情報処理学会論文誌 Vol.65 No.2 563–574 (Feb. 2024)

推薦論文

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

久末 瑠紅[1,a)] 稲村 浩[2] 石田 繁巳[2]

受付日 2023年6月2日, 採録日 2023年11月7日

概要：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，攻撃トラフィックをパルス形状にすることで平均帯域使用率を低くし，攻撃検知機構による検知を回避するステルス性を持つ．しかし，攻撃対象トラフィックが 1 秒にも満たない短時間に転送完了すると，攻撃トラフィックと衝突する確率が低くなることが想定される．そのため，攻撃者は攻撃開始タイミングのずれが生じても攻撃を実現できる新たな方法で LDoS 攻撃を実行する可能性が考えられる．本論文では，攻撃の初期パルス幅を拡大することで，トラフィック衝突を起こしうる攻撃開始タイミングの許容誤差性能を向上させる初期パルス幅拡大 Shrew（Fawe-Shrew; First-Attack Pulse Width Expansion Shrew）手法を提案し，提案手法を用いた攻撃による TCP スループット低下条件をモデル式として定式化した．実機を用いた実験用ネットワーク環境下において，提案手法を用いた際の許容誤差性能を計測し，モデル式から算出した予測値とよく一致していることを示した．さらに，従来手法と比較し，提案手法が短時間転送に対する有効性が高いことを明らかにした．

キーワード：Low-rate DoS 攻撃，再送タイマ，短時間転送，タイミング誤差，ネットワークセキュリティ

Evaluation of a Low-rate DoS Attack Method against TCP Short Transfer with Attack Timing Skew

Ryuku Hisasue[1,a)] Hiroshi Inamura[2] Shigemi Ishida[2]

Received: June 2, 2023, Accepted: November 7, 2023

Abstract: Low-rate DoS (LDoS) attacks are one of the cyber attacks. LDoS attacks are stealthy and evade detection methods using pulse-shaped attack traffic, which lowers the average bandwidth utilization. However, the probability of traffic collisions with the targeted traffic is low when the targeted transfer time is short. Therefore, attackers might execute a new LDoS attack method that can attack even if there is a timing skew in the attack start timing sacrificing stealthiness. In this paper, we propose the First-Attack Pulse Width Expansion Shrew (Fawe-Shrew) method that improves the timing skew tolerance of the attack start timing by expanding the initial pulse width, and formulated a model equation for throughput degradation conditions using the proposed method. We measured the timing skew tolerance performance of the proposed method in a test-bed network, and showed that it is in good agreement with the predictions calculated from the model equations. Furthermore, the proposed method is more effective for short transfers than the conventional methods.

Keywords: Low-rate DoS attack, retransmission timer, short transfers, timing skew, network security

1. はじめに

2003 年から，パルス形状の攻撃トラフィックを用いて

[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
Graduate School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido 041–8655, Japan
[2] 公立はこだて未来大学 システム情報科学部
School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido 041–8655, Japan
[a)] g2122054@fun.ac.jp

本論文の内容は 2022 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO2022）シンポジウムで報告され，モバイルコンピューティングと新社会システム研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

通信品質を低下させる LDoS（Low-rate DoS）攻撃がサイバー攻撃の 1 つとして議論されている．LDoS 攻撃はパルス形状のトラフィックを用いることで，大量トラフィックを用いて攻撃する従来の FDoS（Flooding DoS）と比較し平均帯域使用率が低く，ネットワークベース FDoS 攻撃検知機構による検知を回避する攻撃のステルス性を持つ．このステルス性によって，LDoS 攻撃を受けた場合でも被害者が攻撃を認知できないケースが存在する [1]．攻撃被害報告が少ないことや研究途上であることから，LDoS 攻撃手法についてまだ明らかになっていないことがいくつか存在する．そのうちの 1 つが，短時間転送に対する LDoS 攻撃の実現性である．

これまで，著者らの知る限り，TCP を用いた 1 秒未満の短時間転送に対する LDoS 攻撃について議論がなされていない．既存研究 [2], [3], [4], [5], [6], [7], [8], [9] では，FTP などで大量トラフィックを送信する際に発生する長時間転送を攻撃対象としていた．

LDoS 攻撃では，攻撃トラフィックと攻撃対象トラフィックの両方が同時にルータキューに存在する**トラフィック衝突**を発生させ，輻輳状態を引き起こし TCP セグメントを損失させる必要がある．攻撃対象の TCP コネクションに対し，プロトコルの脆弱性を悪用可能な周期でリンク帯域幅以上の攻撃トラフィックを瞬間的に送信することにより，平均帯域使用率を下げ，検知機構から回避するステルス性を保ちながら攻撃することを実現している．

しかし，転送時間が 1 秒にも満たない短時間転送が攻撃対象である場合，正確なタイミング推定ができなければトラフィック衝突を発生させることが難しい．LDoS 攻撃は，ステルス性を維持することを目的にパルス形状の攻撃トラフィックを用いる特性を持つ．**図 1** に示すように，攻撃パルスのタイミングを短い転送周期に合わせられない場合，攻撃トラフィックを送信する前に攻撃対象の転送が完了したり，攻撃のパルス間を正規トラフィックが通過したりする可能性が考えられる．すなわち，攻撃対象が短時間転送を行う場合には攻撃開始タイミングの推定が必要となる．

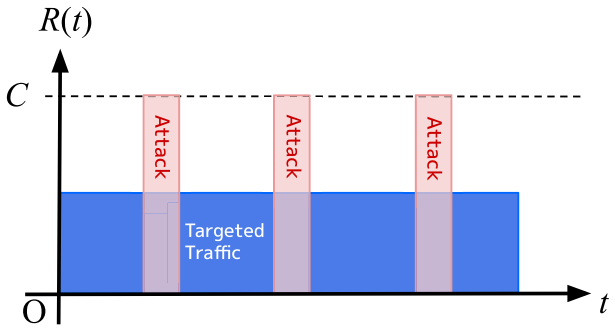
一般に，通信内容は暗号化されているため，攻撃者が通信内容を傍受し攻撃開始タイミングの推定に利用することは困難である．攻撃開始タイミングを推定する方法の 1 つとして，暗号化がなされない接続確立処理のセグメントを用いることが考えられる．多くの通信で利用されている TLS を利用する場合，TCP ヘッダ情報から 3 ウェイハンドシェイク（3WHS; Three-Way HandShake）処理の実行を検知することは，通信内容を傍受するよりも実現可能性が高い．たとえば，セッションタイムアウトによる接続の再確立時に 3WHS 処理を検出することが可能であり，アクティブセッションハイジャックと呼ばれるサイバー攻撃手法ではこの特性を利用して攻撃を実現している [10]．

3WHS 処理などを用いて攻撃開始タイミングを推定する場合，推定したタイミングには誤差が含まれることが考えられる．先行研究 [11] で，タイミング推定の誤差を考慮せずに実験を行ったところ，結果に大きく揺らぎが発生していることが確認できた．これは，通信環境における遅延や 3WHS 処理から送信されるまでの処理時間などにより，実際の攻撃開始タイミングとずれが生じている可能性が高い．

以上のことから，短時間転送が攻撃対象である場合，攻撃パルスの送信タイミングを攻撃対象のトラフィック転送周期に合わせることが攻撃の成否を左右するが，LDoS 攻撃が成功する適切なタイミングを推定することは難しい．そのため，攻撃者は攻撃開始タイミングのずれが生じても攻撃を実現できる新たな方法で LDoS 攻撃を実行する可能性が考えられる．

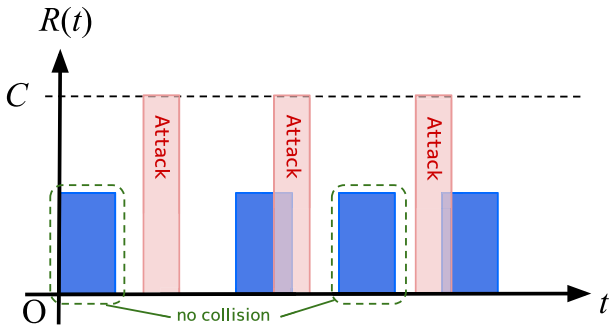
本研究は，従来の LDoS 攻撃手法に比べ短時間転送に対する攻撃の実現可能性が高い新たな LDoS 攻撃手法を提案し，提案手法を用いた攻撃による影響の程度をより正確に評価することで，防御につなげることを目的としている．

本論文では，攻撃の初期パルス幅を拡大することで，トラフィック衝突を起こしうる攻撃開始タイミングの許容誤差



(a) 長時間転送に対する攻撃

(a) Attacking against long transfers



(b) 短時間転送に対する攻撃

(b) Attacking against short transfers

図 1 時刻 t における攻撃対象である正規トラフィックと攻撃トラフィックの送信レート．長時間転送では攻撃のタイミング推定が不要だが (a)，短時間転送では必要 (b)

Fig. 1 Targeted traffic and attack traffic rate at time t. (a) When the target is long transfers, timing estimation is not required, though (b) the estimation is required for short transfers.

性能を向上させる初期パルス幅拡大 Shrew（Fawe-Shrew; First-Attack Pulse Width Expansion Shrew）手法を提案し，そのモデルで攻撃の成功条件を示した．筆者らはこれまでに，攻撃の初期パルス幅を拡大することで攻撃開始タイミングの許容誤差性能を向上させることができることを確認した [12]．本論文では文献 [12] を拡張し，提案手法を用いた際のトラフィック衝突発生条件を解析的に導出したうえで，導出したトラフィック衝突発生条件に基づいて予測される攻撃効果について検証する．

本論文のコントリビューションは次の 2 点である：

- 短時間転送向けの LDoS 攻撃手法である Fawe-Shrew 手法を提案し，提案手法を用いた攻撃による TCP スループット低下条件をモデル式として定式化した．
- 実機を用いた実験用ネットワーク環境下において，提案手法を用いた際の許容誤差性能を計測し，モデル式から算出した予測値とよく一致していることを示した．さらに，従来手法と比較し，提案手法が短時間転送に対する有効性が高いことを明らかにした．

本論文の構成は次のとおりである．1 章で背景と目的を示した．2 章では，関連研究を示し，既存の Shrew 手法に注目する．3 章では，攻撃開始タイミングの許容誤差性能を向上させる提案手法の原理を述べる．4 章では，許容誤差性能の評価方法を説明し，その結果について議論する．最後に，5 章でまとめとする．

2. 関連研究

本章では，まず既存の LDoS 攻撃手法を紹介し，Shrew 手法に基づいて提案手法を考案した理由を述べる．次に，Shrew 手法を用いた LDoS 攻撃の既存手法について述べ，本研究の位置付けを明らかにする．

2.1 既存の LDoS 攻撃手法

DoS 攻撃は，大量トラフィックを使用する FDoS 攻撃と，少量のトラフィックを使用する LDoS 攻撃の 2 つに分類される．FDoS 攻撃は通信帯域を占領できるほどの大量のトラフィックを攻撃対象に対し送信するため検知が容易である．しかし，LDoS 攻撃はパルス状の攻撃トラフィックを使用し平均帯域使用率を下げることで，攻撃検知機構による検知を回避するステルス性を有する [1]．

TCP を攻撃対象とする LDoS 攻撃手法として，再送タイムアウト（RTO; Retransmission Time Out）の再送タイマ管理アルゴリズムを悪用する Shrew 手法 [2]，Loss-based 輻輳制御アルゴリズムを悪用する RoQ 手法 [3]，RTO の再送タイマアルゴリズムと Loss-based 輻輳制御アルゴリズムの両方を悪用する FB-Shrew 手法 [5] があげられる．いずれの LDoS 攻撃手法もパルス状の攻撃トラフィックを使用するため，平均帯域利用率を低く抑えることができ，ステルス性を高めている [1]．

FB-Shrew 手法では，RTO と輻輳制御アルゴリズムの両方を悪用することで，従来の Shrew 手法よりもパルス周期を長くしステルス性を向上させている [5], [6]．文献 [4] では，パルス周期が 5 秒より長い場合は RoQ 手法，5 秒より短い場合は Shrew 手法と分類している．短時間転送を攻撃対象として考えた場合，パルス周期が長いほど攻撃の実現が困難になることが予想される．そこで，パルス周期が最も短い Shrew 手法に基づき，短時間転送に対する LDoS 攻撃手法を考案した．

2.2 Shrew 手法における攻撃メカニズム

Shrew 手法では，TCP が再送制御で用いる再送タイマ管理アルゴリズムが有している周期性を悪用して攻撃する．

TCP では，再送タイマ切れを RTO といい，RTO の初期値 $minRTO$ は RFC6298 [13] により，次の式で設定される：

$$minRTO = SRTT + \max(G, 4 \times RTTVAR) \tag{1}$$

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，$RTTVAR$ は RTT の平均偏差である．

式 (1) で定義される $minRTO$ は，コンピュータスペックに影響を受け，値が変化する．この問題を解決するため，RFC6298 では，$minRTO$ の値を定数にすることを推奨しており，多くの場合で

$$SRTT + \max(G, 4 \times RTTVAR) < 1 \tag{2}$$

が成り立つため，$minRTO$ の推奨値を 1 秒としている [13]．

TCP 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次の式に定義される：

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

なお，RTO の上限値は 60 秒に制限されている．すなわち，$minRTO = 1$ のとき，$n > 7$ となると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，明瞭で分かりやすいというメリットを持つが，再送タイミングに予測可能な規則性が存在する．

Shrew 手法は，多くの場合に $minRTO$ が 1 秒という定数に設定されている特性を悪用し，1 秒周期で 0.2–0.3 秒程度の攻撃トラフィックを送信することによって，再送開始のタイミングに合わせて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衝突状態を発生させ，通信品質を低下させる [1], [2]．

Shrew 手法において，トラフィック衝突により輻輳を発生させるためには，攻撃トラフィックレートがボトルネックリンク帯域幅よりも大きい必要がある [1], [2]．攻撃トラ

フィックレートがボトルネックリンク帯域幅よりも小さい場合，リンク帯域幅に余裕があり通常セグメントが通過可能な状態となる．これにより，セグメントに含まれるACKの値が更新され，RTOによる再送制御が発生せず攻撃効果が低くなる．この特性から，Shrew手法を用いて攻撃する際にはボトルネックリンク帯域幅より高いレートの攻撃トラフィックを用いる．

2.3 Shrew手法を用いたLDoS攻撃

はじめに，一般的なShrew手法の攻撃対象としてあげられ，短時間転送と長時間転送の両方が多く行われるクラウドデータセンタネットワークに対するShrew手法の適用例 [7] 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がShrew手法に適していると考えた [7]．

データセンタネットワーク（DCN; Data Center Network）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における遅延をノードの経路を示すホップ数の推定に利用することは困難である．

そこで，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 [7]．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手法は有効な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り，それらの計測には時間を要するため，攻撃対象が短時間転送である場合攻撃を成功させることが難しいと考えられる．つまり，短時間転送への攻撃の可能性やその課題に言及されていないことが課題である．

次に，ボトルネックリンク帯域幅の計測手法に関し，LDoS攻撃の自動化の研究 [8] について述べる．

2.2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．Shrew手法を行う際に，攻撃レートが小さすぎる場合には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．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ため，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．

この課題を解決するためTakahashiらは，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 [8]．はじめに，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，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，攻撃のパルスレートR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Rを加算する．

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．

2.4 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$minRTO$秒周期で連続送信し，RTOによる再送処理を発生させる．そのため，パルス周期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再送処理が発生せず攻撃が失敗する．

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許容誤差性能を向上させる手法を提案する．

3. 初期パルス幅拡大 Shrew（Fawe-Shrew）手法

短時間転送に対して従来の 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において，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．

この課題を解決するため，本研究では攻撃の初期パルス幅のみを拡大させることで攻撃開始タイミング誤差を許容可能とする「初期パルス幅拡大 Shrew（Fawe-Shrew; First-Attack Pulse Width Expansion Shrew）手法」を提案する．

本章では，提案手法を用いた際にトラフィック衝突が発生する条件を導出したうえで，発生条件をもとに予測される攻撃効果を述べる．

3.1 許容誤差性能向上に向けたアプローチ

提案手法では，攻撃開始タイミングの許容誤差性能を高めるため，初期パルス幅のみを拡大する．

大きな幅の初期パルスを使用することにより，攻撃開始の推定タイミングに誤差が含まれている場合においても，攻撃トラフィックが攻撃対象トラフィックと衝突し，RTO による再送処理を発生させる確率が高くなると推測できる．すなわち，攻撃対象トラフィックに対して攻撃トラフィックの正確なタイミング同期をしなくても攻撃の実現可能性を向上させることができるといえる．

初期パルスによる攻撃成功後は RTO 再送処理が発生するため，*minRTO* 秒周期の短時間パルスによる攻撃を行う従来の Shrew 手法と同様のアプローチを行う．これにより，Fawe-Shrew 手法は大量トラフィックを送信する一般的な FDoS 攻撃と比較し，高いステルス性を有した状態で短時間転送に対する攻撃効果を高めることが可能となる．

3.2 提案手法のモデル化とパラメータの定義

本節では，攻撃成功条件の導出に先立ち，提案手法のモデル化とパラメータの定義を行う．**図 2** に Fawe-Shrew 手法のモデルを示し，**表 1** に図中で使用しているパラメータの意味を示す．

攻撃対象トラフィックは時刻 O から転送を開始する．グラフを描写する際の簡略化のため，O を $t = 0$ とする．攻撃対象トラフィックの転送時間は L_{r} とする．

攻撃トラフィックについて，初期パルス幅を L_{init}，後続パルス幅を L とし，$L_{\mathrm{init}} > L$ とする．トラフィックレート R は帯域幅 C 以上の値とする．初期パルスは時刻 t_{init} に送信開始され，これが攻撃開始時刻となる．i 番目の後続パルスは時刻 t_i から送信を開始する．t_{init} および t_i の L_{f} 秒後に，攻撃トラフィックによってルータのバッファが満たされた状態となる．攻撃トラフィックは $T = minRTO$ 秒周期で送信する．

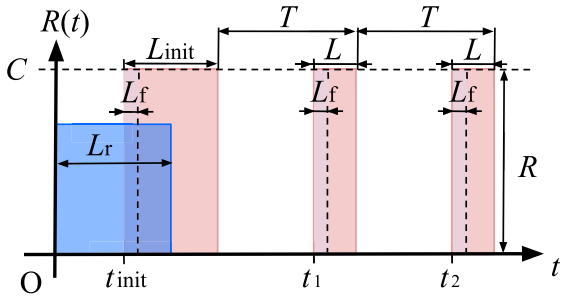


図 2 Fawe-Shrew 手法のトラフィックモデル
Fig. 2 The traffic model of Fawe-Shrew method.

表 1 図 2 で用いたパラメータ
Table 1 Parameters used in Fig. 2.

意味	パラメータ
攻撃開始時刻	t_{init} [秒]
i 番目のパルスによる攻撃開始時刻	t_i [秒]
攻撃対象トラフィックの転送開始時刻	O [秒]
攻撃なし状態における正規トラフィックの転送時間	L_{r} [秒]
初期パルス幅	L_{init} [秒]
バッファを埋める時間	L_{f} [秒]
後続パルス幅	L [秒]
パルス周期	T [秒]
攻撃パルスレート	R [Mbps]
ボトルネックリンク帯域幅	C [Mbps]

攻撃開始時刻 t_{init} と攻撃対象トラフィック転送開始時刻 O の差を P と定義する．

攻撃トラフィックによってバッファが満たされている期間に，送信された攻撃対象トラフィックがバッファに到着した状態をトラフィック衝突と呼ぶ．攻撃対象トラフィックが，L_{r} 秒のうち X 秒分のパケット送信が完了し，その後トラフィック衝突によりパケットロスが発生した場合，未送信のパケットが $2^{n-1}T$ 秒後に $L_{\mathrm{r}} - X$ 秒間送信される．ただし，n は再送処理の連続発生回数とする．

3.3 初期パルス幅拡大によるトラフィック衝突の発生条件

攻撃対象トラフィックの転送開始時刻 O と攻撃開始時刻 t_{init} の差 P が攻撃効果にどのような影響を与えるのかを示すため，本節では 3.2 節で定義したパラメータを用いて，提案手法のアプローチである初期パルス幅の拡大によるトラフィック衝突発生条件を述べる．

攻撃を成功させるためにはトラフィック衝突を発生させることが必要となるため，$P = [-0.9, 0.9]$ における A) 初期パルスのみトラフィック衝突が発生する条件，B) 初期パ

ルスと第 1 後続パルスの両方でトラフィック衝突が発生する条件，C) 第 1 後続パルスのみでトラフィック衝突が発生する条件を述べる．

A) 初期パルスと攻撃対象トラフィックが衝突する条件

初期パルスによるトラフィック衝突の発生させるためには，攻撃対象トラフィックの送信期間と初期パルスのトラフィック衝突が可能となる期間が重なる必要がある．攻撃対象トラフィックの送信期間は

$$[\mathrm{O},\ \mathrm{O}+L_\mathrm{r}] \tag{i}$$

となり，初期パルスのトラフィック衝突が可能となる期間は，初期パルスの送信を開始しバッファを満たしてから初期パルスの送信が終了するまでの期間であるため

$$[t_\mathrm{init}+L_\mathrm{f},\ t_\mathrm{init}+L_\mathrm{init}] \tag{ii}$$

となる．

(i) と (ii) の両区間が重なるには，攻撃対象トラフィックの転送開始時刻 O が (ii) の区間に挟まれるか，(ii) の始端が (i) の区間に含まれる必要がある．この時刻の関係は

$$t_\mathrm{init}+L_\mathrm{f}\le \mathrm{O}\le t_\mathrm{init}+L_\mathrm{init}\ \vee\ \mathrm{O}\le t_\mathrm{init}+L_\mathrm{f}\le \mathrm{O}+L_\mathrm{r} \tag{e4.1}$$

となり，O を消去し時刻を時間に直すと

$$-L_\mathrm{init}\le P\le -L_\mathrm{f}\ \vee\ -L_\mathrm{f}\le P\le L_\mathrm{r}-L_\mathrm{f} \qquad (\because P=t_\mathrm{init}-\mathrm{O}) \tag{e4.2}$$

となる．$L_\mathrm{init}>L>L_\mathrm{f}$, $L_\mathrm{r}>0$ より

$$-L_\mathrm{init}\le P\le L_\mathrm{r}-L_\mathrm{f} \tag{4}$$

という条件が求まる．

B) 初期パルスと後続パルスの両方が衝突する条件

この条件においては，L_r に依存するか否かで場合分けがされる．

時刻 t_1 に到着した後続パルスによりトラフィック衝突を引き起こすことが可能な期間は，攻撃トラフィックを送信開始しバッファを満たしてから送信が終了するまでの期間であるため

$$[t_1+L_\mathrm{f},\ t_1+L] \tag{iii}$$

となる．

初期パルスの衝突から T 秒後に再送が開始することより，L_r の大きさに依存せず攻撃が成功するためには，初期パルスで衝突した T 秒後の攻撃対象トラフィックの転送開始時刻が以下のとおり (iii) の区間に挟まれる必要がある：

$$t_1+L_\mathrm{f}\le \mathrm{O}+T\le t_1+L \tag{e5a.1}$$

ここで，(iii) の区間を $-T$ シフトした区間において初期パルスによるトラフィック衝突が発生する必要がある．この条件から t_1 を t_init 起点で考えると $t_1=t_\mathrm{init}+L_\mathrm{init}+T-L$ となり，これを式 (e5a.1) に代入すると

$$t_\mathrm{init}+L_\mathrm{init}+T-L+L_\mathrm{f}\le \mathrm{O}+T\le t_\mathrm{init}+L_\mathrm{init}+T \tag{e5a.2}$$

が成り立つ．式 (e5a.2) の時刻を時間に直すと

$$P+L_\mathrm{init}+T-L+L_\mathrm{f}\le T\le P+L_\mathrm{init}+T \tag{e5a.3}$$

となり，この式は攻撃対象トラフィックの通信時間 L_r に依存しない．式 (e5a.3) を P について整理すると

$$-L_\mathrm{init}\le P\le -L_\mathrm{init}+L-L_\mathrm{f} \tag{5a}$$

という条件が求まる．

次に，初期パルスによるトラフィック衝突は発生し，P が式 (5a) の区間に含まれない場合を考える．初期パルスによるトラフィック衝突が発生するため，t_init は (i) の区間に含まれる．トラフィック衝突の発生後，T 秒後から再送処理が行われることから，後続パルスと衝突するためには，攻撃対象トラフィックの転送時間 L_r と T の和が区間 (iii) の始端以上となればよい．これを式で表すと

$$\begin{aligned} & t_1+L_\mathrm{f}\le \mathrm{O}+L_\mathrm{r}+T \\ \Longleftrightarrow\ & t_\mathrm{init}+L_\mathrm{init}-L+L_\mathrm{f}\le \mathrm{O}+L_\mathrm{r} \end{aligned} \tag{e5b.1}$$

が成り立つ．式 (e5b.1) を時間に直すと

$$P+L_\mathrm{init}-L+L_\mathrm{f}\le L_\mathrm{r} \tag{e5b.2}$$

となり，P について整理すると

$$P\le -L_\mathrm{init}+L_\mathrm{r}+L-L_\mathrm{f} \tag{e5b.3}$$

となる．ここで，P は (i) の区間であり，かつ $L_\mathrm{init}-L>0$ であるため

$$-L_\mathrm{init}+L-L_\mathrm{f}\le P\le -L_\mathrm{init}+L_\mathrm{r}+L-L_\mathrm{f}\ \wedge\ L_\mathrm{init}-L>0 \tag{5b}$$

が成り立つ．

C) 初期パルスとは衝突しないが，後続パルスとのみ衝突する条件

式 (4) の導出と同様の流れで

$$t_1+L_\mathrm{f}\le \mathrm{O}\le t_1+L\ \vee\ \mathrm{O}\le t_1+L_\mathrm{f}\le \mathrm{O}+L_\mathrm{r} \tag{e6.1}$$

となり，t_1 を t_init を用いて表すと

$$\begin{aligned} & t_\mathrm{init}+L_\mathrm{init}+T-L+L_\mathrm{f}\le \mathrm{O}\le t_\mathrm{init}+L_\mathrm{init}+T \\ \vee\ & \mathrm{O}\le t_\mathrm{init}+L_\mathrm{init}+T-L+L_\mathrm{f}\le \mathrm{O}+L_\mathrm{r} \end{aligned} \tag{e6.2}$$

となる．式 (e6.2) の時刻を時間に変更すると

$$P + L_{\text{init}} + T - L + L_{\text{f}} \leq 0 \leq P + L_{\text{init}} + T \\ \vee \ -L_{\text{f}} \leq P + L_{\text{init}} + T - L \leq L_{\text{r}} - L_{\text{f}} \quad \text{(e6.3)}$$

となり，P について整理すると

$$-L_{\text{init}} - T + L_{\text{f}} \leq P \leq -L_{\text{init}} + L_{\text{r}} - T + L - L_{\text{f}} \quad (6)$$

という条件が求まる．

以上より，初期パルスのみトラフィック衝突が発生する条件は式 (4)，初期パルスと第 1 後続パルスの両方でトラフィック衝突が発生する条件は式 (5a)，(5b)，第 1 後続パルスのみでトラフィック衝突が発生する条件は式 (6) となることが分かる．

これらの条件が正しいことを示すことで，想定される攻撃効果を推測できることに加え，今後防御機構を構築する際にも Fawe-Shrew 手法の特性として用いることが可能であると考えられる．

トラフィック衝突により発生する RTO 再送処理の発生回数をもとに，スループット低下率は，攻撃対象トラフィックの転送時間 L_{r}，RTO 再送処理の発生回数 n，RTO タイマの初期値 $minRTO$ を用いて，予測 TCP スループット低下率 E_{calc} を次の式で算出できる：

$$E_{\text{calc}}(n) = 1 - \frac{L_{\text{r}}}{L_{\text{r}} + minRTO \cdot (2^n - 1)} \quad (7)$$

たとえば，$minRTO$ の値を RFC6298 [13] の推奨値である 1 秒に設定されていると仮定すると，転送中に RTO 再送処理が 1 回発生したとき，転送時間が 0.1，0.5，1.0 秒の転送では，TCP スループットはそれぞれ 91，67，50%まで低下する．

3.4 攻撃開始タイミングの推定において考えられるシナリオ

本研究の攻撃対象とする短時間転送の増加要因として，Web アプリケーションサーバやクラウドデータセンタネットワークのリソース管理ツールなどで採用されているマイクロサービスアーキテクチャの普及や，通信速度の向上があげられる．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 [14]．

マイクロサービスアーキテクチャを使用しているサーバに対し提案手法による攻撃を実施した場合，マイクロサービス間の通信時間増加によって Web サービスの応答時間増加や，クラウドデータセンタネットワークにおけるサーバリソースの制御が正常に行えなくなる事象が発生し，QoS の低下や SLA（Service Level Agreement）不順守による経済的被害が発生する可能性が高くなる．

ウェブページの表示時間は，QoS とユーザ満足度に大きく影響を与え，ビジネスに関係する．ユーザが許容できるウェブ待ち時間は 2 秒であることや，表示時間が 1 秒から 3 秒まで増加した場合には直帰率が 32%上昇することが報告されている [15], [16]．1 日に 10 万ドルの売り上げをあげる EC サイトの場合，ページ表示が 1 秒遅くなると年間で 250 万ドルの売り上げを失う可能性がある [17]．以上のことから，ウェブサイトの表示ページは最大でも 2 秒以内に表示が完了していることが望ましい．しかしながら，マイクロサービスアーキテクチャを採用している Web サーバは，提案手法により複数のマイクロサービス間通信が妨害された場合，ウェブページの表示に 2 秒を超えた時間を要する可能性が高くなる．

以上のように，提案手法による攻撃の影響によりスループット低下が発生した場合，経済的被害が生じる可能性が高い．

提案手法を用いて対時間転送に対し攻撃を行う場合，攻撃開始タイミングの推定が必要となる．このタイミング推定にはいくつかの方法が考えられる．

たとえば，サービス提供者が使用する OSS の脆弱性を悪用し，タイミング推定に必要な情報を外部に知らせるマルウェアを組み込むことが考えられる．企業における OSS の採用率は 90%以上となっており，クラウドデータセンタにおいてもコンテナ技術の Docker やコンテナオーケストレータの Kubernetes といった OSS がコントロールプレーンにて利用されている [18]．Docker では，設定ミスなどにより API が露出している場合，マルウェアがルート権限を取得可能であることが知られている [19], [20]．ルート権限が付与されたマルウェアであれば，tcpdump などを実行しトラフィック盗聴が可能となる．Kubernetes においても，すべてのリクエストが経由する Kube-api と呼ばれる API サーバにマルウェアが侵入した場合，通信のタイミングが露出されることにより，データセンタ内の通信に対し攻撃できる可能性が存在する．

OSS に対するサプライチェーン攻撃は年々増加傾向にあり，隠蔽性の高いマルウェアの侵入は今後より増えていくことが考えられる [21]．本手法において必要な情報は，通信が発生するタイミングの推定に必要な情報のみであり，通信内容を盗聴することと比較し容易である．設定ミスを悪用する攻撃や隠蔽性の高いマルウェア被害が年々増加していることから，タイミング推定に必要な情報は盗聴できる可能性が高い．

4. 実機による計測データと予測値の比較

提案する Fawe-Shrew 手法による許容誤差性能の向上を検証するため，実機を用いて構築した実験用ネットワーク

において攻撃を行い得られた結果と，得られたデータポイントについてモデル式から算出した予測値を，グラフ上で比較することで評価した．

4.1 評価環境

図 3 に実験で使用したネットワークのトポロジを示す．

Sender と 3 台の Attacker を Router に接続し，Router からボトルネックリンクで Receiver に接続している．

Router は Sender のデータを Receiver に向け転送する．Attacker は Router に対して，提案手法の図 2 に示したパルス形状になるよう攻撃トラフィックを送信し，1 秒周期で一定時間 Router のキューを占有した状態にする．

ボトルネックリンクには，リンク内で通信されるトラフィックを監視するため Observer を設置している．Observer は Linux tcpdump コマンドを用いて，評価条件ごとにパケットキャプチャ（PCAP）データを取得する．

ボトルネックリンクを作るため，仮想的な帯域制限をかける Linux tc コマンドを用いて，ボトルネックリンクの帯域幅を 60 Mbps，ルータの送信側の帯域幅を 300 Mbps，ルータのキューサイズを 1000 パケットに設定した．

計測結果によると，ルータのバッファを埋めるために最低限必要な時間 L_{f} は約 5 ミリ秒であった．無負荷状態における Sender と Receiver 間の RTT 平均値は 0.98 ミリ秒であった．

各エンティティで用いた機材およびプロトコルを，**表 2** および**表 3** に示す．本実験の Sender と Receiver のアプリケーション層では，対話型トランザクション行う際に用いられる 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 再送処理を発生させることが可能である．

4.2 評価方法

本節では，提案手法による攻撃の影響度を明示するための指標を定義する．

提案する Fawe-Shrew 手法で，初期パルス幅を 0.5，0.7，1.0 秒で試行し，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）と比較することで，初期攻撃パルス幅に対する許容誤差を評価する．

リンク内で通信されるトラフィックを監視する Observer で取得した PCAP データを実験データとして用いる．

タイミング合わせの誤差を表現するために，攻撃側ノードは受信側に対して時刻 $t = t_{\mathrm{init}}$ に攻撃トラフィックを送信した．攻撃開始タイミング t_{init} を区間 $[-0.9, 0.9]$ で 0.1 秒単位で変更し，各 t_{init} における攻撃効果 E を次の式で計算した：

$$E(t) = 1 - \frac{\alpha}{\tau} \tag{8}$$

ここで，α と τ はそれぞれ，攻撃開始タイミング $P = t$ であるときの，攻撃あり状態における TCP スループットと攻撃なし状態における TCP スループットであり，$E(t)$ は TCP スループットの低下率を示している．なお，RTO の値が 60 秒以上となり，セッションタイムアウトが発生した場合，$E = 1.0$ と定義する．

各パラメータに沿った処理を実行するため，Linux sleep コマンドおよび C usleep 関数を用いてトランザクションタイミングの調整を行った．

初期パルスの拡大による攻撃効果を明らかにするため，初期パルス幅 L_{init} は 0.3，0.5，0.7，0.9 秒の 4 パターンで実施した．

後続の攻撃パルス幅 L は，60 Mbps の帯域幅でルータのバッファを満たし，RTO 再送処理によるデータの再送信を引き起こすために十分な 0.3 秒に設定した．

正規トラフィックの転送時間 L_{r} と攻撃効果の関係を確認するため，1–3 MB のデータごとに上記の実験を行い，PCAP データを取得した．試行回数は各条件で 50 回であった．

構築した実験環境において，L_{r} の値は 1 MB では 0.13 秒，2 MB では 0.22 秒，3 MB では 0.32 秒であった．

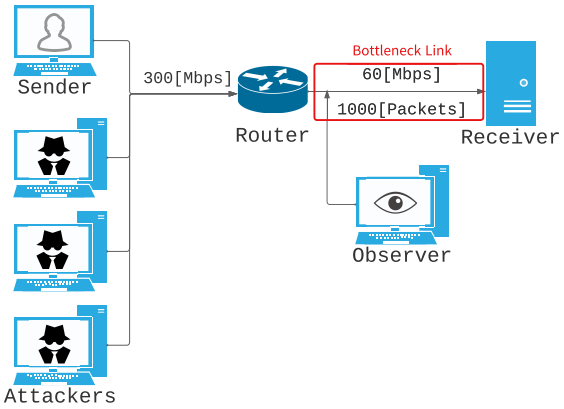


図 3 実験用ネットワークのトポロジ
Fig. 3 The topology of the test-bed network.

表 2 各エンティティで用いた機材
Table 2 Equipment of each entities

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

表 3 各エンティティで用いたプロトコル
Table 3 Protocols of each entities

エンティティ	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	-

取得した全試行分の PCAP データに対して式 (8) を用いて攻撃効果 E を算出した．算出した E の値には外れ値が含まれることを考慮し，各条件下における E の中央値を評価に用いた．

攻撃タイミングの誤差に対するロバスト性を示す許容誤差性能 D は，P がとりうる値の集合を A としたとき，攻撃効果 E（$t \in A$）が閾値 E_{th} 以上となる t の割合を用いた次の式にて評価する：

$$D = \frac{1}{|A|}\left|\{\, t \in A \mid E(t) \geq E_{\mathrm{th}} \}\right| \tag{9}$$

LDoS 攻撃では，ボトルネックリンク帯域幅に対して平均 20–30%程度の攻撃トラフィックを用いることで検知されにくいステルス性を実現している．攻撃が成功することで正常通信の TCP の転送が抑制され，リンク帯域幅の利用率が 100%を下回り，未使用のリンクシェアが発生する．そこで，抑制された TCP，攻撃トラフィック，および未使用分のリンクシェアが 1 : 1 : 1 となるよう分割されるケースを想定し，目標とする攻撃の閾値 E_{th} を 0.65 とした．

4.3 トラフィック衝突発生条件を用いて予測される攻撃効果と許容誤差性能

本節では，データサイズごとに許容誤差性能がどのように変化するか述べる．なお，攻撃なし状態における正規トラフィックの転送時間 L_{r} は，4.2 節で述べた値を用いて，$L_{\mathrm{r}} = 0.13$（1 MB），0.22（2 MB），0.32（3 MB）秒とした．

3.3 節で述べたトラフィック衝突発生条件に基づき，提案手法の攻撃実験を実施するデータサイズが 1–3 MB に対して予測される許容誤差性能 D_{calc} を**表 4** に示す．この表から，初期パルス幅 L_{init} を拡大することで予測される許容誤差性能 D_{calc} の値が上昇していることが確認できる．

ここから，許容誤差性能の算出に必要な攻撃効果の予測値について説明する．

いずれのデータサイズ，初期パルス幅 L_{init} においても，攻撃開始タイミング P が区間 $[-L_{\mathrm{init}}, L_{\mathrm{r}} - L_{\mathrm{f}}]$ であるとき，式 (4) の条件にあてはまる．つまり，L_{init} を拡大することで，最低でも 1 回のトラフィック衝突が発生する P の範囲は負の方向へ $-L_{\mathrm{init}}$ まで拡大されることが予測される．式 (4) の条件にあてはまるとき，トラフィック衝突が 1 回のみ発生することが予測される．

式 (4) の条件のうち，式 (5a)，(5b) の条件にあてはまる攻撃開始タイミング P の範囲を**表 5** に示す．この表より，初期パルス幅 L_{init} が 0.3 のときは式 (5b) の条件にあてはまる場合がないが，初期パルス幅 L_{init} が 0.5 以上のすべての場合において，式 (5b) の条件にあてはまる P が存在していることが分かる．式 (5a)，(5b) の条件にあてはまるとき，2 回以上のトラフィック衝突が発生することが予測される．

初期パルス幅 L_{init} が 0.3，0.5 であるとき，式 (6) の条件にあてはまり，トラフィック衝突が 1 回のみ発生する場合が存在する．

これらの条件をもとに，式 (7) を用いて算出した予測攻撃効果から，式 (9) を用いて許容誤差性能を算出すると表 4 のようになり，初期パルス幅の拡大により許容誤差性能が向上することが分かる．

表 4 攻撃開始タイミングの予測許容誤差性能の予測値と実測値の比較

Table 4 Expected timing skew tolerance of attack start timing.

データサイズ	L_{r}	L_{init}	D_{calc}
1 MB	0.13	0.3	0.32
		0.5	0.37
		0.7	0.47
		0.9	0.58
2 MB	0.22	0.3	0.42
		0.5	0.42
		0.7	0.53
		0.9	0.63
3 MB	0.32	0.3	0.53
		0.5	0.53
		0.7	0.58
		0.9	0.68

表 5 式 (5a)，(5b) の条件にあてはまる攻撃開始タイミング P の範囲

Table 5 The range of P where the conditions of equations (5a) and (5b).

データサイズ	L_{init}	条件 (5a)	条件 (5b)
1 MB	0.3	$[-0.3, -0.1]$	–
	0.5	$[-0.5, -0.3]$	$[-0.3, -0.1]$
	0.7	$[-0.7, -0.5]$	$[-0.5, -0.3]$
	0.9	$[-0.9, -0.7]$	$[-0.7, -0.5]$
2 MB	0.3	$[-0.3, -0.1]$	–
	0.5	$[-0.5, -0.3]$	$[-0.3,\ 0.0]$
	0.7	$[-0.7, -0.5]$	$[-0.5, -0.2]$
	0.9	$[-0.9, -0.7]$	$[-0.7, -0.4]$
3 MB	0.3	$[-0.3, -0.1]$	–
	0.5	$[-0.5, -0.3]$	$[-0.3,\ 0.1]$
	0.7	$[-0.7, -0.5]$	$[-0.5, -0.1]$
	0.9	$[-0.9, -0.7]$	$[-0.7, -0.3]$

4.4 実機を用いた実験用ネットワークにおける攻撃効果と許容誤差性能

本節では，実機を用いた実験用ネットワーク環境下において提案手法による許容誤差性能を示し，**表 6** で 4.3 節で予測した許容誤差性能 D_{calc} とよく一致していることを述べ，許容誤差性能 D が従来手法と比較して向上していることを示し，提案手法が短時間転送に対する有効性が高いことを述べる．

図 4，**図 5**，**図 6** に，$t_{\mathrm{init}} = [-0.9, 0.9]$ における，実機を用いて構築したネットワーク環境下における攻撃効果 E

表 6 攻撃開始タイミングの許容誤差性能 D

Table 6 Timing skew tolerance of attack start timing D

データサイズ	L_{init}	D_{calc}	D_{actual}	差
1MB	0.3	0.32	0.32	0.00
	0.5	0.37	0.37	0.00
	0.7	0.47	0.42	0.05
	0.9	0.58	0.53	0.05
2MB	0.3	0.42	0.42	0.00
	0.5	0.42	0.42	0.00
	0.7	0.53	0.47	0.06
	0.9	0.63	0.58	0.05
3MB	0.3	0.53	0.42	0.11
	0.5	0.53	0.47	0.06
	0.7	0.58	0.53	0.05
	0.9	0.68	0.63	0.05

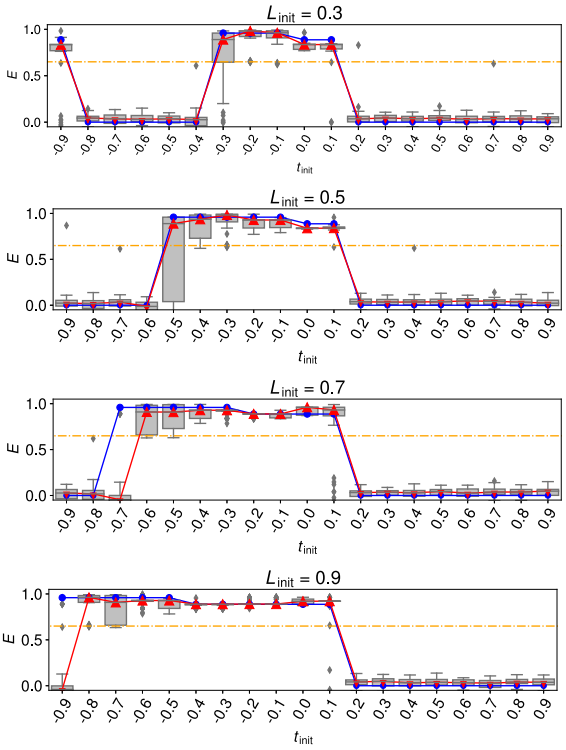


図 4 データサイズが 1 MB における攻撃効果 E の計算値と実測値（$L_{\text{r}} = 0.13$）

Fig. 4 Theoretical and experimental attack effectiveness E with data size of 1 MB ($L_{\text{r}} = 0.13$).

の箱ひげ図および中央値と，4.3 節で述べた予測攻撃効果 E_{calc} をデータサイズごとに示す．

青軸 (○) は攻撃開始タイミング P における予測攻撃効果 E_{calc} を折れ線グラフで示している．黄破線は 4.2 節で述べた閾値 E_{th}（$= 0.65$）を示している．赤軸は，式 (8) を用いて算出した攻撃効果 E の中央値を示しており，閾値を超えたものは「△」，超えていないものは「▽」で描画した．

図 4–図 6 より，予測した攻撃効果と実測した攻撃効果が類似していることが確認できる．

表 6 に，各条件下における，実機を用いた実験用ネットワーク環境で観測したデータから算出した許容誤差性能

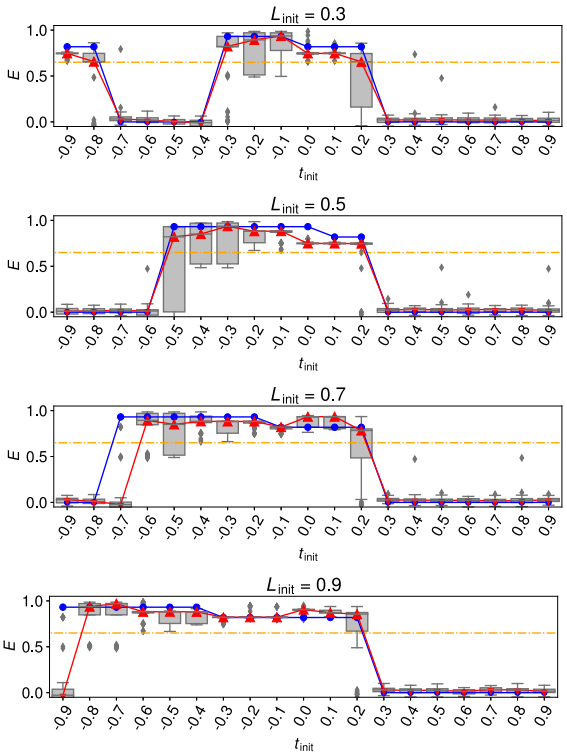


図 5 データサイズが 2 MB における攻撃効果 E の計算値と実測値（$L_{\text{r}} = 0.22$）

Fig. 5 Theoretical and experimental attack effectiveness E with data size of 2 MB ($L_{\text{r}} = 0.22$).

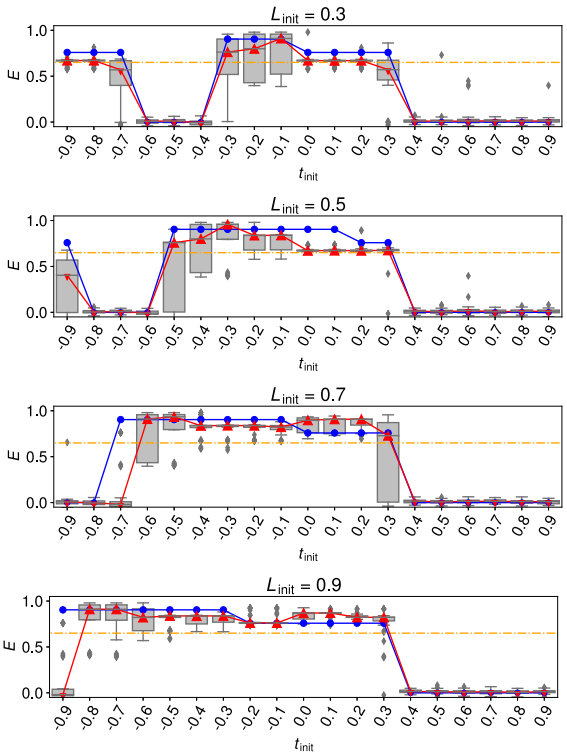


図 6 データサイズが 3 MB における攻撃効果 E の計算値と実測値（$L_{\text{r}} = 0.32$）

Fig. 6 Theoretical and experimental attack effectiveness E with data size of 3 MB ($L_{\text{r}} = 0.32$).

D_{actual} と，式 (4)，(5a)，(5b)，(6) を用いて算出した許容誤差性能 D_{calc} を示す．

データサイズが 1 MB および 2 MB の場合について，L_{init} が 0.3，0.5 のとき，D_{actual} と D_{calc} に差がないことが確認できる．L_{init} が 0.7，0.9 であるとき，D_{actual} と D_{calc} の差が 0.05–0.06 となっているが，$P = -L_{\mathrm{r}}$ 付近における分散が大きいことから，トランザクションタイミングの制御精度によるものであると考えられる．これらのことから，式 (4)，(5a)，(5b)，(6) に示した条件が実環境におけるデータとよく一致していることが確認できる．

データサイズが 3 MB の場合についても，L_{init} が 0.7，0.9 のとき，D_{actual} と D_{calc} の差が 0.05 となっているが，これについてもトランザクションタイミングによるものであると考えられる．

外乱のない実験用ネットワーク環境で実際の機材を用いた実験と比較し，提案手法による許容誤差性能は 4.3 節で述べた結果に対して最大でも 0.11 の誤差で収まっており，実際の機材での運用結果を十分説明できているといえる．

以上より，攻撃トラフィックの初期パルス幅を拡大することにより，攻撃開始タイミングの許容誤差性能が向上するという仮説が正しいことが示された．

5. おわりに

本研究では，初期パルス幅を拡大することで攻撃開始タイミングの許容誤差性能を向上させ，従来手法と比較し短時間転送に有効な Fawe-Shrew（First-Attack Pulse Width Expansion Shrew）手法を提案した．

提案手法の許容誤差性能を検証するために，攻撃開始タイミングを変化させ攻撃を行う実験的評価を行った．対象としたトラフィック転送開始タイミングは，後続パルス幅と等しい初期パルス幅 $L_{\mathrm{init}} = 0.3$ を用いる従来の Shrew 手法と，提案手法で拡大した初期パルス幅 $L_{\mathrm{init}} = 0.5$，0.7，0.9 の合計 4 パターンとし，式 (8) で導出される攻撃効果 E を用いて評価した．

評価結果から，初期パルス幅を拡大することで，攻撃開始タイミングの許容誤差性能を向上させることができることが分かった．

提案する Fawe-Shrew 手法では，初期パルス幅の拡大とそれによるデメリットのトレードオフについて，定量的かつ定性的な議論が必要である．従来の Shrew 手法では，パルス状のトラフィックを用いることで攻撃トラフィックレートを下げ，大量のトラフィックを検知する FDoS 攻撃検知機構による検知を回避している．しかし，Fawe-Shrew 手法はパルス幅を拡大するため，トラフィック量の増加によって FDoS 攻撃検知機構に検知される可能性がある．したがって，許容誤差性能 D を大きくして検出機構を回避するためには，初期パルス幅の拡大範囲をトレードオフの観点から検証する必要がある．

これらの内容について，本論文で示した攻撃成功の条件を用いて議論が可能となった．Fawe-Shrew 手法のより詳細な特性を追求し，防御につなげることが必要である．

謝辞 本研究の一部は，JSPS 科研費 JP20K11772 の助成を受けたものです．また，本研究に関し議論を交わしてくださった池山安杜里氏に感謝します．

参考文献

[1] 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).
[2] Kuzmanovic, A. and Knightly, E.W.: Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants, *Proc. Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp.75–86 (2003).
[3] Guirguis, M., Bestavros, A. and Matta, I.: Exploiting the transients of adaptation for RoQ attacks on Internet resources, *Proc. 12th IEEE International Conference on Network Protocols* (*ICNP*), pp.184–195 (2004).
[4] 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).
[5] Guirguis, M., Bestavros, A. and Matta, I.: On the impact of low-rate attacks, *Proc. IEEE International Conference on Communications*, Vol.5, pp.2316–2321 (2006).
[6] Yue, M., Wang, M. and Wu, Z.: Low-high burst: a double potency varying-rtt based full-buffer shrew attack model, *IEEE Trans. Dependable and Secure Computing*, Vol.18, No.5, pp.2285–2300 (2019).
[7] Feng, Z., Bai, B., Zhao, B. and Su, J.: Shrew attack in cloud data center networks, *Proc. 7th International Conference on Mobile Ad-hoc and Sensor Networks*, pp.441–445 (2011).
[8] Takahashi, Y., Inamura, H. and Nakamura, Y.: A Low-rate DDoS strategy for unknown bottleneck link characteristics, *Proc. IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events* (*PerCom Workshops*), pp.508–513 (2021).
[9] Maciá-Fernández, G., Díaz-Verdejo, J.E. and García-Teodoro, P.: Evaluation of a low-rate DoS attack against iterative servers, *Computer Networks*, Vol.51, No.4, pp.1013–1030 (2007).
[10] Baitha, A.K. and Vinod, S.: Session hijacking and prevention technique, *Int. J. Eng. Technol*, Vol.7, No.2.6, pp.193–198 (2018).
[11] 久末瑠紅，稲村 浩，石田繁巳，中村嘉隆：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，マルチメディア，分散，協調とモバイルシンポジウム 2022 論文集，Vol.2022, pp.1497–1504 (2022).
[12] Hisasue, R., Inamura, H. and Ishida, S.: A New Low-rate DoS Attack Method Robust to Timing Skew for TCP Short Transfers, *2023 14th International Conference on Ubiquitous and Future Networks* (*ICUFN*), pp.237–242 (2023).
[13] Paxson, V., Allman, M., Chu, J. and Sargent, M.: RFC 6298: Computing TCP's retransmission timer (2011).
[14] Thönes, J.: Microservices, *IEEE Software*, Vol.32, No.1, p.116 (2015).
[15] Nah, F.F.-H.: A study on tolerable waiting time: how

long are web users willing to wait?, *Behaviour & Information Technology*, Vol.23, No.3, pp.153–163 (2004).
[16] An, D.: Find out how you stack up to new industry benchmarks for mobile page speed, *Think with Google-Mobile, Data & Measurement*, p.24 (2018).
[17] Work, S.: How loading time affects your bottom line, *KISSmetrics* (2011).
[18] synopsys: Open source security and risk analysis report (2023).
[19] Aqua: Threat alert: Maneuver docker api for host takeover (2019), available from ⟨https://blog.aquasec.com/threat-alert-docker-api-host-takeover⟩.
[20] Threat actors abuse ICS-specific, H.: Featured in this issue: Exploitable hosts used in cloud native cyber attacks, *Network Security* (2020).
[21] Ladisa, P., Ponta, S.E., Sabetta, A., Martinez, M. and Barais, O.: Journey to the Center of Software Supply Chain Attacks, arXiv preprint arXiv:2304.05200 (2023).

推薦文

DICOMO2022 の発表論文の中で特に評価が高かったため.

（モバイルコンピューティングと新社会システム研究会主査　山口弘純）

久末 瑠紅　（学生会員）

2022 年公立はこだて未来大学情報アーキテクチャ学科卒業．2024 年同大学大学院システム情報科学研究科修士課程修了予定．ネットワークセキュリティの研究に従事.

稲村 浩　（正会員）

1990 年慶應義塾大学大学院理工学研究科修士課程修了．同年日本電信電話株式会社入社，1998 年より NTT ドコモ株式会社．2016 年より公立はこだて未来大学システム情報科学部教授．博士（工学）．モバイルコンピューティング・スマートデバイス向けシステムソフトウェア・モバイルネットワークに関する研究に従事．電子情報通信学会，ACM，IEEE 各会員．本会業績賞．本会フェロー.

石田 繁巳　（正会員）

2006 年芝浦工業大学工学部卒業．2008 年東京大学大学院新領域創成科学研究科修士課程修了．2012 年同大学院工学系研究科博士課程修了．博士（工学）．2008 年（株）アクティス入社．2013 年米国ミネソタ大学客員研究員．2013 年九州大学システム情報科学研究院助教．2021 年公立はこだて未来大学准教授．無線通信，センサネットワークに関する研究に従事．2016 年度山下記念研究賞，2023 年 IPSJ/IEEE CS Young Computer Researcher Award．IEEE，電子情報通信学会各会員.