攻撃タイミングの誤差を許容する短時間通信向け Low-rate DoS 攻撃の提案

久末 瑠紅[1]　稲村 浩[2]　石田 繁巳[2]　中村 嘉隆[3]

概要：近年，マイクロサービスアーキテクチャの普及や通信速度の向上により，対話型トランザクションなどで発生する短時間転送が多く行われている．これに伴い，短時間転送に対する安全性の提供が要求されている．サイバー攻撃の 1 つとして，パルス形状の攻撃トラフィックを用いることで平均帯域利用率が低い Low-rate DoS（LDoS）攻撃が議論されている．LDoS 攻撃に関する既存研究では，FTP などを用いた大容量のデータ転送時に発生する長時間転送を攻撃対象としていた．LDoS 攻撃はパルス形状の攻撃トラフィックを用いるため，転送時間が短い場合には攻撃パルスが攻撃対象トラフィックと衝突する確率が低くなる事が想定される．本研究では，gRPC を用いた短時間で転送が終了する短時間通信を攻撃対象とし，LDoS 攻撃の 1 つである Shrew 手法を用いた攻撃手法の実現性を示す．短時間転送に対する Shrew 手法では，攻撃対象のトラフィックと攻撃トラフィックとの時間差，すなわち攻撃タイミングの誤差が与える影響が大きいことから，この誤差が存在する場合の攻撃効果を高める手法として初期パルス幅拡大 Shrew 手法を提案し，攻撃開始タイミングの誤差許容性能が向上可能であることを示した．

1. はじめに

近年，マイクロサービスアーキテクチャの普及や通信速度の向上により，短時間転送は多く行われている．マイクロサービスとは，ビジネスドメインに基づいてモデル化された独立してデプロイ可能なサービスを意味し，マイクロサービスアーキテクチャでは，複数のマイクロサービスをネットワークを介して連携させ，ユーザが必要とするサービスを提供する [1]．マイクロサービスアーキテクチャでは，マイクロサービスが互いに通信してサービスを実現するため，従来のモノリスティクアーキテクチャと比較し，小容量のデータを高い頻度で転送する必要がある．すなわち，短時間転送の発生頻度が高い．マイクロサービスアーキテクチャは，私たちが日常でも使用する Cookpad，Square，Spotify などのサービスでも実装に用いられており [2–4]，安全性の提供が必要である．

サイバー攻撃の 1 つとして，Low-rate DoS（LDoS）攻撃が議論されている．LDoS 攻撃は，ネットワークのプロトコルで用いられているアルゴリズムを悪用し，パルス波形のトラフィックを用いて攻撃を実現する．具体的には，TCP の再送タイムアウト（RTO）のアルゴリズムを悪用する Shrew 手法 [5]，Loss-based 輻輳制御アルゴリズムを悪用する Reduction of Quality（RoQ）DoS 手法 [6]，HTTP で用いる KeepAlive のメカニズムを悪用する LoRDAS 手法 [7] などがある．いずれの LDoS 攻撃手法においても，パルス形状の攻撃トラフィックを用いており平均帯域利用率が低い．必要十分な攻撃トラフィックのみをネットワーク内 に存在させることで，従来のネットワークベースの DDoS 攻撃検知手法による検知を回避する攻撃の隠蔽性（ステルス性）を持つ．そのため，LDoS 攻撃を受けた場合でも，このステルス性によって被害者が攻撃を認知できないケースも存在する [8]．

これまで，Shrew LDoS 攻撃手法 [5] について，短時間で転送が終了する短時間通信を対象とした議論はあまり成されていない．既存研究では，攻撃対象を FTP などを用いた大容量のデータ転送時に発生する長時間転送としている．LDoS 攻撃は，パルス形状の攻撃トラフィックを用いる．転送時間が短い場合には，攻撃パルスと攻撃対象トラフィックが同時にルータキューに存在する「トラフィックの衝突」を発生させることが難しく，TCP セグメントを損失させる確率が低くなる事が予想される．

攻撃パルス間隔以内に転送が終了してしまう短時間転送トラフィックを攻撃目標とした場合，この短時間の転送期間に攻撃パルスの送信タイミングを合わせられなければ，攻撃パルスが送信されていない間に攻撃目標トラフィックの転送が終了するため攻撃が失敗する．Shrew 手法では，

[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

RTO における再送タイマの初期値 $minRTO$ 秒間隔の攻撃パルスを用いて RTO 処理を連続して発生させる [5]．攻撃パルスを攻撃対象トラフィックと衝突させることで，ルータのキューを溢れさせ対象トラフィックの TCP セグメントを損失させることが可能となる．$minRTO$ は推奨値が 1 秒 [9] であるため，パルス間隔は 1 秒程度となる．攻撃パルス同士の間の期間では攻撃トラフィックが送信されていない．その間隔に全体が収まる程度の長さとなる，例えば 1 秒弱の短時間攻撃対象トラフィックには，タイミングがずれると攻撃トラフィックが衝突しないため，セグメントの損失が発生せず攻撃が失敗することがある．

従って，このような攻撃パルス間隔の期間に転送が終了する短時間転送トラフィックを攻撃目標とした場合には，攻撃パルスの送信タイミングを攻撃目標のトラフィック転送期間に合わせることが攻撃の成否を決定付けることになる．これまでの長時間転送を対象とした攻撃では，目標トラフィックの転送期間に攻撃開始タイミングを合わせる必要がなかった．このことから，長時間転送を攻撃対象としたときと比較し，短時間転送に対する LDoS 攻撃は難しい．しかしながら，日常的に多く発生する短時間転送に対してステルス性が高い LDoS 攻撃が有効である場合，サービスの安全性を低下させる脅威となる．

本研究では，LDoS 攻撃の一種である Shrew 手法に着目し，短時間転送を行う通信に対して有効な攻撃手法を提案する．先に述べた通り，LDoS 攻撃はパルス形状の攻撃トラフィックを用いるため，攻撃パルスと攻撃対象トラフィックを衝突させ，TCP セグメントを消失できる確率が低くなる．つまり，短時間転送に対する Shrew 手法では，攻撃対象のトラフィックと攻撃トラフィックとの時間差，すなわち攻撃タイミングの誤差が与える影響が大きい．この誤差が存在する場合の攻撃効果を高める手法として，初期パルス幅拡大 Shrew 手法を提案する．この手法では，Shrew 手法における一番初めのパルス幅のみを拡大することで，確実に攻撃トラフィックと攻撃対象トラフィックがルータキューに存在する状態にし，TCP セグメントを損失させる．

本稿では，初期パルス幅拡大 Shrew 手法の初期パルスと，許容できる攻撃タイミングの推定誤差の関係性を調査した結果を示す．

本稿の構成は以下の通りである．まず，2 節にて本稿を理解する上で必要となる Shrew 手法の原理について説明する．3 節では従来の Shrew 手法に関する関連研究を示し，4 節で提案する Fawe-Shrew 手法の原理を説明する．5 節で実験的評価を行い，最後に 6 節にてまとめとする．

2. Shrew 手法の原理

本節では，本研究で議論する LDoS 攻撃の 1 つである Shrew 手法について動作原理を述べる．

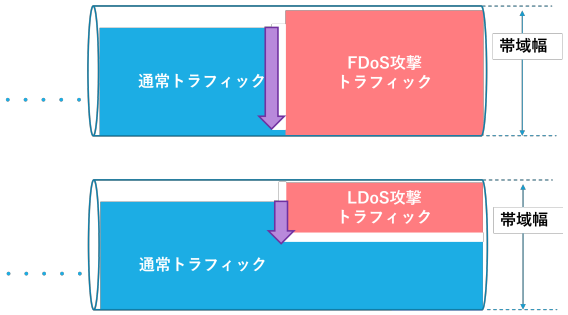

図 1 FDoS 攻撃（上）と LDoS 攻撃（下）の攻撃レートを平均化した帯域利用率の概念図

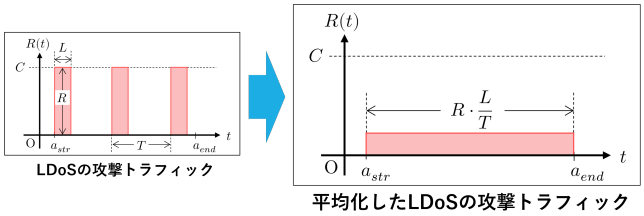

図 2 LDoS 攻撃の RLT モデルと平均化した LDoS 攻撃トラフィック

2.1 DoS 攻撃の概要

DoS 攻撃には，大量トラフィックを送信する Flooding DoS（FDoS）攻撃と，小量の攻撃トラフィックを送信する LDoS 攻撃の 2 種類が存在する．FDoS 攻撃および LDoS 攻撃の攻撃レートを平均化し，帯域利用率としてリンク帯域幅に対比させた概念図を**図 1** に示す．図のように，FDoS 攻撃はリンク帯域幅の 100 %に近い攻撃トラフィックを送信することにより，ネットワークの通信経路で氾濫を引き起こし，正規トラフィックの通信を妨害する．大量トラフィックを送信する FDoS 攻撃に対し，LDoS 攻撃はリンク帯域幅の 10-30 %程度の攻撃トラフィックを送信する．

2.2 LDoS 攻撃のステルス性

LDoS 攻撃は，パルス波形の攻撃トラフィックを用いることで平均帯域利用率を低くし，高いステルス性を有する．

LDoS 攻撃の攻撃トラフィックはパルス波形になっていることから，パルスレート R，パルス間隔 L，パルス幅 T の 3 パラメータを用いてモデル化できる．このモデルを RLT モデルと呼ぶ．RLT モデルを用いて，平均化した LDoS 攻撃の攻撃トラフィックを**図 2** に示す．$R(t)$ は時刻 t 秒時点におけるトラフィックの送信レート，C はボトルネックリンク帯域幅，a_{str} は攻撃開始時刻，a_{end} は攻撃終了時刻とする．区間 $[a_{str}, a_{end}]$ におけるパルス波形の攻撃トラフィックを平均化したトラフィック量 R_{avr} は式 (1) となる．

$$R_{avr} = R \cdot \frac{L}{T} \quad (R \geq C) \tag{1}$$

例えば，$C = R = 10\,\text{Mbps}$，$L = 300\,\text{ms}$，$T = 1000\,\text{ms}$ としたとき，平均レート $R_{avr} = 3\,\text{Mbps}$ となるため，この攻撃トラフィックにおけるボトルネックリンク帯域幅の占有率は 30 %となる．LDoS は低い平均レートで攻撃が可能なため，平均レートが高いことを指標に用いる従来の FDoS 検出機構では LDoS 攻撃の検知が難しい [8]．

2.3 TCP が使用する RTO の仕組み

TCP は，再送処理を時間で制御する再送タイマを使用し，再送タイマ切れを再送タイムアウト（RTO: Retransmission Time Out）と呼ぶ．TCP は，クライアントリクエスト（CR）セグメントを送信した際に再送タイマをスタートさせ，RTO 以内に送信したサーバレスポンス（SR）セグメントの ACK が返ってきた場合，再送タイマをリセットする．Fast Retransmit が失敗した後は，再送タイマによるセグメント再送信が用いられる [10]．

RTO の初期値は RFC6298 [9] により，式 (2) で定義される．

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

ここで，$SRTT$ は平滑化した往復遅延時間（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．RFC6298 [9] では，$minRTO$ の推奨値を 1 秒としている．

TCP 通信において，n 回目の RTO の値 RTO_n は，指数バックオフを用いる式 (3) に定義される．

$$RTO_n = 2 \cdot RTO_{n-1},\ RTO_1 = minRTO \quad (3)$$

RTO の上限値には，一般に 60 秒が用いられている．すなわち，$minRTO = 1$ のとき，$n > 7$ となると，TCP コネクションのタイムアウトが発生する．

指数バックオフを用いた再送タイマ管理アルゴリズムは，明瞭でわかりやすいというメリットをもつが，それゆえに再送タイミングが予測可能という脆弱性を有する．この脆弱性を悪用する攻撃方法が，次で説明する Shrew 手法である．

2.4 Shrew 手法

LDoS 攻撃にはいくつか種類が存在するが，代表的なものとして，TCP を標的とした Shrew 手法がある．”Shrew” という名称は，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 [5] [11]．

Shrew 手法は，シンプルで予測可能な指数バックオフを用いる RTO 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 **3** に示す．攻撃の流れは以下のとおりである．

はじめに，送信者は受信者へ通常トラフィックの転送を開始する．転送開始から数秒後，攻撃者はボトルネックリンク帯域幅 C を満たすレートで攻撃パルスを送信する．送信した攻撃パルスを構成するパケットはルータにキューイングされ，バッファが攻撃トラフィックによって埋め尽くされる．これにより，通常トラフィックに含まれるパケットの損失が発生する．複数のパケットの損失後，送信者による再送タイマを用いた再送処理が行われる．この再送開始の直前に攻撃者が再度攻撃パルスを送信することによってパケット損失を発生させ，さらに RTO を引き起こす．上記のプロセスを複数回繰り返し，TCP コネクションのタイムアウトを発生させる．

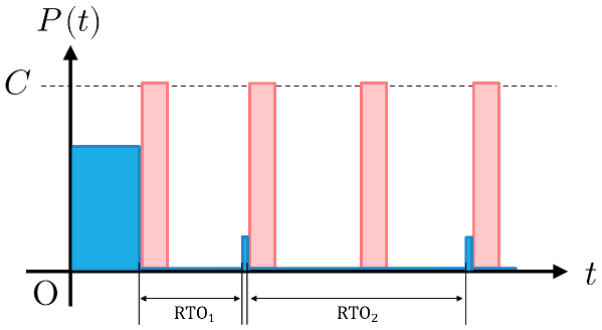

図 **3** Shrew 手法の基本原理

RTO 再送直前に攻撃パルスを送信するためには RTO 再送のタイミングを知る必要があるが，n 回目の再送タイマ待機時間 RTO_n は RTO の初期値である $minRTO$ に依存し，その整数倍のいずれかの位置になる．

以上のことから，バッファサイズを B とし，RLT モデルを用いて表現すると，式 (4) の（i）-（iii）を満たすことで Shrew 攻撃は実現する [5]．

$$\text{(i) } R \geq C, \quad \text{(ii) } L > \frac{B}{R}, \quad \text{(iii) } T = minRTO \quad (4)$$

3. 関連研究

Shrew 手法の攻撃対象トラフィックの転送時間について，既存研究は明示的な仮定を置かず，暗黙に長時間転送を想定したものが殆どである．ここでは，現実に即した攻撃シナリオを議論した研究を例示し，攻撃対象トラフィックの長さへの仮定を確認する．

3.1 クラウドデータセンターネットワークにおける Shrew 手法

本研究で対象とする gRPC が利用される状況として想定される，クラウドデータセンターネットワークに対する Shrew 手法 [14] の適用例を述べる．

クラウドコンピューティングのサービスモデルでは，サービス提供者がテナント（顧客）の必要に応じて仮想マシンを提供する．サーバ上のコンピューティングリソースは仮想マシンを通して分割されるが，ネットワークリソースに

ついてはテナント間で直接共有される形となる．このことから Feng らは，ネットワークリソースがテナント間で共有されるという特性は，Shrew 手法に適していると考えた [14].

データセンターネットワーク（DCN）において，ネットワークのボトルネックリンク帯域幅は動的であり，一過性のものである．そのため，DCN における遅延はノードの経路を示すホップ数を推定するために利用することが難しい．

そこで Feng らは，送信側仮想マシンを送信先までのフロー経路でグループ化する Loss-based アルゴリズムを採用した [14]．中間スイッチバッファを輻輳させるほどフローレートが高い場合，フローパスの論理ホップ数に応じて損失率も単調に増加した．この特性により，同じボトルネックを通過するフローは同じレベルの輻輳が発生するため，バックグラウンドトラフィックの存在にかかわらず，輻輳発生時の損失率に類似する値を記録する．この観測は，どの仮想マシンが同じスイッチの下に存在しているか，あるいは最も長いノードのフロー経路を共有しているか判断するために使用できる．さらに，中間スイッチバッファで輻輳が発生するほどフローレートが高い場合，フロー経路の論理ホップ数に応じて損失率も単調に増加することができる．この観測結果を用いて，どの仮想マシングループが他の仮想マシングループよりも宛先から遠いかがさらに明らかとなる．スイッチが利用できる最大のバッファサイズは，バーストトラフィックを処理するキャパシティと同義となる．そのため，この値をボトルネックリンク帯域幅として扱う．

測定した仮想マシングループのフロー経路とボトルネック帯域幅を用いて，クラウド DCN 内で Shrew 手法を実行した．検証の結果，攻撃対象となった仮想マシンのダウンリンクにおける TCP スループット損失率が最大で 83 %上昇し，クラウド DCN において Shrew 手法は有効攻撃であることが示された．

しかしこの手法では，攻撃ごとにフロー経路の計測とボトルネックリンク帯域幅の計測を行う必要がある．加えて，複数のテナントが存在する DCN で行われる通信データ量は大きい．以上のことから，短時間転送に対する Shrew 手法の実現性については視野に入っていないことがわかる．

3.2 特性が未知のボトルネックリンクに対する分散 LDoS 攻撃の自動化

2 節で述べたとおり，Shrew 手法の実現には，攻撃パルスの送信レートを標的のボトルネックリンク帯域幅以上とする必要がある．すなわち，攻撃対象となるボトルネックリンクの特性が明らかではない場合，攻撃を行うことが難しい．

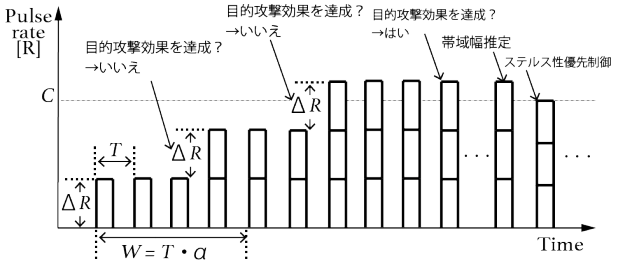

図 4 髙橋のボトルネックリンク帯域幅探索手法による自動分散型 LDoS 手法 [15]

この課題を解決するため髙橋は，探索的にパルスレートを増加させ，理想攻撃レートを算出し攻撃を行う手法を考案した [15]．多くの場合，攻撃者は攻撃対象のボトルネックリンク帯域幅を知らない．Shrew 手法を行う際に，攻撃レートが不十分であれば十分な攻撃効果は発揮できず，攻撃レートが大きすぎる場合にはステルス性を失ってしまう．つまり，LDoS 攻撃成功に必要な攻撃トラフィックレートで攻撃することは困難である．

攻撃に必要な情報であるボトルネックリンク帯域幅を取得するため，まず標的ネットワーク内にボットノードを構築し，攻撃効果を測定可能とする．

次に，初期パルスレート ΔR をボトルネックリンク帯域幅より低くなるよう攻撃トラフィックを送信する．ボットノードで観測した攻撃効果を用いて，目標攻撃効果が得られるまで ΔR ずつ加算される（図 **4**）．

この手法では，攻撃者が攻撃に必要なネットワークパラメータを把握する必要なく攻撃を実現できる．しかし，理想的な攻撃パルスレートの探索工程は平均で 60 秒程度を必要としており，本研究で取り扱う短時間転送については考慮されていない．

3.3 既存研究の課題

既存研究では，攻撃対象となる通常トラフィックの転送時間は長期のものであった．

Shrew 手法は, 攻撃パルスを RTO 初期値である $minRTO$ 秒間隔で連続送信し，RTO を発生させる．そのため，パルス間隔 T よりも転送時間が短いトラフィックに対して攻撃パルスの送信タイミングが合わせられなかった場合，RTO が発生せず Shrew 攻撃が失敗する．

筆者らの調査した範囲では，対話型トランザクションなどで発生しうる短時間転送を攻撃対象とし，Shrew 手法による LDoS 攻撃を実施している研究は，これまでのところ報告されていない．本研究では，攻撃開始タイミングの誤差許容性能を向上させる手法を提案する．

4. 初期パルス幅拡大 Shrew 手法

短時間転送に対して Shrew 手法を用いる場合，攻撃対象トラフィックに攻撃開始タイミングを合わせることができ

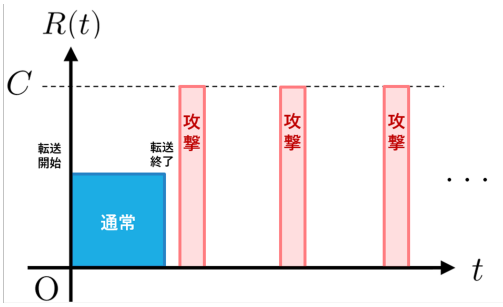

図 5　攻撃開始タイミングの推定に誤差が生じたとき，Shrew 手法は攻撃失敗

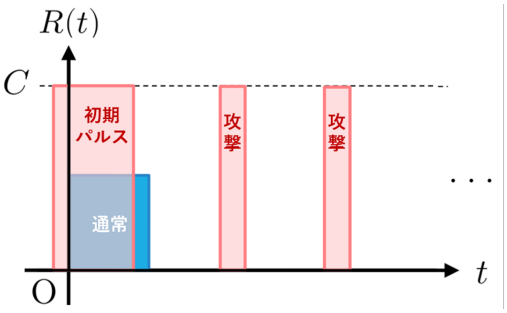

図 6　攻撃開始タイミングの推定に誤差が生じたとしても，誤差を許容可能

るかが課題となる．しかしながら，現実世界に存在する攻撃対象の環境を考えると，正確な攻撃開始タイミングを推定できるよう通信を監視することは難しい．

本研究では，攻撃の初期パルスのみパルス幅を拡大させることで，攻撃開始タイミング誤差のカバーを可能にする初期パルス幅拡大 Shrew（Fawe-Shrew: First Attack-pulse Width Expansion Shrew）手法を提案する．

4.1　従来の Shrew 手法における攻撃開始タイミング合わせの重要性

攻撃パルス間隔の期間に転送が終了してしまう短時間転送トラフィックを攻撃目標と想定したときのトラフィックを図 5 に示す．この図は，時刻 t における攻撃対象トラフィック（青）と攻撃トラフィック（赤）の転送トラフィック量を表している．図の通り，この攻撃目標の短時間転送トラフィックの転送期間に攻撃パルスの送信タイミングを合わせることに失敗してしまうと，攻撃パルスが送信されていない間に攻撃目標の転送が終了してしまい，攻撃が失敗することになる．

3 節で述べた通り，Shrew 手法は $minRTO$ 秒間隔で攻撃トラフィックを送信する．そのため，攻撃トラフィックによってルータのバッファが埋め尽くされる前に転送が完了した場合，RTO 処理が発生せず攻撃効果を得ることができない．従って，このような攻撃パルス間隔の期間に転送が終了してしまう短時間転送トラフィックを攻撃目標とした場合には，これまでの長時間転送を対象とした攻撃では問題になっていなかった，攻撃パルスの送信タイミングを攻撃目標のトラフィックの転送期間に合わせることが攻撃の成否を決定付けることになる．

4.2　攻撃開始タイミングの推定に関する課題

昨今，通信内容が暗号化され攻撃対象の通信内容を傍受することは一般に難しいが，TLS が用いられている場合，TCP のヘッダ情報をもとに 3 ウェイハンドシェイク（HS）処理の実行を検知することは，通信内容傍受と比較し実現可能性が高い．セッションタイムアウトなどの要因によってコネクションを再確立する際に HS 処理が行われていることを検知することは可能である．実際に，アクティブセッションハイジャックという攻撃手法では，この特性を悪用して攻撃を実行している [12]．つまり，攻撃開始タイミングの推定方法の 1 つとして HS 処理を攻撃開始のトリガーとして使用可能であることがわかる．

しかしながら，HS 処理を攻撃開始タイミングの推定に用いる場合には，通信環境におけるレイテンシや HS 処理後に実際が送信されるまでの処理時間などの影響で，図 5 のように，実際の攻撃開始タイミングとズレてしまう可能性がある．推定攻撃タイミング誤差の大きさは環境によって異なる上に，正確な攻撃開始タイミングを知ることは攻撃対象のシステム管理者でない限り困難である．

4.3　攻撃開始タイミング推定の誤差許容性能を向上させる提案手法

本研究では，短時間転送への攻撃有効性向上を目的に，攻撃開始タイミング推定の許容誤差性能を向上させる Fawe-Shrew 手法を提案する．

図 6 に，短時間転送トラフィックを攻撃目標と想定し，Fawe-Shrew 手法を用いて攻撃を実施した際のトラフィックを示す．この図は，時刻 t における攻撃対象トラフィック（青）と攻撃トラフィック（赤）の転送トラフィック量を表している．Fawe-Shrew 手法は，攻撃対象トラフィックに対するタイミング誤差の許容幅を拡大するため，最初の攻撃のみパルス幅の大きいトラフィックを発生させる．幅の大きい初期パルスを用いることで，推定攻撃開始タイミングに多少の誤差が生じたとしても攻撃対象トラフィックに攻撃トラフィックが衝突し，より確実に RTO による再送処理を発生させることが可能となる．すなわち，攻撃対象トラフィックに対する攻撃トラフィックの正確なタイミング同期をせずとも攻撃を実現できる．

初期パルスによる攻撃成功後は RTO 処理が発生するため，$minRTO$ 秒間隔での短時間パルスによる攻撃という従来の Shrew 手法と同様の攻撃を行う．これにより，ステルス性を維持したまま短時間転送に対しての攻撃効果を高めることが可能となる．

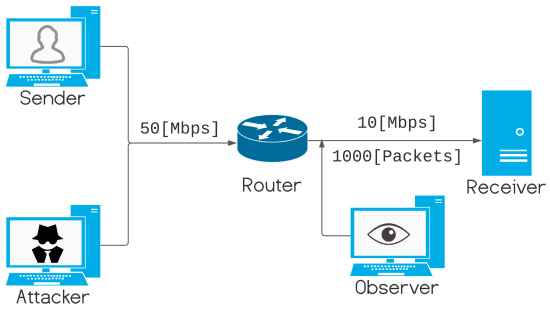

図 7　実験環境

本稿では，Fawe-Shrew 手法における初期パルス幅と許容誤差の関係性を明らかにすることを目的に，初期パルス幅ごとに許容できる攻撃タイミングの推定誤差を調査した結果を示す．

5. 評価

本節では，提案手法の短時間転送に対する有効性を示すため行った実験的評価の結果を述べる．まず，5.1, 5.2 にて実験に使用した環境や条件を述べる．5.3 にて，従来の Shrew 手法において問題であった，攻撃タイミングの誤差による RTO 発生頻度の変化により，転送時間が短いほど RTO 発生回数が減少し，攻撃効果も低下することを明らかにする．最後に，5.4 にて提案手法を用いて初期パルス幅を延伸することで，推定攻撃開始タイミングの許容誤差を拡大できることを示す．

5.1 評価環境

実験には，**図 7** に示したネットワークトポロジを用いた．Sender は Router を経由して Receiver にデータを転送する．Shrew 手法では，ボトルネックリンクに対して瞬発的に大量トラフィックを送信し，Router のバッファを埋める必要がある．Router をボトルネックリンクとするため，Sender 側のネットワーク帯域幅を 50 Mbps，Receiver 側の 10 Mbps と設定している．加えて，ルータがキューイングできるパケット数を 1000 パケットに制限した．帯域幅およびキューイングするパケット数の制限には，Linux の tc コマンド [13] を用いた．Attacker は，Router 方向に攻撃パルスを送信し，Router のキューを占有する．

各エンティティで用いた機材およびプロトコルを**表 1** および**表 2** に示す．本実験の Sender および Receiver のアプリケーション層では，マイクロサービスアーキテクチャにて対話型トランザクションを行う際に用いられている gRPC を使用した．gRPC はトランスポート層で TCP を用いており，パルス形状の攻撃トラフィックを用いて RTO 処理を発生させることが可能である．

無負荷の状態での Sender と Reciever 間の RTT 平均値は 0.977ms である．

表 1　各エンティティで使用した機材

Entity	OS	CPU
Sender	Raspberry Pi OS	ARM Cortex-A53
Receiver	Raspberry Pi OS	ARM Cortex-A53
Router	OpenWRT	Intel(R) Core(TM) i7-10700
Attacker	Raspberry Pi OS	ARM Cortex-A53
Observer	Debian	Intel(R) Celeron(R) J4125 CPU

表 2　各エンティティで使用したプロトコル

Entity	ネットワーク層	トランスポート層	アプリケーション層
Sender	IP	TCP	gRPC
Receiver	IP	TCP	gRPC
Router	IP	-	-
Attacker	IP	UDP	-
Observer	IP	TCP	-

5.2 攻撃効果の定義

攻撃対象トラフィックについて，攻撃なしのときに占有できた平均スループット T_{normal} と，攻撃下での平均スループット $T_{onAttack}$ を用いて，攻撃効果 E を式 (5) と定義した．

$$E = 1 - \frac{T_{onAttack}}{T_{normal}} \times 100\ [\%] \qquad (5)$$

E は攻撃による攻撃対象トラフィックのスループットの低下率を示しており，$E = 100\,\%$ であれば対象の通信が完全に遮断されていることを表す．

5.3 従来の Shrew 手法における攻撃タイミングの誤差による RTO 発生頻度の変化

従来の Shrew 手法を短時間転送に適用した場合，長時間転送を攻撃対象とした場合と比べると，RTO の発生頻度は少なく攻撃効果は低いことが予想される．これは，攻撃パルス間隔で攻撃対象が通信を完了したとき，攻撃対象トラフィックに攻撃トラフィックが衝突しない可能性があるためである．つまり，短時間転送部分においては RTO 発生頻度が低いが，連続的に転送時間を伸ばしていくと，RTO 発生頻度の上昇が観測されるはずである．

上記について確認するには，転送データサイズを変えた試行を行う必要がある．攻撃タイミングのずれによって発生する RTO 発生頻度の変化について調査するため，図 7 に示す実験環境にて，攻撃開始タイミングを攻撃対象トラフィックの転送開始から 1.0 秒後とし，1-5 MB の 5 パターンのサイズのデータ転送に対して従来の Shrew 手法で攻撃を行う実験を 200 回繰り返し検証した．

各転送試行に対して，従来手法による攻撃で発生した RTO 回数を転送データサイズごとに集計し，1 MB あたりで示した結果を**表 3** に示す．平均転送時間が 0.94 秒となる 1 MB のデータ転送時には，転送終了付近から攻撃トラフィックの送信を開始されているケースが含まれているた

表 3　各転送データサイズにおける 1 MB あたりの RTO 発生頻度

size[MB]	RTO 発生回数 [回]
1	5.75
2	27.22
3	28.94
4	29.69
5	29.57

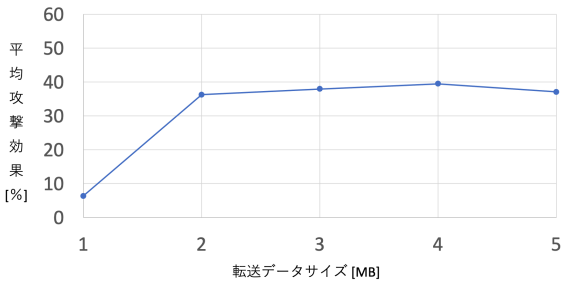

図 8　各転送データサイズにおける攻撃効果の平均値

め，RTO 発生回数が減少している．加えて，平均転送時間が 1.81 秒となる 2 MB のデータを転送した際には，1 MB のデータ転送時と比較し RTO 発生回数が 4.73 倍に上昇していることが確認できる．言い換えると，攻撃開始タイミングよりも遅く初期攻撃パルスを送信し，転送時間が短い場合には RTO 発生回数が低くなるが，転送時間が長く攻撃トラフィックが初期パルスに衝突した場合には RTO 発生回数が多くなることを確認できた．

各データサイズにおける攻撃効果 E の平均値をプロットした折れ線グラフを**図 8** に示す．転送データサイズが 1 MB のとき，攻撃効果 E の平均値は 10 %に満たないが，2 MB 以上においては 40 %程度の攻撃効果を記録している．

以上のことから，転送時間が短いほど攻撃トラフィックと攻撃対象トラフィックのタイミング誤差が RTO 発生回数が減少し，攻撃効果も低下することが明らかとなった．すなわち，長時間転送を攻撃対象としたときと比較し，短時間転送を対象とした際には攻撃成功の難易度が高いことがわかる．

5.4　パルス幅ごとの攻撃許容タイミング誤差許容性能

従来の Shrew 手法と比較したとき，提案手法によって初期パルス幅を延伸することで，推定攻撃開始タイミングの許容誤差の拡大が予想される．先ほど確認した通り，Shrew 手法の攻撃トラフィックはパルス形状になっている特性から，パルス間隔に攻撃対象トラフィックが転送された場合には RTO 発生頻度が低下し，攻撃効果が低下する．提案手法は，攻撃開始タイミングに多少の誤差があっても，初期パルス幅が延伸されていることから攻撃対象トラフィックに攻撃トラフィックを当てる確率を高めることが可能である．本手法によって攻撃効果が担保される範囲を理解するには，パルス幅ごとに攻撃開始タイミングをずらして外来の誤差を含ませ，本手法の制御パラメータである初期パルス幅を変化させたとき，攻撃効果がどのように変化するか確認する必要がある．

そこで，提案する Fawe-Shrew 手法による攻撃開始タイミング誤差の許容性能を評価するため，実験による評価を行った．Fawe-Shrew 手法にて初期パルス幅は 0.5, 1.0 秒の 2 パターンで試行し，一般的な Shrew 手法を用いた場合（すなわち，初期パルス幅が 0.3 秒である場合）と比較し，各パルス幅における許容誤差を検証した．

Sender から Receiver への攻撃対象トラフィック発生時刻を $t = 0$ として，タイミング合わせの誤差を表すため，時刻 $t = \Delta t$ に Attacker からの攻撃を開始した．攻撃パルスのレートは帯域幅である 10 Mbps，幅はルータのバッファを埋めるのに十分な 0.3 秒とし，攻撃開始後は 1 秒間隔で攻撃パルスを発生させた．攻撃の初期パルス幅 $L_i = 0.3, 0.5, 1.0$ 秒のそれぞれについて，Δt を -1.0 から 1.0 秒まで変化させ攻撃を行った．試行回数は各条件下で 100 回である．スループットの低下率を示す攻撃効果 $E = 70\,\%$ を目標値とし，目標値を満たした試行割合で攻撃タイミング誤差の許容性能を評価した．

Δt に対するパルス幅ごとの目標攻撃効果達成率を**図 9** に示す．初期パルス幅 $L_i = 0.3$ における目標攻撃効果達成率のピーク値 10 %を閾値とし，各初期パルス幅 L_i における閾値を超える Δt の最小値 Δt_{min} と最大値 Δt_{max} を用いて，許容誤差性能 D を式 (6) と定義した．

$$D = \Delta t_{max} - \Delta t_{min} \tag{6}$$

パルス幅ごとの許容誤差性能 D を**表 4** に示す．

従来の Shrew 手法による達成率のピーク値 10 %は，区間 $(0.0, 0.2)$ の一部でしか達成していない．達成率 10 %を閾値とすると，Fawe-Shrew 手法にて初期パルス幅 $L_i = 0.5$ のときは区間 $[-0.1, 0.4]$ で達成しており，初期パルス幅 $L_i = 1.0$ のときは区間 $[-0.5, 0.8]$ まで拡大している．すなわち，攻撃開始タイミングの許容誤差性能 D は，$L_i = 0.5$ のときは 0.5 秒，$L_i = 1.0$ のときは 1.3 秒まで向上した．

加えて，従来の Shrew 手法と比較し，初期パルス幅を拡大した Fawe-Shrew 手法の目標攻撃効果達成率は区間

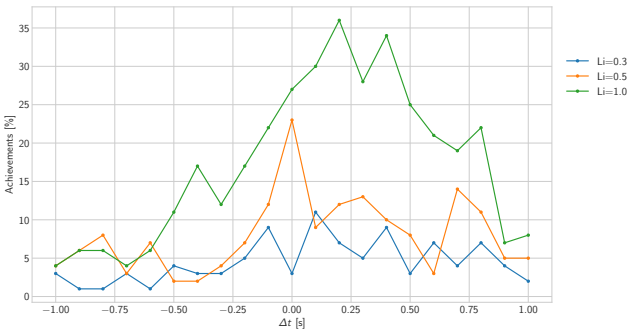

図 9　攻撃タイミング誤差 Δt における目標攻撃効果の達成率

表 4　初期パルス幅ごとの許容誤差性能

初期パルス幅 L_i	Δt_{min}	Δt_{max}	許容誤差性能 D
0.3	0.10	0.10	0.00
0.5	−0.10	0.40	0.50
1	−0.50	0.80	1.30

$[-0.5, 1.0]$ にて明らかに上昇していることが確認できる．提案する Fawe-Shrew 手法では，バッファを攻撃トラフィックで占領している時間が延長され，RTO 発生回数が上昇したからと考えられる．

以上のことから，提案した Fawe-Shrew 手法に初期パルス幅を拡大することで，表 4 のとおり攻撃開始タイミングの誤差許容性能を向上可能であることが明らかとなった．

6. おわりに

本稿では，従来の Shrew 手法では対応が難しかった短時間で転送が終了する短時間通信に対して，初期パルス幅を拡大し攻撃開始タイミングの誤差許容性能を向上させる Fawe-Shrew 手法を提案した．Fawe-Shrew 手法の誤差許容性能を検証するため，従来の Shrew 手法である初期パルス幅 $L_i = 0.3$ と，拡大した初期パルス幅 $L_i = 0.5, 1.0$ の 3 パターンにおいて，攻撃開始タイミングと攻撃対象トラフィックの転送開始タイミングをずらし，目標攻撃効果 $E > 70\,\%$ の達成率を用いて評価した．評価結果より，提案した Fawe-Shrew 手法に初期パルス幅を拡大することで，攻撃開始タイミングの誤差許容性能を向上可能であることが明らかとなった．

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] James Lewis, Martin Fowler.: Microservices - a definition of this new architectural term, https://martinfowler.com/articles/microservices.html (閲覧日: 2022/05/22).
[2] mineroaoki.: クックパッド基幹システムの microservices 化戦略 〜お台場プロジェクト 1 年半の軌跡〜, https://techlife.cookpad.com/entry/2018-odaiba-strategy (閲覧日: 2022/05/22)
[3] Kevin Goldsmith.: Microservices at Spotify, https://www.slideshare.net/kevingoldsmith/microservices-at-spotify (閲覧日: 2022/05/22)
[4] Snow Pettersen.: The Road to an Envoy Service Mesh, https://developer.squareup.com/blog/the-road-to-an-envoy-service-mesh/ (閲覧日: 2022/05/22)
[5] 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, pp. 75–86 (2003).
[6] M. Guirguis, A. Bestavros, and I. Matta.: Exploiting the transients of adaptation for RoQ attacks on Internet resources, in Proc. 12th IEEE Int. Conf. Netw. Protocols (ICNP), pp. 184–195 (2004).
[7] E. Adi, Z. Baig, C. P. Lam, and P. Hingston, Low-rate Denial-of-service attacks against HTTP/2 services, in Proc. 5th Int. Conf. IT Converg. Secur. (ICITCS), pp. 133–139 (2015).
[8] W. Zhijun, L.Wenjing, L. Liang, and Y. Meng.: Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey, IEEE Access, 8, pp. 43920–43943 (2020).
[9] V.Paxson, M.Allman, J.Chu, M.Sargent.: Computing TCP's Retransmisson Timer, https://datatracker.ietf.org/doc/html/rfc6298 (閲覧日: 2022/05/22).
[10] アンドリュー・S・タネンバウム, デイビッド・J・ウエザロール (訳: 水野忠則, 相田仁, 東野輝夫, 太田賢, 西垣正勝, 渡辺尚), コンピュータネットワーク 第 5 版, 日経 BP 社 (2013).
[11] 髙橋佑太, 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, 修士論文 (2020).
[12] A. Baitha and S. Vinod.: Session Hijacking and Prevention Technique, International Journal of Engineering & Technology, 7-2.6, pp. 193-198 (2018).
[13] man7.org, tc(8) - Linux manual page, https://man7.org/linux/man-pages/man8/tc.8.html (閲覧日: 2022/05/22)
[14] Z. Feng, B. Bai, B. Zhoa, J. Su.: Shrew Attack in Cloud Data Center Networks, 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks, pp.441-445 (2011).
[15] Y. Takahashi, H. Inamura, Y. Nakamura.: A Low-rate DDoS Strategy for Unknown Bottleneck Link Characteristics, 19th IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2021, Kassel, Germany, March 22-26, pp.508-513 (2021).