5V-08

WREDに対する高いIP Precedenceを用いたLDoS攻撃の分析

佐藤　大介†　稲村 浩†　中村 嘉隆†
公立はこだて未来大学　システム情報科学部†

1　はじめに

分散型サービス妨害（DDoS: Distributed Denial of Service）攻撃は，ネットワークセキュリティ分野における脅威の一つとなっている．従来のDDoS攻撃は大量のデータストリームをフラッディングすることでネットワークサービスを妨害する．しかし，このようなDDoS攻撃は攻撃トラフィックが大量であるために特徴を捉えやすく，検出と防御が可能になってきている[1]．

DDoS攻撃の検知を回避することが可能な攻撃手法として低量DoS（LDoS:Low-rate DoS）攻撃が注目されている.LDoS攻撃はKuzmanovicらによって示された[2].LDoS攻撃トラフィックの平均通信量はDDoS攻撃トラフィックの通信量と比較して小さいため，DDoS攻撃と同様の検知手法や防御手法では対応することができない.そのため，LDoS攻撃の分析や検知手法，防御手法に関する研究は活発に行われている．

2　目的

本研究の目的は，AQM（Active Queue Management)手法の一つであるWREDに対して高いIP Precedence（Precedence:パケット優先度)を用いたLDoS攻撃手法の提案と提案手法の有効性を明らかにすることである.提案手法の分析を行い，TCPの正規化スループットの観点から攻撃効果を明らかにする．

3　関連技術

LDoS攻撃はTCP再送信タイムアウトを利用し，TCPのスループットを低下または，限りになくゼロに近づける．LDoS攻撃は図1のような短いバースト通信と無通信を一定の周期で繰り返し，矩形波状の攻撃トラフィックを送信することで攻撃を行う．攻撃トラフィックはバースト間隔T，バースト長L，バーストレートRの3つのパラメータで形成される．LDoS攻撃は，TをminRTO，Lをラウンドトリップ時間（RTT:Round Trip Time）以上，Rをボトルネックリンクのバッファを十分に満たす大きさに設定した場合に高い攻撃効果を示す．LDoS攻撃者の1回目のバースト通信によりボトルネックリンク帯域幅が充足し，バッファが枯渇することで，正常トラフィックのパケットが損失する．送信者側TCPは再送制御によるパケット再送信をするためにminRTOだけ待機した後，廃棄されたパケットの再送信を行う．攻撃者はTをminRTOとすることで，送信者側TCPが廃棄されたパケットの再送信を行うタイミングとバースト通信を被せることができ，TCP通信が再び失敗する．以降，TCPが廃棄されたパケットの再送信を行うタイミングはRTOに依存する（RTOの整数倍）ため，TCP通信が抑止された状態が継続される．

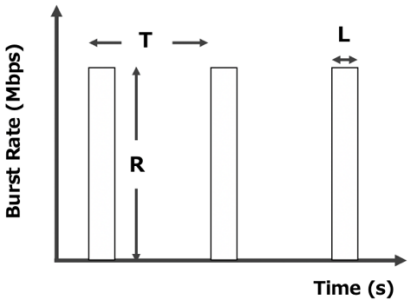

図1 LDoS攻撃のバーストトラフィック

4　アプローチ

本稿では以下で新たなLDoS攻撃手法の提案を行い，その攻撃手法に関する説明および，従来のLDoS攻撃手法に対する提案手法の有効性を明らかにするアプローチについて示す.提案する攻撃手法は，対象のボトルネックリンクのキューがWREDアルゴリズムで制御されていることを前提に，Precedenceを高く設定したパケットによる攻撃トラフィックを用いたLDoS攻撃である.Precedenceの高い攻撃トラフィックが優先的にキューイングされ，反作用的に攻撃対象のTCPコネクションのキューにおける廃棄率を高め従来のLDoS攻撃と比べて，低い平均通信量で攻撃を成功させることを狙う．

5　実験

5.1　実験内容

WREDに対する高いPrecedenceを用いたLDoS攻撃を分析し，TCPの正規化スループットの観点から攻撃効果を明らかにすることを目的に実験を行う．実験にはns3ネットワークシミュレータを用いる．我々は既存のREDのコードを基にWRED

Analysis of LDoS Attack with High IP Precedence against WRED
† Daisuke Sato, Hiroshi Inamura, Yoshitaka Nakamura, School of Systems Information Science, Future University Hakodate

アルゴリズムを実装した．

図 2 に示す簡易なネットワークを用い，低い Precedence を 0，高い Precedence を 6 と設定したパケットを用いて LDoS 攻撃を行った．攻撃トラフィックのパラメータは R を 15Mbps，L を 240ms，T を 1.2s とした．実験は 20 秒間行い，Attacker は実験開始から 2.5 秒後に攻撃を開始した．

5.2 結果・考察

図 3 は Router2 で観測したボトルネックリンクにおけるスループットを示しており，以降はこれを分析する．図 3 のうち LDoS 攻撃下における Total スループットが，ボトルネックリンクの帯域幅 15Mbps よりも明らかに低い値を示しているため，LDoS 攻撃が成功している．

表 1 は LDoS 攻撃下における TCP スループットの平均を示している．表 1 より Precedence が高い LDoS 攻撃の方が低い LDoS 攻撃と比べて，TCP スループットをより抑制していることが明らかになった．

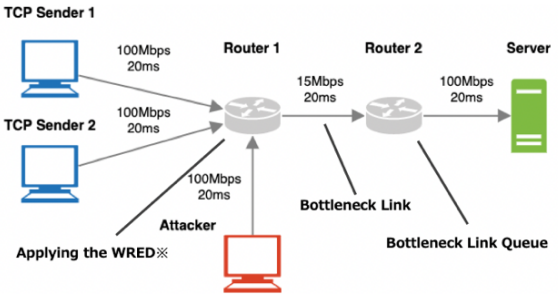

図 2 実験用ネットワーク

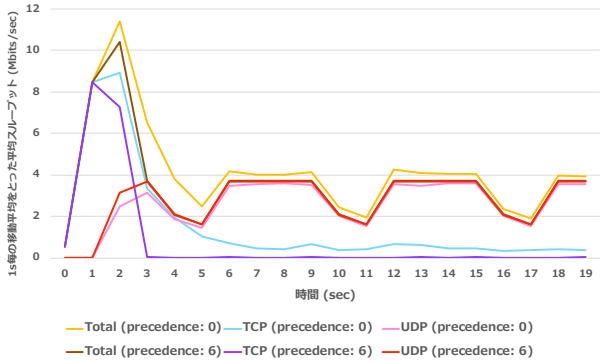

図 3 Router2 で観測したボトルネックリンクにおける Precedence 別スループット

表 1 2.5〜19.5s の Precedence 別 TCP 平均スループット

	TCPスループットの平均[Mbits/sec]
precedence: 0	0.8501
precedence: 6	0.0328

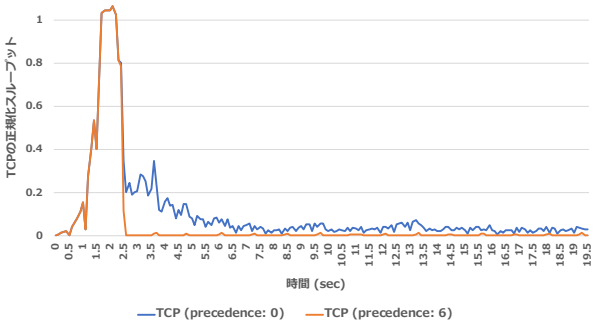

図 4 Precedence 別 TCP 正規化スループット

表 2 2.5〜19.5s の Precedence 別 TCP 正規化スループットの平均

	TCP正規化スループットの平均[Mbits/sec] (割合)
precedence: 0	0.0567 (5.67%)
precedence: 6	0.00213 (0.21%)

ボトルネックリンクの帯域幅 15Mbps に対する TCP 正規化スループットを図 4 に，攻撃下における TCP 正規化スループットの平均と割合を表 2 に示している．

図 4，表 2 から Precedence の低い LDoS 攻撃の方が Precedence の高い LDoS 攻撃よりボトルネックリンクの帯域幅に占める割合が高く，TCP スループットが高いことが示されている．TCP 正規化スループットの平均に関して，低い Precedence の LDoS 攻撃下におけるスループットは高い Precedence の LDoS 攻撃下におけるスループットの 25 倍程度であることが明らかになった．

6 おわりに

本研究では，WRED に対する高い Precedence を用いた LDoS 攻撃を分析し，TCP の正規化スループットの観点から攻撃効果を示すことで，提案手法の有効性を明らかにすることができた．

参考文献

[1] Kottler, S.: February 28th DDoS Incident Report, The GitHub Blog, available from 〈 https://github.blog/2018-03-01-ddos-incident-report/〉 (accessed 2020-09-26).
[2] A. Kuzmanovic et al: Low-rate TCP-targeted denial of service attacks and counter strategies, in IEEE/ACM Transactions on Networking, vol. 14, no. 4, pp. 683-696, Aug. 2006.