4ZC-03

QUIC通信に対するLDoS攻撃の可能性の検討

川内谷玲己斗† 久末瑠紅† 稲村浩† 石田繁巳† 中村嘉隆†
†公立はこだて未来大学システム情報科学部 ‡京都橘大学 工学部情報工学科

1 はじめに

DoS 攻撃の一種として LDoS（Low-rate Denial of Service）攻撃が議論されている．LDoS 攻撃は，プロトコルが持つアルゴリズムの規則性を狙い，パルス形状の攻撃トラフィックを送信し，平均攻撃レートを抑えることで，従来の DoS 攻撃の検知機構に検知されにくい特性をもつ．代表的な LDoS 攻撃の手法として Shrew 手法がある．この手法は TCP の再送タイマ（RTO）の規則性を悪用する [1]．RTO に類似したものを有するプロトコルも Shrew 手法の対象となる可能性が高い．

2021 年に IETF により標準化されたトランスポート層プロトコルの QUIC は，TCP に類似した再送タイマ（PTO）を有している．QUIC は Facebook や YouTube の半数以上の通信に利用されているため，QUIC に対して Shrew 手法が有効であれば脅威となりうる [2] [3]．

本研究の目的は，攻撃への対策に貢献するために，QUIC に対する LDoS 攻撃に利用可能なアルゴリズムの存在を明らかにすることである．本稿では，ネットワークシミュレータ ns-3 を使用し，QUIC 通信に対する Shrew 手法の効果検証と，攻撃を可能にしている QUIC のアルゴリズムについて報告する．

2 関連研究

QUIC 通信へ LDoS 攻撃を行う研究は著者らの知る限り存在しない．ここでは QUIC と同様のトランスポートプロトコルである TCP 通信へ LDoS 攻撃を行う研究をあげる．

2.1 Shrew 手法

Shrew 手法は，TCP の再送タイマ（RTO）の挙動を利用する LDoS 攻撃である [1]．この手法では，RTO の初期値が 1 s から以降 2 倍づつ増加し，タイムアウト再送が行われるタイミングが外部から予測可能であることを利用して攻撃を行う [1]．

2.2 RoQ（Reduction of Quarity）手法

RoQ 手法は，TCP の Loss-based 輻輳制御アルゴリズムを利用する LDoS 攻撃である [4]．この手法では，データの送信量が輻輳を検知する前の状態に戻る前にパケットロスを起こすことで，データの送信量が低下していくことを利用して攻撃を行う．

3 従来の LDoS 攻撃手法の効果検証

本章では，ネットワークシミュレータを使用し，関連研究にあげた Shrew 手法の QUIC 通信に対する攻撃効果を検証する．

3.1 評価方法

本実験の評価は，TCP 通信と QUIC 通信へ Shrew 手法による攻撃の結果と攻撃なしの正常通信の結果から平均スループット低下率とボトルネックリンク帯域占有率の指標を用いて評価する．平均スループット低下率 D と帯域占有率 W をそれぞれ式 (1)，(2) で定義する．ここでボトルネックリンクの帯域幅を w，攻撃開始からシミュレーション終了までの攻撃トラフィックの平均スループットを α_A，攻撃時の正常トラフィックの平均スループットを α_{NonA}，攻撃なしの正常トラフィックの平均スループットを α_{NnotA} とする．

$$D = (\alpha_{NnotA} - \alpha_{NonA})/\alpha_{NnotA} \quad (1)$$

$$W = (\alpha_A + \alpha_{NonA})/w \quad (2)$$

3.2 実験環境

本実験は，図 1 にある構成のネットワークでシミュレーションを行った．シミュレータには，ネットワークシミュレータである ns-3 を使用する．シミュレータ中で，QUIC 通信を動作させる module には Paro らが拡張したものを使用する [5]．実験は，65 s 間行い，攻撃を行う場合は通信が安定する 5 s から攻撃を開始する．攻撃には，ボトルネックリンクを十分に占有する，攻撃間隔 1 s, 攻撃持続時間 0.3 s のトラフィックを用いる．

A Study on the Possibility of LDoS Attacks on QUIC Communications

Akito Kawauchiya†, Ryuku Hisasue, Hiroshi Inamura†, Shigemi Ishida†, Yoshitaka Nakamura†
†School of Systems Information Science, Future University Hakodate, Japan, ‡Kyoto Tachibana University, Japan
†{b1019110, b1018015, inamura, ish}@fun.ac.jp, y-nakamr@ieee.org

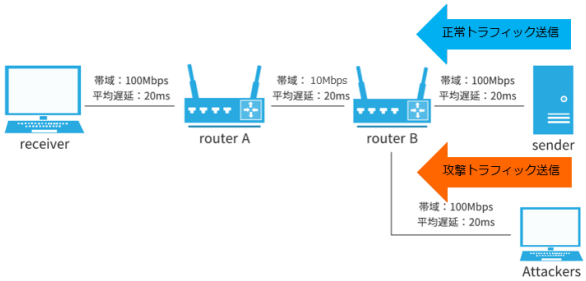

図 1: 実験に使用したネットワークトポロジ

表 1: 平均スループットの低下率と帯域の占有率

プロトコル	帯域占有率 W（%）	平均スループット低下率 D（%）
TCP	29.4	98.5
QUIC	27.1	92.6

3.3 実験結果

TCP と QUIC 通信への Shrew 手法での攻撃時の平均スループットを図 2，図 3 に示す．青が正常なトラフィック，赤が攻撃トラフィックを示す．結果から算出した平均スループット低下率と帯域占有率を表 1 に示す．表 1 の帯域占有率から平均攻撃レートが 30%以下の低い値を示すため両者ともに攻撃が成功しており，表 1 の平均スループット低下率から両者ともに平均スループットを 90%以上落とし高い攻撃効果を示している．以上より，今回使用したシミュレーションでは，既存の Shrew 手法は QUIC 通信に対しても高い攻撃効果を示すことが明らかになった．

本実験で Shrew 手法が QUIC 通信に対しても高い攻撃効果を示す原因を特定するため，シミュレーション内での再送タイマの挙動と輻輳ウィンドサイズ cwnd の値をログ出力した結果から原因を考察する．

TCP に見られるように，正常通信の帯域幅の抑制がタイムアウトの挙動により構成されているかどうかを確認するために，攻撃中にタイムアウトが発生するかどうかをシミュレータにて確認した．その結果，QUIC 通信への Shrew 手法による攻撃においては，タイムアウトは発生していなかった．輻輳ウィンドサイズ cwnd の値は 5 s から 11 s には低下し続け，11 s 以降には 2920Bytes であった．

攻撃中にタイムアウトせず，輻輳ウィンドサイズ cwnd の値が著しく低下していることから，本実験で生成した攻撃トラフィックが Delay-based 輻輳制御に対して継続的に輻輳であると誤認させ，cwnd を低下

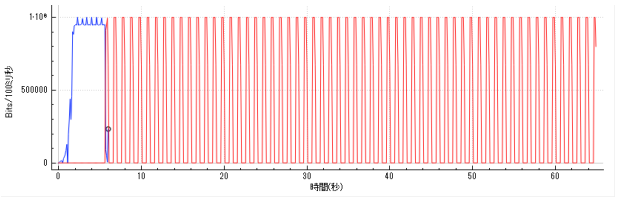

図 2: Shrew 攻撃下の TCP スループット (青)

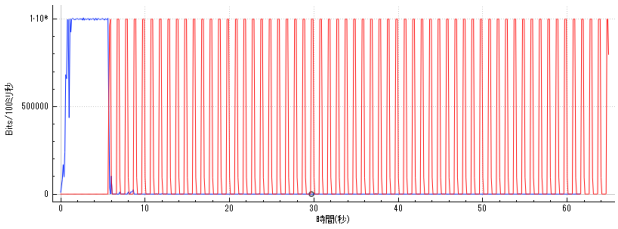

図 3: Shrew 攻撃下の QUIC スループット (青)

させ続けることができたと言える．

4 おわりに

本稿では，QUIC 通信への Shrew 手法が有効であり，輻輳制御の変更が Shrew 手法に影響を与えていたことを ns-3 上のシミュレーションで明らかにした．TCP に対する Shrew 攻撃において継続的な帯域幅の抑圧は連続的な再送タイムアウトで構成されるが，QUIC においては攻撃によって同様な結果が得られるものの，輻輳制御の動きで構成されており Shrew 攻撃の機序が異なることが分かった．

参考文献

[1] 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).

[2] Joras, M. and Yang, C.: How Facebook is bringing QUIC to billions, `https://engineering.fb.com/2020/10/21/networking-traffic/how-facebook-is-bringing-quic-to-billions/` (2020).

[3] IETF 106 Proceedings, `https://datatracker.ietf.org/meeting/106/proceedings/QUICdeploymentUpdate`.

[4] Guirguis, M., Bestavros, A. and Matta, I.: Exploiting the transients of adaptation for roq attacks on internet resources, *Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004.*, Berlin, Germany, IEEE, pp. 184–195 (online), (2004).

[5] Paro, U., Chiariotti, F., Deshpande, A. A., Polese, M., Zanella, A. and Zorzi, M.: Extending the ns-3 QUIC Module, *Proceedings of the 23rd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Alicante Spain, ACM, pp. 19–26 (online), (2020).