Vol.2025-MBL-117 No.28
Vol.2025-ITS-103 No.28
2025/11/27

代理再送機構を用いたLow-rate DoS攻撃への緩和手法の効率化

児玉 拓海[1]　稲村 浩[2]　石田 繁巳[2]

概要：DoS 攻撃の 1 種として，Low-rate DoS（LDoS）攻撃が議論されている．LDoS 攻撃手法には，TCP の再送制御アルゴリズムを悪用する Shrew 手法が存在する．Shrew 手法では，TCP の再送タイミングと攻撃トラフィックの転送タイミングを同期させることで攻撃を成立させている．既存研究では，攻撃を受ける TCP の制御アルゴリズムを変更する対策手法などが提案されている．しかし，攻撃される TCP の代理で再送を行い LDoS 攻撃を緩和する手法はあまり研究されていない．我々はこれまで，攻撃される TCP を変更せずに外部ノードを設置し，その代理再送機構を用いて，再送と攻撃タイミングの同期を外し，LDoS 攻撃を緩和する手法を提案し，実現性を示した．本研究では，代理再送機構を用いた攻撃緩和手法の改善を目的とする．代理再送機構を用いた攻撃緩和手法の改善スループットのモデル化を行い，代理再送の開始タイミングの最適化を行った．実機を用いたテストベッドネットワークにおいて，最適化された代理再送の開始タイミングを用いた場合の LDoS 攻撃緩和効果を評価した．

キーワード：Low-rate DoS（LDoS）攻撃，PEP，TCP

1. はじめに

インターネットの通信を支えるトランスポートプロトコルとして TCP が存在する．TCP は 1981 年に標準化 [1] されてから，現在でも長期的に活躍している．Web の閲覧やメールの送受信など，インターネットで使われる代表的なアプリケーションには TCP が使用されており，暗号化技術と組み合わせることで高いセキュリティが必要となる通信にも使用されている．TCP は長期的に多くの通信に使用されていることから，TCP の脆弱性に注目して標的とするサイバー攻撃も存在しており，TCP を用いる通信の安全性の向上が必要である．

2003 年から，サイバー攻撃である DoS 攻撃の 1 つとして，Low-rate DoS（LDoS）攻撃が議論されている [2]．LDoS 攻撃は，通信プロトコルで用いられているアルゴリズムの脆弱性を悪用し，パルス形状の攻撃トラフィックを用いて攻撃を実現する．LDoS 攻撃には，TCP の再送制御で用いる再送タイムアウト（Retransmission Time Out; RTO）の再送タイマ管理アルゴリズムを悪用する Shrew 手法 [2] が存在する．

LDoS 攻撃手法では，パルス形状の攻撃トラフィックを用いており，低い平均通信量で攻撃を実現している．そのため，従来の平均通信レートを用いる Flooding DoS（FDoS）攻撃に対する検知機構を回避する攻撃のステルス性を持つ．この特性により，LDoS 攻撃の被害を受けた場合でも被害者が攻撃を認知できていないケースが存在し，FDoS 攻撃と比べると LDoS 攻撃による被害の報告は少ない [3] が，この攻撃への理解と対策手法を確立することは重要である．

既存研究 [2], [4] など，TCP の制御アルゴリズムに変更を加えることで LDoS 攻撃耐性を付与する手法が提案されているが，現在も多くの通信で用いられる TCP の制御アルゴリズムを直接変更することは展開コストが大きい．既存の LDoS 攻撃の対策手法について，現行の TCP を変更するコストを避けるために PEP（TCP Performance Enhancement Proxy）[5] を応用した代理再送を用いる手法について，著者らの知る限り議論されていなかった．

そこで著者らは，攻撃を受ける TCP には変更を加えずに，代理再送機構を実装した外部ノードを追加する新たな LDoS 攻撃緩和手法の初期的検討を行い，攻撃緩和が可能であることを示した．LDoS 攻撃パルス幅を変えても追随して動作するように代理再送の開始タイミングを決定する方式を定め，一定の緩和効果も得られた [6], [7]．

しかしながら，攻撃トラフィックの特性に合わせて代理再送の開始タイミングを決定する方式では，代理再送開始の遅延と改善スループットについて，最適化されていな

[1] 公立はこだて未来大学院 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

かったため，攻撃緩和手法を改善する余地がある．

本稿では，代理再送機構を用いた攻撃緩和手法の改善スループットのモデル化を行い，代理再送の開始タイミングの最適化を行う．

本稿の構成は以下の通りである．まず，2 章にて本稿で扱う Shrew 手法の原理について説明する．3 章では，Shrew 手法の緩和手法に関する関連研究を示し，4 章で代理再送機構を用いた Shrew 手法に対する攻撃緩和手法の効率化について説明する．5 章で最適化した代理再送機構の攻撃緩和効果について実験的評価を行い，最後に 6 章にてまとめとする．

2. Shrew 手法の原理

本章では，本稿で扱う LDoS 攻撃手法である Shrew 手法の原理について述べる．

2.1 DoS 攻撃の概要

DoS 攻撃は，ルータやサーバに攻撃トラフィックを転送することで，通信の妨害や通信品質を低下を発生させるサイバー攻撃の 1 つである．DoS 攻撃には，大量トラフィックを用いて攻撃する FDoS 攻撃と，低量の攻撃トラフィックを用いる LDoS 攻撃の 2 種類が存在する．FDoS 攻撃は，リンク帯域幅を埋め続けるために攻撃トラフィックを継続して転送するため，平均通信量が非常に大きくなり，容易に検知することが可能である．それに対して，通信プロトコルの脆弱性を悪用する LDoS 攻撃には，パルス形状の攻撃トラフィックを用いるため平均通信量が低いという特徴がある．

2.2 LDoS 攻撃の概要

LDoS 攻撃では，パルス形状の攻撃トラフィックを用いて攻撃することで平均通信量を低量にし，攻撃にステルス性を持たせる．LDoS 攻撃に用いられるパルス形状のトラフィックを攻撃長 R，攻撃パルス幅 L，攻撃周期 T として**図 1** に示す．平均通信レートの高さを指標に用いる従来の FDoS 攻撃に対する検知機構では，LDoS 攻撃の検知は難しい [3]．本稿で扱う LDoS 攻撃手法の 1 つである Shrew 手法においてもこれらの特性を持つ．

2.3 TCP の再送タイマ管理アルゴリズム

TCP は，再送タイマを用いて再送処理を時間で制御している．再送タイマでは，送信セグメントに対応する ACK が返送されるまでの待機時間を RTO として設定する．送信セグメントに対応する ACK が返送されるまでの時間が RTO のタイマ値を超えた場合にセグメントを損失したと判断し，再送処理を行う．RTO のタイマ値以内の時間で送信セグメントに対応する ACK が返送された場合，再送タイマをリセットする．Fast Retransmit が失敗した後は，

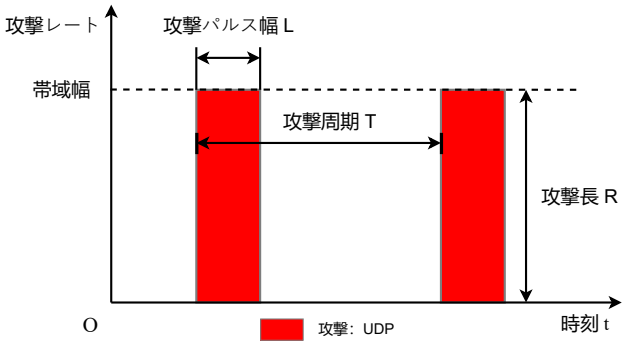

図 1 パルス形状の LDoS 攻撃トラフィック

RTO を用いたセグメントの再送信が行われる [8]．TCP の再送タイマである RTO は，以下の式 (1) で計算される [9]．

$$\max(minRTO, SRTT + \max(G, 4 \times RTTVAR)) \quad (1)$$

RTO は，$minRTO$ と $SRTT + \max(G, 4 \times RTTVAR)$ の最大値により計算される．$minRTO$ は RTO の初期値のことであり，RFC6298 [9] では 1 秒が推奨値とされている．$SRTT$ は外れ値による影響を軽減するために RTT を平滑化したものである．実環境において多くの場合で $SRTT + \max(G, 4 \times RTTVAR)$ は 1 秒よりも小さい値となる．そのため，式 (1) により計算される RTO は，1 秒が設定され，外部から容易に推測することが可能となっている．

式 (1) で計算される RTO を使用した場合も再送に失敗したとき，指数バックオフを用いる以下の式 (2) で 2 回目以降の RTO が計算される [9]．

$$RTO_n = 2 \times RTO_{n-1},\ RTO_1 = minRTO \quad (2)$$

式 (2) から計算される RTO は，2 回目以降にもパケットのロスの発生した場合，2 倍ずつ増加する．TCP の再送制御では，式 (2) の計算でパケットの送信タイミングを制御することで，より確実なパケットの再送を行っている．しかし，RTO の最大値は一般に 60 秒と設定されており，RTO が 60 秒を超えた場合には，TCP はネットワークに異常ありと判断して，コネクションを切断し，セッションタイムアウトとなる．

指数バックオフを用いた再送タイマアルゴリズムの RTO が外部から容易に推測可能である点は，2.4 節で説明する Shrew 手法で悪用されている．

2.4 Shrew 手法

LDoS 攻撃にはいくつかの攻撃手法が存在するが，代表的な攻撃手法として，TCP を標的とする Shrew 手法がある．Shrew 手法では，容易に推測が可能である指数バックオフを用いる再送タイマ管理アルゴリズムを悪用する．Shrew 手法による LDoS 攻撃の原理を**図 2** に示す．Shrew 手法の攻撃成立までの流れは以下の通りである．まず，送

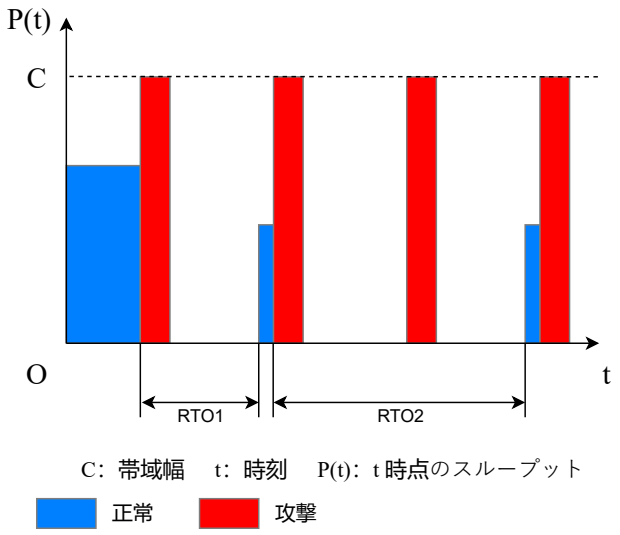

図 2　Shrew 手法の攻撃トラフィック

信者は受信者に向けて正常トラフィックの転送を開始する．転送開始後，攻撃者はボトルネックリンク帯域幅を満たすレートで攻撃トラフィックを転送する．転送した攻撃トラフィックはルータにキューイングされ，ルータバッファが攻撃トラフィックによって占有される．これにより，正常トラフィックに含まれているセグメントの損失が発生する．複数セグメントの損失により，送信者による再送タイマを用いた再送処理が行われる．この再送のタイミングは，2.3 節で説明したように予測が容易であるため，攻撃者が攻撃トラフィックの転送タイミングを再送タイミングと同期させることで再度セグメントを損失させ，さらに RTO を発生させる．このプロセスが複数回繰り返されることで，TCP コネクションのタイムアウトが発生する．

LDoS 攻撃の Shrew 手法では，送信者の再送タイミングと同期するように攻撃トラフィックを転送することで，攻撃を成立させている．このことから，送信者の再送タイミングと攻撃トラフィックの転送タイミングの同期を外すことで，Shrew 手法の攻撃を緩和することができる．

3. 関連研究

Shrew 手法の攻撃対策手法として，代理再送を用いる手法はあまり議論されていない．本章では，これまで議論されている Shrew 手法に対する対策手法について述べ，従来手法の課題を確認する．

3.1 再送タイマ管理アルゴリズムの変更

TCP の再送タイマ管理アルゴリズムに変更を加えることで，Shrew 手法の攻撃を緩和する手法が存在する．

Kuzmanovic らは，RTO 再送と攻撃トラフィックの衝突を回避するために，$minRTO$ を一定の範囲でランダムに選ぶ手法を提案した [2]．しかし，$minRTO$ をランダマイズする手法は，TCP の輻輳制御機能を維持するためにランダマイズの幅を大きく取ることができず，攻撃の緩和効果はわずかであることが報告されている．

細井らは LDoS 攻撃に対しての攻撃緩和効果のある RTO 計算アルゴリズムを提案した [4]．提案アルゴリズムでは，RTO の増加方法を式 (3) に変更し，有理数 u を区間 $(0,\ 1)$ の範囲内でランダマイズすることで連続する再送での RTO の値は式 (4) となる．

$$RTO_n = (1+u)RTO_{n-1} \quad (0 < u < 1) \tag{3}$$

$$RTO_n = (1+u)^{n-1} minRTO \tag{4}$$

u に有理数を選ぶことで，RTO 再送の周期が $minRTO$ の整数倍ではなくなるため，RTO 再送と攻撃タイミングの同期が外れる機会が生まれ，LDoS 攻撃の緩和が可能となる．この緩和手法では，従来の RTO の計算アルゴリズムと比較して LDoS 攻撃による被害を緩和できることが報告されている．しかし，この手法では，現行の TCP と $minRTO$ の値が同じであるため，攻撃周期が $minRTO$ の値と等しい場合に 1 回目の RTO 再送が攻撃トラフィックと衝突し，攻撃回避に失敗する可能性が高い．そのため，攻撃トラフィックとの衝突を回避し，攻撃を緩和するまでにパケットの送信が 2 回以上失敗してしまう．

これら 2 つの手法はどちらも攻撃を受ける TCP 自体に変更を加えることが必要である．現在多くの通信で用いられている TCP に変更を加えることは展開のコストが大きいことも課題として考えられる．

3.2 攻撃トラフィックの特性に合わせて LDoS 攻撃を緩和する代理再送機構

著者らは，攻撃トラフィックの特性に合わせて代理再送の開始タイミングを決定する方式を提案し，多様な攻撃パルス幅を持った LDoS 攻撃に対応可能であることを示した [6], [7]．この手法では，代理再送の開始タイミングの決定方式を攻撃に用いられる UDP トラフィックの受信により攻撃を検知し，一定秒数後に再送する方式から，攻撃 UDP トラフィックの転送終了を契機に決定する方式へ変更している．攻撃 UDP トラフィックの受信間隔から攻撃パルスの転送終了を判定することで，多様な攻撃パルス幅を持った LDoS 攻撃に対して代理再送トラフィックと攻撃トラフィックの衝突を回避し，攻撃緩和効果を得ることが可能となる．

しかし，攻撃パルスの転送終了判定により発生する代理再送開始までの遅延と改善スループットについて最適化されていないため，攻撃緩和手法を改善する余地がある．

本稿では，代理再送機構を用いた攻撃緩和手法の改善スループットのモデル化を行い，代理再送の開始タイミングの最適化を行う．

4. 代理再送を用いたLDoS攻撃への緩和手法の効率化

代理再送機構を用いてLDoS攻撃のShrew手法の攻撃を緩和するためには，代理再送の開始タイミングが重要である．なぜなら，代理再送トラフィックと攻撃トラフィックの衝突が発生することで，代理再送セグメントが損失すると，攻撃緩和効果が得られないからである．従来手法では，攻撃トラフィックであるUDPトラフィックの転送終了を契機に代理再送の開始タイミングを決定することで，多様な攻撃パルス幅を持つLDoS攻撃下でも，代理再送トラフィックと攻撃トラフィックの衝突を回避することができる．

しかし，従来手法では，代理再送の開始タイミングの決定において代理再送開始までの遅延，改善スループットとキューイングディレイについて，十分な検討ができていないことが課題である．

本稿では，代理再送を用いた攻撃緩和手法における改善スループットのモデル化を行い，キューイングディレイに基づいて代理再送の開始タイミングの最適化を行う．

4.1 代理再送を用いた攻撃緩和手法の原理

本手法で用いる代理再送機構は，攻撃トラフィックとTCPの再送タイミングの同期を外すことで，LDoS攻撃によるスループット低下を緩和することを目的としている．LDoS攻撃はパルス形状の攻撃トラフィックを用いて攻撃するため，攻撃パルス間に攻撃トラフィックが転送されていない時間が必ず存在する．TCPのRTOを用いる再送処理を悪用するShrew手法の攻撃原理から，この時間では攻撃を受けるTCPのセグメント転送は行われない．そこで，代理再送機構は，攻撃中に転送される正規のTCPセグメントを一時的にキャッシュする．その後，代理再送機構は，攻撃パルスの終了を判定した後に，そのキャッシュを用いて攻撃で喪失したTCPセグメントをオリジナルの送信ノードの代理として再送を行う．攻撃パルス終了後から概ねminRTO期間においてオリジナルの送信ノードはタイムアウト待ちのため再送動作を行えない．代理再送を成功させることで，再送したTCPセグメントに対するACKが返送され，オリジナルの送信ノードによる正規のTCP通信が再開される．これにより，LDoS攻撃下でも正規のTCPの通信量を増加させて攻撃によるスループットの低下を緩和することができる．

代理再送の成功により増加する通信量のイメージを**図 3**に示す．LDoS攻撃下で代理再送によって増加する通信量は代理再送の開始タイミングによって変化し，攻撃パルスの終了から代理再送の開始までの時間が長いほど少量になる．

本手法で用いる代理再送機構は，正規のTCPセグメントのキャッシュと，攻撃パルスの終了判定を行う必要があるため，**図 4**に示すSenderとAttackerの通信をキャプチャできる位置に設置する．

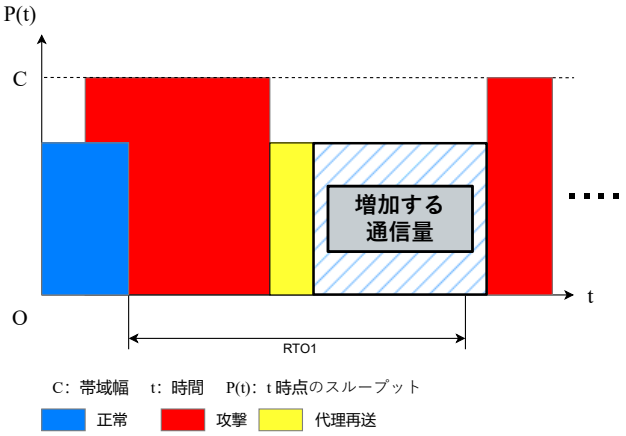

図 3 代理再送によって増加する通信量

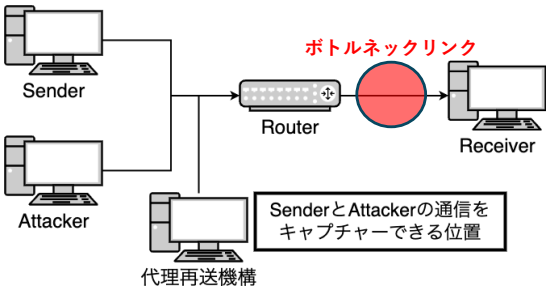

図 4 代理再送機構の設置位置

4.2 代理再送開始遅延の原因と従来手法の課題

従来手法でも使用している攻撃パルス終了判定は，攻撃に用いられるUDPパケットの受信間隔から攻撃トラフィックの転送中であるかを判別する．LDoS攻撃トラフィックの転送中は，非常に短い間隔で攻撃UDPパケットが観測される．攻撃1パルスの終了時には，最後の攻撃UDPパケットが転送されてから，次の攻撃パルスの最初の攻撃UDPパケットの転送開始までの時間が存在する．そこで，攻撃トラフィックのUDPパケット受信間隔を監視し，受信間隔が閾値以上に拡大した時点を攻撃1パルス終了と判定して代理再送を開始する．この方式は，攻撃パルス幅が変動しても追随できる利点を持つ一方で，再送セグメントへのACK返送が想定よりも遅く，期待された緩和効果と乖離があった．

本研究では，その原因として以下の状況を確認した．攻撃の最終UDPパケットが送信された直後にも，ボトルネックキューには攻撃パケットが依然として滞留しており，それらがすべて出力されるまでリンク帯域を占有するため，代理再送セグメントが送出されてもキューが空くまで待た

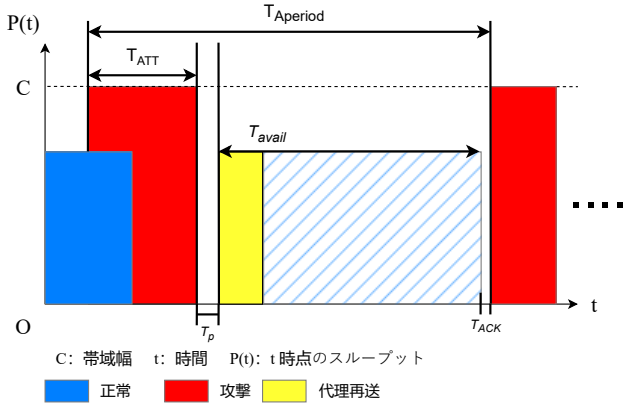

図 5　代理再送を用いた LDoS 攻撃の緩和モデル

され，対応する ACK の返送が想定より遅延する状況が発生していた．その結果，見かけ上は攻撃パルス終了直後に代理再送を開始しているが，実際にはキューの残留パケットの占有時間により，代理再送セグメントがキューから送信されるまでに遅延が発生した．

代理再送機構が攻撃終了後の帯域を有効に活用するためには，攻撃終了から再送開始までの遅延を単純に最小化するのではなく，ボトルネックキューに滞留する攻撃パケットが排出されるまでのキューイングディレイを考慮し，その時間を差し引いた上で，利用可能な転送時間を評価する必要がある．本研究では，このキューイングディレイを最適な開始タイミングの基準として導入することで，再送セグメントのブロックを回避し，代理再送によるスループット改善効果を最大化する手法を検討する．

4.3　改善スループットのモデル化

代理再送機構を用いた LDoS 攻撃への緩和手法のスループットの改善を定量化するためのモデルのパラメータ一覧を**表 1**，互いの関係を図示したものを**図 5** に示す．代理再送が可能な最大時間 T_{avail} は，式 (5) を用いて，LDoS 攻撃周期 $T_{Aperiod}$，LDoS 攻撃パルス幅 T_{ATT}，ACK 受信遅延 T_{ACK}，代理再送遅延 T_p から計算する．代理再送遅延 T_p は，攻撃 1 パルスの終了から代理再送の開始までの時間を示し，攻撃終了判定に用いる UDP パケットの受信間隔の閾値と同じ値になる．代理再送失敗率 P は，代理再送機構が攻撃パルスの転送中にも関わらず閾値 T_p 以上の受信間隔を観測し，誤って攻撃パルスの終了を判定する確率を示す．代理再送失敗率 P は，**図 6** に示す本研究の評価環境で観測した攻撃 UDP パケットの受信間隔の分布から式 (6) を用いて計算する．攻撃下の UDP 受信間隔の分布は指数分布として扱う．代理再送を用いた LDoS 攻撃への緩和手法の改善スループット E は，代理再送が可能な最大時間 T_{avail}，攻撃周期 $T_{Aperiod}$，正常スループット R_0，代理再送失敗率 P から式 (7) を用いて計算する．

表 1　改善スループットのモデル化に用いるパラメータ

LDoS 攻撃パルス幅	T_{ATT}
LDoS 攻撃周期	$T_{Aperiod}$
代理再送遅延	T_p
ACK 受信遅延	T_{ACK}
正常スループット	R_0

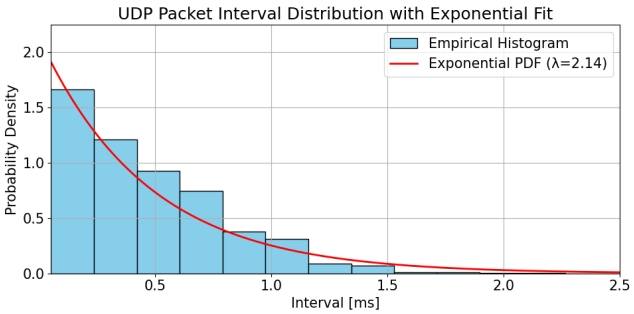

図 6　攻撃 UDP パケットの受信間隔の分布

$$T_{avail} = T_{Aperiod} - T_{ATT} - T_{ACK} - T_p \tag{5}$$

$$P = e^{-\lambda T_p} \tag{6}$$

$$E = \frac{T_{avail}}{T_{Aperiod}} \cdot R_0 \cdot (1 - P) \tag{7}$$

4.4　代理再送の開始タイミングの決定方法と攻撃緩和可能時間

本稿では，キューイングディレイを最適な開始タイミングの基準として導入することで，再送セグメントのブロックを回避し，代理再送によるスループット改善効果を最大化する手法を検討する．

攻撃対象となっているボトルネックキューのキューイングディレイを以下に示す．ルータが 1 パケット送出するために要する時間 T_{pkt} を，1 パケットを 1514 bytes として式 (8) から計算する．攻撃 UDP の転送停止後にルータのキューから攻撃パケット以外のパケットを送信可能になるまでに要する時間 T_{qdelay} を，設定したルータのキューサイズを Q_{size} とし，式 (9) で計算する．

本稿の評価では，式 (7) で計算する改善スループットが最大となる代理再送遅延 T_p を設定する．すなわち攻撃パケットの到着間隔が代理再送遅延 T_p 以上になったところで代理再送を開始するものとする．T_{qdelay} は，設定キューサイズ毎で計算して，設定する．攻撃緩和可能時間，つまり代理再送が可能な最大時間 T_{avail} は，この T_{qdelay} を考慮して式 (10) と改める．

$$T_{pkt} = \frac{12112}{10 \cdot 10^6} = 0.0012112\ s = 1.211\ ms \quad (8)$$

$$T_{qdelay} = Q_{size} \cdot T_{pkt} \quad (9)$$

$$T_{avail} = T_{Aperiod} - T_{ATT} - T_{ACK} - T_p - T_{qdelay} \quad (10)$$

5. 評価

最適化した代理再送の開始タイミングを設定した場合のスループットと，モデルにより得られた改善後のスループットの計算値の一致率を検証するために実施した実験的評価とその結果，考察について述べる．

5.1 評価環境

実験の使用機材を**表 2**，使用した評価環境のトポロジを**図 7**に示す．Sender，Receiver，3 台の Attacker の各ノードで用いたプロトコルを**表 3**に示す．Sender と 3 台の Attacker は帯域幅 1 Gbps で Router に接続している．Router はボトルネックリンクで Receiver に接続しており，Sender からのデータを Receiver に向けて転送する．ボトルネックリンクには，通信されるトラフィックを監視する Observer を接続している．Observer は Linux tcpdump のコマンドを使用して，pcap データを取得する．Router は Linux tc コマンドを使用して帯域幅を 10 Mbps，ルータのキューサイズは，200，300，400 パケットの 3 パターンの設定で，それぞれ帯域制限をかけてボトルネックリンクを作成している．

3 台の Attacker は，Router に対してパルス形状の攻撃トラフィックを転送する．LDoS 攻撃で用いられる攻撃トラフィックの多くは UDP パケットである [3] ことから，Attacker の 3 台が送信する攻撃トラフィックは UDP パケットとする．RFC6298 [9] で *minRTO* の推奨値が 1 秒であると定義され，1 回目の RTO のタイマ値は多くの場合で *minRTO* が設定されることから Attacker の LDoS 攻撃周期 1.0 秒に設定する．LDoS 攻撃パルス幅は，0.3 秒に設定する．攻撃トラフィックの転送は Sender の送信が終わるまで続けるように設定する．

今回の評価実験では，Sender から Receiver に向けて 10 MB のデータを転送する．Sender のデータ送信開始から送信終了を 1 試行とし，ルータのキューサイズ 200 パケット，300 パケット，400 パケットの 3 パターンの設定を用意し，代理再送機構の導入前，従来手法の代理再送機構の導入時，提案手法の代理再送機構の導入時で，それぞれ 50 試行分の実験の pcap データを，Observer で取得する．取得した pcap データから，平均スループットを算出して攻撃効果を求め，攻撃効果から改善率，平均スループットとモデルにより得られた改善後のスループットから計算値と実測値の一致率を計算する．

表 2 実験で用いた機材

ノード	OS	CPU
Sender	Raspberry Pi OS	ARM Cortex-A72
Receiver	Raspberry Pi OS	ARM Cortex-A72
Attacker1	Raspberry Pi OS	ARM Cortex-A72
Attacker2	Raspberry Pi OS	ARM Cortex-A72
Attacker3	Raspberry Pi OS	ARM Cortex-A72
Router	OpenWRT	Intel(R)N100
Observer	Ubuntu	Intel(R)N100
代理再送機構 (PEP)	Ubuntu	Intel(R)N100

表 3 各ノードで用いたプロトコル

ノード	ネットワーク層	トランスポート層
Sender	IP	TCP
Receiver	IP	TCP
Attacker1	IP	UDP
Attacker2	IP	UDP
Attacker3	IP	UDP

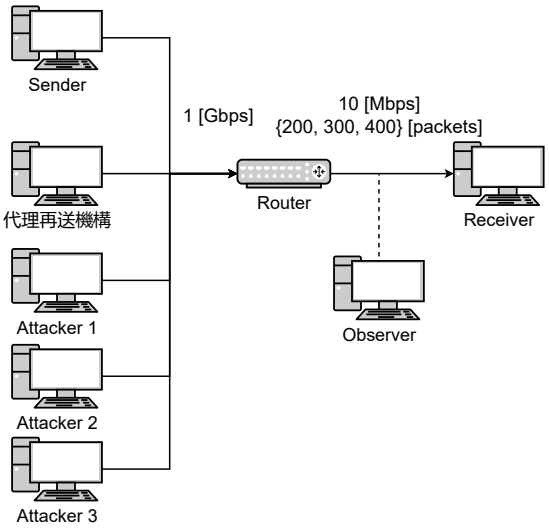

図 7 実験環境のトポロジ

5.2 攻撃効果と攻撃の改善率の定義

久末らは，攻撃がない状態の正常トラフィックの平均スループットを T_n ，攻撃下での平均スループットを T_a とし，式 (11) から LDoS 攻撃の攻撃効果を計算している [10]．本稿では，式 (12) から攻撃効果を計算し，評価に用いる．攻撃下で代理再送機構の導入時の平均スループットを T_p とし，攻撃効果 E_a, E_p を式 (12) を用いて計算する．攻撃効果 E_a, E_p から攻撃の緩和率 R を式 (13) を用いて計算する．

$$E_a = 1 - \frac{T_a}{T_n} \quad (11)$$

$$E_p = 1 - \frac{T_p}{T_n} \quad (12)$$

$$R = \frac{E_a - E_p}{E_a} \quad (13)$$

攻撃効果 E_a, E_p は攻撃による正常トラフィックのスルー

表 4 評価実験で設定した改善スループットのモデルのパラメータ

LDoS 攻撃パルス幅	T_{ATT}	300
LDoS 攻撃周期	$T_{Aperiod}$	1000
ACK 受信遅延	T_{ACK}	25
代理再送遅延	T_p	3.402
正常スループット	R_0	10
UDP 受信間隔の分布平均	m	0.370

プット低下率を示しており，改善率 R は，代理再送機構の導入前と導入時の攻撃効果から算出した攻撃効果の変化率であり，正常トラフィックのスループット改善率を示す．

5.3 改善スループットの計算値の定義

本稿の評価で用いる改善スループットの計算値 E_t は，式 (16) から計算する．**表 4** に示す代理再送遅延 T_p と UDP 受信間隔の分布平均 m から，式 (14) を用いて指数分布のパラメータ λ，式 (15) を用いて代理再送失敗率 P_t を計算する．

$$\lambda = \frac{1}{m} = 2.137 \tag{14}$$

$$P_t = e^{-\lambda T_p} \tag{15}$$

$$E_t = \frac{T_{avail}}{T_{Aperiod}} \cdot R_0 \cdot (1 - P_t) \tag{16}$$

5.4 計算値と実測値の一致率の定義

本稿では，式 (17) から計算値と実測値の一致率を計算し，評価に用いる．一致率 A は，モデルから計算した改善後のスループットの計算値と実験データから算出した平均スループットがどのくらい一致するのかを示す．改善スループットのモデルから得られたスループットの計算値を T_t，実験で取得したデータから算出したスループットの実測値を T_m とし，一致率 A を式 (17) を用いて計算する．

$$A = 1 - \frac{T_m}{T_t} \tag{17}$$

表 4 に，評価実験で設定したパラメータと，改善スループットの計算に用いたパラメータを示す．今回の評価実験では，LDoS 攻撃周期 $T_{Aperiod}$ を 1000，LDoS 攻撃パルス幅 T_{ATT} を 300，ACK 受信遅延 T_{ACK} を 25，正常スループット R_0 を 10 として，実験環境の設定と改善後のスループットの計算を行った．

5.5 結果

ルータのキューサイズを 200，300，400 パケットに設定した場合の，従来手法と提案手法の代理再送機構の攻撃緩和効果，それぞれのスループットとモデルにより得られたスループットの計算値の一致率を比較し，本稿のモデルにより代理再送の開始タイミングが最適化されているのかを評価した．

表 5 にルータのキューサイズを 200 パケットに設定した場合における従来手法と提案手法の代理再送機構の導入時，代理再送機構の導入前の平均スループット，攻撃効果 E，改善率 R，平均スループットとモデルにより得られたスループットの計算値の一致率 A を示す．従来手法では平均スループットは 3.11 Mbps，攻撃効果は 67.5%，改善率は 30.1%，一致率は 72.5%であった．それに対して，提案手法では．平均スループットは 3.54 Mbps，攻撃効果は 63.0%，改善率は 34.7%，一致率は 82.5%であった．ルータのキューサイズを 200 パケットに設定した場合，従来手法と比較すると提案手法の方が高い改善率と一致率が得られた．

表 6 にルータのキューサイズを 300 パケットに設定した場合における従来手法と提案手法の代理再送機構の導入時，代理再送機構の導入前の平均スループット，攻撃効果 E，改善率 R，平均スループットとモデルにより得られたスループットの計算値の一致率 A を示す．従来手法では平均スループットは 2.55 Mbps，攻撃効果は 72.9%，改善率は 24.3%，一致率は 82.8%であった．それに対して，提案手法では．平均スループットは 2.90 Mbps，攻撃効果は 69.1%，改善率は 28.2%，一致率は 94.2%であった．ルータのキューサイズを 300 パケットに設定した場合，従来手法と比較すると提案手法の方が高い改善率と一致率が得られた．

表 7 にルータのキューサイズを 400 パケットに設定した場合における従来手法と提案手法の代理再送機構の導入時，代理再送機構の導入前の平均スループット，攻撃効果 E，改善率 R，平均スループットとモデルにより得られたスループットの計算値の一致率 A を示す．従来手法では平均スループットは 1.22 Mbps，攻撃効果は 87.4%，改善率は 9.5%，一致率は 65.3%であった．それに対して，提案手法では．平均スループットは 1.70 Mbps，攻撃効果は 82.4%，改善率は 14.7%，一致率は 91.0%であった．ルータのキューサイズを 400 パケットに設定した場合，従来手法と比較すると提案手法の方が高い改善率と一致率が得られた．

今回の評価実験では，ルータのキューサイズを 200，300，400 パケットに設定したすべての場合において，従来手法よりも提案手法の代理再送の開始タイミングを最適化した代理再送機構の方が高い改善率が得られ，モデルにより得られたスループットの計算値ともよく一致する結果が得られた．

5.6 考察

今回の評価実験から，提案手法の代理再送の開始タイミングの最適化は，従来手法と比較して高い改善率を得られた．モデルから計算した改善スループットと実測値が約 90%と高い一致率が得られた．この結果から，本稿で説明し

表 5 平均スループットと攻撃効果と改善率 [攻撃パルス幅: 300 ms, 設定キューサイズ: 200 packets]

攻撃	PEP	Throughput (Mbps)	攻撃効果 E (%)	改善率 R (%)	一致率 A (%)
なし	なし	9.58	N/A	N/A	N/A
あり	なし	0.33	96.6	N/A	N/A
あり	[7]	3.11	67.5	30.1	72.5
あり	提案	3.54	63.0	34.7	82.5

表 6 平均スループットと攻撃効果と改善率 [攻撃パルス幅: 300 ms, 設定キューサイズ: 300 packets]

攻撃	PEP	Throughput (Mbps)	攻撃効果 E (%)	改善率 R (%)	一致率 A (%)
なし	なし	9.40	N/A	N/A	N/A
あり	なし	0.35	96.3	N/A	N/A
あり	[7]	2.55	72.9	24.3	82.8
あり	提案	2.90	69.1	28.2	94.2

表 7 平均スループットと攻撃効果と改善率 [攻撃パルス幅: 300 ms, 設定キューサイズ: 400 packets]

攻撃	PEP	Throughput (Mbps)	攻撃効果 E (%)	改善率 R (%)	一致率 A (%)
なし	なし	9.67	N/A	N/A	N/A
あり	なし	0.33	96.6	N/A	N/A
あり	[7]	1.22	87.4	9.5	65.3
あり	提案	1.70	82.4	14.7	91.0

た改善スループットのモデルが，LDoS 攻撃周期 $T_{Aperiod}$，LDoS 攻撃パルス幅 T_{ATT}，ACK 受信遅延 T_{ACK}，及びルータのキューサイズと蓄積されたパケット数に基づくキューイングディレイ T_{qdelay} について適切に扱い，代理再送が可能な最大時間 T_{avail} を代理再送が実際に有効に働く時間として推定できていると考えられる．

ルータのキューサイズの条件を変化させた場合に，提案手法の方が従来手法よりも高い改善率を得られた点は，攻撃パルスの終了判定にキューイングディレイを閾値として設定したことが，評価環境の遅延特性において，有効だったと考えられる．

キューサイズが大きい設定では，代理再送を用いる手法の攻撃緩和効果は小さく，攻撃の影響が強く残っていることがわかった．式 (9) で示したように，キューイングディレイ T_{qdelay} を増大させてしまい，結果的に代理再送が可能な最大時間 T_{avail} を縮小させたことが原因である．

今回の評価では，代理再送を用いた LDoS 攻撃の緩和手法において，代理再送の開始タイミングをキューイングディレイに基づき最適化することで，従来手法より高い改善率を達成できることを示した．

6. おわりに

本稿では，代理再送機構を用いた LDoS 攻撃への緩和手法の改善スループットのモデル化を行い，代理再送の開始タイミングの最適化を行った．代理再送の開始タイミングの最適化を行った代理再送機構と従来手法 [7] を比較し，本稿のモデルによる代理再送の開始タイミングの最適化を評価するために，実機を用いたテストベッドネットワークにて評価実験をおこなった．評価実験では，ルータのキューサイズを 200，300，400 パケットに設定した場合の従来手法 [7] と提案手法の攻撃下における攻撃緩和効果と，それぞれのスループットとモデルにより得られたスループットの計算値の一致率を算出した．今回の評価実験で用いた全てのルータのキューサイズ設定において，従来手法 [7] よりも高い攻撃緩和効果と，モデルと約 90%一致する結果が得られた．評価結果から，本稿で行った改善スループットのモデル化と代理再送の開始タイミングの最適化により，代理再送機構を用いた攻撃緩和手法を改善することができた．

参考文献

[1] Postel, J.: Transmission Control Protocol, RFC 793 (1981).
[2] 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*, pp. 75–86 (2003).
[3] 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).
[4] 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).
[5] Griner, J., Border, J., Kojo, M., Shelby, Z. D. and Montenegro, G.: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations, RFC 3135 (2001).
[6] 児玉拓海，久末瑠紅，稲村　浩，石田繁巳：Low-rate DoS 攻撃の緩和のための代理再送機構の実現性の検討，情報処理学会第 86 回全国大会講演論文集，pp. 3:131–132 (2024).
[7] 児玉拓海，久末瑠紅，稲村　浩，石田繁巳：Low-rate DoS 攻撃を緩和するための代理再送機構の再送タイミング制御，マルチメディア，分散，協調とモバイルシンポジウム 2024 論文集，Vol. 2024, pp. 66–73 (2024).
[8] タネンバウムアンドリューＳ，ウエザロールデイビッドＪ：コンピュータネットワーク 第 5 版，日経 BP 社 (2013).
[9] Paxson, V., Allman, M., Chu, J. and Sargent, M.: RFC 6298: Computing TCP's retransmission timer (2011).
[10] 久末瑠紅，稲村　浩，石田繁巳：攻撃タイミングの誤差を許容する TCP 短時間転送向け Low-rate DoS 攻撃の提案と評価，情報処理学会論文誌， Vol. 65, No. 2, pp. 563–574 (2024).