1Y-02

RTO計算変更によるLDoS攻撃耐性のシミュレーション評価

藤本陽人† 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

ネットワークサービスを標的とした攻撃に LDoS（Low-rate DoS）攻撃がある．LDoS 攻撃は，パルス形状のトラフィックを繰り返し送信することで平均攻撃通信量を抑え，既存の DoS 攻撃検知機構での検知を困難にさせつつ通信の品質を低下させる [1].

LDoS 攻撃の 1 つである Shrew LDoS 攻撃は，TCP のタイムアウトによる再送のタイミングの決定が規則的であることを悪用して成立している [2]．RTO タイマ値は RFC6298 [3] にて式 (1) で定義される（n は 1 つのセグメントについて RTO 処理が行われた回数）：

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

$minRTO$ は一般的に 1 秒に設定されている．$SRTT + \max(G, 4 \times RTTVAR)$ の値は多くの場合 1 秒を下回るため，RTO タイマ値に $minRTO$ が採用される．このため，攻撃者は攻撃トラフィックの送信周期を $minRTO$ と同値に設定することで，再送タイミングと攻撃トラフィックの送信タイミングを同期させ，連続したセグメントの損失を発生させる．

LDoS 攻撃の被害を緩和するためには，RTO タイマ値が一様に決定することを防ぐ必要がある．本稿では，RTO 処理の再送タイマ管理アルゴリズムに変更を加え，LDoS 攻撃の耐性を確かめる．

2 関連研究

LDoS 攻撃に対して，再送タイマ管理アルゴリズムを変更することによって攻撃を緩和する手法はいくつか存在する．

Yang らは，$minRTO$ をランダマイズすることによって LDoS 攻撃による被害を緩和する手法を提案し [4]，スループットを改善することに成功している．しかし，アルゴリズム中における $minRTO$ の影響力は変わっていないことから，$minRTO$ と攻撃トラフィックの送信周期が一致したときに，コネクションを切断できる程度の攻撃効果を出すことが可能となる．

細井らは，式 (2) で使用されている係数にランダマイズを導入することによって LDoS 攻撃による被害を緩和する手法を提案し，従来の TCP からスループットを改善することに成功した [5]．しかし，$minRTO$ は定数であることは従来の TCP と変わらないので，最初の再送が失敗する可能性が高い．

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

3 PTO 処理による再送制御

本研究では，トランスポートプロトコルである QUIC の再送タイマ管理アルゴリズムに着目した．QUIC は Google によって開発が行われ，2021 年に IETF（Internet Engineering Task Force）によって標準化された [6]．QUIC には再送制御が備わっているが，PTO（Probe Timeout）処理という TCP とは異なるアルゴリズムを用いて再送タイミングの管理が行われている．PTO タイマ値は RFC9002 [7] にて式 (3) で定義される：

$$PTO = SRTT + \max(G, 4 \times RTTVAR) + max\_ack\_delay \quad (3)$$

式 (3) で使用されているパラメータの中で，$SRTT, RTTVAR, max\_ack\_delay$ は動的なパラメータである [3, 6]．このことから，PTO 処理の再送タイマ管理アルゴリズムでは，再送タイマ値が一様に決定される可能性は低いと考えられる．

PTO 処理の LDoS 攻撃への耐性は検証されていない．川内谷らは，QUIC に対して Shrew DoS 攻撃を行い，輻輳ウィンドウサイズの大幅な抑制によりスループットを下げることはできるが，PTO 処理による再送は行われていないことを示した [8]．そこで本稿では，RTO 処理の再送タイマ管理アルゴリズムを，PTO 処理で用いられている式（3）の計算式を用いるアルゴリズムに変更する．

4 評価

ネットワークシミュレータ（ns-3）を用いて 2 つの評価を行う．1 つ目は，従来の TCP の正規化スループットと提案手法の正規化スループットを比較し，通信品質の評価である．2 つ目は，RTO タイマ値の増減を比較し，再送タイミングと攻撃トラフィック送信タイミングの同期を外す効果の評価である．

A Simulation of LDoS Attack Migigation with Modified RTO Calculation on TCP
Haruto Fujimoto†, Ryuku hisasue, Hiroshi inamura†, shigemi isida†
†Future University Hakodate, Japan
†{b1020060, g2122054, inamura, ish}@fun.ac.jp

表 1: パルス幅（ミリ秒）ごとの正規化スループット

パルス幅	RTT: 10 ミリ秒		RTT: 100 ミリ秒	
	TCP	提案手法	TCP	提案手法
150	0.000	0.590	0.014	0.019
200	0.000	0.616	0.012	0.013
250	0.000	0.479	0.001	0.007

4.1 実験環境

本研究では，従来の TCP と提案手法を実装した TCP の 2 つを用意し，シミュレーションを行う．図 1 に，実験するネットワークのトポロジを示す．2 つのルータ間がボトルネックリンクとなる．提案手法の再送タイマ管理アルゴリズムは RTT によって変化する可能性があるため，リンクごとの伝搬遅延の値を調整し，RTT が 10 ミリ秒，100 ミリ秒の 2 つの場合で実験する．バッファサイズは，帯域遅延積に基づいて設定する．送信者は受信者に対して 65 秒間のバルク転送を行い，攻撃者は 30 Mbps の UDP トラフィックを 1 秒周期で送信する．最初の 5 秒は，通信を安定させるために攻撃を行わない．攻撃パルス幅は，150 ミリ秒，200 ミリ秒，250 ミリ秒の 3 種類を用いてそれぞれ実験する．

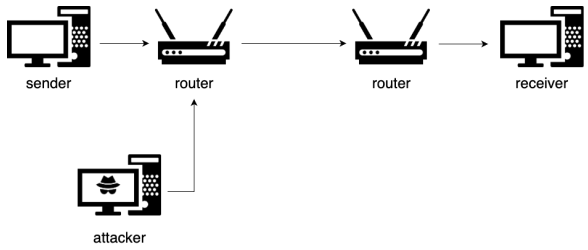

図 1: 実験環境

4.2 評価結果

取得した正規化スループットを表 1 に示す．いずれのパルス幅でも改善効果が見られ，特に，RTT が 10 ミリ秒の環境では高い緩和効果が見られた．RTT が短いほうが緩和効果が高いのは，輻輳ウィンドウサイズが高頻度で更新されてて大きくなり，より多くのデータを送ることができたためと考えられる．RTT が 100 ミリ秒の環境では緩和効果は大きくないが，従来の TCP では，通信開始 10 秒後からデータを送ることができなかった．よって，長い通信時間で実験を行った場合には正規化スループットの差がより広がると考えられる．

図 2，図 3 は，攻撃パルス幅 250 ミリ秒で LDoS 攻撃を行ったときの再送タイマ値の推移を示している．従来の TCP では攻撃トラフィックの送信タイミングとセグメントの再送タイミングが同期し，連続してセグメントの損失が起こることによって再送タイマ値が大幅に上昇しており，セグメント 1 つあたりに対して行われた再送回数は最大で 6 回であった．一方で提案手法では再送タイマ値の大幅な上昇は見られず，RTT が 10 ミリ秒の環境ではセグメント 1 つあたりに対して最大 2 回，RTT が 100 ミリ秒の環境では最大 1 回の再送でセグメントの送信に成功した．これらのことから，提案手法によって攻撃トラフィックの送信タイミングとセグメントの再送タイミングの同期を外すことができたといえる．

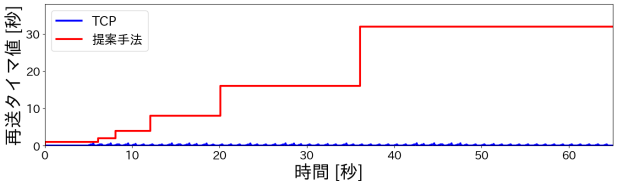

図 2: タイマ値の変化（RTT:10 ミリ秒）

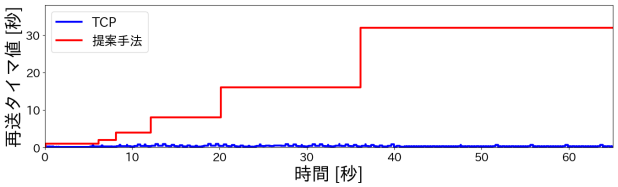

図 3: タイマ値の変化（RTT：100 ミリ秒）

5 おわりに

本稿では，TCP の再送タイマ管理アルゴリズムに QUIC の再送タイマ管理アルゴリズムを導入することで，LDoS 攻撃による被害が緩和されることをシミュレーションで明らかにした．

謝辞

本研究の一部は JSPS 科研費 (JP21K11847) の助成で行われた．

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] Sargent, M. et al.: Computing TCP's Retransmission Timer, RFC 6298 (2011).
[4] Yang, G. et al.: Defense against low-rate TCP-targeted denial-of-service attacks, *IEEE ISCC*, Vol. 1, pp. 345–350 (2004).
[5] 細井琢朗，松浦幹太ほか: 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論文集， Vol. 2013, No. 4, pp. 957–964 (2013).
[6] Iyengar, J. and Thomson, M.: QUIC: A UDP-Based Multiplexed and Secure Transport, RFC 9000 (2021).
[7] Iyengar, J. and Swett, I.: QUIC Loss Detection and Congestion Control, RFC 9002 (2021).
[8] 川内谷玲己斗ほか: QUIC 通信に対する LDoS 攻撃の可能性の検討， 情報処理学会第 85 回全国大会講演論文集, pp. 3:409–3:410 (2023).