1Y-01

攻撃タイミング推定による短時間転送向けLDoS攻撃手法の提案

野上竜杜† 久末瑠紅† 稲村浩† 石田繁巳†
†公立はこだて未来大学

1 はじめに

2003年から，通信プロトコルの脆弱性を悪用し，パルス状の攻撃トラフィックによりネットワークに攻撃を行う LDoS (Low-rate Denial of Service) 攻撃が議論されている．LDoS攻撃ではパルス状の攻撃トラフィックを用いることで平均帯域使用率を低くし，大量トラフィックを用いて攻撃する従来の FDoS (Flooding DoS) に対する検知機構を回避するステルス性を持つ [1].

LDoS 攻撃手法の 1 つである Shrew 手法は，攻撃対象の TCP コネクションに対し，TCP の特性を悪用可能な周期で攻撃トラフィックを送信し輻輳を発生させることで，ステルス性を保ちつつ攻撃対象の通信品質を低下させる [2].

LDoS 攻撃はパルス状の攻撃トラフィックを用いるため，短時間転送に対し LDoS 攻撃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．LDoS 攻撃では攻撃対象トラフィックの転送中に攻撃トラフィックを送信し輻輳を発生させることが重要である．攻撃トラフィックの転送タイミングを攻撃対象トラフィックに合わせられない場合，攻撃トラフィックのパルス間に攻撃対象トラフィックが通過することや，攻撃トラフィックの送信前に攻撃対象の転送が完了し，攻撃効果を得られない可能性がある．

本研究は，攻撃タイミングの推定による短時間転送に対する LDoS 攻撃の実現を目的とする．

2 関連研究

久末らは，短時間転送に対してロバスト性を持つ LDoS 攻撃手法として Fawe-Shrew 手法を提案し，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 [3]．この研究では，短時間転送に対する LDoS 攻撃においてネットワーク遅延や，TCP の 3 ウェイハンドシェイク（3WHS）処理による送信時間のずれにより正確な攻撃タイミングの推定が難しいことを課題とし，初期パルス幅のみを拡大することで攻撃のステルス性を維持し攻撃タイミング推定の許容誤差性能を向上させた．

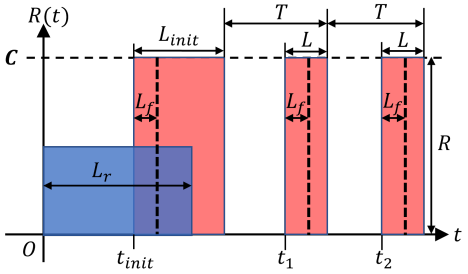

図 1: Fawe-Shrew 手法のトラフィックモデル

久末らは，図 1 に示すトラフィックモデルにおいて初期パルスのみが衝突する条件と初期パルスと後続パルスの両方が衝突する条件式を示し，衝突回数に応じて再送タイマの秒数が計算できることを利用し攻撃効果を算出した．モデル式について実機を用いて構築した実験用ネットワークにおいて提案手法の検証を行い，結果と比較してよく一致することを示した [3]．しかしながら，短時間転送に対して攻撃タイミングの推定は行っておらず，各種の外乱による攻撃タイミングの誤差への影響は明らかになっていない．

3 トラフィックの周期性推定による攻撃タイミング推定

本研究ではクラウドコンピューティングサービスなどで提供される死活管理機能が周期性を持つトラフィックを送信する特性を利用し攻撃タイミングを推定し攻撃を行う．死活管理機能とは，ロードバランサ等が提供する機能の 1 つであり TCP や HTTP 通信等を用いて定期的に通信を行いサーバからのレスポンスの有無でサーバの死活状況を確認する機能である．通信が一定回数タイムアウトした際にサーバが機能していないと判断しトラフィックの振り分けを停止するなどの処理を行う．

実ネットワーク上では，様々な通信がされており通信の周期性を測定するには攻撃対象トラフィックの識別を行う必要がある．TCP を用いた死活管理機能では，多くは 3WHS 処理の成否によりサーバの異常を判断している．3WHS のみ行う通信は少ないと考えられるた

LDoS Attack Method with Attack Timing Estimation for Short Transfers
Ryuto Nogami†, Ryuku Hisasue, Hiroshi Inamura†, Shigemi Isida†
†Future University Hakodate, Japan
†{b1020187, g2122054, inamura, ish}@fun.ac.jp

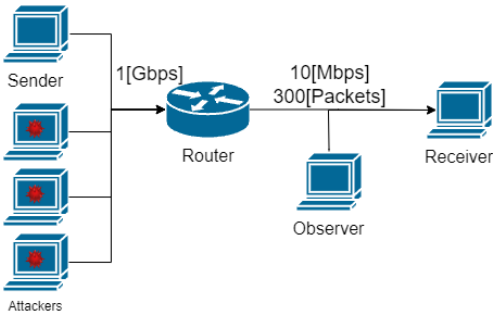

図 2: 実験用ネットワークのトポロジー

め，本研究ではこの特性を利用し攻撃対象トラフィックの識別を行う．

識別した攻撃対象トラフィックの通信間隔を測定することで周期を特定し，攻撃効果を最大化するために観測した通信間隔の分布から，攻撃トラフィックと衝突する最も範囲が大きくなるように攻撃タイミングにオフセットをかける．

ネットワークのジッタにより通信タイミングに誤差が生じ攻撃に失敗するケースが考えられる．誤差に対し初期パルス幅を拡大することで攻撃が成功する確率を上げられると考えられる．本稿では，観測した通信間隔の分布をもとにした初期パルス幅拡大による攻撃効果の変化について報告する．

4 評価

本稿では，サーバが異常と判定された期間を用いて攻撃効果の評価を行う．死活管理機能では 1 回の通信のタイムアウト時間が定められており，タイムアウト時間を連続で超過した回数が閾値を越えるとサーバに異常が生じたと判定し，通信が連続で成功した回数が閾値を超えると正常と判定する．Fawe-Shrew 手法による攻撃成功確率を比較するため，従来の Shrew 手法と Fawe-Shrew 手法の 2 つについて実験を行う．

本稿ではタイムアウト時間と超過回数の閾値として，Google Cloud Platform[1]で用いられているデフォルト値を用いタイムアウト時間を 5 秒，異常・正常閾値を 2 回とする．

4.1 実験方法

図 2 に示すネットワークのトポロジーで実験を行った．Sender と Attacker 3 台を 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．

Sender は 5 秒ごとに Receiver に向けて 100kB のファイル送信を行い，Attacker はそれを観測する．Attacker は Sender の通信を 50 回観測し周期性を特定する．その

[1]Google: ヘルスチェックの概要 (2023). https://cloud.google.com/load-balancing/docs/health-check-concepts (2023-12-02 アクセス).

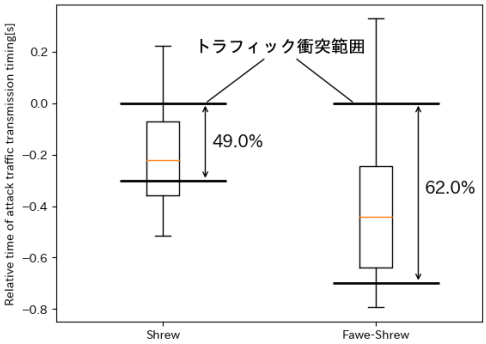

図 3: 正規トラフィックに対する攻撃トラフィック送信タイミングの相対時刻とトラフィック衝突範囲

後，Sender の通信に対し特定した周期を用いて Sender に向けて攻撃パルスを送信する．攻撃開始から Sender の通信が 100 回行われる間に Observer が観測したデータを評価に用いる．

4.2 結果と考察

Shrew 手法を用いた攻撃により異常と判定された期間は 150 秒であり，Fawe-Shrew 手法を用いた攻撃により異常と判定された期間は 185 秒であった．

実験における正規トラフィックに対する攻撃トラフィック送信タイミングの相対時刻の分布を図 3 に示す．従来の Shrew では $[-0.3, 0]$ が衝突する範囲であり観測した正規トラフィックのうち 49.5%が範囲内であった．Fawe-Shrew 手法を用い初期パルス幅を 0.698 秒へ拡大することでトラフィック衝突が生じる範囲が $[-0.698, 0.0]$ まで拡大され，観測した正規トラフィックのうち 62.6%が範囲内となり攻撃効果が向上したと考えられる．このことより，短時間転送に対し攻撃タイミングの推定誤差がある場合でも，Fawe-Shrew 手法を用いることで従来の Shrew 手法に比べ高い攻撃効果を得られるといえる．

5 おわりに

死活管理機能が持つ特性を用いることで攻撃タイミングの推定を行い，攻撃タイミングに誤差が生じる場合でも Fawe-Shrew 手法を用いることで短時間転送に対し攻撃の成功確率が向上することを示した．

参考文献

[1] Zhijun, W. et al.: 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, *ACM SIGCOMM*, pp. 75–86 (2003).
[3] Hisasue, R. et al.: A New Low-rate DoS Attack Method Robust to Timing Skew for TCP Short Transfers, *ICUFN*, pp. 237–242 (2023).