Vol.2022-CSEC-99 No.9
Vol.2022-SPT-49 No.9
Vol.2022-EIP-98 No.9
2022/12/22

フロー内のパケット損失率に着目した 低レート DDoS 攻撃緩和手法の提案

横山 友紀[1,a)]　今泉 貴史[2]

概要：LDDoS(Low-rate Distributed Denial of Service) 攻撃は，TCP/IP プロトコルやルーティングキュー管理機構の脆弱性を悪用することによって，低い平均通信量で TCP リンクの品質を低下させる．そのため，LDDoS 攻撃は従来の DDoS 攻撃と異なり，隠密性が高く検知が困難である．本研究ではこの LDDoS 攻撃の緩和手法を提案する．提案手法は，LDDoS 攻撃下でフローごとのパケット損失率を監視し，パケット損失率を閾値によって判定し，プライオリティキューに追加する．この提案手法により，LDDoS 攻撃によりネットワークの輻輳が起こっているボトルネックリンクでは，LDDoS 攻撃中に被害を受けているフローを優先的に処理することができるため，攻撃の緩和が可能である．この提案手法の有効性を確認するため，ns-3 を用いてシミュレーションを行った．

Low-rate DDoS attack mitigation method focusing on packet loss rate

1. はじめに

インターネットの急速な発展により，ネットワークを介した様々なサービスが提供され，利便性が増している．その一方で，悪意を持った第三者がサービスを提供するコンピュータや機器に攻撃を行い，一般ユーザの利用を妨げる DDoS(Distributed Denial of Service) 攻撃が深刻な問題となっている．実際に，2016 年には，DNS サーバを提供する Dyn に対する攻撃が観測されており [1]，この攻撃の影響により，多くのサービスが一時的に利用できなくなる事象が報告されている．DDoS 攻撃にも多種多様なものが確認されており [2]，CDNetworks のレポートによると，2018 年の 1 月から 3 月にかけて最も多かった攻撃は SYN Flood 攻撃であると報告されている [3]．この手法は，ボットネットから大量の攻撃トラフィックを送信することによって，標的周辺のネットワーク帯域幅や標的の CPU，メモリなどの資源を可能な限り消費し，サービスの提供を停止させるという特徴をもつ．単純で強力な攻撃効果を生むことが可能であるが，大量の攻撃トラフィックを用いて負荷を与えるため，検知や緩和が容易である．

Kuzmanovic らは，低量分散型サービス妨害 (LDDoS: Low-rate Distributed Denial of Service) 攻撃によって，TCP 通信を継続的に妨害可能であることを明らかにした [4][5]．LDDoS 攻撃は TCP 再送信タイムアウトの仕様を利用して低い平均通信量で TCP 通信を妨害することが可能であり，攻撃が完全に成功した場合，標的 TCP は継続してタイムアウトを引き起こし，スループットはほぼ 0 まで低下する．長さが短く高レートな矩形波のバーストトラフィックを用いて攻撃することで，攻撃トラフィックの平均通信量が一般的なフラッド型 DDoS 攻撃のものと比較して低量となるため，既存の DDoS 攻撃トラフィックの検知手法で LDDoS 攻撃トラフィックを検知することは困難である．一般的な DDoS 攻撃への対策が進んできている一方で，LDDoS 攻撃への対策はほとんど取られていない．さらに，LDDoS 攻撃の対策として，標的のボトルネックリンクルータ上で LDDoS 攻撃を防御する手法 [6], [7], [8] は提案されているが，攻撃トラフィックを分離することが難しいことや，評価実験が不十分であるという課題がある [9], [10].

そこで，本研究では，フローに着目することで LDDoS 攻撃を緩和する．具体的には，shrew attack protection(SAP)[11] がある．SAP とはポートパケットの損失率を監視し，パケット損失率の高いパケットの優先度を調整し，全てのパケットが公平に処理されるようにするシステ

[1] 千葉大学 融合理工学府
[2] 千葉大学 統合情報センター
[a)] yokoyama_yuki@chiba-u.jp

ムである．この手法ではパケットにラベル付けをして，優先度の割り当てを行っている．また，キューを分割して，ドロップしたパケット用のキューを用意してラベルのそのパケットに割り当てを行うので，キューの中でパケットが回ってしまう．本研究では，パケットごとの分類ではなくフローごとのパケット損失率に着目し，プライオリティキューを利用することで LDDoS 攻撃の緩和する手法を提案する．

2. LDoS/LDDoS 攻撃

2.1 TCP 再送信タイムアウト

TCP では，パケットを送信した端末に対し，ある一定時間以内に対応する ACK が届かなかった場合には，そのパケットが廃棄されたとみなして，送信端末が当該パケットを再送する．この一定時間は，再送タイマーにより管理される．再送信タイマーの最大待ち時間を再送信タイムアウト（RTO:Retransmisson Time Out）と呼び，RTO 以内に送信したパケットの応答が返ってこない場合，TCP は当該パケットが廃棄されたと判断し再送信する．RTO の初期値は RFC6298[12] により，次の式で設定される．

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

ここで $minRTO$ は RTO の最小値，$SRTT$ は平滑化したラウンドトリップタイム（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，$RTTAVR$ は RTT の平均偏差である．$minRTO$ は RFC6298 により，1 秒に設定することが推奨されている．多くの場合で (1) 式の右辺では

$$minRTO > SRTT + max(G, 4 \times RTTAVR) \quad (2)$$

が成り立つため，これ以降 RTO の初期値は $minRTO$ に設定されるものとする．

$$RTO_1 = minRTO \quad (3)$$

TCP 通信において，2 回以上連続して同じパケットがタイムアウトした場合，当該パケットが再送なく正常に応答を返すまでタイムアウトごとに RTO の値を 2 倍ずつ増加させていく．RTO_i を i 回連続でタイムアウトしたパケットの RTO の値とすると，この値は以下の (4) 式により設定される．ただし，RTO の上限値は 60 秒以上となるように制限されている．

$$RTO_i = 2RTO_{i-1} \quad (4)$$

当該パケットの送信と応答が成功した場合，(3) 式により RTO は $minRTO$ に再設定される．このアルゴリズムはほとんどの TCP で実装されているが，RTO_i が $minRTO$ に依存して一意に決定されるという単純な仕様が LDoS/LDDoS 攻撃に利用されている．

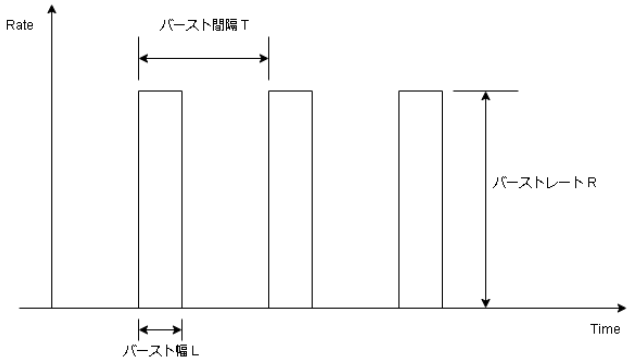

図 1 LDoS 攻撃フロー
Fig. 1 LDDoS Attack Flow

2.2 LDoS 攻撃

LDoS 攻撃は短いバーストトラフィックと無通信が一定の周期で繰り返される矩形波状の LDoS 攻撃フローを連続して送信することで，TCP で通信をしている標的サーバが喪失したパケットを再送信するわずかな時間の間のみ，対象の TCP コネクションのボトルネックリンクに輻輳を発生させてクライアントとの通信を妨害する攻撃手法である．LDoS 攻撃フローは**図 1** のようにバースト間隔 T，バースト幅 L，バーストレート R，の 3 つのパラメータにより定義される．ここで，T を $minRTO$ と等しい長さ，L を RTT 程度の長さ，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最も大きな効果を得られ，標的サーバの TCP コネクションのスループットを完全に抑止できる [13].

このときの攻撃について説明する．はじめに，攻撃者による 1 回目のバーストトラフィックにより，ボトルネックリンクのバッファが枯渇し正規の送信トラフィックにパケット喪失が発生する．次に，標的サーバは，$minRTO$ だけ再送信タイムアウトを待ったあと通信に失敗したパケットを再送信する．このとき，攻撃者が繰り返しバーストトラフィックを送信することで，再びボトルネックリンクのバッファが枯渇するため標的サーバの通信が再び失敗する．攻撃者はその後も標的サーバの $minRTO$ と同じバースト間隔でバーストトラフィックを送信し続けることで，標的サーバの RTO が，$minRTO$ の倍数の値を取り続けるため，バーストトラフィックと再送信のタイミングが重なり，通信が抑止された状態が継続される．

2.3 LDDoS 攻撃

LDDoS 攻撃は LDoS 攻撃フローを複数の攻撃ノードから分散して送信し，標的のボトルネックリンク上で集約することで LDoS 攻撃と同様に通信を妨害する攻撃手法である．バーストトラフィックを複数の攻撃ノードから分散して送信することで，攻撃ノード一台から送信されるトラフィックの大きさが LDoS 攻撃の場合と比較してさらに低

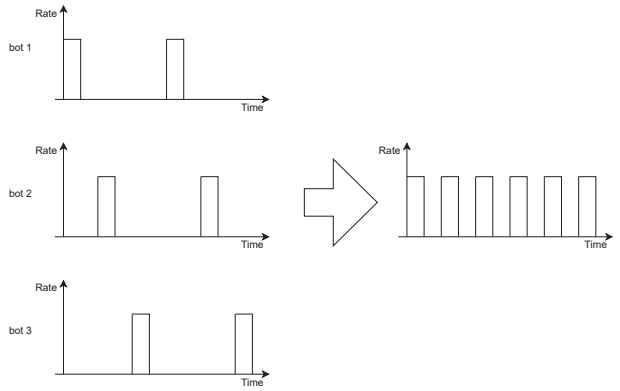

図 2 LDDoS 攻撃の例
Fig. 2 Examples of LDDoS attacks

量になるため，攻撃の検知をより困難にすることや，より強力な攻撃フローを生成することが可能になる [14]．**図 2** に LDDoS 攻撃の集約の例を示す．文献 [15] では，さらに詳細にモデル化されている．

3. 提案手法

LDDoS 攻撃の目的は，正常通信の再送を引き起こすことである．本研究では攻撃パケットであるかどうかの特定は行なわず，正常な通信のパケットロスを緩和する手法を提案する．本手法は，まずボトルネックリンクにおいて，一定時間におけるフローごとの受信時にキューからドロップしたパケット数を計測する．次にパケット損失率を次の式で求める．

$$D_R = \frac{D_n}{R_n} \tag{5}$$

ここで，D_R はパケット損失率，D_n はドロップしたパケット数，R_n は受信したパケット数である．攻撃フローはボトルネックリンクのキューを溢れさせる必要があるため，キューより多くのパケットを送信する．そのため，攻撃フローのパケットのパケット損失率は高くなる傾向がある．求めたパケット損失率と閾値を比較し，閾値以上のフローを優先度の低いプライオリティキューに入れる．プライオリティキューは優先度の高いキューから処理を行うため，優先度の低い攻撃フローの影響が緩和される．**図 3** に本手法のフローチャートを示す．

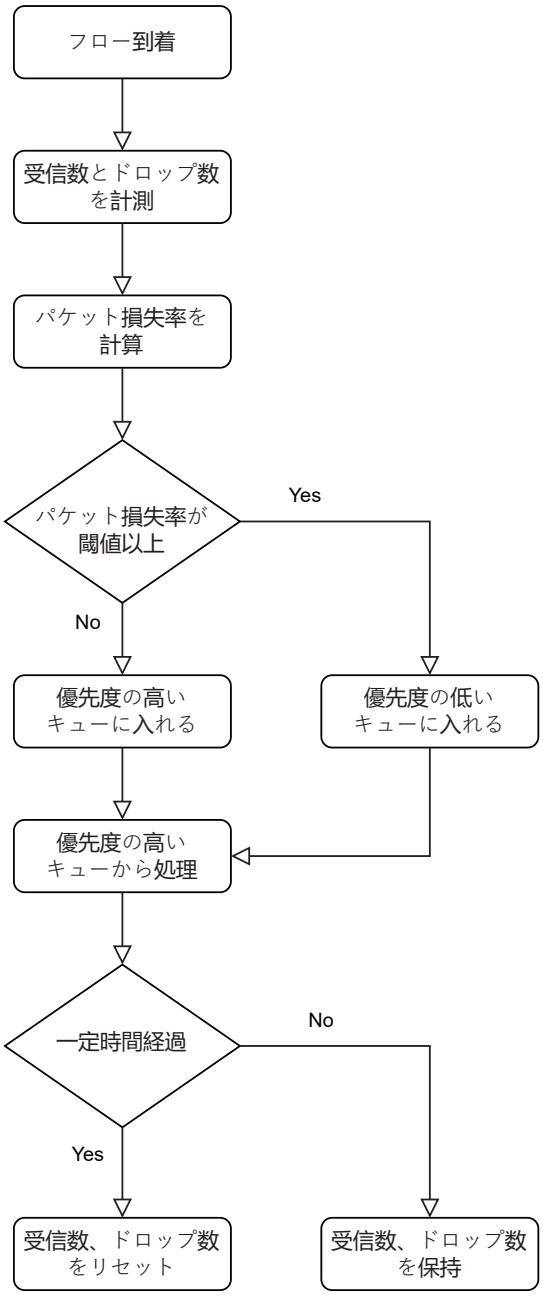

図 3 提案手法のアルゴリズム
Fig. 3 Algorithm of the proposed method

4. シミュレーション実験

4.1 シミュレーション環境の設定

提案手法の有効性を確認するために，シミュレーションを行った．シミュレーションはネットワークシミュレータ ns-3[16] を使用した．標的 TCP 送信サーバ 1 台，標的 TCP 受信クライアント 1 台，攻撃者 1 台，ルーター 2 台を作成し，それぞれを単純なダンベルトポロジーとなるように接続した．ボトルネックリンクの帯域幅は 1.5Mbps，RTT は 40ms とし，それ以外のリンクの帯域幅は 100Mbps，RTT は 2ms とした．作成したネットワーク構成を**図 4** に示す．

4.2 シミュレーションシナリオ

実験は以下の 3 つのシナリオファイルを用意して，実験を行った．

4.2.1 攻撃通信無しのシナリオ

このシナリオは攻撃者は攻撃通信を送信せず，標的 TCP 送信サーバからの通信のみ行う．ボトルネックリンクのキューはキューサイズが 1000 パケットの Drop Tail キュー

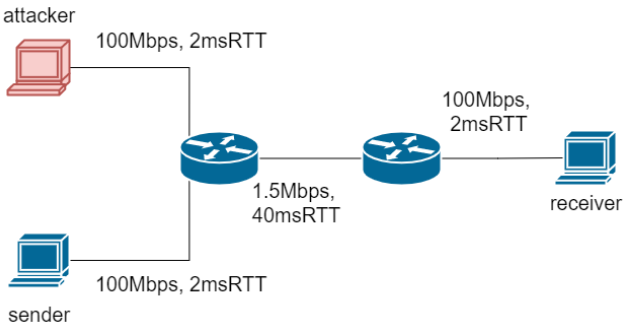

図 4 実験のネットワーク構成
Fig. 4 Network configuration of the experiment

表 1 シナリオ 4.2.1，シナリオ 4.2.2，シナリオ 4.2.3 の比較
Table 1 Comparison of scenario4.2.1, scenario4.2.2 and scenario4.2.3

	攻撃無し	攻撃有り	提案手法
送信パケット数	4066	93	587
受信パケット数	4066	91	484
パケットロス数	0	2	103
平均スループット (Kbps)	1444.44	8.42727	147.713

を利用する．標的 TCP 送信サーバは標的 TCP 受信サーバに対して，2MB のデータを 50 秒間可能な限り Bulk Send で送信し，スループットを計測する．また，フローごとの送信パケット数，受信パケット数，パケットロス数，平均スループットを計測する．

4.2.2 LDDoS 攻撃のシナリオ

このシナリオは攻撃者から標的 TCP 受信クライアントに対して，$T = 1s$，$L = 250ms$，$R = 12Mbps$ の UDP 通信を送信する．ボトルネックリンクのキューの設定，TCP 通信の設定は 4.2.1 と同様に設定する．また，TCP 通信のスループット，フローごとの送信パケット数，受信パケット数，パケットロス数，平均スループットを計測する．

4.2.3 提案手法のシナリオ

このシナリオは攻撃通信は 4.2.2 と同様に設定し，TCP 通信の設定は 4.2.1 と同様に設定する．ボトルネックリンクのキューは，提案手法を実装するためプライオリティキューを設定する．ボトルネックリンクでは，それぞれのフローのパケット損失率を計算し，プライオリティキューに割り当てる．また，また，TCP 通信のスループット，フローごとの送信パケット数，受信パケット数，パケットロス数，平均スループットを計測する．

4.3 実験結果

シナリオ 4.2.1 のシミュレーション結果を**図 5**，シナリオ 4.2.2 のシミュレーション結果を**図 6**，シナリオ 4.2.3 のシミュレーション結果を**図 7** に示す．また，それぞれのシナリオでの送受信パケット数，パケットロス数，平均スループットを**表 1** に示す．

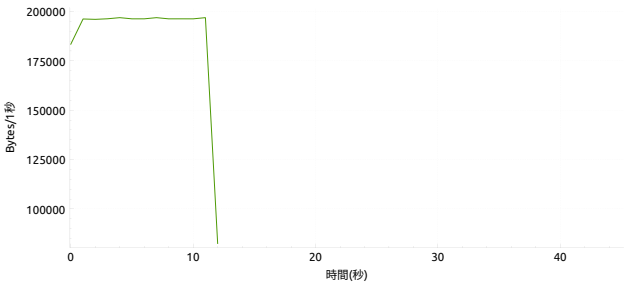

図 5 シナリオ 4.2.1 のスループットの遷移
Fig. 5 Transition of the throughput of scenario4.2.1

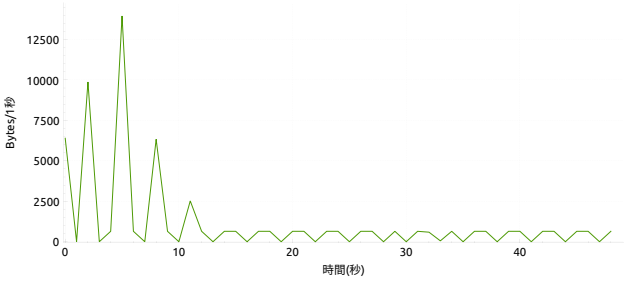

図 6 シナリオ 4.2.2 のスループットの遷移
Fig. 6 Transition of the throughput of scenario4.2.2

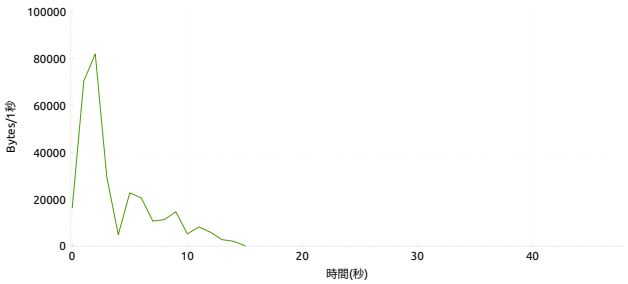

図 7 シナリオ 4.2.3 のスループットの遷移
Fig. 7 Transition of the throughput of scenario4.2.3

図 5，図 6，表 1 より，LDDoS 攻撃下では大幅にスループットが下がることがわかる．また，図 6，図 7，表 1 より，提案手法によってスループットが向上し，攻撃の影響を緩和できていることがわかる．実験結果より，提案手法を適用することによって LDDoS 攻撃を緩和し，平均スループットを約 18 倍に向上させることができた．また，送受信パケット数も提案手法を適用しない場合に比べて大幅に向上している．

4.4 考察

4.4.1 パケットロスの増加

実験結果より，提案手法を適用することによってパケットロス数が増えていることがわかる．これは，提案手法のない攻撃下では正常通信のフローはほとんど再送信の処理が行われており，パケットが失われていないと考えられる．一方で，提案手法では正常通信の処理が行われているため，

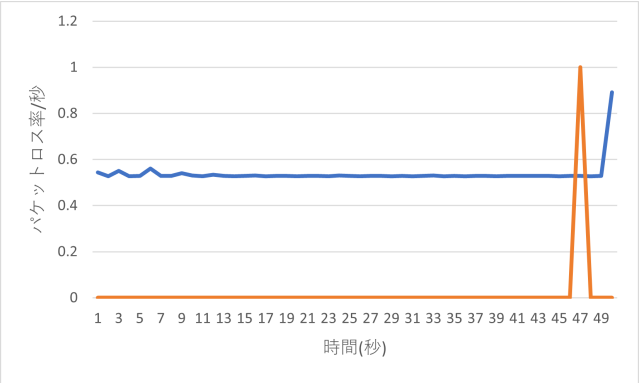

図 8 シナリオ 4.2.2 のパケットロス率の遷移
Fig. 8 Transition of the number of packet loss in scenario 4.2.2

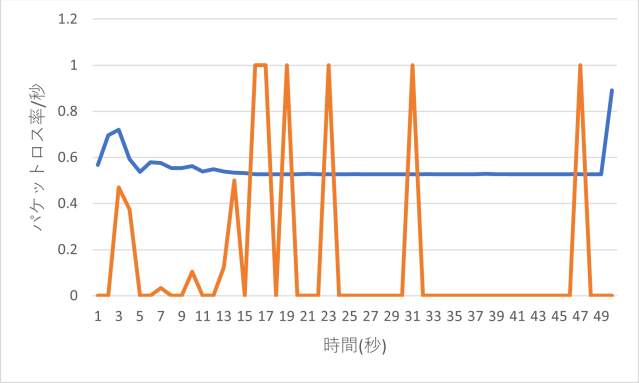

図 9 シナリオ 4.2.3 のパケットロス率の遷移
Fig. 9 Transition of the number of packet loss in scenario 4.2.3

攻撃通信によって溢れてしまったパケットは失われてしまい，その結果パケットロス数が大きくなったと考えられる．

4.4.2 閾値の設定

本研究では，閾値決定のために攻撃フローと正常フローのパケットドロップ数を比較した．提案手法を適用しない場合の結果を**図 8** に，提案手法を適用した場合の結果を**図 9** に示す．

図 8 より，パケットロス率に違いができているため，本研究においては閾値を 0.4 として実験を行った．しかし，図 9 より，正常通信のパケットロス率が 0.4 以上となる点が見られる．このことから，閾値を静的に決定すると提案手法の適用により，正常通信の優先度が低くなってしまう可能性がある．

5. おわりに

5.1 まとめ

本稿ではパケットロス率に着目し，プライオリティキューを利用することにより，LDDoS 攻撃を緩和する手法について提案した．ns-3 を使用したシミュレーションにより，提案手法を用いることでスループットを約 18 倍に向上させることが可能であることを示した．また，提案手法によって増加したパケットロス数や，閾値の影響についても考察した．

5.2 今後の展望

今回の実験で発見した課題について述べる．今回の実験では攻撃者が単一のマシンから攻撃を行う LDoS モデルでの実験であった．そのため，複数マシンからの攻撃であれば，攻撃を成功させるための条件がより複雑になる．また，今回のトポロジーは単純なダンベルトポロジーを用いて実験を行ったが，現実のネットワークはより複雑に構成されている．以上のことから，今後の課題は複数マシンからの攻撃での有効性の確認と，より現実のネットワークに近い構成での実験が挙げられる．さらに，4.4.2 で述べたように，静的な閾値では正常通信の優先度を下げてしまう可能性がある．そのため，閾値を動的に決定し，正常通信のフローを効率的に処理できるように改良していく必要がある．

参考文献

[1] : DNS サービスの「Dyn」に大規模 DDoS 攻撃、Twitter などが影響受けダウン — 日経クロステック（xTECH），https://xtech.nikkei.com/it/atcl/news/16/102203079/.
[2] : 000014123.pdf, https://www.ipa.go.jp/files/000014123.pdf.
[3] : 最多の DDoS 攻撃は「SYN フラッド」、CDNetworks が 2018 年第 1 四半期の動向を発表：中国で激増 - @ IT，https://www.atmarkit.co.jp/ait/articles/1808/17/news043.html.
[4] Kuzmanovic, A. and Knightly, E. W.: Low-rate TCP-targeted denial of service attacks and counter strategies, *IEEE/acm transactions on networking*, Vol. 14, No. 4, pp. 683–696 (2006).
[5] : Shrew's Homepage, https://users.cs.northwestern.edu/~akuzma/rice/shrew/.
[6] Kieu, M. V., Nguyen, D. T. and Nguyen, T. T.: Using CPR metric to detect and filter low-rate DDoS flows, *Proceedings of the Eighth International Symposium on Information and Communication Technology*, pp. 325–332 (2017).
[7] Jadhav, P. N. and Patil, B.: Low-rate DDOS attack detection using optimal objective entropy method, *International Journal of Computer Applications*, Vol. 78, No. 3 (2013).
[8] Xiang, Y., Li, K. and Zhou, W.: Low-rate DDoS attacks detection and traceback by using new information metrics, *IEEE transactions on information forensics and security*, Vol. 6, No. 2, pp. 426–437 (2011).
[9] 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).
[10] Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I. and Savenko, O.: Detection of the botnets' low-rate DDoS attacks based on self-similarity, *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 4, p. 3651 (2020).
[11] Chang, C.-W., Lee, S., Lin, B. and Wang, J.: The taming of the shrew: Mitigating low-rate TCP-targeted attack, *IEEE Transactions on Network and Service Management*, Vol. 7, No. 1, pp. 1–13 (2010).
[12] : RFC 6298: Computing TCP's Retransmission Timer,

https://www.rfc-editor.org/rfc/rfc6298.
[13] Efstathopoulos, P.: Practical study of a defense against low-rate TCP-targeted DoS attack, *2009 International Conference for Internet Technology and Secured Transactions,(ICITST)*, IEEE, pp. 1–6 (2009).
[14] 高橋佑太：低レート DDoS 攻撃の自動化に関する研究 (2021).
[15] Zhang, C., Cai, Z., Chen, W., Luo, X. and Yin, J.: Flow level detection and filtering of low-rate DDoS, *Computer Networks*, Vol. 56, No. 15, pp. 3417–3431 (2012).
[16] : ns-3 — a discrete-event network simulator for internet systems, https://www.nsnam.org/.