本章では無線 LAN で接続されている単一の攻撃ノードから LDoS 攻撃フローを正確に生成可能であるか検証する．

7.2　実験環境

実験環境を図 7.1 に示す．クライアント，ルータ 2，攻撃ノード 1 は第 5 章から第 7 章で使用していた機器と同じものを用いた．ルータ 1 は市販の無線 LAN ルータの Buffalo-WHR-1166DHP4[22] に変更し，攻撃ノードとルータ 1 を周波数 2.4GHz 帯の Wi-Fi によって接続した．その他のリンクは有線 LAN によって接続した．本実験では LDoS 攻撃フローを正確に生成できるのかについてのみに着目した検証であるため，帯域幅や遅延の設定は行わなかった．

7.3　実験手順

攻撃ノード 1 台から第 5 章の実験で AFI を用いて生成した集約後の LDDoS 攻撃フローと同じ大きさの LDoS フローを 30 秒間クライアントへ送信した．攻撃の間，ルータ 2 で Wireshark を用いて攻撃ノード 1 が生成した LDoS 攻撃フローのパケットキャプチャデータを取得した．

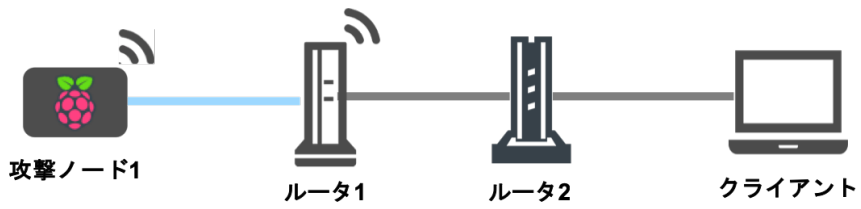


図 7.1: 実験環境

7.4 評価

LDoS 攻撃フローを正確に生成できた場合，第 5 章の実験で AFI を用いて生成した集約後の LDDoS 攻撃フローと同様の攻撃フローになることから，パケットキャプチャデータからプロットした攻撃フローの外形が，図 7.2 と同様の外形となるかを目視によって評価した．

7.5 実験結果と考察

攻撃ノード 1 が生成した LDoS 攻撃フローの外形を図 7.3 に示す．この外形は明らかに想定したバーストの形を成しておらず，図 7.2 と比較しても正確に攻撃フローを生成できているとは言えない結果となった．

今回の実験で有線 LAN を用いた場合と同様に正確な攻撃フローの生成ができなかった原因として，実験環境の周辺に約 30 の Wi-Fi のアクセスポイントが設置されていたため，電波干渉が発生し Wi-Fi が不安定だったことが考えられる．このことから，無線 LAN でネットワークに接続されている攻撃ノードから LDDoS 攻撃を構成することは，周囲のネットワーク環境の影響を大きく受けるため，現実的には困難だと考える．したがって，LDDoS 攻撃は通信環境が安定したネットワークにおいて有効な攻撃であると考える．今後の課題として，安定した Wi-Fi の環境下において検証し，無線環境下における LDoS/LDDoS 攻撃の攻撃効果について明らかにすることと，正確な攻撃フローの生成が可能な環境を検討し，それぞれの環境に最適な対策手段を確立することが挙げられる．

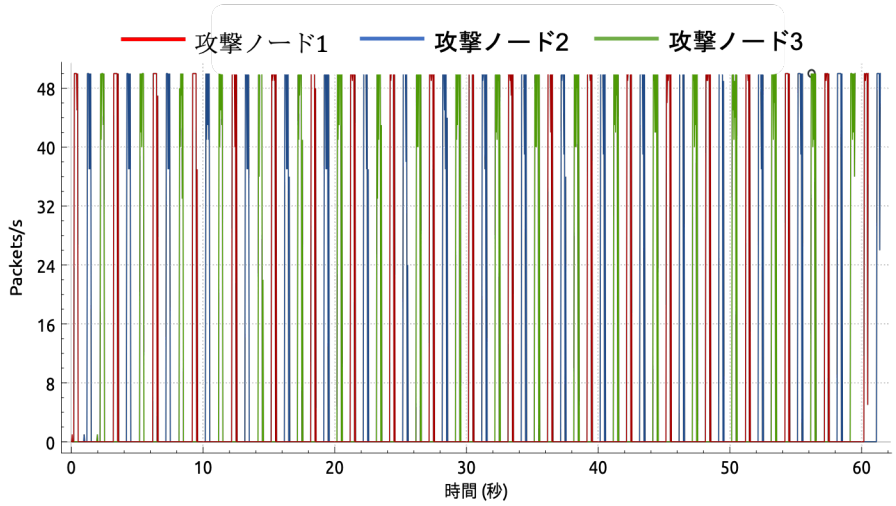


図 7.2: 攻撃ノード 1 が生成すると期待する正確な LDoS フローの外形（図 5.2 再掲）

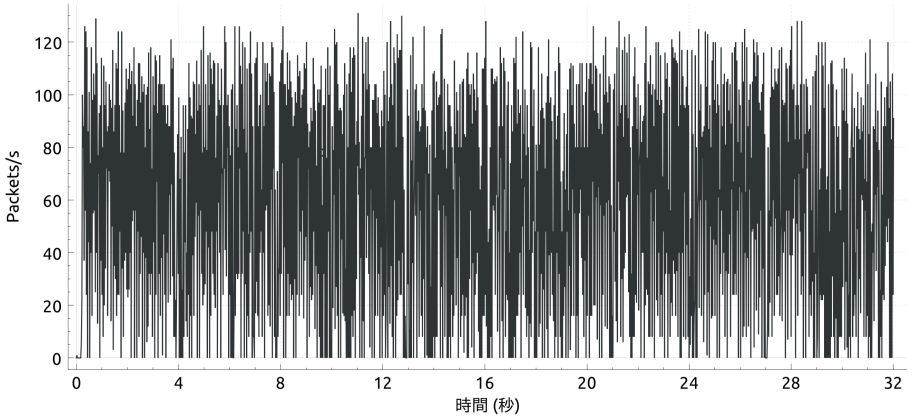


図 7.3: Wi-Fi で接続された攻撃ノード 1 が生成した LDoS 攻撃フローの外形

第8章　標的サーバのminRTOが未知の場合における効果的なLDDoS攻撃の可能性についての検討

4.1 節で述べた通り，実ネットワーク環境下において，標的サーバの minRTO の値は RFC6298[17] で推奨値とされている 1 秒とは限らず，攻撃者が効果的な LDDoS 攻撃を構成する際はこの値を取得する必要がある．本章では，標的サーバの minRTO の値を特定する手法を指摘し，提案手法の有効性を検証する．

8.1　標的サーバのminRTOの値を取得する手法

TCP ではサーバが送信したパケットに対する ACK パケットがクライアントから返ってこない場合，2.1 節で解説した再送信タイムアウトだけ待ってから同じパケットを再送信する．本手法では，この仕組みを利用して以下の手法により標的サーバの minRTO の値を取得する．

図 8.1 に攻撃の流れを示す．はじめに，攻撃者は自身のネットワークから標的サーバと通信するクライアント（以下：攻撃クライアント）を用いて正規の利用者を装いサーバと通信を開始する．次に，意図的にサーバから送信された TCP パケットに対する ACK を攻撃クライアントが送信しないことで標的サーバの再送信タイムアウトを引き起し，その挙動を攻撃クライアントからパケットキャプチャツールで観察する．ここで，再送信されているパケットについて，1 回目の該当パケットを受信した時刻を t_1，再送信タイムアウトにより再び送信された該当パケットの受信時刻を t_2 とし，以下の（8.1）式によって minRTO の値を推定する．

$$minRTO = t_2 - t_1 \tag{8.1}$$

攻撃者は攻撃者ネットワークから外部ネットワークへの ACK 送信を遮断するだけであるため，外部のネットワークからは通常のパケット廃棄が発生したようにしか見えず悪意を持った挙動の観察が行われていることを隠蔽できることが本手法の特徴である．

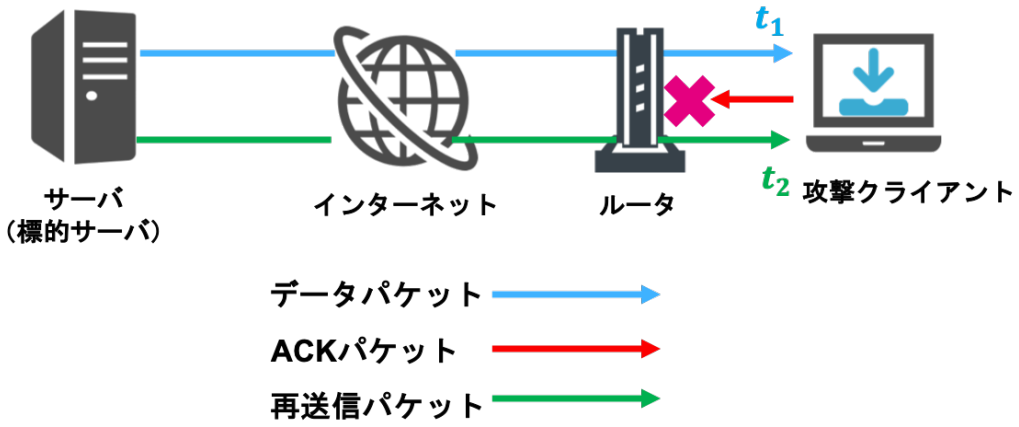


図 8.1: minRTO の値を取得する流れ

8.2 標的サーバの minRTO の値を取得する実験

前節で説明した提案手法が小規模なネットワークに対して有効であるかを検証する．

8.2.1 実験環境

図 8.2 に実験環境を示す．実験で使用したすべての機器は第 5 章の実験で使用したものと同じものである．標的サーバの minRTO の値は 1 秒に設定した．

8.2.2 実験手順

攻撃クライアントのファイアフォールに標的サーバへの通信を遮断する設定をしたあと，iPerf で標的サーバからデータ受信を開始し，60 秒間通信を継続させた．通信を行っている間，攻撃クライアントで Wireshark を用いてパケットキャプチャデータを取得した．

8.2.3 評価

提案手法を用いて算出した minRTO の値が標的サーバに設定した minRTO の値（1 秒）との誤差によって本手法の有効性を評価した．

8.2.4 実験結果と考察

図 8.3 は攻撃クライアントで Wireshark を用いて取得したパケットキャプチャデータの一部である．攻撃クライアントが標的サーバと通信を開始した時点から ACK パケットを廃棄しているため，このデータに表示されているパケットは，すべて 1 番目に受信したパケットの再送信のデータである．No.1 の再送信パケットの受信時刻と No.2 の再送信パケットの受信時刻から $t_1 = 0$，$t_2 = 0.997597201$ であることから，提案手法によって算出される標的サーバの minRTO の値は 0.997597201 秒となった．

提案手法により算出した minRTO の値は標的サーバに設定した 1 秒とわずかに誤差が生まれる結果となった．しかし，その誤差は約 0.0024 秒であり，現実的に設定する minRTO

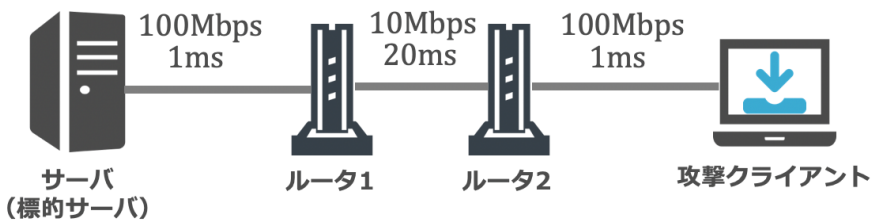
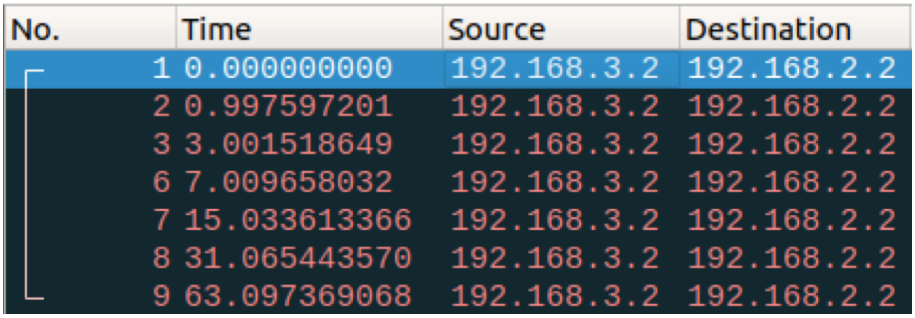


図 8.2: 実験環境



No.	Time	Source	Destination
1	0.000000000	192.168.3.2	192.168.2.2
2	0.997597201	192.168.3.2	192.168.2.2
3	3.001518649	192.168.3.2	192.168.2.2
6	7.009658032	192.168.3.2	192.168.2.2
7	15.033613366	192.168.3.2	192.168.2.2
8	31.065443570	192.168.3.2	192.168.2.2
9	63.097369068	192.168.3.2	192.168.2.2

図 8.3: 攻撃クライアントが標的サーバから取得した再送信パケット

の値は少数第一位までが一般的であるため，少数第三位の誤差を切り上げることは問題ないと考えられる．このことから，提案手法を用いて minRTO の値を取得することは可能であるといえる．具体的な対策は検討中であるが，提案手法を利用することで，標的サーバの minRTO の値と等しいバースト間隔の LDDoS 攻撃フローが送信される可能性があることを考慮しておく必要がある．第 2.2.3 項で説明した細井らの TCP 再送信タイマ管理の変更手法 [16] であれば，本手法をによって minRTO の値が取得された場合でも．攻撃を緩和することが可能であるため，このような手法と本提案手法の位置付けについても今後検討していく．

第9章　結言

9.1　まとめ

本稿では，一般家庭や小規模事業所を想定した小規模ネットワークにおいて攻撃ノードの端末，ボトルネックリンクルータの送信キュー容量，無線 LAN 環境，標的サーバの minRTO の値が未知の場合について実践的な LDDoS 攻撃の検証を行った．その結果，IoT 機器を踏み台とした LDDoS 攻撃は可能であり，現実的な送信キュー容量の大きさのルータに対しても攻撃ノードを増やし LDDoS 攻撃フローを増幅させることで高い効果の LDDoS 攻撃が可能であることがわかった．さらに，攻撃者が標的サーバの minRTO を取得することが可能であることがわかったことから，小規模で安定したネットワークにおいて LDDoS 攻撃は脅威となり得る攻撃手法であると考える．一方で，攻撃ノードが無線 LAN で接続されている場合においては正確に攻撃フローを生成することができなかったことから，通信が安定しない無線環境下において LDDoS 攻撃は有効な攻撃手段ではないと考える．

9.2　今後の課題

一般家庭や小規模事業所へのサービス妨害は大規模なインターネットサービスに対してサービス妨害をおこなったときのような金銭価値を生むことは考えにくいため，一般的な事例のように大規模なインターネットサービスを対象とした際にどれくらいの驚異となり得るかを明らかにする必要がある．そのため，今後の課題として既存研究や本研究で今回使用したような単純なネットワークではなく，さらに複雑なネットワークにおいても大きな効果を発生させることが可能であるかを検証する必要がある．小規模ネットワーク下における LDDoS 攻撃の対策手法の確立や，提案手法を用いて標的サーバの minRTO の値を特定された場合の対策についても検討していく．

謝辞

本研究を勧めるにあたり，研究テーマの選定から論文の校閲や発表資料の添削など熱心にご指導をしていただいた稲村浩教授，中村嘉隆准教授に深く感謝申し上げます．また，日頃から大変お世話になりました稲村浩研究室，中村嘉隆研究室の皆様と発表に際して大変有益なご指導，ご鞭撻を賜りました学生と教員の皆様に深く感謝申し上げます．

発表実績

[1] 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，第 89 回モバイルコンピューティングとパーペイシブシステム・第 75 回高度交通システムとスマートコミュニティ合同研究発表会，Work in Progress(WiP)，Work in Progress 奨励賞受賞，2018 年 11 月.

参考文献

[1] 三上洋:「IoT 乗っ取り」攻撃でツイッターなどがダウン, YOMIURI ONLINE(オンライン), 入手先〈https://www.yomiuri.co.jp/science/goshinjyutsu/20161028-OYT8T50051.html〉(参照 2018-12-19).

[2] Scott Hilton:Dyn Analysis Summary Of Friday October 21 Attack, Dyn(オンライン), 入手先〈https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/〉(参照 2018-12-19).

[3] Rob van der Meulen:Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Gartner(オンライン), 入手先〈https://www.gartner.com/newsroom/id/3598917〉(参照 2018-07-30).

[4] Rik Ferguson: New IoT-malware grew three-fold in H1 2018, Kaspersky(オンライン), 入手先〈https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018〉(参照 2018-12-19).

[5] トレンドマイクロ株式会社: 2019 年セキュリティ脅威予測, トレンドマイクロ株式会社(オンライン), 入手先〈https://resources.trendmicro.com/〉(参照 2018-12-19).

[6] Rik Ferguson: 2018 年夏「インターネットの現状／セキュリティ：ウェブ攻撃」レポート, Akamai(オンライン), 入手先〈https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf〉(参照 2018-12-19).

[7] Akamai: DDoS 緩和, Akamai(オンライン), 入手先〈https://www.akamai.com/jp/ja/resources/ddos-mitigation.jsp〉(参照 2018-12-19).

[8] NTT テクノクロス: TrustShelter, NTT テクノクロス (オンライン), 入手先〈https://www.trustshelter.jp/waf/〉(参照 2018-12-19).

[9] A. Kuzmanovic et al:Low-rate TCP-targeted Denial of Service Attacks and Counter Strategies, IEEE/ACM Transactions on Networking, Vol.14, No.4, pp.683-696, 2006.

[10] Zhang et al:Flow level detection and filtering of low-rate DDoS, Computer Networks, Vol.56, No.15, pp.3417-3431, 2012.

[11] Kieu et al: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.

[12] P. N.Jadhav and B. M. Patil: Low-rate DDOS Attack Detection using Optimal Objective Entropy Method, International Journal of Computer Applications, Vol.78, No.3, pp.33–38, 2013.

[13] Y. Xiang, K. Li, and W. Zhou:Low-rate DDoS attacks detection and traceback by using new information metrics, IEEE Transactions on Information Forensics and Security, Vol.6, No.2, pp.426–437, 2011.

[14] Z.Feng et al:Shrew Attack in Cloud Data Center Networks, 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks, pp.441–445, 2011.

[15] 山本ら:深層学習を用いた無線 LAN パケット解析に基づく輻輳の予測，マルチメディア，分散，協調とモバイル (DICOMO2018) シンポジウム，pp.1772-1769，2018.

[16] 細井 琢朗，松浦 幹太: TCP 再送信タイマ管理の変更による低量 DoS 攻撃被害の緩和効果，コンピュータセキュリティシンポジウム 2013 論文集，Vol.2013，No.4，pp.957-964，2013.

[17] V. Paxson 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 2018-07-30).

[18] Alexey N. Kuznetsov: tc-tbf (8), Linux Man Pages(オンライン)，入手先〈https://www.systutorials.com/docs/linux/man/8-tc-tbf/〉(参照 2018-10-18).

[19] iPerf - The ultimate speed test tool for TCP, UDP and SCTP, 入手先〈https://iperf.fr/〉(参照 2018-10-18).

[20] Wireshark, 入手先〈https://www.wireshark.org/〉(参照 2018-1-14).

[21] Aleksandar Kuzmanovic: Shrews: Low-Rate TCP-Targeted Denial of Service Attacks, Shrew's Homepage(オンライン), 入手先〈http://www.cs.northwestern.edu/~akuzma/rice/shrew/〉(参照 2018-12-19).

[22] BUFFALO WHR-1166DHP4, 入手先〈http://buffalo.jp/product/wireless-lan/ap/whr-1166dhp4/#spec〉(参照 2018-1-14).

[23] PLANEX 300Mbps 対応 無線 LAN マルチポケットルータ MZK-MF300N 入手先〈https://www.planex.co.jp/product/router/mzk-mf300n/spec.shtml〉(参照 2018-1-22).

図 目 次

表 目 次