修士論文

低レート DDoS 攻撃の自動化に関する研究

公立はこだて未来大学大学院　システム情報科学研究科
情報アーキテクチャ領域

髙橋 佑太

指導教員　　稲村 浩

提出日　　2021 年 2 月 15 日

Master's Thesis

A Study on Automated Low-rate DDoS Attacks

by

Yuta TAKAHASHI

Graduate School of Systems Information Science, Future University Hakodate
Media Architecture Field
Supervisor:　　Hiroshi INAMURA

Submitted on February 15, 2021

Abstract– Low-rate Distributed Denial of Service (LDDoS) attacks degrade the quality of TCP links with low average traffic by exploiting vulnerabilities in the TCP/IP protocol and routing queue management mechanisms. The ideal transmission rate of the attack pulse in the most classical RTO-based LDDoS attacks (aka: Shrew attacks) is greater than or equal to the bandwidth of the target bottleneck link, and it is assumed that the attacker is able to set a suitably large transmission rate. However, the attacker does not always know the bandwidth of the target bottleneck link in attacks in wild.

In this thesis, we propose a strategy for executing a low-rate shrew DDoS attack against a bottleneck link of unknown bandwidth and buffer size. The proposed attack strategy degrades downstream traffic from a specific service to the target network to the desired quality while keeping the attack traffic stealthy by exploratively increasing the pulse rate while estimating the attack effect by building bot nodes in the target network. In addition, to maintain the stealthiness of the attack, excessive transmitted pulses are suppressed by estimating the bottleneck link bandwidth from the strength of the attack pulses received by the observation node.

The proposed strategy is intended to be executed by targeting a home or office network connected by a fixed broadband line. Based on past cybercrime cases, we discussed that the proposed strategy can be implemented by IoT botnets targeting home networks and targeted malware attacks targeting enterprise networks. Since the traffic of the LDDoS attack by the proposed strategy is expected to be concentrated at the edge routers of the Internet Service Provider network, it is necessary to deploy an appropriate detection method at the edge routers of the ISP network.

The proposed strategy is evaluated by simulation using ns-3, and the results show that the proposed strategy can be executed to determine the transmission rate of the attack pulse in an exploratory manner when the characteristics of the bottleneck link are unknown. In addition, we show that by increasing the buffer size of the bottleneck link, the proposed strategy compromises stealth and increases the risk of being detected by existing flood DDoS attack detection schemes.

Keywords: Network security, Low-rate DDoS (LDDoS) attacks, Sophisticated attacks strategy

概 要：

Low-rate DDoS 攻撃は，TCP/IP プロトコルやルーティングキュー管理機構の脆弱性を悪用することによって，低い平均通信量で TCP リンクの品質を低下させる．最も古典的な RTO ベースの LDDoS 攻撃（別名：Shrew 攻撃）における攻撃パルスの送信レートの理想値は標的ボトルネックリンクの帯域幅以上の値であり，攻撃者が適切な大きさの送信レートを設定できることが前提となっている．しかし，現実において攻撃者が常に標的ボトルネックリンクの帯域幅を把握しているとは限らない．

本論文では，帯域幅とバッファサイズが未知のボトルネックリンクに対する Low-rate Shrew DDoS 攻撃の実行戦略と対策を提示する．提案戦略は，標的ネットワーク内に構築したボットノードである観測ノードを用いて攻撃効果を推定しながら，フィードバック制御によって反復的にパルスレートを増加することで，標的ネットワークに向けて送信される TCP フローの品質を目的値以下に低下することを目的に動作する．加えて，攻撃のステルス性を維持するために，観測ノードが受信した攻撃パルスの強度から，ボトルネックリンク帯域幅を推定することで過剰に送信したパルスを抑制する．

提案戦略は，固定ブロードバンド回線で接続された家庭またはオフィスネットワークを標的に実行されることを想定している．過去のサイバー犯罪の事例を下に，家庭ネットワークを標的とした IoT ボットネットや，企業ネットワークを標的とした標的型マルウェア攻撃によって，提案戦略を実行可能であることを議論した．提案戦略による LDDoS 攻撃のトラフィックは，ISP（Internet Service Provider）ネットワークのエッジルータに集中することが予想されるため，ISP ネットワークのエッジルータに適切な検知手法を展開する必要がある．

提案戦略を ns-3 を用いたシミュレーションにより評価した結果，提案戦略を実行することにより，ボトルネックリンクの特性が未知の場合においても，攻撃パルスの送信レートを探索的に決定可能なことを示した．加えて，ボトルネックリンクのバッファサイズを増加することによって，提案戦略はステルス性を損ない，既存のフラッド型 DDoS 攻撃の検知スキームに発見されるリスクが高まることを示した．

キーワード： ネットワーク・セキュリティ, 低レート DDoS 攻撃, 洗練された攻撃戦略

目次

第 1 章　序論

1.1　背景

Distributed Denial of Service（DDoS）攻撃は，インターネットを代表する脅威のひとつである．DDoS 攻撃とは，DoS（Denial of Service）攻撃の一種であり，攻撃トラフィックと呼ばれるサービス妨害を目的として送信される大量のトラフィックを分散した攻撃ノードから送信することで，標的サービスの可用性を低下させるサイバー犯罪の手法である．単位時間あたりに送信されるトラフィックの速度は，一般的にデータ転送レートと呼ばれており，DDoS の攻撃トラフィックの過去最大のデータ転送レートは，2020 年 2 月に Amazon 社が観測した 2.3Tbps にまで達している [1]．DDoS 攻撃の発生件数は 2020 年 3 月から急速に増加し続けている [2]．この背景には，新型コロナウイルス感染症（COVID-19）の世界的な流行の影響により，人々の社会活動や日々の業務においてインターネットへの依存度が高まっていることが挙げられる．一方で，高い転送レートを持つ攻撃トラフィックの特徴を検出することは容易であることから，対策が確立されており，DDoS 攻撃に対する様々な防御・緩和サービスが展開されている [3][4][5].

DDoS 攻撃の対策方法が確立されたことにより, 攻撃者は, より洗練された低レート DDoS（LDDoS: Low-rate DDoS）攻撃を使用して，TCP を利用したサービスの品質を低下させることを狙っている．LDDoS 攻撃とは，インターネット上で利用されているプロトコルの脆弱性を悪用することで，必要な攻撃トラフィックの平均通信量を低く抑えることを可能にした TCP に対する DDoS 攻撃の一種である．最大の特徴は，短く高レートなオンオフパルスを周期的に送信することである [6][7][8]．LDDoS の攻撃トラフィックのデータ転送レートは，平均すると通常のトラフィックのデータ転送レートと判別がつかないため，DDoS 攻撃と比較してデータ転送レートの大きさに基づいて LDDoS 攻撃を検出することは困難である．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 [9], LDDoS 攻撃はインターネットの新たな脅威として認識されている．以上の背景から，近年におけるネットワーク・セキュリティの研究分野では，LDDoS 攻撃の検知，防御，攻撃モデルの解析に関する研究が活発であるが，対策は確立されていない [8].

最近，産業界においても，Pulse Wave DDoS 攻撃 [10] や Short burst 攻撃 [11] という呼び名で LDDoS 攻撃の存在が認知されている．しかし，その事例の報告はほとんど存在しない．文献 [8] では，事例の報告が少ない理由について以下のように述べられている．

1. **攻撃発生頻度が少ない．**LDDoS 攻撃の実行にはネットワークに関する高度な技術が必要であるため，これを実行できる攻撃者の数が少ない.
2. **被害者が攻撃を認識していない．**LDDoS 攻撃は従来の DDoS 攻撃検知手法による検知を容易に回避することが可能である．LDDoS 攻撃の結果は，システムが実行不可能になるのではなく，品質の低下（処理速度の低下）として現れる．その結果，攻撃

の被害者は，攻撃を考慮せずに，このような状況をシステムの設備障害や回線障害のせいにしてしまう．

3. **被害者が攻撃を公表しない．**特に LDDoS 攻撃の標的になり得ると懸念されているクラウドプラットフォームは，LDDoS 攻撃を検知しても，攻撃の侵入や破壊を阻止するための有効な手段や能力を持っていない．そのため，顧客を不安にさせないために，一般的には報告や公表はしない．

これらの背景から，現実のインターネットにおける LDDoS 攻撃の潜在的な脅威の大きさや攻撃の有効性は明らかではない．そのため，本研究分野において，現実における LDDoS 攻撃の有効性を明らかにすることは，重要な研究課題の一つである．

1.2 モチベーション

現実的な脅威や有効性についての分析が不十分である場合，LDDoS 攻撃への適切な対策が困難であることは否定できない．本研究では，その第一歩として，既存研究で暗黙的に設定されている非現実的な前提の一つを取り払ったシナリオで LDDoS 攻撃を評価した．具体的には，LDDoS 攻撃を成功させるために最も重要なパラメータである攻撃パルスの大きさを攻撃者が事前に決定可能であるという前提を取り払った．この前提を検討する主な動機は，LDDoS 攻撃を成功させるためには，送信される攻撃パルスの合計ピークレートが，標的 TCP フローの経路上のボトルネックリンクの帯域幅以上の値に設定される必要がある [7][12] が，現実の攻撃シナリオにおいて，攻撃者がこの値を正確に取得できるとは限らないためである．第 3 章では，既存研究の評価実験において暗黙的に設定されている前提について詳細に説明する．

本論文では，ボトルネックリンクの帯域幅が未知であるという前提の下で，LDDoS 攻撃をオーケストレーションするための自動化戦略（以下，提案戦略）を提示する（第 4 章）．提案戦略は，標的ネットワーク内に構築したボットノードである観測ノードを用いて攻撃効果を推定しながら，フィードバック制御によって反復的にパルスレートを増加することで，標的ネットワークに向けて送信される TCP フローの品質を目的値以下に低下することを目的に動作する．加えて，攻撃のステルス性を維持するために，観測ノードが受信した攻撃パルスの強度から，ボトルネックリンク帯域幅を推定することで過剰に送信したパルスを抑制する．

1.3 研究目的

現実的な攻撃シナリオにおける LDDoS 攻撃の評価（第 4，5 章）．本論文の一つ目の目的は，現実的な仮定の下で LDDoS 攻撃を評価することによって，実際の攻撃時に求められるシナリオと制約を明らかにすることである．この目的を達成するために，ボトルネックリンクの帯域幅が未知であるという前提の下で LDDoS 攻撃を実行する提案戦略について検討す

る．検討の結果，ボトルネックリンクの帯域幅が未知であるという前提の下では，標的 TCP の受信ノードが接続されている LAN 内部に観測ノードを構築する必要性を提示した（第 4 章）．さらに，シミュレーションに提案戦略を実装して評価することで提案戦略の有効性を示した（第 5 章）．

検知手法の適用箇所の検討（第 6 章）．本論文の二つ目の目的は，提案戦略の現実における具体的な標的を検討することによって，検知手法の展開箇所を議論することである．この目的を達成するために，過去のサイバー犯罪の事例を下に，家庭ネットワークを標的とした Mirai botnet や，企業ネットワークを標的とした標的型攻撃によって，提案戦略を実行可能であることを議論した．提案戦略による LDDoS 攻撃のトラフィックは，ISP（Internet Service Provider）ネットワークのエッジルータに集中することが予想されるため，ISP ネットワークのエッジルータに適切な検知手法を展開する必要があると結論づけた．

提案手法に対する防御策の検討（第 7 章）．本論文の三つ目の目的は，提案手法に対する防御策を検討することである．この目的を達成するために，ボトルネックリンクルータのバッファサイズを増加することで，必要な攻撃パルスのレートを増加させ，提案戦略のステルス性を損なわせる手法の有効性を示した．

1.4 システム情報科学における本研究の位置付け

本研究は，現実における LDDoS 攻撃の有効性を探求する研究として位置付けられる．LDDoS 攻撃は，ネットワークの安全性を脅かす重大な脅威であるため，近年，ネットワーク・セキュリティの分野において研究が活発である．LDDoS 攻撃の標的には，大量にトラフィックが集中するクラウドプラットフォームやビックデータプラットフォームが懸念されている [8][13]．しかし，攻撃事例の報告が極めて少なく，実行難易度が高いことから，現実における LDDoS 攻撃の脅威の大きさは未知であるため，これを明らかにすることは研究分野への貢献につながる．

1.5 論文の構成

本論文は以下のように構成される．2 章では，本研究の理解に必要不可欠な LDoS 攻撃，並びに LDDoS 攻撃の攻撃原理を説明する．3 章では，関連研究を紹介する．4 章では，特性が未知のボトルネックリンクに対する LDDoS 攻撃の自動化戦略に関する要件を整理した後，攻撃シナリオをモデル化し，提案戦略の実装について述べる．5 章では，提案戦略をシミュレータ上に実装し，有効性と性能を評価する．6 章では，昨今のサイバー犯罪の動向から，現実のインターネットの環境下で，提案戦略を実際に適用する攻撃シナリオ議論し，検知手法の展開箇所について議論する．7 章では，提案戦略に対して有効な対策手法について議論する．8 章では，本論文をまとめる．

第 2 章　低レート DoS 攻撃の原理

本章では，本論文の内容を理解するために必須となる低レート DoS/DDoS 攻撃の基本原理を説明する．

2.1　低レート DoS 攻撃

低レート DoS(LDoS: Low-rate DoS) 攻撃は，ネットワークリンクやアプリケーションサーバの処理能力を超える大きさを持った長さの短いパルスを周期的に標的に送信することで，ネットワークやアプリケーションのリソース利用率を悪化させる．

図 2.1 に示すように LDoS 攻撃のモデルは 3 つのパラメータ $< R, L, T >$ で表すことができる．ここで，R は攻撃パルスのレート，L は攻撃パルスの持続時間，T は隣接する攻撃パルス間の間隔である．攻撃が低レートであるためには，L は T に対して非常に小さい値である必要がある [12]．攻撃パルスの平均レートは $R \cdot L/T$ で算出される．例えば，帯域幅 $C = 10Mbps$ のボトルネックリンク*に対して，$R = 10Mbps$，$L = 200ms$，$T = 1000ms$ の攻撃パルスを送信した場合，平均レートは $2Mbps$ であるため，この攻撃パルスがボトルネックリンクを占める割合は 20% となる．この例のような大きさの攻撃パルスは，フラッド型 DDoS 攻撃の検知手法では検出することができない [8]．各攻撃パラメータの理想値は標的のプロトコルによってそれぞれ異なる．

LDoS 攻撃は，トランスポート層，ネットワーク層，アプリケーション層のいずれかに存在するプロトコルの脆弱性を利用して実行される [8]．表 2.1 に主な LDoS 攻撃の分類を示す．本研究で取り扱う LDoS 攻撃は Shrew 攻撃である．Shrew 攻撃への理解をより深めるため，以下に各 LDoS の特徴をまとめる．

Shrew：Shrew 攻撃は，2003 年に Kuzmanovic と Nightly[6] によって示された最も古典的な LDoS 攻撃である．TCP の再送信タイムアウト（RTO:Retransmission Time Out）

表 2.1　LDoS 攻撃の分類（文献 [8] を参考に作成）

LDoS 攻撃の分類	脆弱性レイヤー	脆弱性	
		プロトコル	仕組み
Shrew	トランスポート層	TCP	RTO
RoQ	トランスポート層	TCP	輻輳制御
Full-buffer Shrew	トランスポート層	TCP	RTO & 輻輳制御
LoRDAS	アプリケーション層	HTTP	KeepAlive

*ボトルネックリンクとは，ネットワーク内で最も帯域幅が低いリンクのことである．

機構の時間間隔が単純かつ予測可能であるという脆弱性が攻撃に利用される．TCP フローが流れるボトルネックリンクに対して，上述した攻撃パルスを送信することで，ボトルネックリンクに繰り返し瞬間的な輻輳を発生させて TCP フローを妨害する．"Shrew"攻撃という名前は，小さいながらも攻撃的であり，毒によってゾウのような大きな動物も殺してしまう”トガリネズミ”に由来している [6][7]．本論文では LDoS 攻撃の手法に Shrew 攻撃を用いる． Shrew 攻撃の攻撃原理の詳細は次節で説明する．

RoQ (Reduction of Quality)：RoQ 攻撃は，2004 年に Guirguis ら [14] によって示された，TCP の Loss-based 輻輳制御アルゴリズムを悪用する LDoS 攻撃である．Loss-based 輻輳制御とは，パケットロスの兆候からネットワークの輻輳を判断して輻輳ウィンドウ（cwnd: Congestion window）を制御をすることを指す．Loss-based 輻輳制御では，パケットロスの兆候を検知するまで加算的に cwnd の大きさを増加させ，パケットロスを検知すると乗算的に cwnd を減少させる．このような cwnd の制御は，AIMD（Additive-Increase / Multiplicative-Decrease）と呼ばれる．

RoQ 攻撃は，攻撃パルスによって TCP パケットを損失させて，AIMD による cwnd の制御サイクルを連続して誘発することで，cwnd が段階的に減少されて，標的 TCP のスループットを低下させる．これは，1 パケット損失させるだけで攻撃が成功するため，必要な攻撃パルスの大きさが RTO を発生させなければならない Shrew 攻撃と比較して，小さくなる．文献 [15] では，パルス間隔 T は 5 秒以上の攻撃を RoQ，5 秒未満の攻撃を Shrew に分類している．したがって，RoQ は，攻撃効果は低いが，ステルス性が非常に高い LDoS 攻撃であり，QoS (Quality of Service) が要求されるトラフィックに有効である．

Full-buffer Shrew：Full-buffer Shrew (FB-Shrew) 攻撃は，TCP の RTO と輻輳制御アルゴリズムの 2 つの脆弱性を利用した Shrew 攻撃の変形である．Shrew 攻撃は RTO の直後に次の攻撃パルスを送信することに対し，FB-Shrew 攻撃では，輻輳制御アルゴリズムによって cwnd がボトルネックリンクルータのバッファを満たす大きさまで増加するのを待ってから，次の攻撃パルスを送信する．これによってパルス間隔 T が延長されるため，Shrew 攻撃と比較して FB-Shrew 攻撃に必要な攻撃パルスの総通信量は少なくなる．しかし，FB-Shrew 攻撃はいくつかの TCP パケットが正常に通信されることを許容しているため，Shrew 攻撃と比較して攻撃効果は低い．

LoRDAS (Low-Rate DoS attack against Application Servers)：LoRDAS は，HTTP の KeepAlive を悪用したアプリケーションサーバに対する低レート DoS 攻撃である [16]．LoRDAS の目的は，アプリケーションサーバのサービスキューを飽和させることで，標的サーバ（主にクラウド）のリソースを使い果たすことである．HTTP の KeepAlive は，クライアントと接続を持続するために一定時間接続を確立する．接続が確立されている間，アプリケーションサーバのプロセス，またはスレッドは 1 つのコネクションに割り当てられる．このとき，サーバの処理能力を超えた数のリクエストは一度アプリケーションサーバのサービスキューで待機し，サービスキューが埋まっている場合そのリクエストは廃棄され

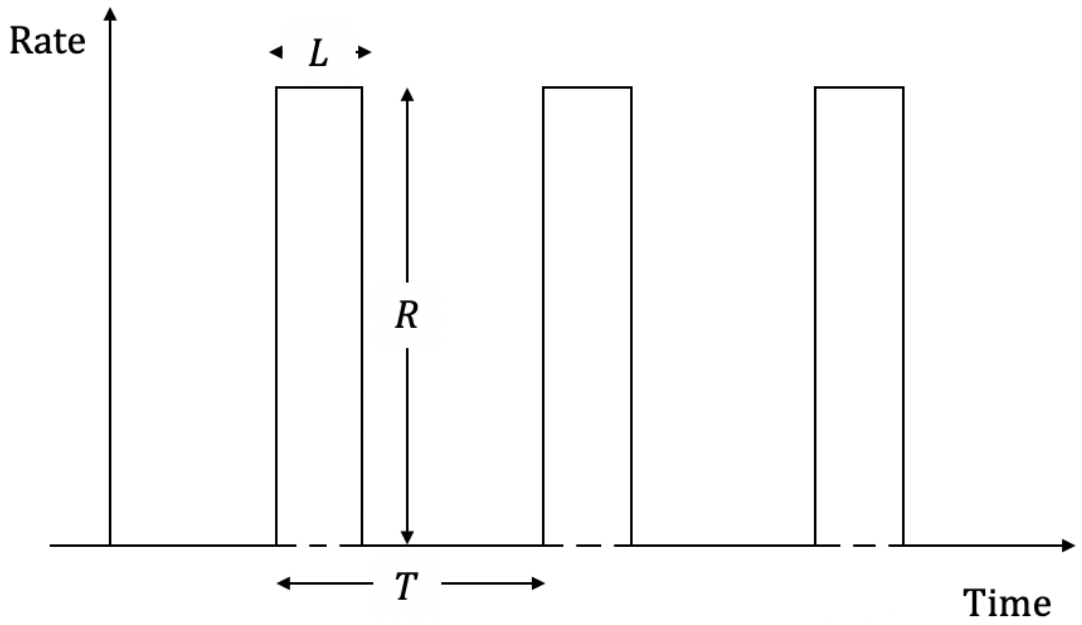

図 2.1 Shrew 攻撃の一般的な攻撃モデル

る．LoRDAS では，この特性を利用する．攻撃によって生成された HTTP コネクションがタイムアウトする時間を予測して，周期的に攻撃者が HTTP リクエストを送信してサービスキューを専有することで，正規の HTTP リクエストのサービスを妨害する．したがって，予測の精度が高いほど，攻撃トラフィックの伝送レートは低くなる [17].

2.2 Shrew 攻撃

Shrew 攻撃は，TCP の RTO を脆弱性を利用した LDoS 攻撃の一つである [8]．RTO とは，言い換えると，TCP 再送信タイマーの最大待ち時間を意味する．TCP は RTO 以内に送信したパケットの応答が返ってこない場合，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[18] により，次の式で設定される．

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

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[18] 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（2.2.1）式の右辺では

$$minRTO > SRTT + max(G, 4 \times RTTAVR) \tag{2.2.1}$$

が成り立つ [7] ため，RTO の初期値は $minRTO$ に設定されるとする．

$$RTO_1 = minRTO \tag{2.2.2}$$

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（2.2.3）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 [18].

$$RTO_i = 2RTO_{i-1} \tag{2.2.3}$$

当該パケットの送信と応答が成功した場合，（2.2.2）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 に実装されている．

Shrew 攻撃は，RTO_i が $minRTO$ に依存して一意に決定される単純を仕様を利用して，図 2.1 に示した矩形波のパルストラフィックをボトルネックリンクに送信することで，TCP 通信を妨害する．具体的には，初めのパルスで TCP パケットが損失すると，$minRTO$ 後に損失されたパケットが再送信される．ここで，2 回目以降のパルスを $minRTO$ の間隔で送信（すなわち，$T = minRTO$）することで，再送信された TCP パケットを連続して損失させる．これによって，正当な TCP フローのスループットは非常に低いか，ほぼゼロになる [12]．ここで，LDoS の攻撃パルスは，パルスのレート R，持続時間 L，間隔 T でモデル化されることを思い出してほしい（図 2.1）．ボトルネックリンクの帯域幅とバッファサイズをそれぞれ C と B とおくと，Shrew 攻撃では，攻撃を成功させるためには，R が C 以上，L が B を埋めるために十分な長さまたは標的 TCP フローの RTT 以上，T が標的 TCP 送信者の初期 RTO 以上の間隔であることが必要である [8][12]．T が固定された Shrew 攻撃は非同期型と呼ばれる [8]．非同期型の Shrew 攻撃は，攻撃者が任意のタイミングで RTO を狙うことができ，T の値の設定によって攻撃効果を調整できるためほとんどの Shrew 攻撃は非同期型である [8]．一方で，T を標的 TCP の RTO に合わせて，RTO, 2RTO, 4RTO, $\cdots$ のように増加する種類を同期型と呼ぶ．これは理想的な攻撃形態であるが，ネットワークパラメータの影響によって，一部の TCP パケットが RTO を回避したり，RTO の変化を正確に予測しなければ，攻撃効果を得られないという観点から現実的な実行は非常に困難である [8]．したがって，本研究では，非同期型の Shrew 攻撃を用いる．

2.3 低レート DDoS 攻撃

LDDoS 攻撃は，同期した複数の LDoS 攻撃から構成される．LDoS の総数を m とすると，各 LDoS のパルスレートは R/m でなければならない．図 2.2 に示すように，複数の

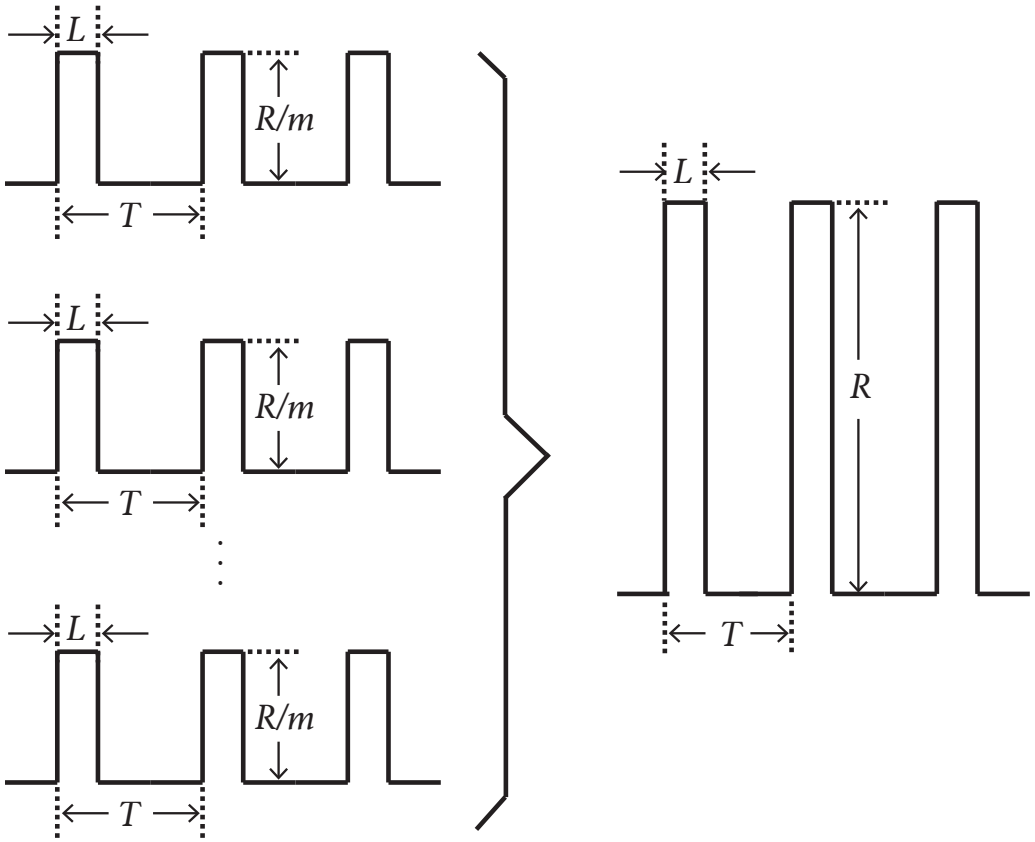

図 2.2 LDDoS 攻撃モデル．m 個の攻撃フローによるパルスレート R の集約

LDoS パルスを対象のボトルネックリンクで正確に集約して，R のパルスレートで攻撃することができる．攻撃ノード m 台分の攻撃パルスをボトルネックリンクで適切に集約できた場合，集約されたトラフィックのパルスレートは R となる．攻撃パルスを分割することにより，個々の攻撃パルスの平均通信量がさらに低くなるため，検知が困難になる．本論文では以降，複数の攻撃ノードから実行される Shrew 攻撃を LDDoS 攻撃と呼ぶ．

第 3 章　関連研究

本章では，既存の研究のリサーチギャップを示し，研究課題を整理するために，関連研究をまとめる．関連研究は，検知，防御，攻撃モデル，実証的研究の 4 つのカテゴリに分類される．

3.1　LDoS/LDDoS 攻撃の検知

LDoS 攻撃並びに LDDoS 攻撃の検知は，本研究分野において最も研究が活発な領域である．

文献 [19] において，スペクトル分析から得られる LDDoS 攻撃のパルス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．文献 [20] 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，バックボーンネットワークの自律システム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 [21] 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，攻撃者がパルス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 [22] では，フィッシャーの g 統計検定とシーゲル検定を利用した LDoS 攻撃の検出手法を提案した．この結果では，周期が一定の攻撃パルスにはフィッシャーの g 統計検定が良好な結果を示しており，複数の周期をもつ攻撃パルスにはシーゲル検定が良好な結果を示した．この手法の利点は，攻撃の被害者側で受信した乱れた攻撃パルスを利用できることである．文献 [23] 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．この手法の優位性は，バックグラウンドトラフィックに隠蔽された同期型 LDoS のパルスシーケンスを検出することが可能なことである．

3.2　LDDoS 攻撃の防御

本節では，提案戦略の対策手法を検討するために，LDDoS 攻撃の防御に関する既存研究をまとめる．

3.2.1 RTO のランダム化

Shrew 攻撃を可能にしている要因の一つは，TCP の RTO の値が $minRTO$ に依存しているためである．したがって，LDDoS 攻撃から TCP を防御するための最もシンプルな手法は RTO の値をランダム化することである．文献 [7] では，$minRTO$ の値を 1 秒から 1.5 秒の間でランダム化する戦略が提案された．この手法によって，TCP がパケットを再送する時刻を予測することが難しくなり，LDDoS の周期から外れた TCP パケットが正常に通信できるようになるため，一定の緩和効果が期待できる．しかし，LDDoS 攻撃を受けていない間の TCP の性能が低下することに加え，オペレーティングシステムのカーネルに実装するコストが高いため，実現性が低いと指摘されている [8].

3.2.2 Active Queue Management(AQM)

AQM はネットワークの輻輳を軽減するためにルータのキュー（バッファ）に蓄積されたパケットが満たされる前に，パケットを廃棄するキュイーイングポリシを指す．AQM の中で最も一般的なアルゴリズムは RED(Random Early Detection)[24] である．RED は，キュー長が設定した閾値を超えると，事前に設定した確立に基づいてパケットを廃棄する．文献 [7] によれば，Shrew 攻撃は RED に対しても高い攻撃効果を得られることが明らかになっている．一方で，文献 [25] では，RED に対して Shrew 攻撃を評価した結果，攻撃効果が低下し，良好な TCP スループットを得られる結果が得られている．このような結果の齟齬は，帯域幅やバッファサイズなどのネットワークパラメータや，RED のパラメータ設定が影響していることが考えられる．

文献 [26] では，Shrew 攻撃下においても高い TCP スループットを維持できる Robust RED(RRED) と呼ばれるアルゴリズムが提案された．RRED は，従来の RED に Shrew 検出アルゴリズムを実装したアルゴリズムである．検知手法によって LDoS 攻撃によるパケットを検知してフィルタリングした後，RED を適用することで攻撃時においても高いスループットを維持することが可能である．ただし，パルスが分散された場合（すなわち，LDDoS 攻撃）には対応することができない．

3.2.3 ボトルネックリンクバッファサイズの調整

Shrew 攻撃によって，TCP をタイムアウトするためには，ボトルネックリンク帯域幅 C とボトルネックリンクバッファ B を攻撃パルスによるパケットによって満たすことで，正常な TCP パケットが B にエンキューされるのをブロックする必要がある．このことから，B の値を増やすことが攻撃の緩和につながることが実証されている．文献 [27] では，簡単な数学モデルを用いてルータのキュー動作を解析した．B の値が大きいほど，必要な攻撃パルスのピークレート R が増加し，B の値が小さいほど Shrew 攻撃によって高い効果が得られる

ことをシミュレーションで実証した．文献 [12] では，Shrew 攻撃が検知された場合に一時的に B の値を増加する防御戦略が提案された．シミュレーションによる評価の結果，攻撃時にバッファの増加量を 3 倍に増加することによって約 40% の TCP が通信可能であることが示された．この防御戦略を破るためには，攻撃者は送信速度を大幅に増加させる必要があるが，これは従来の DDoS 防御戦略に対して攻撃をより脆弱にすることになる．

3.3 攻撃モデル

Shrew 攻撃のモデルは 2003 年に Kuzmanovic と Knightly[6] によって示された．2014 年，Luo ら [12] は，ネットワーク環境（遅延，ボトルネックリンク帯域幅など）の影響を考慮した Shrew 攻撃の数学モデルを提案した．文献 [6] で提案された攻撃効果のモデル式は，TCP の輻輳ウィンドウの振る舞いが考慮されていないため，不正確であることを指摘している．Luo ら [12] のモデルによって，攻撃の成功に必要な攻撃パラメータの最小値のモデル式や，最大効果のモデル式が示された．2020 年，Kieu ら [28] は，Luo ら [12] の攻撃効果のモデル式の相対誤差が依然として大きいことを指摘し，より正確な攻撃効果のモデル式を提案した．

Full-buffer Shrew 攻撃のモデルは，2006 年に Guirguis ら [29] によって明らかとなった．2016 年，Yue らは，Guirguis らの FB-Shrew モデルにおける標的 TCP フローの cwnd の挙動が攻撃フローとの競合を無視しているために不正確であることを指摘し，cwnd の動作モデルを再検討し，それに適した攻撃パラメータを提案した [30]．検証の結果，Yue らの提案したモデルは Guirguis らが提案したモデルよりも高い攻撃効果を得た．2019 年，Yue らは，Guirguis らの FB-Shrew モデルでは RTT が固定されているため，正確に FB-Shrew 攻撃を評価できていないことを指摘し，変動する RTT に対応した FB-Shrew の低高バーストモデルを開発した [31]．

3.4 現実的環境を想定した LDDoS 攻撃の実行戦略・評価

本研究は，現実的環境を想定した LDDoS 攻撃の実証的研究に分類される．本カテゴリの研究は他の領域と比較して数が少ないが現実における LDDoS 攻撃の有効性がいくつかの研究によって示されている．

2015 年, Massimo と Massimiliano[32] は, Slowly-Increasing-Polymorphic DDoS Attack Strategy(SIPDAS) を提案した．SIPDAS の目的は，目標とする攻撃効果が得られるまで，攻撃期間ごとに攻撃速度を 1 単位ずつ増加させることで攻撃による被害額と攻撃コストの比率を最大化することである．SIPDAS は，クラウドアプリケーションの計算資源を枯渇させるために Deeply-Nested XML 攻撃を用いており，検知を回避するためにできるだけ長い時間を書けてゆっくりと攻撃強度を増加させる．

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．この障壁を攻撃者が解決する可能性として，文献 [33] 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．

2020 年, Park ら [34] は, 現実的なネットワーク同期を前提とした Very Short Intermittent DDoS 攻撃（VSI-DDoS）の有効性の評価を行った．VSI-DDoS は，数ミリ秒単位で攻撃トラフィックがサーバに集中することを前提としている攻撃であり，現実における有効性を過大評価されている側面があった．検証の結果，VSI-DDoS は約 90ms の小さな同期のずれが発生しただけで 85.7% の効果が失われ，有効性が低下することを実証した．

3.5 リサーチギャップ

リサーチギャップとは，さらに研究を進める余地のある未開拓の研究領域を指す．本節では，LDoS 攻撃の研究に関するリサーチギャップを述べる．

3.5.1 現実における LDDoS 攻撃の戦略

LDDoS 攻撃の現実における攻撃戦略について検討している既存研究は少ない．その中でも特に，トランスポート層を標的とした LDDoS 攻撃は，アプリケーション層が標的の LoRDAS と比較すると自動化に対する難易度が高く，筆者の知る限りではこれまでに検討されていない．昨今の一般的な DDoS 攻撃は，LDDoS 攻撃代行サービス [35] によって自動化されてサービスとして提供されている背景がある．したがって，LDDoS 攻撃の自動化によるインターネットへの被害は考慮するべき重要なシナリオである．そこで，本研究では，Shrew 攻撃の手法を利用した LDDoS 攻撃の攻撃戦略を検討する．

LDDoS 攻撃の自動化は，一般的な DDoS 攻撃と同様に任意の様々な標的に対して実行されると考えられる．LDDoS 攻撃の自動化に求められる最も重要な要件は，標的に対して高すぎず，低すぎない適切な強度の攻撃トラフィックを生成することである．したがって，Shrew 攻撃の自動化には，標的ごとに攻撃パルスのピークレート R を，ボトルネックリンク帯域幅 C 以上の適切な値に設定する必要がある．しかし，Shrew 攻撃には，次に説明する暗黙的な前提が存在するため，自動化の有効性は明らかではない．

3.5.2 パルスレートの設定に関する暗黙的な前提

既存研究では，攻撃者が理想的な攻撃パラメータを決定できるという暗黙的な前提が存在する．これを言い換えると，現実の攻撃シナリオにおいて，攻撃者が標的 TCP フローの経路上のボトルネックリンク帯域幅をあらかじめ知っていること前提となっている．しかし，現実の攻撃シナリオにおいて，攻撃者が常に標的ボトルネックリンクのパラメータを熟知しているとは限らない．そこで，本研究では，LDDoS 攻撃の自動化の実現性と有効性を確認するために，ボトルネックリンクの帯域幅とバッファサイズが未知の場合における，攻撃強度の自動最適化のための LDDoS 攻撃戦略（以下，提案戦略）について検討する．

3.6 研究課題

上記のリサーチギャップから本研究では，以下の研究課題を設定する．

1. 提案戦略をモデル化し，有効性を明らかにすること．
2. 提案戦略が実行可能な現実の攻撃シナリオと防御策の展開箇所を議論すること．
3. 提案戦略に対して有効な防御策を議論すること．

第 4 章　提案戦略

本章では，特性が未知のボトルネックリンクに対する LDDoS 攻撃の自動化戦略に関する詳細を説明する．4.1 節では，特性が未知のボトルネックリンクに対して，LDDoS 攻撃を自動化するための前提と要件を整理し，攻撃シナリオをモデル化する．4.2 節では，提案戦略の実装について詳細に説明する．

4.1　特性が未知のボトルネックリンクに対する攻撃強度自動最適化のための LDDoS 攻撃戦略

インターネット上で攻撃者が任意のボトルネックリンクを標的として LDDoS 攻撃を実行する場合，パルスレート R をボトルネックリンク帯域幅 C 以上のレートに設定する必要があることを 2 章で説明した．これまでの LDDoS 攻撃の研究 [6][7][8][12] では，攻撃者にボトルネックリンク帯域幅 C が与えられていることが前提となっている．このような前提のもとでは，パルスレート R を容易に決定することが可能であるが，現実の攻撃シナリオでは，攻撃者に C が与えられていない可能性も十分に考えられる．この場合，攻撃者が最初から理想的な強度のパルスレートを設定することは困難であり，パルスレート R が適当に決定された場合，次の問題で攻撃に失敗する可能性がある．

攻撃の失敗例 1：ボトルネックリンク帯域幅に対して攻撃パルスが小さく，十分な攻撃効果を達成できない．

攻撃の失敗例 2：ボトルネック帯域幅に対して攻撃パルスを過剰に送信し，攻撃フローの平均がフラッド型 DDoS の攻撃平均転送レートに近づくことでステルス性を失い，既存の検知手法で検知されてしまう．

したがって，本研究では，特性が未知のボトルネックリンクに対する LDDoS 攻撃の有効性を評価するために，以下の前提条件と要件，および攻撃シナリオを満たした提案戦略を検討する．

4.1.1　前提条件と要件

提案戦略では，ボトルネックリンクの特性（帯域幅とバッファサイズ）が攻撃者に与えられないことを前提とする．この前提を攻撃者，並びに提案戦略の観点から言い換えると，理想的な攻撃強度（攻撃パルスのピークレート R）を事前に決定することができないことを意味する．提案戦略には，上記の前提のもとで効果的な LDDoS を実行するために，以下に示す要件が求められる．

要件 1：標的の TCP フローのスループットを目的値以下に低下させるために必要なパルスレート R を自動で決定できること．

要件 2：高レート DDoS 攻撃の検知を回避するために，攻撃フローの平均レートがボトルネックリンクを占める割合を可能な限り小さくすること．

4.1.2 提案戦略の概要

提案戦略は，要件 1 を達成するためのパルスレートの探索的増加機能と要件 2 を達成するためのステルス性優先機能をもつ．2 つの機能の概要を以下に示す．

1．パルスレートの探索的増加機能：提案戦略による攻撃パルスの制御を図 4.1 に示す．提案戦略は，標的 TCP が目的攻撃効果（スループット）未満になるまでパルスレート R を段階的に増加する．目的攻撃効果とは，提案戦略によって低下させる標的 TCP フローのスループットの目的値を指す．R の初期値は，ボトルネックリンク帯域幅 C に対して十分に小さい初期攻撃レート ΔR が設定される．その後，一定の最適化間隔 W（W は T の倍数）ごとに攻撃に成功しているか（すなわち，標的 TCP のスループットが攻撃効果未満であるか）を判定する．目的攻撃効果を達成した場合，以後，現在の R の値で LDDoS 攻撃を続ける．目的攻撃効果を達成していない場合，R の値を ΔR だけ増加して LDDoS 攻撃を続ける．

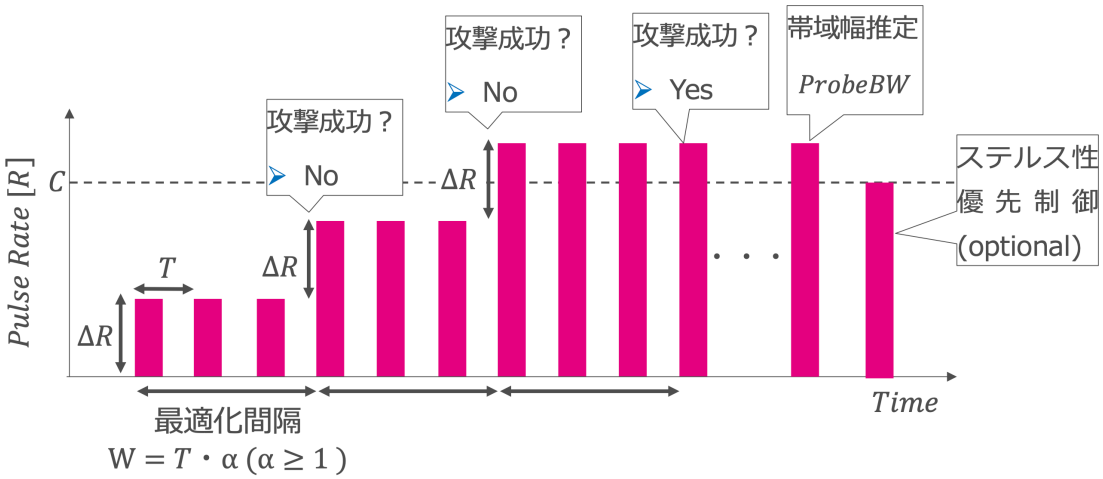

図 4.1 パルスレートの探索的増加

2．ステルス性優先機能：パルスレートの探索的増加機能によって目的攻撃効果を達成したとき，パルスレート R がボトルネックリンク帯域幅 C を超える可能性がある．ステルス性優先機能は，目的攻撃効果の達成後に，ボトルネックリンク帯域 C を推定し，R を推定された C まで低下する．実行は，攻撃者が任意で有効または無効化することができる．本論文では，ステルス性をボトルネックリンク帯域幅に対する攻撃トラフィックの平均使用率と定義する．ステルス性が 50% を下回る場合，攻撃が低レートであると判断する．

4.1.3 攻撃シナリオのモデル化

表 4.1 に本論文で使用する記号を示す.

上記の要件を満たすために必要な攻撃シナリオを図 4.2 に示す．標的 TCP 送信ノード $Sender_{target}$ は，標的 TCP 受信ノード $Receiver_{target}$ からのリクエストに対して，バルク転送の TCP フロー ϕ_{target} を送信する.

攻撃者は，観測ノード $Receiver_{observe}$ を $Receiver_{target}$ が接続されている LAN に構築する．$Receiver_{observe}$ の役割は，攻撃効果の観測と，攻撃パルスの受信と観測である．$Receiver_{observe}$ は $Receiver_{target}$ と同様に，正規のリクエストによって，$Sender_{target}$ からバルク転送の観測 TCP フロー $\phi_{observe}$ を受信する．$\phi_{observe}$ は，パルスレートの探索的増加機能において，目的の攻撃効果を達成しているかを判別するために使用する．$\phi_{observe}$ は，正規のリクエストによって通信する正常なトラフィックであるため，攻撃トラフィックに含まれない．さらに，m 台の攻撃ノード $Attacker_{1\cdots m}$ のうち，アクティブな $c(\forall c \in [1..m])$ 台の攻撃ノード $Attacker_{1\cdots c}$は, $Receiver_{observe}$ に対して LDDoS 攻撃フロー $\Phi_{A_c} = (\phi_{A_1} \cdots \phi_{A_c})$ を送信することで，同じボトルネックリンクを共有する ϕ_{target} の平均スループット δ_{target} を低下させる．アクティブ攻撃ノード数 c の制御については次節で説明する.

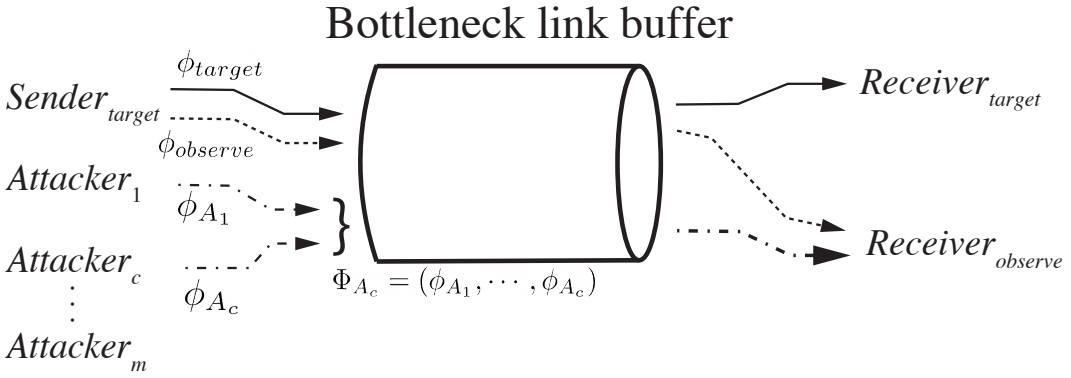

図 4.2 攻撃シナリオ

4.2 提案戦略の実装

提案戦略では，図 4.3 に示すフィードバック制御によって，攻撃強度を最適化する．攻撃制御ノード $Master$ が攻撃全体を制御する役割を持つ．$Master$ は目的攻撃効果 $throughput_{objective}$ を入力として受け取り, フィードバックされた観測 TCP フロー $\phi_{observe}$ のスループットのサンプル値 $\theta = (\vartheta_1 \cdots \vartheta_t)$ をもとに，アクティブ攻撃ノード数 c を決定する．ここで，ϑ_t は，$\phi_{observe}$ の通信開始後の $t-1$ 秒から t 秒までの間に $Receiver_{observe}$ で計測したスループットである（t は自然数）．1 回のフィードバック動作につき，観測窓幅 W

表 4.1 本論文で使用する記号

記号	定義
C	ボトルネックリンク帯域幅
B	ボトルネックリンクバッファのサイズ
R	攻撃パルスの合計ピークレート
L	各攻撃パルスの長さ
T	各攻撃パルスの間隔
m	攻撃ノードの総数
c	攻撃に参加するアクティブな攻撃ノード数
$incrementC$	1 回のフィードバック制御ごとに計算される アクティブ攻撃ノード数の増加量
ΔR	各攻撃パルスのピークレート
$Sender_{target}$	標的 TCP フローの送信ノード
$Receiver_{target}$	標的 TCP フローの受信ノード
$Receiver_{observe}$	攻撃観測ノード
$Attacker_i$	攻撃ノード i
ϕ_{target}	標的 TCP フロー
δ_{target}	標的 TCP フローの平均スループット
$\phi_{observe}$	観測 TCP フロー
$\delta_{observe}$	観測 TCP フローの平均スループット
ϕ_{A_i}	攻撃ノード i が送信する攻撃フロー
Φ_{A_c}	ϕ_{A_1} から ϕ_{A_c} の合成フロー
W	攻撃効果の観測窓幅
$throughput_{objective}$	目的攻撃効果
$\theta = (\vartheta_1, \cdots, \vartheta_t)$	t 秒間における 1 秒間ごとの $\phi_{observe}$ のサンプル集合 $incrementC$ の計算に使用される
θ_{max}	最後に c を増加した時刻から最新のサンプリング時刻 t までにおける θ の最大値 $incrementC$ の計算に使用される
θ_{min}	最後に c を増加した時刻から最新のサンプリング時刻 t までにおける θ の最小値 $incrementC$ の計算に使用される
$\theta_{average}$	標的 TCP フローの平均スループット

秒の長さだけ θ を計測する（W は自然数）．例えば，$W = 3$ のとき，1 回目のフィードバックでは，$\theta = (\vartheta_1, \cdots, \vartheta_3)$，2 回目のフィードバックでは，$\theta = (\vartheta_1, \cdots, \vartheta_3, \cdots, \vartheta_6)$ を得る．そして，アクティブな c 台の各攻撃ノードは，$< \Delta R, L, T >$ のパラメータで攻撃パルスを送信し，ボトルネックリンクで合成される攻撃パルスのパラメータは $< R = \Delta R \cdot c, L, T >$ となる．もう 1 つのフィードバック値 R_{max} は，目的攻撃効果の達成後にボトルネックリンク帯域幅 C を推定するために使用される．$Master$ はこの値を使用して，攻撃のステルス性を低下させる．

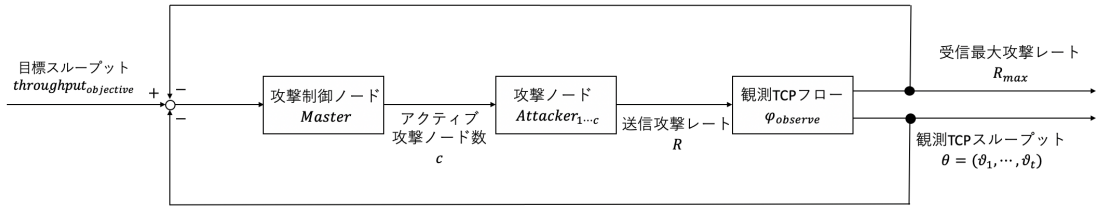

図 4.3　提案戦略のフィードバック制御

Algorithm1 ～ Algorithm3 に，上記のフィードバック制御を $Master$ に実装したより詳細な手順を示す．関数 $ControlAttack$ は，$Master$ によって観測窓幅 W 秒ごとに繰り返し実行されフィードバック制御を実現する．処理の内容を要約すると，各攻撃ノードが送信するパルスパラメータを初期化（4.2.1 項で説明）した後，攻撃パルス送信毎に現在の攻撃効果の推定値（4.2.2 項で説明）をもとに，アクティブ攻撃ノード数 c の増加量 $incrementC$ を決定（4.2.3 項で説明）し，$SendAttackPulse$ を実行して W 秒間 LDDoS 攻撃を実行する命令を $Attacker_{1\cdots c}$ に送信する．さらに，攻撃のステルス性を維持するために，目的攻撃効果の達成後にボトルネックリンクを推定し，その大きさまで合成後の攻撃パルス R の大きさを下げる機能をもつ（4.2.4 項で説明）．

4.2.1　攻撃パルスのパラメータ設定

アクティブな各攻撃ノード $Attacker_{1\cdots c}$ は，パラメータ $< \Delta R, L, T >$ で定義される攻撃パルスを送信する．提案戦略では，複雑さを軽減するために，L，T は固定の値を設定し，ΔR のみ，ボトルネックリンクの帯域幅に応じた値を使用する．パルス間隔 T は，標的 TCP 送信ノード $Sender_{target}$ の初期 RTO である $minRTO_{target}$ 以上の値を設定する必要がある．RFC6298[18] では，$minRTO$ を 1 秒に設定することが推奨されているため，T を 1 秒に設定する．パルス幅 L は，タイムアウトを発生させるために，標的 TCP フローの RTT 以上の長さで，かつ T に対して十分に小さくなければならない [12]．そのため，本研究では，ϕ_{target} 及び，$\phi_{observe}$ の RTT が $300ms$ 以下であるという前提をおき，L を 300ms に固定する．各攻撃ノードが送信するパルスレート ΔR は，ボトルネック帯域幅 C を超えない値

に設定する必要がある．そこで，提案戦略では攻撃パルスの送信（関数 $ControlAttack$）前の安定したスループットの平均値を ΔR に設定する．具体的には，Algorithm1 の 2 行目において，$Receiver_{observe}$ からフィードバックされた θ の，直近 W 秒分のスループットサンプル $(\vartheta_{t-W+1}, \cdots \vartheta_t)$ から，それらの平均値 $\delta_{observe}$ を算出する．このために，攻撃を開始する数十秒前から $\phi_{observe}$ の通信を開始し，輻輳ウィンドウ値がある程度安定した後に，攻撃パルスの送信（関数 $ControlAttack$ の実行）を開始する必要がある．$\delta_{observe}$ は必ず C 以下になるため，C を超えない ΔR が設定され，安全に攻撃を開始できる．

4.2.2 攻撃効果の推定

標的 TCP フローのスループットを直接観測することはできないため，提案戦略では，現在の合計パルスレート R によって目的の攻撃効果を達成しているかどうかを判断するために，観測 TCP フロー $\phi_{observe}$ を用いて，間接的に攻撃効果を推定する．図 4.2 より，ϕ_{target} と $\phi_{observe}$ は，同じボトルネックリンクを共有する同種フローであるため，TCP 親和性のモデル式 [36] により $\delta_{target} \simeq \delta_{observe}$ が成り立つ．この特性を利用して，$\delta_{observe}$ から δ_{target} への攻撃効果を間接的に推定する．スループットの値は常に可変であるため，提案する手法では，過去 W 秒間の $\phi_{observe}$ のサンプル値の平均値である $\delta_{observe}$ を計算し，この値が目標攻撃効果以下であれば，目標攻撃効果が達成されたとみなす．

4.2.3 アクティブ攻撃ノード数 c の決定

フィードバックごとに，Algorithm1 の条件式 2a 及び，Algorithm2 の条件式 3 を満たしている場合，前回のフィードバック時に送信した攻撃パルスのレート R では目的の攻撃効果を達成できないと判断し，アクティブ攻撃ノード数 c を増加する処理を実行する．アクティブ攻撃ノード数 c の増加量は，Algorithm2 の 3 行目の関数 $computeIncrementC$ によって計算される．この関数は，TCP スループットの損失に比例して，攻撃ノードの増加量を決定する．計算される値は，以下の経験的に設計された式 (4.2.1) によって，攻撃ノード 1 台あたりの TCP 損失量に比例して攻撃ノードを増加する．

$$incrementC = |round\left(\frac{\theta_{average} - throughput_{objective}}{\frac{\theta_{max}-\theta_{min}}{\theta_{average}} \cdot \Delta R \cdot c}\right)| \tag{4.2.1}$$

ここで，θ_{max} は，最後に c を増加した時刻から最後のサンプリング時刻 t までにおける θ の最大値，θ_{min} は，θ_{max} と同範囲における θ の最小値，$\theta_{average}$ は，時刻 $t-W+1$ から t までの θ の平均値（$\delta_{observe}$ と同様）である．

算出した $incrementC$ は単純に c に加えるのではなく，合計攻撃ノード数を上回らない範囲で加える（条件式 4a, 5a, 5b）．条件式 4b は，c を増加するべきであると条件式 2a と条件

式 3 によって判断されたが，$incrementC$ の値が 0 になってしまったときに 1 度だけ実行される調整処理である．このケースは主に，目的攻撃効果の達成まで c がわずかに足りない場合，すなわち式 (4.2.1) の $round$ 内の項の分子が 0 に近い場合を想定している．

4.2.4 ステルス性の優先制御

ステルス優先制御は，目的の攻撃効果が達成された後に $Receiver_{observe}$ によって受信された攻撃パルスの最大レートを使用して，ボトルネックリンクの帯域幅の推定値である BW_{probe} を求め，合成パルスレート R をそれに等しい値に減少させる．攻撃者は，攻撃開始前にステルス性優先制御を有効にするか選択できる．有効化しなかった場合，ステルス性優先制御は実行されない．

ステルス性優先制御の詳細を Algorithm3 に示す．初めに，関数 $getRmax$ により，$Receiver_{observe}$ が，100 ミリ秒間隔で計測した Φ_{A_c} のスループットの最大値 R_{max} を取得する．例えば，$R = 10Mbps, L = 300ms, T = 1000ms$ のパルスを 100 ミリ秒間隔で計測した場合，理想的には $[10, 10, 10, 0, \cdots, 0]\,(Mbps)$ のような結果が得られる．R_{max} はこの計測値の中の最大値となるため，この例では，R_{max} は 10Mbps である．ただし，攻撃パルスと TCP が競合しており，ボトルネックリンクの帯域利用率が 100% の状況では，競合 TCP によって攻撃パケットの一部がボトルネックリンクバッファで損失してしまうため，$Receiver_{observe}$ で計測される R_{max} は，実際に送信した R よりも低下する．例えば，計測値が $[8, 9, 9, 0, \cdots, 0]\,(Mbps)$ の場合，R_{max} が 9Mbps となってしまう．そこで，関数 $CeilTop1$ により，R_{max} の上位一桁の概数を切り上げで求めることによって，C の値を推定する（Algorithm3，4 行目）．上位一桁の概数とは，上位二桁目を切り上げて，上位三桁以下を切り捨てた数である．ボトルネックリンクの帯域幅の推定値である BW_{probe} は，Algorithm3 の 6 行目から 10 行目において，決定される．BW_{probe} は，測定された R_{max} の概数である $ApproximateR_{max}$ が，R_{max} よりも遥かに大きい場合は R_{max}，異なる場合は $ApproximateR_{max}$ が設定される．現在送信しているピークレート R が，ここで得られたボトルネックリンクの推定帯域幅 BW_{probe} よりも大きい場合，R が高すぎると判断し，ΔR に BW_{probe} を現在の攻撃ノード数 c で割った値（小数点未満切り上げ）を設定する（条件式 7）．

Algorithm 1 Core Algorithm of Master Node

Require: ΔR ▷ 攻撃ノード 1 台あたりのパルスレート（Kbps）
Require: $L \Leftarrow 300$ ▷ 攻撃ノード 1 台あたりのパルス幅（ms）
Require: $T \Leftarrow 1000$ ▷ 攻撃ノード 1 台あたりのパルス間隔（ms）
Require: $W \Leftarrow W_{initial}$ ▷ 観測窓幅
Require: $c \Leftarrow 0$ ▷ アクティブ攻撃ノード数
Require: $m \Leftarrow m_{initial}$ ▷ 攻撃ノードの総数
Require: $prev\_\delta_{observe} \Leftarrow \infty$ ▷ 前回のフィードバックにおける $\delta_{observe}$
Require: $throughput_{objective} \Leftarrow throughput_{objective_initial}$ ▷ 目的攻撃効果
Require: $initDeltaR \Leftarrow false$ ▷ ΔR 初期化フラグ
Require: $ajust \Leftarrow false$ ▷ c の調整フラグ
Require: $loweredRToBW \Leftarrow false$ ▷ パルスレート R をボトルネック帯域幅の推定値まで低下させたかを表すフラグ
Require: $prioStealthy \Leftarrow true$ **or** $false$ ▷ ステルス性優先制御のオンオフ

function $ControlAttack$
  $\delta_{observe} \Leftarrow computeLatestAverageObserveTp()$
  $noMoreIncrease = loweredRToBW$ **and** $prioStealthy$
  if $!(initDeltaR)$ **then** ▷ 条件式 1
    $\Delta R \Leftarrow \delta_{observe}$
    $initDeltaR \Leftarrow true$
    $c \Leftarrow 1$
  end if
  if $\delta_{observe} > throughput_{objective}$ **and** $!(noMoreIncrease)$ **then** ▷ 条件式 2a
    $IncrementActiveAttackerNum()$ ▷ Algorithm2 を実行
  else if $noMoreIncrease$ **then** ▷ 条件式 2b
    print ’ステルス性優先制御によって設定されたパルスレートを維持する’
  else ▷ 条件式 2c
    print ’攻撃成功：目的攻撃効果を達成’
    if $prioStealthy$ **then** ▷ 条件式 6
      $LowerPulseRateToProbedBW()$ ▷ Algorithm3 を実行
    end if
  end if
  $prev\_\delta_{observe} \Leftarrow \delta_{observe}$
  $SendAttackPulse(\Delta R, L, T, c, W)$
end function

Algorithm 2 アクティブ攻撃ノード数 c の更新処理

function $IncrementActiveAttackerNum$
  if $\delta_{observe} > prev\_\delta_{observe}$ **then** ▷ 条件式 3
    $incrementC \Leftarrow computeIncrementC(\Delta R, c, throughput_{objective})$
    if $incrementC > 0$ **then** ▷ 条件式 4a
      if $(c + incrementC) \leq m$ **then** ▷ 条件式 5a
        $c \Leftarrow c + incrementC$
      else if $c! = m$ **then** ▷ 条件式 5b
        $c \Leftarrow m$
      end if
    else if $c < m$ **and** $!(ajust)$ **then** ▷ 条件式 4b
      $c \Leftarrow c + 1$
      $ajust \Leftarrow true$
    end if
  end if
end function

Algorithm 3 ステルス性優先制御

function $LowerPulseRateToProbedBW$
  $R_{current} \Leftarrow \Delta R \cdot c$
  $R_{max} \Leftarrow getRmax()$
  $ApproximateR_{max} \Leftarrow CeilTop1(R_{max})$
  $BW_{probe} \Leftarrow 0$
  if $R_{max} + 0.1 * ApproximateR_{max} < ApproximateR_{max}$ **then**
    $BW_{probe} \Leftarrow R_{max}$
  else
    $BW_{probe} \Leftarrow ApproximateR_{max}$
  end if
  if $R_{current} > BW_{probe}$ **then** ▷ 条件式 7
    $\Delta R \Leftarrow ceil\,(BW_{probe}/c)$
    $loweredRToBW \Leftarrow true$
  end if
end function

第 5 章　評価実験と考察

本章では，提案戦略が，固定ブロードバンド回線を想定したボトルネックリンクに対して正常に機能することを検証し，攻撃性能を評価する．

5.1　評価実験の内容

5.1.1　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[37] を用いたシミュレーション環境で行う．図 5.1 にシミュレーションに用いたネットワークトポロジと関連する構成を示す．$Sender_{target}$ の $minRTO$ は，推奨値の 1 秒 [18] に設定した．$Sender_{target}$ が送信する TCP パケットのサイズは 590Byte である．TCP 輻輳制御アルゴリズムは NewReno を使用する．すべてのノードは DropTail 方式でバッファに蓄積されたパケットを処理する．$Sender_{target}$ と $Receiver_{target,observe}$ の TCP ソケットの送受信バッファサイズはそれぞれ 512KByte に設定した．各ノードが送信するトラフィックは図 4.2 で示した攻撃シナリオと同様である．$Attacker_{1\cdots c}$ が送信する攻撃トラフィックのプロトコルは UDP である．攻撃パケットのサイズは 80Byte である．攻撃制御ノード $Master$ はトポロジ上に配置せず，ns-3 のイベント動作として実行される．したがって，今回のシミュレーションでは，フィードバック制御に本来発生する $Master$ が関与する通信の遅延は無視される．パルス幅 L は，通常ネットワークの RTT が $10ms$ から $100ms$ であることを踏まえ，タイムアウトを起こすために十分な $300ms$ を設定した．目的攻撃効果 $throughput_{objective}$ は，動画配信サービスの Netflix が公表している必要最低帯域幅 [38] の $500kbps$ に設定した．攻撃ノードの総数 m は 300 ノードである．攻撃の観測窓幅 W は，3 秒に設定した．

外乱トラフィック送信ノードである $Cross_1$，$Cross_2$, $Cross_3$ は，$Receiver_{target}$ に対して TCP バルク転送でデータを送信するためのノードである．外乱トラフィックは一部のシミュレーションでのみ送信される．

5.1.2　評価実験の構成

評価実験は，提案戦略の動作とネットワークパラメータ並びにトラフィックパターンの組み合わせが異なる計 32 通りのシミュレーションから構成される．シミュレーションは，評価実験 A，評価実験 A^+，評価実験 B，評価実験 B^+ の 4 つに分類される．各評価実験の概要を以下に示す．

評価実験 A：提案戦略の基礎的な攻撃性能を評価するために，外乱トラフィックが存在しない環境で，ステルス優先制御を無効化し，目的攻撃効果を達成できるかどうかを検証する．

評価実験 A^+：提案戦略の攻撃性能のロバスト性を評価するために，外乱トラフィックが存在

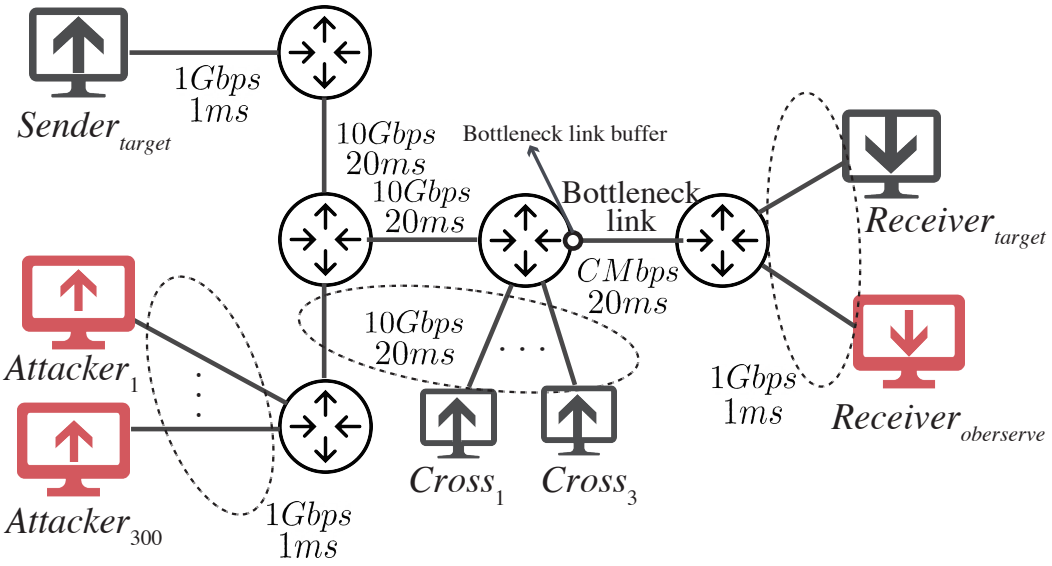

図 5.1 ns-3 シミュレーションで使用したネットワークトポロジ

する環境で，ステルス優先制御を無効化し，目的攻撃効果を達成できるかどうかを検証する．

評価実験 B：提案戦略の基礎的なステルス性能を評価するために，外乱トラフィックが存在しない環境で，ステルス優先制御を有効化し，目的攻撃効果の達成後に C の値を推定し，推定値まで R を減少できるかどうかを検証する．

評価実験 B^+：提案戦略のステルス性能のロバスト性を評価するために，外乱トラフィックが存在する環境で，ステルス優先制御を有効化する．目的攻撃効果の達成後に C の値を推定し，推定値まで R を減少できるかどうかを検証する．

表 5.1 に各評価実験の構成を示す．各評価実験ごとに，複数のボトルネックリンク帯域幅 C とそれに対応するバッファサイズ B を設定したシミュレーションを実行する．C は 10Mbps から 150Mbps まで 20Mbps ごとの値を設定する．これらの C の値は，文献 [39] で予測された 2018 年から 2023 年までの固定ブロードバンド回線速度の予測に基づいている．ボトルネックリンクのバッファサイズ B は，文献 [40] で提案されているバッファサイズの計算式 $B = C \cdot \overline{RTT}/\sqrt{n}$（$n$ はフロー数）に $n = 16$ を代入した値を計算して設定する．

評価項目を表 5.1.2 に示す．

5.1.3 シミュレーションの実行時間と各通信の開始時刻

各シミュレーションの実行時間は，評価実験 A の $a_1 \sim a_8$ および評価実験 B の $b_1 \sim b_8$ が 120 秒間，評価実験 A^+ の $a_1^+ \sim a_8^+$ および，評価実験 B^+ の $b_1^+ \sim b_8^+$ が 180 秒間である．

各通信は，すべてのシミュレーションで，標的 TCP フロー ϕ_{target} が 0 秒，観測 TCP フロー $\phi_{observe}$ が 5 秒，1 ノード目の攻撃フロー ϕ_{A_1} が 25 秒から開始される．ϕ_{A_2} 以降の攻

表 5.1 評価実験の構成

評価実験 A	評価実験 A^+	評価実験 B	評価実験 B^+	C	B
a_1	a_1^+	b_1	b_1^+	10Mbps	38,750Bytes
a_2	a_2^+	b_2	b_2^+	30Mbps	116,250Bytes
a_3	a_3^+	b_3	b_3^+	50Mbps	193,750Bytes
a_4	a_4^+	b_4	b_4^+	70Mbps	271,250Bytes
a_5	a_5^+	b_5	b_5^+	90Mbps	348,750Bytes
a_6	a_6^+	b_6	b_6^+	110Mbps	426,250Bytes
a_7	a_7^+	b_7	b_7^+	130Mbps	503,750Bytes
a_8	a_8^+	b_8	b_8^+	150Mbps	581,250Bytes

表 5.2 評価項目

評価項目名	説明
success/failure	提案戦略による目的攻撃効果を達成可否の判断 Algorithm 1 の条件式 2c の実行が目的攻撃効果の達成を意味する 以下のシンボルで表す 達成できた場合: ✓ 達成できなかった場合: ×
$t_{success}$	目的攻撃効果の達成時刻 ※ c の最終更新後に，Algorithm 1 の条件式 2c が実行された時刻
ΔR	攻撃ノード 1 台あたりが送信する攻撃パルスのピークレート
c_{final}	シミュレーション終了時のアクティブ攻撃ノード数
R_{final}	シミュレーション終了時の攻撃パルスの合計ピークレート 計算式： $\Delta R \times c_{final}$
R_{over}	ボトルネックリンク帯域幅を超えて送信された 攻撃パルスのピークレート 計算式：$R_{final} - C$
$R_{average}$	R_{final} の平均攻撃レート 計算式：$R_{final} \times L/T$
u	攻撃パルスのボトルネックリンク帯域幅利用率 計算式：$R_{average}/C$
$\delta_{target}^{success}$	$(t_{success})$ 以降における標的 TCP フロー ϕ_{target} のスループットの平均値
$\delta_{observe}^{success}$	$(t_{success})$ 以降における標的 TCP フロー $\phi_{observe}$ のスループットの平均値

撃フローの開始時刻は，提案戦略のアクティブ攻撃ノード数の決定に依存する．ϕ_{target} と $\phi_{observe}$ は通信が開始されてからシミュレーションが終わるまでデータを送信し続ける．

外乱トラフィックは，評価実験 A^+ の $a_1^+ \sim a_8^+$ および，評価実験 B^+ の $b_1^+ \sim b_8^+$ のみで送信される．各外乱トラフィック送信ノードの通信開始時刻は，$Cross_1$ が 8 秒，$Cross_2$ が 13 秒，$Cross_3$ が 18 秒である．いずれの通信も，開始から 30 秒間データを送信し続ける．

5.2 結果と考察

5.2.1 評価実験 A：基礎的な攻撃性能

評価実験 A では，外乱トラフィックが存在しない環境で，ステルス優先制御を無効化し，目的の攻撃効果を達成可能であるかを検証した．評価実験 A の結果を表 5.3 に示す．

$a_1 \sim a_8$ すべてのシミュレーションで，提案戦略は目的攻撃効果を達成することができたと判断した．$\delta_{target}^{success}$ 及び $\delta_{observe}^{success}$ が 500kbps を下回っていることから，提案戦略の判断と実際の結果に齟齬がないことがわかった．図 5.2 及び図 5.3 は，シミュレーション $a_1 \sim a_8$ における，標的 TCP フローと観測 TCP フローのスループットの遷移を示している．標的 TCP フローと観測 TCP フローのスループットが相互に依存しながら変化，もしくは，ほぼ同様に変化している結果から，提案戦略における攻撃効果の推定の有効性が示された．

攻撃のステルス性の側面では，C が 90Mbps 以上の広帯域なボトルネックリンクに対して，提案戦略が有効ではないことがわかった．シミュレーション $a_1 \sim a_4$（すなわち，C が 10Mbps $\sim$ 70Mbps の場合）は，u が約 45% 前後であることから，一般的なフラッド型の高レート DDoS 攻撃と比較して高いステルス性をもっていると言える．一方で，C が 90Mbps 以上に設定されたシミュレーション $a_5 \sim a_8$ では，R_{final} が C に対して遥かに高く設定されてしまい，u が 100% を超える結果が得られた．これは低レート DDoS ではなく，高レート DDoS である．この原因は，c によって決定される R の推移を示した図 5.4 から読み取ることができる．図 5.4 からは，c がフィードバックごとに少しずつ増加するのではなく，最初の増加時に一度に大幅に増加していることが読み取れる．これは，初回のフィードバック時において，c の増加量を決定する式 4.2.1 が，必要以上の値を算出してしまっていることを意味する．提案戦略では，C に対して十分に小さい ΔR から LDDoS 攻撃が開始される．C が低帯域である場合は，R が小さい値であっても，標的 TCP と観測 TCP フローのスループットが低下するため，適切な c の増加量が求められるが，C が高帯域である場合，R が小さい値であると，TCP のスループットはほとんど低下しないため，必要以上の値が増加される．これをボトルネックリンクの回線利用率の側面から考えると，提案戦略のステルス性は，回線利用率が 100% に近づくほど高まり，0% に近づくほど低くなると言える．ステルス性に問題がなかったシミュレーション $a_1 \sim a_4$ では，初回のフィードバック時にボトルネックリンクの回線利用率がほぼ 100% であり，高レート化してしまった $a_5 \sim a_8$ では回線利用率が 100% を下回っていた．C に対して ΔR の値が低すぎる値に設定された場合においても，

表 5.3 評価実験 A の結果

評価項目	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
success/ failure	✓	✓	✓	✓	✓	✓	✓	✓
$t_{success}$ [s]	46	49	58	52	37	37	43	46
ΔR [Mbps]	2.88	15.13	25.01	35.05	37.31	36.94	36.94	36.94
c_{final} [nodes]	5	3	3	3	11	136	60	99
R_{final} [Mbps]	14.41	45.38	75.02	105.16	410.39	5,023.16	2,216.10	3,656.57
R_{over} [Mbps]	4.41	15.38	25.02	35.16	320.39	4,923.16	2,086.10	3,506.57
$R_{average}$ [Mbps]	4.32	13.62	22.51	31.55	123.12	1,506.95	664.83	1,096.97
u [%]	43.23	45.38	45.01	45.07	136.80	1,369.95	511.40	731.31
$\delta_{target}^{success}$ [kbps]	397.95	52.72	12.79	75.66	105.59	62.92	0	4.31
$\delta_{observe}^{success}$ [kbps]	409.87	55.04	12.03	0	79.18	43.52	0	81.32

提案戦略を安定して動作させることは，今後の課題として挙げられる．

以上の結果から，提案戦略は回線利用率が高いリンクに対して，ステルス性を保ちながら目的の攻撃効果までパルスレートを調整できることがわかった．

5.2.2 評価実験 A^+：攻撃性能のロバスト性

評価実験 A^+ では，外乱トラフィックが存在する環境でステルス優先制御を無効化し，攻撃性能のロバスト性を評価した．外乱トラフィックは 5.1.3 項で説明したパターンで通信した．評価実験 A^+ の結果を表 5.4 に示す．

$a_1^+ \sim a_8^+$ すべてのシミュレーションで，提案戦略は目的攻撃効果を達成することができたと判断した．しかし，一部のシミュレーション（a_1^+, a_2^+, a_5^+）の $\delta_{target}^{success}$ 及び $\delta_{observe}^{success}$ は 500kbps を上回る結果となった．これは，外乱トラフィックが途中で終了したことによって，ボトルネックリンクの回線利用率が低下し，標的 TCP フローのスループットが回復したこ

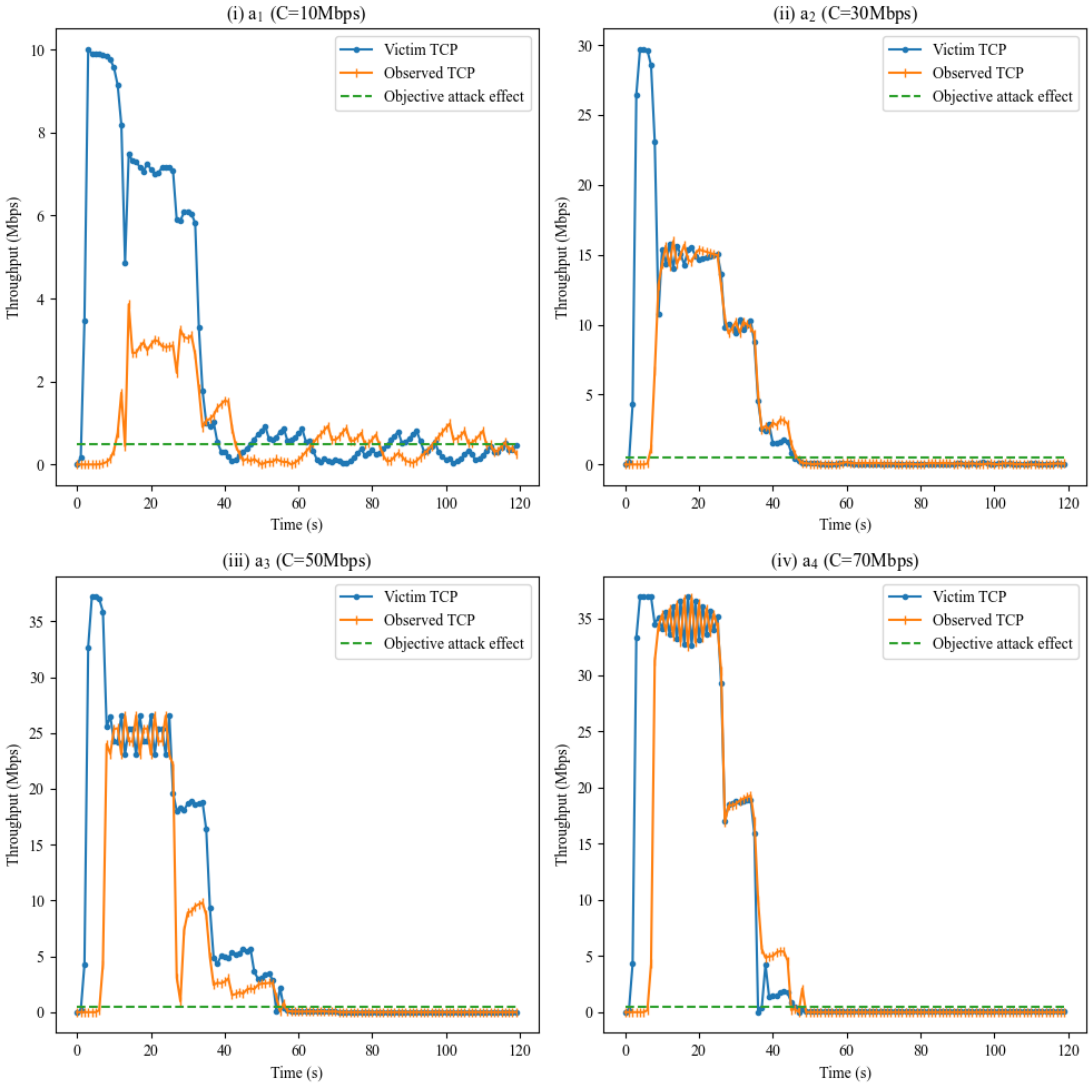

図 5.2　評価実験 A における TCP スループットの遷移 1（$a_1 \sim a_4$）

とと，R_{over} の値が小さかったことが関係していると考えられる．

攻撃のステルス性の側面では，評価実験 A の同条件のシミュレーション（a_i と a_i^+）同士を比較するとすべての条件で u が低下し，ステルス性が向上する結果が得られた．特に，C が 90Mbps 以上の $a_5^+ \sim a_8^+$ では，u について，$a_5 \sim a_8$ と比較して大きな改善が見られた．これは，外乱トラフィックが増えたことによって，ボトルネックリンクの回線利用率が向上したことが影響していると考えられる．

興味深い結果として，外乱トラフィックによって観測 TCP フローのスループットが低下したことで，ΔR の値が減少した結果，c_{final} が増加したことが挙げられる．これは，標的 TCP に競合するフローが多い場合に，必要な攻撃ノード数が増えることを示している．

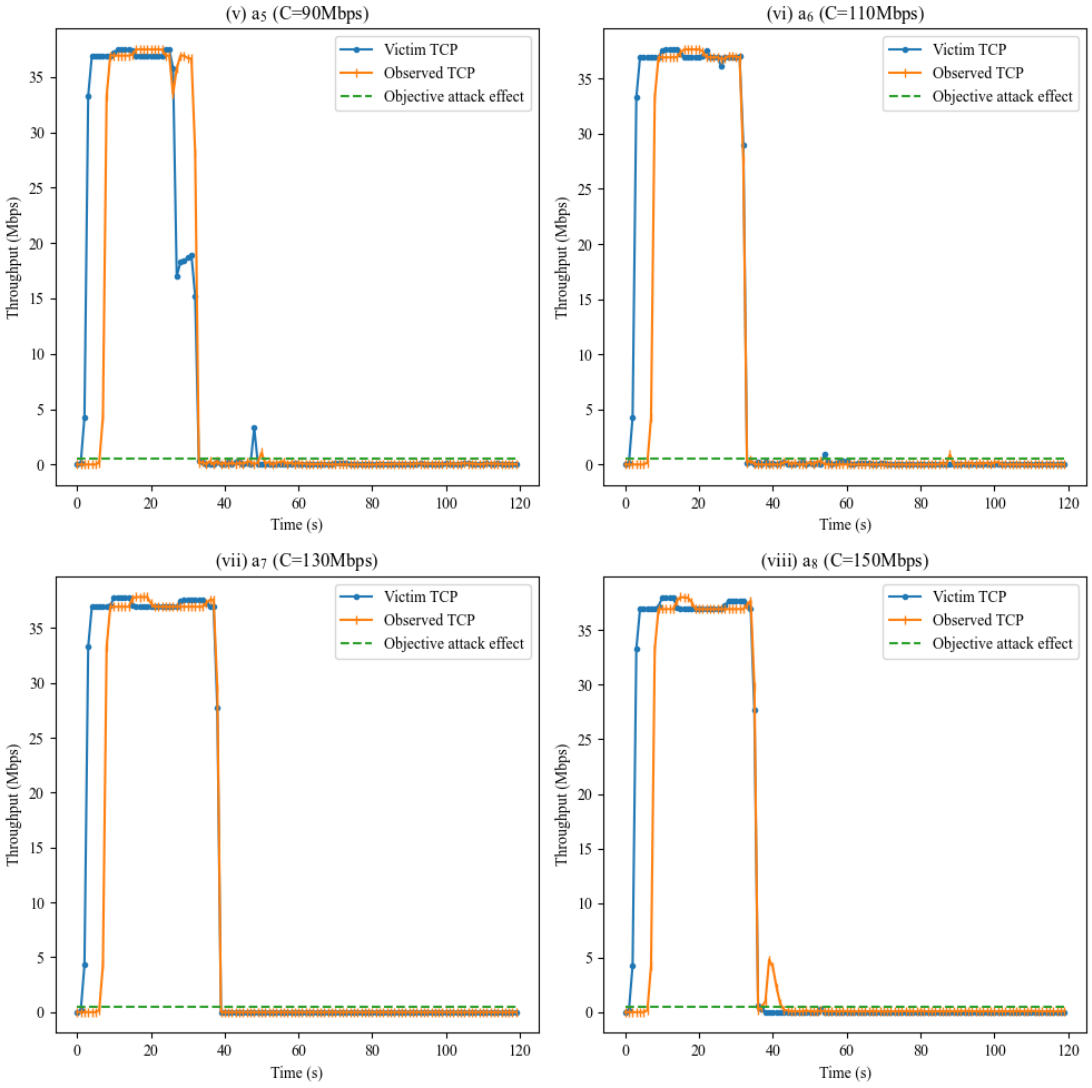

図 5.3　評価実験 A における TCP スループットの遷移 2（$a_5 \sim a_8$）

以上の結果から，提案戦略は，外乱トラフィックが存在する環境下においても，概ねのケースで目的攻撃を達成することができることがわかった．さらに，ボトルネックリンクを共有する外乱トラフィックが増えることによって，c の制御が正確になることがわかった．

5.2.3　評価実験 B：ステルス性の優先機能

評価実験 B では，ステルス性優先制御を有効化し，パルスレートをボトルネックリンク帯域幅以下に維持することが可能であるかを検証した．シミュレーション $b_1 \sim b_8$ ごとの R の推移を図 5.5 及び図 5.6 に示す．

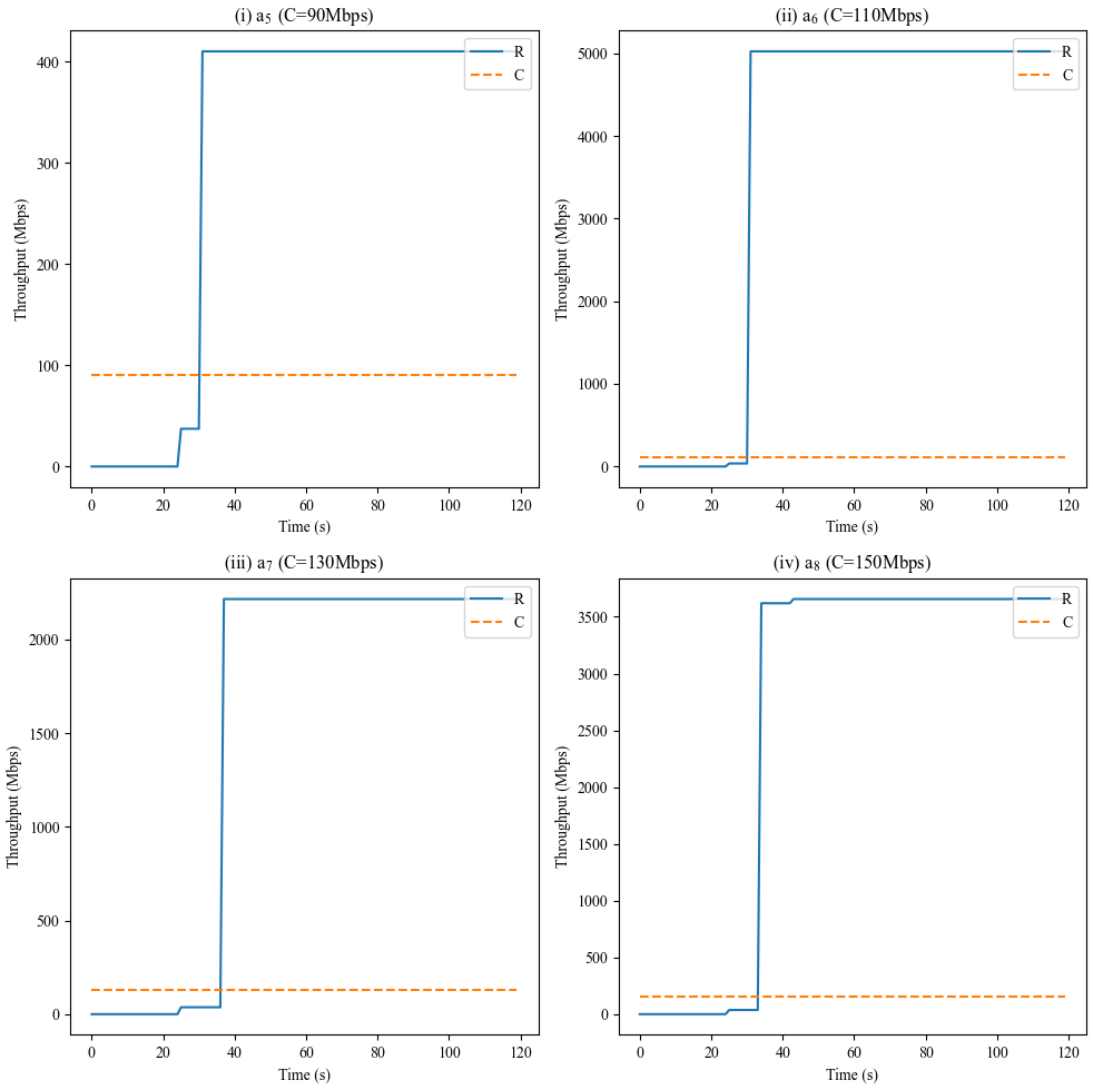

図 5.4　評価実験 A における R の遷移（$a_5 \sim a_8$）

$b_1 \sim b_8$ のすべてのケースで，一度，ピークレート R が，ステルス性を優先しなかったシミュレーション $a_1 \sim a_8$ の R_{final} の値と等しい値まで増加しているが，その後，R が C まで低下していることが確認できた．よって，$b_1 \sim b_8$ のすべてのケースにおいて攻撃フローの帯域使用率 u は 30% となり，シミュレーション $a_1 \sim a_8$ の結果と比較して大幅に減少した．この結果は，ステルス性優先制御によって，ボトルネックリンク帯域幅を正確に推定できていることを示している．特に，評価実験 A において，u が 100% を超えていた C が 90Mbps 以上の環境において，u を 30% に抑えられたことは，ステルス性優先制御の有効性を強調している．一方で，ステルス性を優先したことにより，$b_1 \sim b_8$ のすべてのケースで目的攻撃効果を達成できない結果となった．この結果は，LDDoS 攻撃に失敗しているのではなく，

表 5.4 評価実験 A^+ の結果

評価項目	a_1^+	a_2^+	a_3^+	a_4^+	a_5^+	a_6^+	a_7^+	a_8^+
success/ failure	✓	✓	✓	✓	✓	✓	✓	✓
$t_{success}$ [s]	88	172	40	97	37	37	37	37
ΔR [Mbps]	0.69	2.00	3.83	12.18	7.534	8.05	17.09	33.86
c_{final} [nodes]	20	17	17	7	14	17	16	10
R_{final} [Mbps]	13.88	34.07	65.11	85.26	105.50	136.92	273.49	338.60
R_{over} [Mbps]	3.88	4.07	15.11	15.26	15.50	26.92	143.49	188.60
$R_{average}$ [Mbps]	4.16	10.22	19.53	25.58	31.65	41.08	82.05	101.58
u [%]	41.64	34.07	39.06	36.54	35.17	37.35	63.12	67.72
$\delta_{target}^{success}$ [kbps]	586.20	1015.39	299.19	230.71	664.78	466.79	324.34	313.72
$\delta_{observe}^{success}$ [kbps]	562.45	825.41	141.23	208.19	407.87	292.18	188.17	165.28

R が C と等しい場合に得られる最大攻撃効果が 500kbps 以上であるということを意味する．以上の結果と考察から，攻撃効果とステルス性にはトレード・オフの関係があると言える．

5.2.4 評価実験 B^+：ステルス性の優先機能のロバスト性

評価実験 B^+ では，外乱トラフィックが存在する環境でステルス性優先制御を有効化し，ステルス性の優先機能のロバスト性を評価した．外乱トラフィックは 5.1.3 項で説明したパターンで通信した．シミュレーション $b_1^+ \sim b_8^+$ ごとの R の推移を図 5.7 及び図 5.8 に示す．

シミュレーション b_6^+（$C = 110Mbps$）を除く 7 つのシミュレーションは外乱トラフィックが発生している環境においても，正確に C を予測し，R の低下することができた．ただし，シミュレーション b_6^+ は 10Mbps の誤差が発生してしまった．

以上の結果から，ステルス性優先制御は外乱トラフィックが存在する環境下においては正確性がやや低下することがわかった．

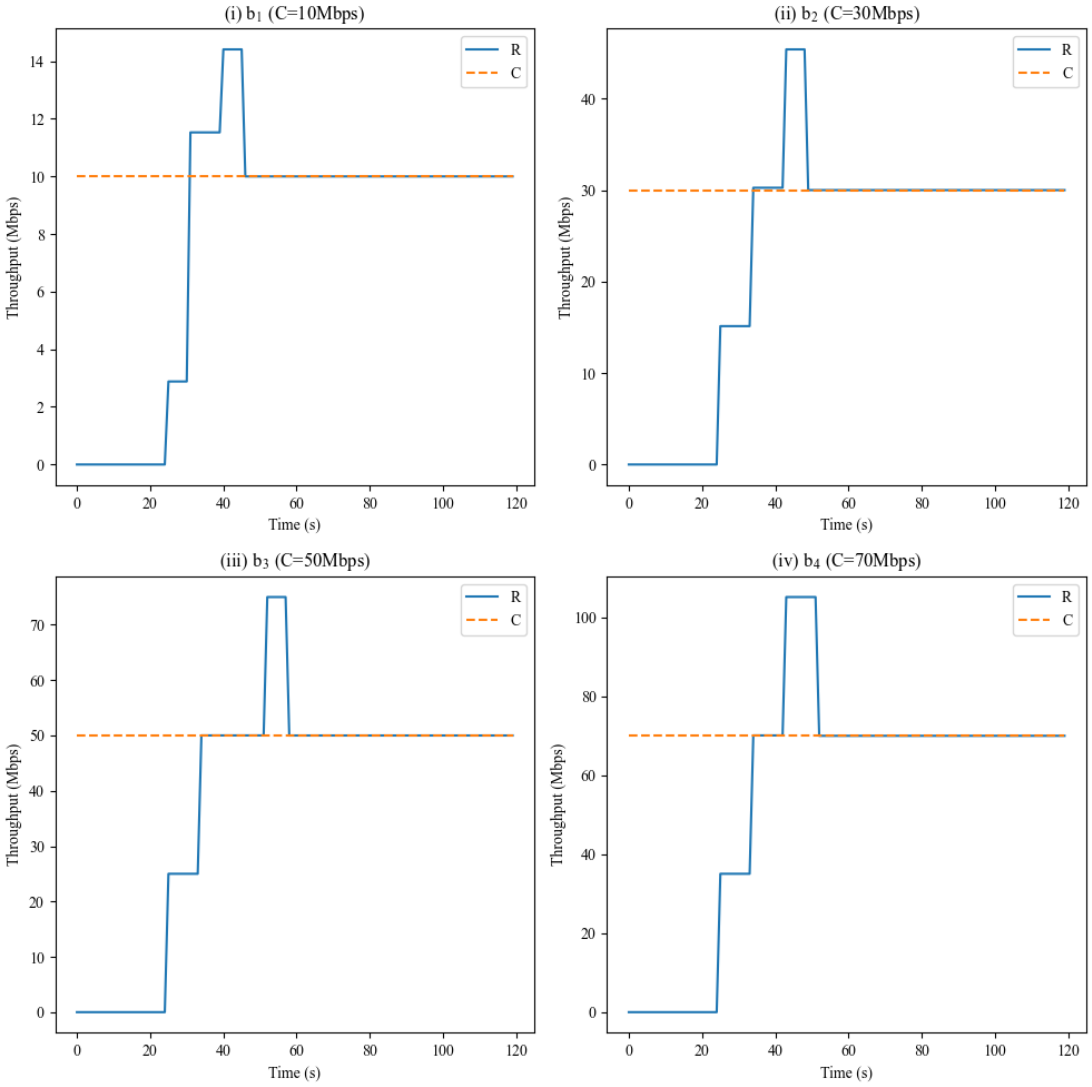

図 5.5　評価実験 B におけるパルスピークレート R の遷移 1（$b_1 \sim b_4$）

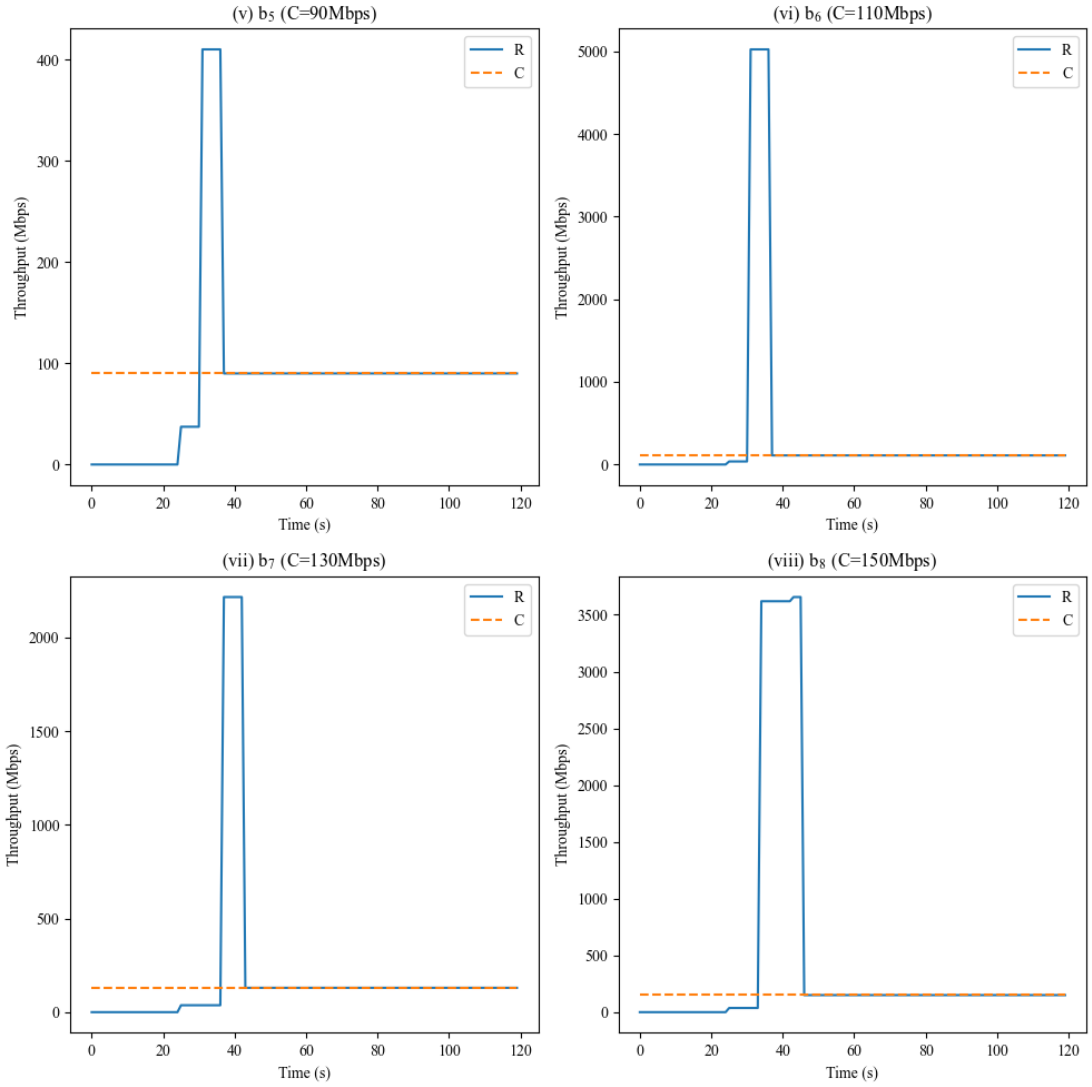

図 5.6　評価実験 B におけるパルスピークレート R の遷移 2（$b_5 \sim b_8$）

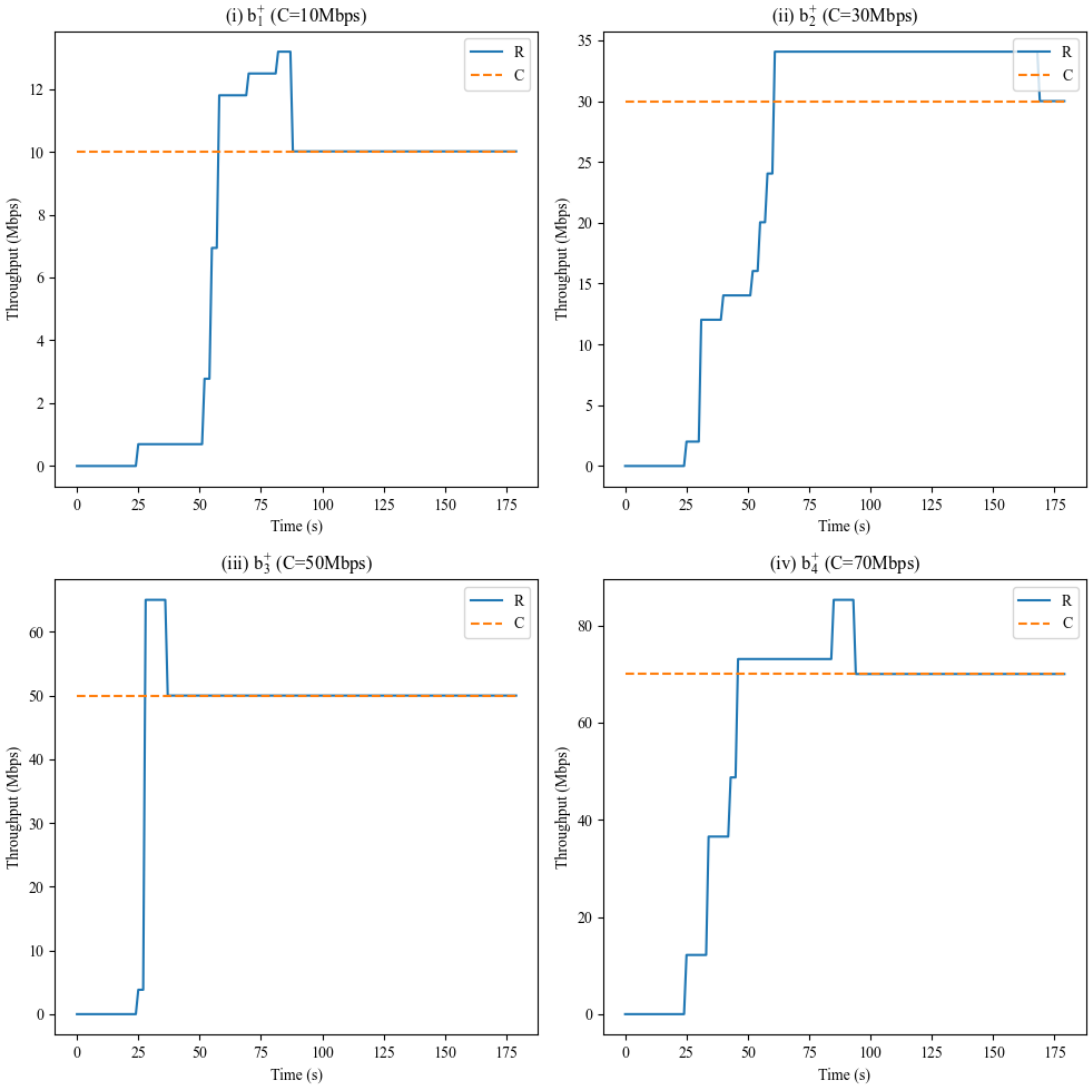

図 5.7　評価実験 B^+ におけるパルスピークレート R の遷移 1（$b_1^+ \sim b_4^+$）

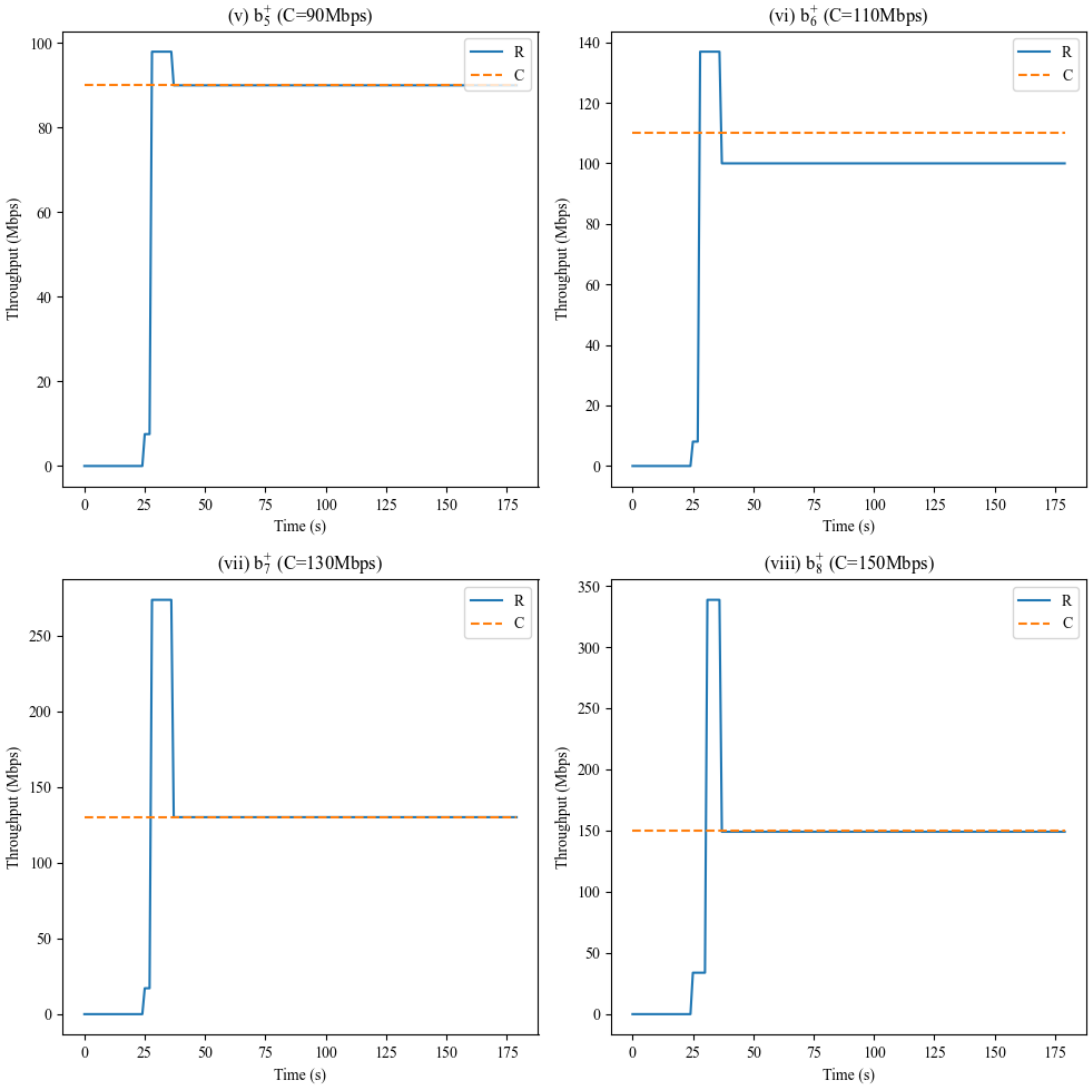

図 5.8 評価実験 B^+ におけるパルスピークレート R の遷移 2（$b_5^+ \sim b_8^+$）

第 6 章　攻撃シナリオの具体例と検知手法の展開箇所

本章では，昨今のサイバー犯罪の動向から，現実のインターネットの環境下で，提案戦略を実際に適用する攻撃シナリオ議論し，検知手法の展開箇所について議論する．

6.1　固定ブロードバンド回線に対する攻撃シナリオ

図 6.1 に提案戦略を用いて実際の適用を議論するための攻撃シナリオの一例を示す．提案戦略は，Web サービスからインターネットサービスプロバイダ（ISP）の固定ブロードバンド回線を通して接続された家庭ネットワークやオフィスネットワークに送信される TCP の一括転送フローに対して，実行することが可能である．以下に，その根拠を説明する．

提案戦略は，標的 TCP フローを受信している $Receiver_{target}$ と同じ LAN 内部に観測ノードである $Receiver_{observe}$ を構築しなければならない．過去のサイバー犯罪の事例から，観測ノードは，ボットネットマルウェアによって家庭ネットワークやオフィスネットワークに構築することが可能である．2016 年に猛威を奮ったマルウェアの Mirai は家庭ネットワーク内の脆弱な IoT 機器に感染して DDoS 攻撃に利用された [41]．近年では，Emotet と呼ばれる組織を標的としたマルウェアが世界的に流行している [42]．これらの事例から，家庭ネットワークやオフィスネットワークを標的とし，そこに観測ノードを構築可能と仮定する．

$Sender_{target}$ の通信を直接観測する手法も考えられるが，その場合，イーサネットであれば標的ネットワークのルータに接続し，プロミスキャス・モードで通信を観測する必要があることや，Wi-Fi の場合，通信の暗号化を解くことが必要となることを考えると，制御を奪取した端末を $Receiver_{observe}$ として利用し攻撃トラフィックや標的フローを単体で観測させるほうが容易に構成可能であると考えられる．

標的となる TCP フローは，Web サービスが家庭ネットワークやオフィスネットワークに接続されたエンドホストに送信するバルク転送の通信である．下りトラフィックの通信量は，上りトラフィックの通信量より多い [43] ため，より多くのフローを標的にするという意味で，この選択は合理的である．標的となる TCP フローの具体例としては，ファイルホスティングサービスからのファイルダウンロード，動画ストリーミングのダウンロード*，業務上のファイルダウンロードを想定している．LDDoS 攻撃の標的として，クラウドコンピューティングが注目されている [8][13] が，2013 年に発生した NTP DDoS 攻撃は，その多くが個人（エンドホスト）を対象に開始されている [45] ことから，家庭ネットワークが狙われる可能性も十分に考えられる．

家庭ネットワークやオフィスネットワークは ISP が提供する固定ブロードバンド回線によってインターネットに接続されている．文献 [46] の家庭ネットワークの測定研究の結果に

*例えば，動画ストリーミングサービスの Netflix では，TCP NewReno が使用されている [44].

よると，ブロードバンド回線のボトルネックリンクは，ISP のエッジルータと家庭内モデムをつなぐラストホップリンクであることが明らかになっている．したがって，固定ブロードバンド回線に対する攻撃シナリオにおいて，$Sender_{target}$ と $Receiver_{target}$ 間のボトルネックリンクとなるのは，家庭ネットワークと ISP ネットワークのラストホップリンクであることが裏付けられる．

上述の TCP フローが送信される方向とボトルネックリンクの位置から，攻撃フロー Φ_{A_c} は，ISP ネットワークの外側から，家庭ネットワークに向けて送信される．攻撃ノード $Attacker_{1\cdots m}$ は，クラウドコンピューティングの特定リージョンの Infrastructure as a Service を利用して構築した仮想マシン上で動作する．これによって，すべての攻撃ノードからボトルネックリンクまでの遅延を統一し，攻撃フローを正確に集約する．

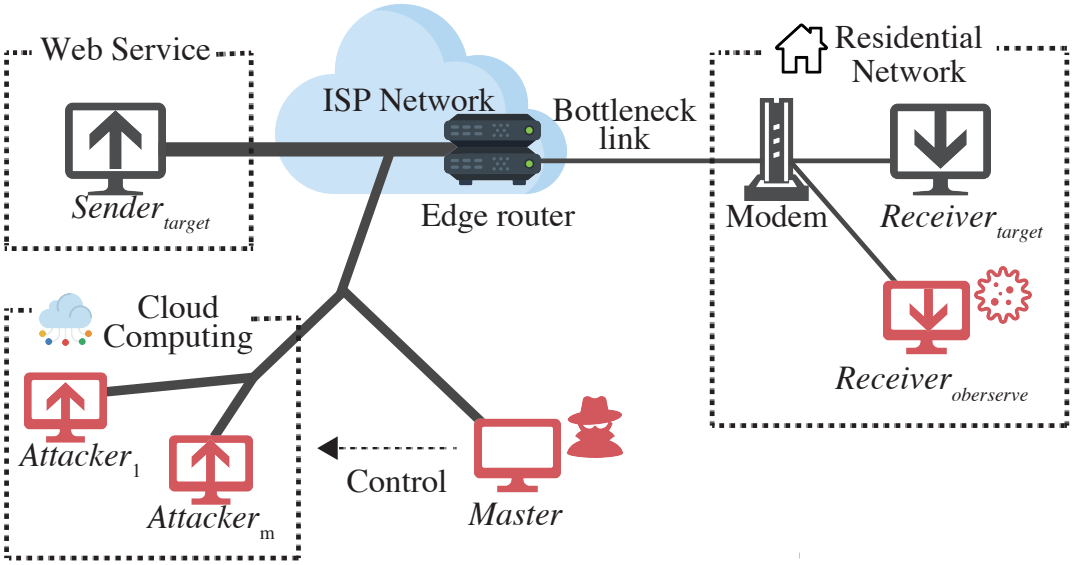

図 6.1　現実における攻撃シナリオの適用例

6.2　検知手法の展開箇所

近年，LDDoS 攻撃の標的にはクラウドコンピューティングが注目されている理由は，クラウドコンピューティングには大量のトラフィックが集中するため，攻撃パルスを隠蔽しやすいことや，高い可用性が求められるクラウドコンピューティングは，少量のサービス劣化で攻撃者が大きなメリットを得られるためである．この背景から，近年はクラウドコンピューティング上で動作することを前提とした検知手法 [47][48] や，Software Defined Network を用いた検知手法の研究 [49][50] が活発である．

前節で提案した攻撃シナリオでは，攻撃パルスは ISP ネットワークのエッジルータに集中する．したがって，提案戦略による LDDoS 攻撃を検知するためには，ISP ネットワークの

エッジルータに検出手法を適用しなければならない.

第 7 章　提案戦略に対する対策の議論

LDDoS 攻撃は，バッファサイズが大きいほど，パルス幅 L の必要最小値が大きくなり，攻撃効果が低下することが明らかになっている [12][27]．ここでは，ボトルネックリンクルータのバッファサイズを大きくすることで，提案戦略によって実行される LDoS 攻撃の攻撃レートを高めることを検討する．攻撃が高レート化するということは，フローの公平性が失われ，ファイアウォールや AQM のような，既存の高レート DDoS のためのメカニズムによって検出可能であることを意味する [12][27]．提案戦略では，目的の攻撃効果が得られるまで，可能な限りパルスレートを増加させるため，ボトルネックバッファサイズを増加することによって必要なパルスレートを引き上げることが可能である．

この対策の有効性を検証するために，バッファサイズを高く設定したボトルネックリンクに対して提案戦略を実行した．上記の防御策の有効性を確認するために，今回の実験の構成は 5 章のシミュレーション a_1 と同様で，ボトルネックリンク帯域幅を 10 Mbps，バッファサイズを 310 KBytes に設定した．このバッファサイズは標的 TCP フローの帯域遅延積（BDP: Bandwidth Delay Product）の 2 倍である．

表 7.1 に示した結果の通り，提案戦略は目的攻撃効果の 500kbps を達成することができないと判断した．終了時の総ピークレートは 23.55Mbps で，バッファサイズを除いた同条件のシミュレーション a_1 と比較して約 9Mbps 増加している．帯域幅が 10Mbps のボトルネックリンクに対して瞬間的にその 2 倍以上の大きさのパルスが送信されることは攻撃を検出する特徴の一つに利用できると考える．パルスレートが高すぎたため，攻撃パケットの一部は損失したが，ボトルネックリンクにエンキューされた攻撃パケットの帯域利用率は 70% を超えていた．これらの結果を見ると，もはや低レート攻撃ではないことがわかる．以上の結果と考察から，ボトルネックバッファサイズの増加は提案戦略への対策の一つとして有効であると考える．

表 7.1　バッファサイズを 2BDP に増加したボトルネックリンクに対して提案手法で攻撃を実行した結果

success/failure	×
ΔR	1.68Mbps
c	14
R_{final}	23.55Mbps
$R_{average}$	7.1Mbps
u	71%

第 8 章　結言

本論文では，標的ボトルネックリンクの帯域幅とバッファサイズが未知であるという仮定に基づいた LDDoS 攻撃のパルスレート最適化戦略について提案した．提案戦略は限定された攻撃シナリオと環境において，標的の TCP 通信の品質を目的の攻撃効果まで低下させるために必要とされるパルスレートを探索的に決定することができる．加えて，目的攻撃効果達成後のパルスレートがボトルネックリンク帯域幅より高い場合，ステルス性を優先してパルスレートを帯域幅まで抑えることができる．ns-3 を利用したシミュレーションによって，提案戦略の攻撃性能と攻撃のステルス性優先制御の有効性を検証した．提案戦略は過去のサイバー犯罪の事例を下に，家庭ネットワークを標的とした Mirai botnet や，企業ネットワークを標的とした標的型マルウェアによって実行可能であることを議論した．このことから，ISP エッジルータに LDDoS による攻撃トラフィックが集中することが予想できる．したがって，提案戦略による LDDoS 攻撃を検知するために，ISP のエッジルータに適切な検知手法を展開する必要がある．提案戦略はボトルネックリンクのインプットバッファサイズを増加することでステルス性を失い，高レート DDoS 攻撃として検知される可能性が高くなる．これは，有効な対策手段の一つと言える．

謝辞

本研究を遂行するにあたり，多くの方々のご指導とご協力を賜りました．

いつも温かく真摯なご指導を賜りました，指導教員の稲村 浩教授に深く感謝致しますとともに，お礼申し上げます．稲村先生には，研究における考え方や進め方や外部発表の意義，コンピュータ・ネットワークの知識について多くのことをご教授賜りました．3 年間，本当にありがとうございました．

研究生活において，様々な面からのご支援と，ご指導・助言を賜りました，副指導教員の中村 嘉隆准教授に感謝致しますとともに，お礼申し上げます．

研究の助けになる様々な助言を賜りました，副査の白石 陽教授，藤野 雄一教授，中村 嘉隆准教授に深く感謝申し上げます．

本研究を遂行するに当たり，経済面でご支援賜りました，日本ビジネスシステムズ株式会社に深く感謝申し上げます．

最後に，経済面・精神面からご支援頂いた両親並びに家族に深く感謝申し上げます．

発表・採録実績

国内会議

[1] 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，情報処理学会，Vol. 2019, pp. 57–63 (2019).

[2] 髙橋 佑太，稲村 浩，中村 嘉隆：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，情報処理学会研究報告マルチメディア通信と分散処理 (DPS)，Vol. 2020, No. 63, pp. 1–8 (2020).

[3] 髙橋 佑太，稲村　浩，中村 嘉隆：特性が未知のボトルネックリンクに対して有効な Low-rate DDoS 攻撃戦略の検討，情報処理学会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. 2020, No. 4, pp. 1–9 (2020). **2020 年度優秀論文賞**.

国際会議 (査読付き)

[1] Takahashi, Y., Inamura, H. and Nakamura, Y.: A Low-rate DDoS Strategy for Unknown Bottleneck Link Characteristics, *2021 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, IEEE, pp. 1–6 (2021). (accepted)

参考文献

[1] AWS Shield Threat Landscape Report – Q1 2020, AWS Shield (online), available from ⟨https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf⟩ (accessed 2020-10-19).

[2] Hao, M.: 2020 Mid-Year DDoS Attack Landscape Report-1, NSFOCUS (online), available from ⟨https://nsfocusglobal.com/2020-mid-year-ddos-attack-landscape-report-1/⟩ (accessed 2020-12-19).

[3] Cloudflare DDoS Protection | Intelligent DDoS Mitigation | Cloudflare, Cloudflare (online), available from ⟨https://www.cloudflare.com/ddos/⟩ (accessed 2020-12-19).

[4] DDoS Protect | Akamai, Akamai (online), available from ⟨https://www.akamai.com/us/en/resources/ddos-protect.jsp⟩ (accessed 2020-12-19).

[5] Cloud DDoS Protection Services | DDoS Prevention & Mitigation, Radware (online), available from ⟨https://www.radware.com/products/cloud-ddos-services/⟩ (accessed 2020-12-19).

[6] Kuzmanovic, A. and Knightly, E. W.: Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew vs. the Mice and Elephants, *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '03, Association for Computing Machinery, p. 75–86 (2003).

[7] 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).

[8] Zhijun, W., Wenjing, L., Liang, L. and Meng, Y.: Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey, *IEEE Access*, Vol. 8, pp. 43920–43943 (2020).

[9] 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).

[10] Understanding Pulse Wave DDoS Attacks | Resource Library, Imprerva (online), available from ⟨https://www.imperva.com/resources/resource-library/white-papers/understanding-pulse-wave-ddos-attacks/⟩ (accessed 2020-12-19).

[11] Yoachimik, O. and Ganti, V.: Network-layer DDoS attack trends for Q3 2020, Cloudflare (online), available from ⟨https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q3-2020/⟩ (accessed 2020-12-19).

[12] 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).

[13] 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).

[14] Guirguis, M., Bestavros, A. and Matta, I.: Exploiting the transients of adaptation for RoQ attacks on Internet resources, *Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004.*, IEEE, pp. 184–195 (2004).

[15] Shevtekar, A. and Ansari, N.: A router-based technique to mitigate reduction of quality (RoQ) attacks, *Computer Networks*, Vol. 52, No. 5, pp. 957–970 (2008).

[16] Maciá-Fernández, G., Díaz-Verdejo, J. E., García-Teodoro, P. and de Toro-Negro, F.: LoRDAS: A low-rate DoS attack against application servers, *International Workshop on Critical Information Infrastructures Security*, Springer, pp. 197–209 (2007).

[17] Maciá-Fernández, G., Díaz-Verdejo, J. E. and García-Teodoro, P.: Mathematical model for low-rate DoS attacks against application servers, *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 3, pp. 519–529 (2009).

[18] 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).

[19] 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. 8–pp (2005).

[20] 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).

[21] 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).

[22] Cotae, P., Kang, M. and Velazquez, A.: Spectral analysis of low rate of denial of service attacks detection based on fisher and Siegel tests, *2016 IEEE International Conference on Communications (ICC)*, IEEE, pp. 1–6 (2016).

[23] 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).

[24] Floyd, S. and Jacobson, V.: Random early detection gateways for congestion avoidance, *IEEE/ACM Transactions on networking*, Vol. 1, No. 4, pp. 397–413 (1993).

[25] Patel, S., Gupta, B. and Sharma, V.: Throughput analysis of AQM schemes under low-rate Denial of Service attacks, *2016 International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, pp. 551–554 (2016).

[26] Zhang, C., Yin, J., Cai, Z. and Chen, W.: RRED: robust RED algorithm to counter low-rate denial-of-service attacks, *IEEE Communications Letters*, Vol. 14, No. 5, pp. 489–491 (2010).

[27] 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).

[28] Kieu, M. V., Nguyen, T. T. et al.: A Way to Estimate TCP Throughput under Low-Rate DDoS Attacks: One TCP Flow, *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, IEEE, pp. 1–8 (2020).

[29] Guirguis, M., Bestavros, A. and Matta, I.: On the impact of low-rate attacks, *2006 IEEE International Conference on Communications*, Vol. 5, IEEE, pp. 2316–2321 (2006).

[30] 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).

[31] 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).

[32] Ficco, M. and Rak, M.: Stealthy Denial of Service Strategy in Cloud Computing, *IEEE Transactions on Cloud Computing*, Vol. 3, No. 1, pp. 80–94 (2015).

[33] 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).

[34] Park, J., Mohaisen, M., Nyang, D. and Mohaisen, A.: Assessing the effectiveness of pulsing denial of service attacks under realistic network synchronization assumptions, *Computer Networks*, p. 107146 (2020).

[35] Booters, Stressers and DDoSers, Imperva (online), available from ⟨`https://www.imperva.com/learn/ddos/booters-stressers-ddosers/`⟩ (accessed 2020-10-28).

[36] Padhye, J., Firoiu, V., Towsley, D. and Kurose, J.: Modeling TCP throughput: A simple model and its empirical validation, *Proceedings of the ACM SIGCOMM'98 conference on Applications, technologies, architectures, and protocols for computer*

communication, pp. 303–314 (1998).

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

[38] Internet Connection Speed Recommendations, Netflix (online), available from ⟨https://help.netflix.com/en/node/306⟩ (accessed 2020-10-27).

[39] Cisco Annual Internet Report (2018–2023) White Paper, CISCO (online), available from ⟨https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html⟩ (accessed 2021-01-12).

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

[41] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M. et al.: Understanding the mirai botnet, *26th USENIX security symposium (USENIX Security 17)*, pp. 1093–1110 (2017).

[42] Security Report 2020 | Check Point Software, Check Point Software Technologies (online), available from ⟨https://pages.checkpoint.com/cyber-security-report-2020.html⟩ (accessed 2021-01-12).

[43] Internet Infrastructure Review（IIR）Vol.48 2020 年 9 月 24 日発行，インターネットイニシアティブ (IIJ)（オンライン），入手先 ⟨https://www.iij.ad.jp/dev/report/iir/048.html⟩（参照 2021-01-12）.

[44] 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).

[45] Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M. and Karir, M.: Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks, *Proceedings of the 2014 Conference on Internet Measurement Conference*, pp. 435–448 (2014).

[46] Dischinger, M., Haeberlen, A., Gummadi, K. P. and Saroiu, S.: Characterizing residential broadband networks, *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pp. 43–56 (2007).

[47] 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).

[48] Agrawal, N. and Tapaswi, S.: Low rate cloud DDoS attack defense method based on power spectral density analysis, *Information Processing Letters*, Vol. 138, pp.

44–50 (2018).

[49] Zhijun, W., Qing, X., Jingjie, W., Meng, Y. and Liang, L.: Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network, *IEEE Access*, Vol. 8, pp. 17404–17418 (2020).

[50] Pérez-Díaz, J. A., Valdovinos, I. A., Choo, K.-K. R. and Zhu, D.: A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning, *IEEE Access*, Vol. 8, pp. 155859–155872 (2020).

図目次

表目次