Robust WREDによるLow-rate Shrew DoS攻撃に対する保護緩和機構の提案

佐藤 大介[1]　稲村 浩[2]　中村 嘉隆[3]

概要：Low-rate Shrew DoS 攻撃は，TCP の再送タイムアウト機構の周期性に対応したパルス波状の攻撃トラフィックを形成することによって，低い平均通信量で TCP 通信の品質を低下させる．平均通信量が低いため DDoS (Distributed DoS) 攻撃に対する検知手法では検出が困難でありステルス性が高く，LDoS 攻撃に対する検知・抑止手法の研究が必要とされている．LDoS 攻撃は，RED (Random Early Detection) アルゴリズムが適用されたネットワークに対しても有効であることが明らかになっており，RED は LDoS 攻撃に対して脆弱であると言える．この脆弱性を解消するため RRED (Robust RED) の研究が行われている．本研究は LDoS 攻撃に対する新しい RRED として，WRED (Weighted RED) の優先制御を利用したロバスト性の高い RED アルゴリズムである Robust WRED (RWRED) を提案する．マルチクラス RED である WRED を用いて所与の攻撃トラフィックが最適パルス波形状である度合いを WRED クラスに対応させ，LDoS 攻撃における多様な 攻撃トラフィック及び攻撃トラフィックに類似したトラフィックに対する識別と緩和を可能にする．提案した RWRED と シングルクラス RRED を適用したネットワークにおいて，複数の攻撃パラメータにてシミュレーションを行い LDoS 攻撃下における標的 TCP のスループットを比較し RWRED の有効性を示した．

1. はじめに

サービス妨害 (DoS: Denial of Service) 攻撃や分散型 DoS (DDoS: Distributed DoS) 攻撃はネットワークセキュリティ分野における脅威の一つである．DDoS 攻撃は DoS 攻撃に比べて大規模な攻撃が多く，より大きな脅威である．大規模な DDoS 攻撃の事例として，2018 年に GitHub を標的とした最大で 1.35Tbps を記録した bps (bits per second) 型で世界最大規模となる DDoS 攻撃 [1] や，2020 年に欧州の大手銀行を標的とした pps (packets per second) 型で史上最大規模となる DDoS 攻撃 [2] が挙げられる．どちらの事例も大量の攻撃トラフィックを発生させることでサービス妨害を成功させているが，それぞれ Akamai 社の対処によって 10 分ほどで復旧している [1][2]．これは DDoS 攻撃の攻撃トラフィックが大量であるために特徴を捉えやすく，容易に検出が可能であることを示している．

低量 DoS (LDoS: Low-rate DoS，別名: Low-rate Shrew DoS) 攻撃 [3] は低い平均攻撃通信量で TCP 通信を妨害可能であることが既存研究により明らかにされている [3][4]．LDoS 攻撃は平均攻撃通信量が低いため，DoS 攻撃や DDoS 攻撃のための通信量にもとづく検知手法では検出困難である [5]．そのため，LDoS 攻撃の検知手法に関する研究が求められている．

AQM (Active Queue Management) 手法の代表的なアルゴリズムである RED (Random Early Detection) や WRED (Weighted RED) は広くインターネットで利用されている [6]．しかし，RED は LDoS 攻撃に対して脆弱であることが既存研究によって示されている [4][7]．LDoS 攻撃に対する RED の脆弱性を解消する方法として，RRED (Robust RED) が提案されている [8]．RRED は RED によるキューイングを行う前に検知器を設置し LDoS 攻撃トラフィックを検出及び廃棄することで，LDoS 攻撃からネットワークリソースを防御し通信を安定させる．しかし，RRED の検知器における LDoS 攻撃の検出条件は偽陽性が高いものとなっており，LDoS 攻撃トラフィック以外の正常な通信も抑制する可能性がある [8]．そのため，LDoS 攻撃トラフィックの検出における偽陽性及び偽陰性を低くする RRED の研究が行われている [9]．

本研究ではマルチクラス RED である WRED を用いて所与の攻撃トラフィックが最適パルス波形状である度合いを WRED クラスに対応させ，LDoS 攻撃における多様な攻撃トラフィック及び攻撃トラフィックに類似したトラフィックに対する識別と緩和が可能な RWRED (Robust

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

WRED) を提案する．

2. LDoS 攻撃と RED について

本節では議論に必要な以下の関連技術について説明を行う．Low-rate Shrew DoS 攻撃は連続的な TCP 再送信タイムアウトを意図的に発生させるものである．本研究では RED とその派生アルゴリズムである WRED を活用する．

2.1 TCP 再送信タイムアウト

TCP 通信の高い信頼性を保証する技術である再送制御の一つとして再送信タイマーを用いる方法がある [10]．TCP 通信では，パケットが送信される度に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である再送信タイムアウト (RTO : Retransmisson Time Out) の最小値 $minRTO$ 以内に送信したパケットの応答が受信側から得られない場合は，当該パケットは損失したと判断しパケットの再送信を行う．RTO の初期値は (1)　式で決定する [11]．

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

ここで $minRTO$ は RTO の最小値，$SRTT$ は平滑化したラウンドトリップ時間 (RTT: Round Trip Time)，G はオペレーティングシステムに依存したクロック粒度，$RTTAVR$ は RTT の平均偏差である．RTO は最小値を 1s に設定することが IETF によって推奨されている [12]．(1)　式は多くの場合，(2)　式が成り立つ [4] ため，RTO の初期値は (3)　式のように minRTO に設定されることが一般的である．

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

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

TCP 通信において，連続して同じパケットの廃棄が発生したと判断された場合，RTO を 2 倍ずつ増加させて再送信するという仕様が RFC6298[11] によって定義されている．i 回連続で送信したパケットの応答が RTO 以内に受信側から得られない場合は，当該パケットの RTO_i は (4)　式で設定される．ただし，RTO は最大値を 60s 以上とすることが RFC6298 にて示されている [11]．当該パケットの送信が成功した場合，RTO は初期値である $minRTO$ に再設定される．これは Karn のアルゴリズムと呼ばれ，ほとんどの TCP において再送制御アルゴリズムとして実装されている [13]．

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

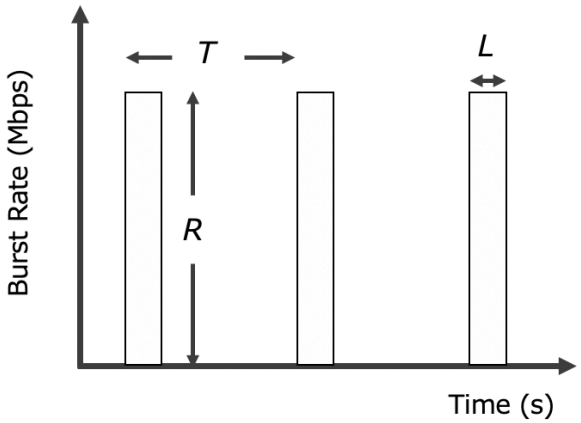

図 1　攻撃パラメータ

2.2 Low-rate Shrew DoS 攻撃

LDoS 攻撃は 2003 年に Kuzmanovic と Nightly[3] によって示された．LDoS 攻撃は図 1 に示すような 3 つのパラメータ〈R, L, T〉で構成されている．ここで，R はバーストレート，L はバースト長，T はバースト間隔である．図 1 のようなパルス波状の攻撃トラフィックを送信することで低い平均通信量で効率的に標的のリソースを枯渇させる．LDoS 攻撃は低い平均通信量で DoS 攻撃を達成するため，一般トラフィックと区別が困難であり，ステルス性が高い DoS 攻撃である．LDoS 攻撃は TCP 再送制御アルゴリズムの再送信タイムアウト機構を悪用したトランスポート層プロトコルに対する攻撃である．TCP 再送制御アルゴリズムがパケット損失を検知する方法の一つとして，再送信タイマーを用いたものがある．TCP は RTO 待っても送信先から ACK が返ってこない場合，パケット損失を検知する．パケット損失が連続で起こった場合，RTO は (4)　式で設定されるため，周期的に増加していく．LDoS 攻撃はこの RTO の周期性を悪用して，効率的に TCP 通信を抑制する．

具体的な攻撃の方針を標的 TCP が通信を行っているネットワーク中における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 とおいて説明する．まず，C と B 十分に満たす攻撃トラフィックを送信することで標的 TCP パケットが損失する．当該パケットが再送信を行うタイミングで再度攻撃トラフィックを送信することで標的 TCP パケットが連続で損失する．当該パケットは損失するたび RTO を周期的に増加させるため，RTO の周期で攻撃トラフィックを送信する．LDoS 攻撃は攻撃トラフィックのパラメータの R を C，L を B を埋めるために十分な長さまたは標的 TCP の RTT，T を標的 TCP の $minRTO$ に設定した場合，より TCP 通信を抑制する [14]．

2.3 RED アルゴリズム

RED アルゴリズムは TCP ネットワークの輻輳回避戦

略の一つとして提案されたバッファ管理手法である [15]. RED アルゴリズムは平均キューサイズを制御することでネットワーク内に発生した輻輳の早期検出を行い，輻輳回避の提供および TCP の性能向上を実現している．

RED アルゴリズムの主な設計目標は平均キューサイズの監視，制御を行うことで輻輳回避をネットワークに提供することである．RED アルゴリズムは平均キューサイズの監視によって輻輳の早期検出を行い，平均キューサイズの制御として行うパケットマークおよび，パケットの早期廃棄によってホストへの通知を行う．早期の輻輳を通知された送信者がトラフィック量を抑えることで，ネットワークの性能低下を抑制する．

RED アルゴリズムによって検知された初期の輻輳は，パケット廃棄または，パケットマークによってホストに通知される．強調性のあるトランスポートプロトコルの場合はパケットマークを行い，そうでない場合はパケット廃棄を行うことで平均キューサイズを維持する．マークおよび廃棄されるパケットは，当該ホストとのトラフィック量に比例する．マークおよび廃棄されるパケットの決定を行う処理について説明する．パケットは平均キューサイズをもとに最大閾値，最小閾値の 2 つの閾値によって区画される 3 区分に分けられ，それぞれの区分によって異なる処理を行う．平均キューサイズが最小閾値未満の場合は，パケットマークおよびパケット廃棄は行わずパケットはエンキューされる．平均キューサイズが最小閾値以上，最大閾値未満の場合は，平均キューサイズに比例して確率が高くなるパケットマーキング確率にもとづきパケットマークおよびパケット廃棄を行う．平均キューサイズが最大閾値以上の場合はすべてのパケットに対してパケットマークまたはパケット廃棄は行う．

2.4 WRED

WRED (Weighted RED) アルゴリズムは，トラフィッククラスに対して個別に RED アルゴリズムを実行する機能を持つ [16][17]．WRED アルゴリズムは，RED アルゴリズムの機能を Precedence 機能と統合することで，Precedence が高いパケットの優先的なトラフィック処理を実現する [6]．ここで，WRED アルゴリズムは Precedence に基づいて最小閾値，最大閾値を設定することができ，閾値は一般的に高い優先度に対する閾値を高く設定する．これにより，Precedence に基づく優先制御を実現している．WRED アルゴリズムはパケット廃棄時に Precedence を参照し，Precedence 別の閾値により廃棄確率を操作することができるアルゴリズムである [15]．Precedence 別に最大閾値と最小閾値をそれぞれ設定することができるため，高い Precedence のパケットを優先的にエンキューすることができる．

3. 関連研究

LDoS 攻撃は RTO 周期で攻撃パルスを発生させることで低い平均攻撃通信量で DoS 攻撃を成功させるため，DoS 攻撃や DDoS 攻撃のための通信量にもとづく検知手法では検出困難である [5]．そのため LDoS 攻撃の検知手法はさまざまなアプローチで研究が行われている．LDoS 攻撃の検知手法として攻撃パラメータであるバースト長 L とバースト間隔 T をベースに攻撃トラフィックの検出を行なっている手法がある [18]．バースト長 L が同じサーバと接続している他の通信フローの RTT 以上で，バースト間隔 T が $minRTO$ である 1 秒の通信フローを LDoS 攻撃トラフィックとして検出する．この検知手法は LDoS 攻撃の特徴であるパルス波状の攻撃トラフィックを検出する基本的な検知手法である．この LDoS 攻撃の検出手法を攻撃パラメータベース LDoS 攻撃検出手法とし，従来の LDoS 攻撃検知手法とする．従来の LDoS 攻撃検知手法では最適化された攻撃パルスのみを想定しており，LDoS 攻撃の攻撃パラメータを操作し最適なパラメータの値から変更すると検出を回避することができると考えられる．

LDoS 攻撃に対する防御方法は，ルータに適用される AQM 手法を利用した方法が多く，AQM 手法のアルゴリズムに変更を加えて拡張することで LDoS 攻撃に対して耐性のある防御機構を構築している [5]．AQM 手法のアルゴリズムで最も一般的なアルゴリズムは RED で，RED を拡張して防御機構とした RRED は zhang ら [8] によって提案されている．RRED は RED によるキューイングを行う前に検知器を設置し LDoS 攻撃トラフィックを検出及び廃棄することで，LDoS 攻撃からネットワークリソースを防御し通信を安定させる．しかし，RRED の検知器における LDoS 攻撃の検出条件は偽陽性が高いものとなっており，LDoS 攻撃トラフィック以外の正常な通信も抑制する可能性がある．そのため，LDoS 攻撃トラフィックの検出における偽陽性及び偽陰性を低くする RRED の研究が行われている [9]．LDoS 攻撃の検知手法における検出精度向上の努力がある一方で，我々は判定結果の信頼性に幅があることを前提とした防御機構の提案が必要であると考える．

Kuzmanovic らが提案した LDoS 攻撃 [3] に対する防御方法の一つとして，ルータにおける検出及びスロットリングによる攻撃緩和に関して検討を行っている [4]．ルータに RED-PD (RED with Preferential Dropping)[19] または RED を適用し，標的 TCP スループットの比較によって LDoS 攻撃の攻撃フローの識別可能性を検証している．RED-PD とは設定された目標帯域幅を超過するフローに対してスロットリングを行い，送信率に応じた確率でパケット廃棄を行うアルゴリズムである．RED-PD は目標帯域を設定して LDoS 攻撃トラフィックの検出を行なっている

が，その性能は検出手法としては不十分であることが示されている．RED-PD の改善策として全ての通信フローを公平な状態で帯域制限をかけるのではなく，LDoS 攻撃トラフィックの可能性が高い通信フローにのみ強い帯域制限を適用することが考えられる．

Chang らは LDoS 攻撃を検出して防御するのではなく，LDoS 攻撃によって被害を受ける通信フローのパケット廃棄率を低く制御しパケット廃棄率の公平化を図ることで LDoS 攻撃を防御する SAP (Shrew Attack Protection) と呼ばれる防御機構を提案している [20]．SAP は通信フローのパケット廃棄率を監視しパケット廃棄率が高い値を示す通信フローに優先度の高いタグを付け，他の通信フローに優先度の低いタグを付けることで通信フロー間における帯域使用の公平化を行なっている．SAP は LDoS 攻撃による TCP 通信の抑制を緩和することが示されているが，SAP は通信帯域を通信フローごとに分割しているため，LDoS 攻撃は通信帯域を圧迫している．そのため，TCP 通信の保護機構として十分である一方で LDoS 攻撃の防御機構としては不十分であると考えられる．

4. 研究の目的と提案手法の概要

本研究の目的は従来手法では扱えない多様な攻撃パルスに対処できる LDoS 攻撃への新たな攻撃緩和機構を提案することである．具体的には，LDoS 攻撃に対する攻撃検知と RED アルゴリズムを基本とした攻撃緩和機構を構成する．既存の Robust RED[8] を参考に，我々の手法では キューイング機構を RED から WRED に入れ替えることでマルチクラスにし，攻撃検知部で識別した当該トラフィックの LDoS 攻撃トラフィックである確率に応じた優先制御をすることで LDoS 攻撃を緩和し TCP 通信を保護する．従来の LDoS 攻撃検知手法を検知条件とした LDoS 攻撃耐性のある RED を攻撃パラメータベース Robust RED とし，提案手法を攻撃パラメータベース Robust WRED (RWRED)，従来手法を攻撃パラメータベース Robust RED とする．提案手法と従来手法を標的 TCP スループットで比較し性能の評価を行う．

5. Robust WRED の設計

5.1 RWRED の概略

RWRED は RRED[8] を参考にして設計しており，図 2 で示すように WRED ブロックの前に Detector ブロックを置いている．RWRED の基本的な動作設計としては，Detector ブロックで入力されたパケットの LDoS 攻撃トラフィックである確率を算出し，WRED ブロックで算出した確率に応じた優先制御を行うことで LDoS 攻撃を緩和する．Detector ブロックでは入力されたパケットを通信フローごとに識別し通信フローごとに LDoS 攻撃トラフィックである確率を算出する．通信フローは入力されたパケットのヘッダから得られる送信元 IP アドレス，送信先 IP アドレス，送信元ポート番号，送信先ポート番号，通信プロトコルの 5 つで識別する．算出した LDoS 攻撃トラフィックである確率に応じて，Detector ブロックでパケット廃棄または Precedence (IP Precedence) へのマーキング処理を行う．マーキング処理を行なったパケットは WRED ブロックに引き渡され，Precedence にもとづいて優先制御される．LDoS 攻撃トラフィックである確率が高い通信フローは劣後的にキューイングされ，LDoS 攻撃トラフィックである確率が低い通信フローは優先的にキューイングされる．LDoS 攻撃トラフィックである確率が低い通信フローのために通信帯域を確保しているような挙動を示す．

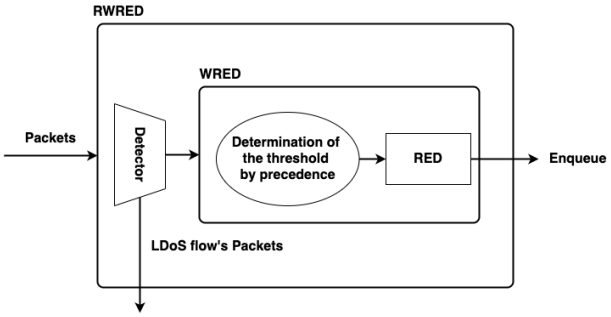

図 2 RWRED 機構概略図

RWRED 機構は LDoS 攻撃トラフィックである確率に応じて優先制御することができるため，正常トラフィックを保護しながら LDoS 攻撃トラフィックの検知及び抑止が可能であると考えられる．

5.2 LDoS 攻撃の検知条件の検討

RWRED の Detector ブロックにおける LDoS 攻撃トラフィックの検知条件を検討する．検知条件を検討するために LDoS 攻撃トラフィックのパケット入力時間の時系列分布を図 3 に示した．図 3 から LDoS 攻撃トラフィックのパケットが周期的に入力されていることがわかる．この周期的なパケット入力は LDoS 攻撃パラメータのバースト長 (L) 及びバースト間隔 (T) によるものである．このことから LDoS 攻撃トラフィックの検知条件をバースト長 (L) 及びバースト間隔 (T) をベースとし，バースト長 (L) 及びバースト間隔 (T) の基準値を定義する．バースト間隔 (T) は標的 TCP 通信の $minRTO$ であるためバースト間隔 (T) の基準値は 1000 ミリ秒 [11]．バースト長 (L) は標的 TCP 通信における RTT の 2〜3 倍程度であることと LDoS 攻撃トラフィックがネットワーク全体の 10 20 %程度を占める [5] ことからバースト長 (L) の基準値は 200 ミリ秒とした．このパラメータが最適化された攻撃パルス形状の定義となる．

バースト長 (L) 及びバースト間隔 (T) の基準値と当該通信フローにおけるバースト長 (L) 及びバースト間隔 (T) の

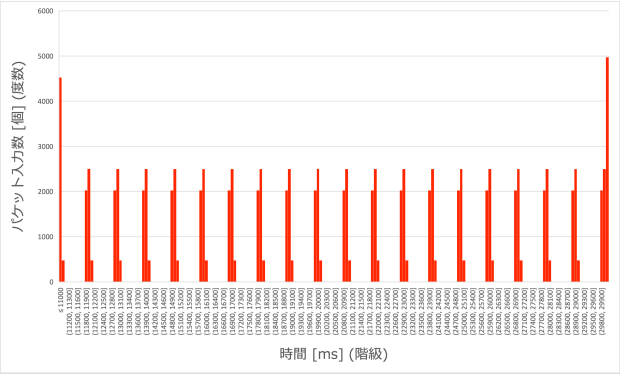

図 3 パケット入力時間の時系列分布

表 1 対象トラフィックが LDoS 攻撃トラフィックである確率に対応した Detector での処理

$P\ ldos$	動作
80 %以上 100 %以下	Detector でパケット廃棄
60 %以上 80 %未満	Precedence:0 でマーキング
40 %以上 60 %未満	Precedence:1 でマーキング
20 %以上 40 %未満	Precedence:3 でマーキング
0 %以上 20 %未満	Precedence:6 でマーキング

近さの度合いで算出されるバースト長 (L) からみた攻撃トラフィックである確率の $P\ attack\ (L)$ とバースト間隔 (T) からみた攻撃トラフィックである確率の $P\ attack\ (T)$ から対象トラフィックが LDoS 攻撃トラフィックである確率の $P\ ldos$ を算出する．表 1 で示すように，$P\ ldos$ に応じて検出する．

5.3 RWRED の実装

RWRED 機構では，対象トラフィックが LDoS 攻撃トラフィックである確率の $P\ ldos$ を算出する．$P\ ldos$ は，バースト長 (L) からみた攻撃トラフィックである確率の $P\ attack\ (L)$ とバースト間隔 (T) からみた攻撃トラフィックである確率の $P\ attack\ (T)$ から式 (5) で算出される．RWRED は表 1 で示すように $P\ ldos$ に応じて優先制御する．

$$P_{ldos} = P_{attack}(L) \times P_{attack}(T) \qquad (5)$$

$P\ attack\ (L)$ と $P\ attack\ (T)$ を算出するアルゴリズムを *Algorithm1* に示す．この *Algorithm1* はパケットが入力され RED によるキューイング処理が行われる前の Detector で呼ばれるアルゴリズムで，パケットが入力される度に呼び出される．*Algorithm1* は基準値となるバースト長 L 及びバースト間隔 T を基点に値の近さの度合いから $P\ attack\ (L)$ と $P\ attack\ (T)$ を算出している．*Algorithm1* の *standard* はバースト長 L またはバースト間隔 T の基点となる基準値，*comparison* は当該通信フローにおける 1 バースト周期前までのバースト長 L またはバースト間隔 T の実測値で，$P\ attack\ (Param)$ は $P\ attack\ (L)$ または $P\ attack\ (T)$ である．$P\ attack\ (Param)$ は *standard* と *comparison* の値の差から値の近さの度合いを求めて算出する．

Algorithm1 の条件式 1 は実測値が 0 から基準値の間に値をとる場合，条件式 2 は実測値が基準値から基準値の 2 倍の間に値をとる場合，条件式 3 は実測値が基準値の 2 倍以上に値をとる場合である．これは式 (6) で示すように実測値が 3 つの範囲のどこの値をとるかで $P\ attack\ (Param)$ の算出式が異なる．以上のように基準値を基点に実測値の値の近さの度合いをもとに $P\ attack\ (L)$ 及び $P\ attack\ (T)$ を算出する．

$$\begin{aligned}
P_{attack}(Param) &= 1.0 - \\
&\quad ((standard - comparison)/standard) \\
&\quad if \quad comparison \ : \ [0, standard) \\
P_{attack}(Param) &= 1.0 - \\
&\quad ((comparison - standard)/standard) \\
&\quad if \quad comparison \ : \ [standard, standard \times 2) \\
P_{attack}(Param) &= 0.0 \\
&\quad if \quad comparison \ : \ [standard \times 2, \infty) \qquad (6)
\end{aligned}$$

6. RWRED の性能の検証

6.1 実験概要

提案手法である攻撃パラメータベース RWRED の性能の評価を従来手法の攻撃パラメータベース RRED との比較にて行う．連続転送トラフィックである標的 TCP 通信に競合するように複数の攻撃パラメータによる LDoS 攻撃トラフィックを加える．提案手法の RWRED でのマルチクラス優先制御の導入によって，複数の攻撃パラメータでの LDoS 攻撃から標的 TCP 通信を保護できていることを検証する．

6.2 実験シナリオ

シミュレーションは 時刻 0 から 60 秒 の 60 秒間で行い，標的 TCP ストリームの送信者はシミュレーション全体の 0 から 60 秒まで通信を継続する．攻撃者は UDP にて構成されるパルス状の攻撃トラフィックを，時刻 10 秒からシミュレーションが終了する 60 秒までの 50 秒間送信する．

ボトルネックキューに攻撃パラメータベース RRED と攻撃パラメータベース RWRED の 2 種類の機構を適用したネットワークそれぞれで LDoS 攻撃を行う．2 種類の機構それぞれで LDoS 攻撃の確率に対する標的 TCP スループットを検証するために，バースト間隔（T）を 1.0 秒で固定してバースト長（L）を 100，150，200，250，300 ミリ秒の 5 パターンでシミュレーションを行う．シミュレーションの試行回数は合計 10 試行である．

Algorithm 1 $P_{attack}(L)$ と $P_{attack}(T)$ を算出するアルゴリズム

Require: $burstLength_{standard} \Leftarrow 200$ ▷ バースト長の基準値 200(ms)
Require: $burstInterval_{standard} \Leftarrow minRTO$ ▷ バースト間隔の基準値 1000(ms)
Require: $burstLength$ ▷ 当該通信フローにおけるバースト長 L の実測値 (ms)
Require: $burstInterval$ ▷ 当該通信フローにおけるバースト間隔 T の実測値 (ms)
Require: $param$ ▷ LDoS 攻撃トラフィックである確率を算出するために用いる攻撃パラメータ (バースト長またはバースト間隔)

function $CalculateP_{ldos}$
  $P_{attack}(Param)$ ▷ $P_{attack}(L)$ または $P_{attack}(T)$
  $standard$ ▷ 攻撃パラメータの基準値
  $comparison$ ▷ 攻撃パラメータの比較値
  if $param =$ "$burst\_length$" **then** ▷ バースト長 (L) を用いて LDoS 攻撃トラフィックである確率を算出する場合
    $standard \Leftarrow burstLength_{standard}$
    $comparison \Leftarrow burstLength$
  else if $param =$ "$burst\_interval$" **then** ▷ バースト間隔 (T) を用いて LDoS 攻撃トラフィックである確率を算出する場合
    $standard \Leftarrow burstInterval_{standard}$
    $comparison \Leftarrow burstInterval$
  end if
  if $((comparison = (standard - standard)$ **or** $comparison > (standard - standard))$
      and $comparison < standard)$ **then** ▷ 条件式 1: $0 \leq$ 比較値 $<$ 基準値
    $P_{attack}(Param) \Leftarrow 1.0 - ((standard - comparison)/standard)$ ▷ 確率の算出式 1
  else if $((comparison = standard$ **or** $comparison > standard)$
      and $comparison < standard \times 2)$ **then** ▷ 条件式 2: 基準値 $\leq$ 比較値 $\leq$ 基準値 $\times$ 2
    $P_{attack}(Param) \Leftarrow 1.0 - ((comparison - standard)/standard)$ ▷ 確率の算出式 2
  else if $(comparison = standard \times 2$ **or** $comparison > standard \times 2)$ **then** ▷ 条件式 3: 基準値 $\times$ 2 $<$ 比較値
    $P_{attack}(Param) \Leftarrow 0.0$ ▷ 確率の算出式 3
  end if
end function

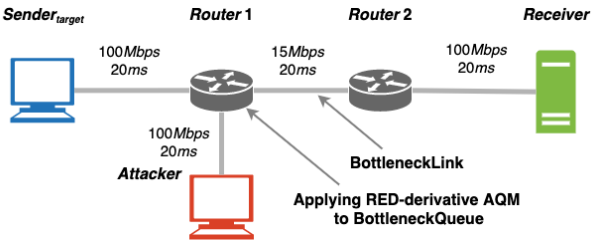

図 4 実験環境

6.3 実験環境

実験に用いる環境は図 4 に示すネットワークとし，離散イベントネットワークシミュレータである ns-3[21] を用いて評価系を構築した．送受信ノードを両側に配置したシンプルなダンベル型トポロジで構成している．ネットワークを構成するのは中間ノードである *Router* 1，*Router* 2，標的 TCP 送信者となる *Sender target*，攻撃者 UDP 送信者となる *Attacker*，*Sender target* および *Attacker* の受信者となる *Receiver* の 5 つのノードである．*Router* 1，*Router* 2 間をボトルネックリンクで接続し，*Router* 1 の出力キューに攻撃パラメータベース RRED と攻撃パラメータベース RWRED を適用した．攻撃パラメータベース RRED と攻撃パラメータベース RWRED の最大キュー長は 1000 パケットで設定した．攻撃パラメータベース RWRED のキュー長を制御する閾値は表 2 で示すように設定した．同様に攻撃パラメータベース RRED は表 2 の Precedence が 0 の時の閾値である最小閾値 50，最大閾値 150 で設定した．

表 2 RWRED における Precedence に対するキュー長閾値の対応表

Precedence	最小閾値	最大閾値
0	50	150
1	80	200
2	100	250
3	120	300
4	150	400
5	200	450
6	220	450
7	220	450

6.4 結果と考察

図 5 に従来手法の攻撃パラメータベース RRED について，図 6 に本研究の提案手法である攻撃パラメータベース RWRED による LDoS 攻撃緩和とそれによって得られる標的 TCP 通信の保護の様子を示す．それぞれ，連続転送トラフィックである標的 TCP 通信に競合するように LDoS 攻撃トラフィックを加えている．LDoS 攻撃トラフィックのパルス形状を決定するパースト長パラメータを変化させ，このシミュレーションシナリオでの最適パルス形状のものを LDoS 攻撃である確率 100 %とし，そこから乖離する度合いに応じて 50 % (100ms)，75 % (150ms)，75 % (250ms)，50 % (300ms) と併わせてパースト長パラメータの 5 通りの変域とした．それぞれのパラメータによる攻撃と標的 TCP による全トラフィックは本緩和機構に加えられている．これらにて行った 5 通りの実験をグラフ上に重

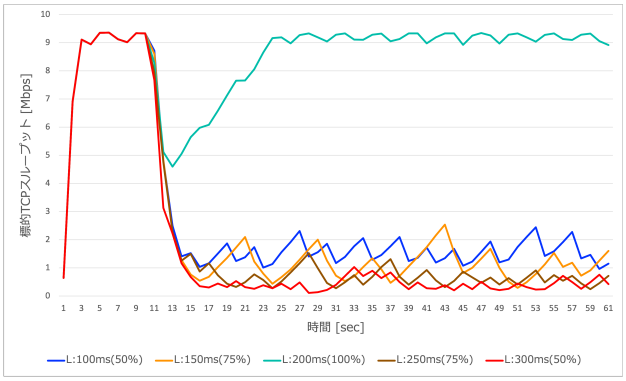

図 5 従来手法：バースト長を変化させた LDoS 攻撃における攻撃パラメータベース RRED 保護下での標的 TCP スループットの時系列変化

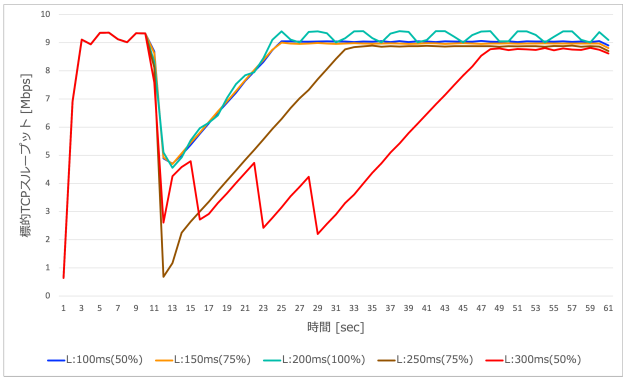

図 6 提案手法：バースト長を変化させた LDoS 攻撃における攻撃パラメータベース RWRED 保護下での標的 TCP スループットの時系列変化

ねて表示している．それぞれのグラフは標的 TCP が獲得できたスループットの時系列を示している．時刻 0 秒から転送を開始し，時刻 11 秒までに安定した帯域を獲得している．時刻 11 秒から LDoS 攻撃が開始され，標的 TCP のスループットは低下している．従来手法であるパラメータベース RRED の挙動を示図 5 では，最適攻撃パラメータであるバースト長 200ms(100 %) のみが継続する LDoS 攻撃下で時刻 27 秒時点で帯域幅を回復できているのに対して，それ以外のパラメータを持つ攻撃下では帯域幅は回復できず，攻撃が継続的に成功していることが判る．提案手法を用いた図 6 では，最適攻撃パラメータであるバースト長 200ms(100 %) だけでなく，他のパラメータを用いた攻撃に対しても標的 TCP がスループットを回復している様子が見てとれる．提案手法を用いた図 6 から，本研究の目的であった，従来手法では扱えない多様な攻撃パルスに対処できる LDoS 攻撃への新たな攻撃緩和機構の動作について，シンプルなダンベル型トポロジを用いたシミュレーションネットワークにおける単一の攻撃ノードによる攻撃トラフィックのパルス形状を決定するパラメータであるバースト長について 5 通りの変化に対して，攻撃の緩和と標的 TCP トラフィックの保護が可能であることを示した．

7. おわりに

7.1 まとめ

本稿では従来手法では扱えない多様な攻撃パルスに対処できる LDoS 攻撃への新たな攻撃緩和機構を提案することを目的に，既存の Robust RED[8] を参考に，RED のキューイング処理の部分に WRED を導入することでマルチクラスにし，LDoS 攻撃トラフィックである確率に応じた優先制御をすることで LDoS 攻撃を緩和し TCP 通信を保護する LDoS 防御機構である Robust WRED 機構の提案及び評価を行なった．シンプルなダンベル型トポロジを用いたシミュレーションネットワークにおける単一の攻撃ノードによる攻撃トラフィックのパルス形状を決定するパラメータであるバースト長について 5 通りの変化に対して，攻撃の緩和と標的 TCP トラフィックの保護が可能であることをパラメータベースの RRED とパラメータベースの RWRED の標的 TCP スループットを比較することで明らかにした．

7.2 今後の展望

本稿で提案した Robust WRED は LDoS 攻撃トラフィックの検知条件に LDoS 攻撃パラメータを利用した基本的な検知条件である．そのため，LDoS 攻撃の攻撃パラメータを変えることで LDoS 攻撃トラフィックである確率を操作することができ，検出を回避することが可能である．今後はより効果的な LDoS 攻撃の防御機構の提案を行う．

謝辞

本研究は JSPS 科研費 JP20K11772 の助成を受けたものです．

参考文献

[1] Kottler, S.: February 28th DDoS Incident Report, available from 〈https://github.blog/2018-03-01-ddos-incident-report/〉 (2018), (accessed 2021-05-06).

[2] Emmons, T.: FLARGEST EVER RECORDED PACKET PER SECOND-BASED DDOS ATTACK MITIGATED BY AKAMAI, available from 〈https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html〉 (2020), (accessed 2021-05-06).

[3] 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, No. 12, pp. 75–86 (2003).

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

[5] 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).
[6] QoS：輻輳回避設定ガイド (2017), available from 〈https://www.nsnam.org/〉 (accessed 2021-05-06).
[7] 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).
[8] 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).
[9] Chen, Z., Diep Pham, T. N., Kiat Yeo, C., Sung Lee, B. and Tong Lau, C.: FRRED: Fourier robust RED algorithm to detect and mitigate LDoS attacks, *2017 Zooming Innovation in Consumer Electronics International Conference (ZINC)*, pp. 13–17 (online), DOI: 10.1109/ZINC.2017.7968651 (2017).
[10] 安永遼真，中山悠，丸田一輝：TCP 技術入門，技術評論社 (2019).
[11] IETF: Computing TCP’s Retransmission Time，available from 〈https://tools.ietf.org/html/rfc6298〉(accessed 2021-05-06).
[12] IETF: TRANSMISSION CONTROL PROTOCOL, available from 〈https://tools.ietf.org/html/rfc793〉 (1981) (accessed 2021-05-06).
[13] Andrew S, T. and Wetherall, D. J.: コンピュータネットワーク，日経 BP 社 (2016).
[14] 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).
[15] 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).
[16] Mark, W.: Analysis and Simulation of Weighted Random Early Detection (WRED) Queues (2002).
[17] Makkar, R., Lambadaris, I., Salim, J., Seddigh, N., Nandy, B. and Babiarz, J.: Empirical study of buffer management scheme for Diffserv assured forwarding PHB, *Proceedings Ninth International Conference on Computer Communications and Networks (Cat.No.00EX440)*, pp. 632–637 (online), DOI: 10.1109/ICCCN.2000.885556 (2000).
[18] Shevtekar, A., Anantharam, K. and Ansari, N.: Low rate TCP denial-of-service attack detection at edge routers, *IEEE Communications Letters*, Vol. 9, No. 4, pp. 363–365 (online), DOI: 10.1109/LCOMM.2005.1413635 (2005).
[19] Mahajan, R., Floyd, S. and Wetherall, D.: Controlling high-bandwidth flows at the congested router, *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, pp. 192–201 (online), DOI: 10.1109/ICNP.2001.992899 (2001).
[20] Chang, C.-W., Lee, S., Lin, B. and Wang, J.: The taming of the shrew: mitigating low-rate TCP-targeted attack, *IEEE Transactions on Network and Service Management*, Vol. 7, No. 1, pp. 1–13 (online), DOI: 10.1109/TNSM.2010.I8P0308 (2010).
[21] nsnam.org: ns-3 — a discrete-event network simulator for internet systems, available from 〈https://www.nsnam.org/〉 (accessed 2021-05-06).