Experimental Evaluation of LDoS Attacks on QUIC

Ryuku Hisasue*, Akito Kawauchiya*, Hiroshi Inamura*, Shigemi Ishida*
* Future University Hakodate, Japan
Email: {g2122054, b1019110, inamura, ish}@fun.ac.jp

***Abstract*—QUIC has been used as a new standard communication protocol and as an alternative to TCP. This protocol has the retransmission control algorithm and congestion control algorithm similar to the TCP's functions. Thus, it can be considered that it is possible to exploit these functions for Low-rate DoS (LDoS) attacks. We aim to identify the existence of vulnerabilities that could be exploited by LDoS attacks and propose a new LDoS attack method on QUIC communications. Based on the hypothesis that LDoS attack methods for TCP are effective against QUIC communications, we performed simulation experiments with LDoS attacks against QUIC communications using the TCP-targeted method to verify the effectiveness of the attacks. We verified the factors of successful LDoS attacks on QUIC communications, proposed an LDoS attack method for QUIC communications, and evaluated the proposed LDoS attack.**

***Index Terms*—Low-rate DoS attack, QUIC**

I. Introduction

Low-rate DoS (LDoS) attacks that exploit vulnerability of TCP using pulse-shaped traffic are discussed [1]. This attack is difficult to detect because it uses pulse-shaped traffic, which results in a low average link bandwidth occupancy and is difficult to distinguish from normal traffic. Therefore, there are still some unanswered issues, one of which is the LDoS attack on QUIC communications.

QUIC is a transport protocol standardized by the Internet Engineering Task Force (IETF) in 2021, and implemented to reduce connection setup time including encryption suite negotiation. QUIC has the functions for highly reliable transfer and makes transfer-starting shorter than TCP, thus this protocol is used as an alternative to TCP. QUIC is used for about 2.8 billion monthly users' communications on Facebook [2], and more than 2 billion monthly users' communications on YouTube [3]. In detail, HTTP/3, the latest standardized version of HTTP, uses QUIC as its transport protocol [4]. These facts indicate that QUIC communication is widely used.

Since it can be predicted that the number of services using QUIC will continue to increase in the future, many communications using QUIC are threatened by LDoS attacks if LDoS attacks are effective for QUIC communications.

We aim to show the existence of algorithms that can be exploited in LDoS attacks effective for QUIC communication. In this paper, we present the results of an experimental evaluation of the potential for exploitation of QUIC's congestion control, BBR, using the ns-3 network simulator.

Our main contributions are twofold:

- Using the ns-3 network simulator QUIC model presented in [5], we showed that existing LDoS attack methods are highly effective against QUIC , and that congestion control is a key factor in the success of LDoS attack methods from the results of the attack implementation.
- Simulation results showed the feasibility of LDoS attacks on BBR on QUIC, and optimizing the parameters reduced the throughput of normal traffic by more than 80% with 25% of attack traffic bandwidth occupancy than the conventional method.

The paper is organized as follows. First, the background and purpose are shown. Section II reviews the related work to highlight existing LDoS methods against TCP. Section III describes the basic principles of QUIC and the retransmission control and congestion control algorithms that can be exploited by LDoS attacks. Section IV presents the results of an existing LDoS attack on QUIC communications, and Section V presents the evaluation results of an experiment to realize an LDoS attack against BBR on QUIC. Finally, Section VI concludes the paper.

II. Related Work

This Section describes existing research in terms of protocols that existing LDoS attack methods exploit to demonstrate the feasibility of LDoS attacks on QUIC.

A. The Model of LDoS Attacks

LDoS attacks use pulse-shaped attack traffic to lower the average bandwidth utilization and have a high degree of stealth [1].

Since pulse-shaped attack traffic of LDoS attacks, it can be modeled using three parameters: pulse rate R, pulse interval L, and pulse width T. The average amount of attack traffic R_{avr} in the range of $[a_{\mathrm{str}}, a_{\mathrm{end}}]$, where the a_{str} and a_{end} are the start and end times of the attack respectively; is given by the equation (1):

$$R_{avr} = R \cdot L\,/\,T \quad (R \geq C) \tag{1}$$

B. Shrew Method

The Shrew method is an LDoS attack method that sends attack traffic repeatedly toward the bottleneck link [6].

This method exploits two features of the retransmission timer in the TCP RTO process 1) the constant initial value of RTO called $minRTO$ and 2) updating the value of RTO by exponential backoff. When RTO is over the maximum value, TCP determines as a network anomaly and disconnects the connection [6]. The value of $minRTO$ is recommended set to 1 sec [7], and this makes it possible to attack.

In QUIC, the retransmission timer algorithm is substituted for other one called PTO, and there is no constant initial value such as $minRTO$. It can be considered that the Shrew method is not effective against QUIC.

C. RoQ Method

The RoQ method is another LDoS attack method that exploits the TCP Loss-Based Congestion Control algorithm [8].

978-4-907626-52-5/23/$31.00 ©2023 IPSJ

The loss-based congestion control algorithm detects congestion by packet loss.

This algorithm changes the congestion window size $cwnd$ to half of the number of sent packets. The RoQ method uses the fact that the number of sending packets can be reduced by half by causing packet loss before the congestion window size $cwnd$ returns to the state before congestion is detected.

The recovery of the congestion window size $cwnd$ is different for each queue control. In the case of a queue control method RED, the attack is succeeded by setting the attack interval T to 5 seconds [8].

III. QUIC Transport Protocol

QUIC is a connection-oriented communication protocol implemented on UDP to improve upon TCP [9]. TCP requires encryption protocols such as TLS [10] to encrypt packet data.

By running an encryption protocol on TCP, it is necessary to establish a connection for the encryption protocol in addition to the TCP three-way handshake. In contrast, QUIC incorporates TLS into the QUIC itself, enabling the connection establishment process to be performed in a single step up to the start of communication. This reduces the connection time to start the communication [11].

QUIC has the functions such as flow control, congestion control, and retransmission control to realize end-to-end, highly reliable connection-oriented communication similar to TCP. However, the specifications of these functions are different from those of TCP, and conventional LDoS attack methods are likely to be inapplicable.

To clarify the control algorithms that are possibly exploited by LDoS attacks, the next Section describes the retransmission timer and congestion control implemented in QUIC.

A. Retransmission Timer

The retransmission timer on QUIC measures the time from sending the packet to the corresponding ACK.

The difference between the retransmission timers of TCP and QUIC is that QUIC uses the calculation algorithm called PTO (Probe TimeOut) defined by equation (2):

$$PTO = SRTT + \max(4\times RTTVAR, 1) + max\_ack\_delay \qquad (2)$$

PTO is calculated from the sum of $SRTT$, $\max(G, 4 \times RTTVAR)$, and max_ack_delay [7]. The $SRTT$ is the smoothed RTT (Round Trip Time) value to reduce the effect of outliers. G is the clock granularity and $RTTVAR$ is the time variation of RTT. The max_ack_delay is a numerical value for delaying ACK time. PTO does not have a constant initial value as opposed to RTO on TCP [12].

QUIC uses max_ack_delay for calculating the initial value of PTO to the retransmission timer being not too short, so that a constant such as $minRTO$ does not require in PTO. Therefore, the value of PTO calculated by the equation (2) is difficult to estimate from the outside.

If a retransmission by the first PTO is failed, the second and subsequent PTO values are calculated as follows [7], same as the TCP retransmission timer RTO:

$$PTO_n = 2 \cdot PTO_{n-1} \qquad (3)$$

As we can see from the equation (3), if packet loss continues to occur after the second packet, the PTO value increases by a factor of two. Similar to TCP, QUIC's retransmission control also staggers the timing of packet transmission by calculating the formula (3) to retransmit packets more reliably. The maximum value of PTO is managed by the variable $idle\_timeout$. The $idle\_timeout$ is determined by end-to-end communication, and the minimum value is three times the current PTO.

The retransmission timer on QUIC differs from that of RTO of TCP, so it is not known what effect LDoS attacks using the Shrew method.

B. Delay-based Congestion Control

QUIC uses a Delay-Based congestion control called BBR (Bottleneck Bandwidth and Round-trip propagation time). The BBR switches control states by detecting changes in the RTT of the transmission delay.

The control state transition of BBR on QUIC is following. ProbeBWG_DOWN, ProbeBWG_CRUISE, ProbeBWG_REFILL, and ProbeBWG_UP to adjust the amount of data sent to about 90% of the bottleneck bandwidth, and ProbeBWQ_RTT detects congestion and suppresses the amount of data sent for a total of seven states classified into three purposes [13].

This behavior of adjusting the number of packets sent based on changes in BDP is different from that of TCP, so it is not known what effect the RoQ method will have when applied to QUIC.

IV. Applying Existing LDoS Methods to QUIC

In order to establish an LDoS attack method for QUIC communication, we hypothesize that the LDoS attack targeting TCP is also effective for QUIC communication with optimization. QUIC is designed to coexist with TCP in the flow and exhibit similar behavior.

LDoS attacks need to generate pulse-shaped attack traffic to maintain stealth, so optimization of the attack period T and attack duration L is required.

Due to the design similarities between TCP and QUIC, it is possible that LDoS attack methods that are effective for TCP are equally effective for QUIC. The retransmission timer RTO of TCP, which is exploited by the Shrew method, is replaced by PTO in QUIC, and the number of parameters used in the calculation is increased. The constant $minRTO$ used in the Shrew method has been removed in PTO, so the same attack as TCP may not succeed. NewReno, a loss-based congestion control method exploited by the RoQ method, has been replaced by a delay-based congestion control called BBR in QUIC. In BBR, the behavior of recognizing congestion triggered by packet loss in NewReno, which was exploited in the RoQ method, has been changed to recognizing congestion when the RTT worsens.

In this Section, we examine whether these differences in behavior affect the attack effectiveness to QUIC communications using the conventional LDoS attack method against TCP. We then clarify the algorithm that constitutes the LDoS attack in QUIC. Finally, we the optimal LDoS attack parameters for QUIC, then modify the parameters and compare the bandwidth utilization and average throughput decrease rate.

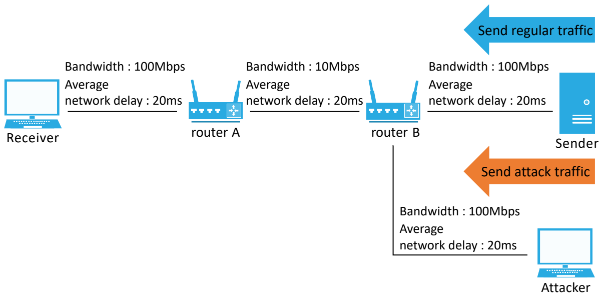

Fig. 1. Network configuration diagram used in the experiment

A. Experiment Setup

We set up a virtual network environment on network simulator tool ns-3 with the topology shown in Fig. 1. We used the module extension for QUIC communication implemented by Paro et al. [5]. We conducted experiments for 35 seconds, and attacks were started 5 seconds after to make the communication stable.

For each parameter, we evaluate the results of the average throughput decrease rate and the bottleneck link bandwidth occupancy rate on TCP and QUIC communications with LDoS Attacks and without the attack.

The average throughput decrease rate D is defined by equation (4):

$$D = (\alpha_{\text{normal}} - \alpha_{\text{onAttack}}) \ / \ \alpha_{\text{normal}} \tag{4}$$

where the throughput of the target traffic with attack is α_{onAttack}, and without attack is α_{normal}.

B. Conducting Shrew Attack to QUIC

We conducted the Shrew attack against TCP and QUIC using traffic which is the attack interval T of 1 second and the attack duration L of 0.3 seconds. Table I shows the results of the evaluation.

First, we calculated the throughput decrease rate D of target traffic on TCP (NewReno) traffic. The values of average throughput with attack α_{onAttack} was 1.07 Mbps and average throughput without attack α_{normal} was 9.13 Mbps. Thus, the throughput decrease rate $D = 88.3\%$ from equation (4).

Next, we calculated the throughput decrease rate D of target traffic on QUIC traffic. The values of average throughput with attack α_{onAttack} was 1.30 Mbps and average throughput without attack α_{normal} was 8.22 Mbps. Thus, the throughput decrease rate $D = 84.2\%$ from equation (4).

These results show conventional LDoS attack is highly effective against TCP (NewReno) and QUIC as the average throughput is reduced by more than 80%, and highly effective against QUIC communications under the simulation.

C. Exploitable algorithm on QUIC

To track the behavior of the retransmission timer, simulate applying LDoS attacks to QUIC communication, and log the calls to the retransmission timer. The log output of the retransmission timer reveals whether the retransmission timer is related to the success of the LDoS attack or not.

Furthermore, in order to track the behavior of BBR which is QUIC's congestion control, we examined the following two types of communications that use BBR for congestion control.

TABLE I
AVERAGE THROUGHPUT DECREASE RATE AND BANDWIDTH OCCUPANCY RATE WHERE $L = 0.3, T = 1.0$

Protocol	α_{normal} (Mbps)	α_{onAttack} (Mbps)	Throughput decrease rate D (%)
TCP	9.13	1.07	88.3
QUIC	8.22	1.30	84.2

We applied the LDoS attack to the TCP and the QUIC, and output the values of the congestion window size $cwnd$. We discuss the similarity of the behavior of the two protocols by logging the values of the congestion window size $cwnd$ of QUIC and TCP. If the change of cwnd is similar to that of TCP (BBR), it can be confirmed that the LDoS attack is launched against BBR. This confirms that a LDoS attack is launched against the BBR. This clarify whether congestion control is involved in the success of the LDoS attack.

First, we have confirmed whether a timeout occurs during an LDoS attack using the Shrew method by using a simulator, and found that no timeouts were observed during the LDoS attack on the QUIC communication. The logs related to the timer were checked from the start of the experiment to the time when the LDoS attack occurred. TLP (Tail Loss Probe) logs were observed about three times from the start of the experiment until the LDoS attack occurred. TLP is an algorithm that sends probes to avoid retransmission timer timeouts and checks for ACKs. [14]. These results indicate that the retransmission timer timeout does not occur and that the above results indicate that the retransmission timer is not involved in the success of the attack.

Next, in order to find whether the bandwidth throttling of normal communication is due to the congestion control behavior, we checked the change in the value of the congestion window size cwnd during the attack on TCP (BBR) and QUIC communications using a simulator. The output results for the change in TCP (BBR) congestion window size $cwnd$ show that the congestion window size is significantly low value 42,520 Bytes from 6 seconds onward when the TCP (BBR) throughput is significantly reduced due to the attack. The congestion window size continues to decrease after 5 seconds, when QUIC throughput is significantly reduced due to the attack, and shows a low value of 536 Bytes after 7 seconds when it is significantly lower. The behavior of the congestion window size $cwnd$ for these two protocols indicates that the LDoS attack has the effect of misleading the congestion control BBR to believe that congestion continues to occur, since the congestion control BBR occupies an average of about 30% of the bandwidth per second. The behavior of $cwnd$ is similar to that of $cwnd$ in QUIC.

These results show that the low-rate DoS attack was effective for QUIC. The application of the pulse used in the Shrew attack for TCP resulted in transmission suppression due to the behavior of the congestion control BBR. This behavior was close to that expected from the RoQ attack.

V. RoQ ATTACK AGAINST BBR ON QUIC

We propose RoQ Attack against BBR on QUIC (RABQ) method based on the key idea of conventional RoQ method described in related work. RABQ method targets BBR con-

TABLE II
PERCENTAGE OF BANDWIDTH OCCUPIED AND AVERAGE THROUGHPUT REDUCED

Attack duration L (s)	Attack period T (s)	Bandwidth occupancy W (%)	Throughput decrease rate D (%)
0.3	1.0	30.0	84.2
0.15	3.0	5.0	77.8
0.2	3.0	6.7	77.8
0.15	2.0	7.5	80.5
0.2	2.0	10.0	80.7
0.15	1.0	15.0	83.7
0.2	1.0	20.0	83.8

gestion control in QUIC communication and $cwnd$ keeps decreasing.

In LDoS attacks, the stealthy is important indicator especially RoQ method. This is also important in RABQ attack, so we define bandwidth occupancy rate of attack traffic W by equation (5):

$$W = L \cdot R \ / \ T \cdot C \tag{5}$$

where attack traffic's duration L, rate R, period T and bottleneck link bandwidth C.

To evaluate the performance of the proposed RABQ method, the results of applying the existing Shrew method to QUIC as described in Section IV, and the results of the RABQ method are shown in table II, which shows the W bandwidth share and D throughput decrease rate.

As shown in Section IV-C, when the Shrew method parameters attack duration $L = 0.3$ and attack period $T = 1.0$, the throughput degradation rate was 84.2%. In this condition, the bandwidth occupancy $W = 30.0$ from the equation (5).

When attack period $L = 1.0$ and attack duration L were varied from 0.2 to 0.15, the difference in throughput degradation rate was at most 0.5%. When the attack period T was set to 2.0, the throughput degradation rate was around 80%. When the attack period T was set to 3.0, the attack effect was less than 80%.

When attack period $L = 2.0$ and attack duration $L = 0.15$, the bandwidth consumption was 7.5%. Thus, the bandwidth occupancy rate of attack traffic is reduced to 25% compared to the bandwidth consumption of $W = 30$ in the Shrew method with optimizing parameters. In addition, link bandwidth utilization is less than 30% in this condition.

These results indicate that the RABQ method can exploit the BBR on QUIC and reduce throughput by more than 80% while reducing bandwidth utilization.

VI. CONCLUSION

The topic of applying LDoS attacks to QUIC communications and verifying their feasibility has not been extensively studied. In this paper, we hypothesized that existing LDoS attacks are electable because of the similarity between the QUIC and TCP designs, and verify their effectiveness by applying LDoS attacks to QUIC communications.

The results revealed that the existing LDoS attack methods, when applied to the ns-3 QUIC model presented in [5], were highly effective against QUIC communications, as hypothesized.

In order to form attack traffic more suitable for QUIC communication, we conducted a verification of the success factors of the LDoS attack method. As a result, it is clear that the LDoS attack against QUIC's communication can make misidentify QUIC's communication into a state of continuous congestion.

Therefore, we examined the kind of attack traffic could be formed to mislead QUIC into believing that it is continuously congested and to improve stealthiness over Shrew LDoS attacks. We proposed the RABQ method as an LDoS attack suitable for QUIC communication based on the existing RoQ method with verifying the condition that can misidentify congestion.

The RABQ method succeeded in reducing bandwidth consumption of attack traffic to 25% with the cost of minor loss in attack effect, compared to LDoS attacks with an attack interval of 1 second and an attack duration of 0.3 seconds, which typically seen in Shrew method, indicating that the proposed method is more stealth.

ACKNOWLEDGMENT

This work was supported by JSPS Grant-in-Aid for Scientific Research JP20K11772.

REFERENCES

[1] W. Zhijun, L. Wenjing, L. Liang *et al.*, "Low-rate DoS attacks, detection, defense, and challenges: A survey," *IEEE access*, vol. 8, pp. 43 920–43 943, 2020, publisher: IEEE.

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

[3] maprg, "Some updates on quic deployment numbers, https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-quic-deployment-update-00."

[4] M. Bishop, "HTTP/3, https://datatracker.ietf.org/doc/rfc9114," Internet Engineering Task Force, Request for Comments RFC 9114, Jun. 2022.

[5] U. Paro, F. Chiariotti, A. A. Deshpande *et al.*, "Extending the ns-3 QUIC Module," in *Proceedings of the 23rd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. Alicante Spain: ACM, Nov. 2020, pp. 19–26. [Online]. Available: https://dl.acm.org/doi/10.1145/3416010.3423224

[6] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, 2003, pp. 75–86.

[7] M. Sargent, J. Chu, V. Paxson *et al.*, "Computing TCP's Retransmission Timer," Internet Engineering Task Force, Request for Comments RFC 6298, Jun. 2011. [Online]. Available: https://datatracker.ietf.org/doc/rfc6298

[8] M. Guirguis, A. Bestavros, I. Matta *et al.*, "Reduction of quality (RoQ) attacks on internet end-systems," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2. IEEE, 2005, pp. 1362–1372.

[9] W. Alyssa, H. Ryan, and S. Ian, "A QUIC update on Google's experimental transport." [Online]. Available: https://blog.chromium.org/2015/04/a-quic-update-on-googles-experimental.html

[10] M. Thomson and S. Turner, "Using TLS to Secure QUIC, https://datatracker.ietf.org/doc/rfc9001," Internet Engineering Task Force, Request for Comments RFC 9001, May 2021.

[11] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport, https://datatracker.ietf.org/doc/rfc9000," Internet Engineering Task Force, Request for Comments RFC 9000, May 2021.

[12] TCPM, "QUIC Loss Detection & Congestion Contorol draft-itef-quic-recovery, https://https://datatracker.ietf.org/meeting/103/materials/slides-103-tcpm-sessb-quic-loss-detection-congestion-control-01."

[13] N. Cardwell, Y. Cheng, S. H. Yeganeh *et al.*, "BBR Congestion Control," Internet Engineering Task Force, Internet Draft, Mar. 2022. [Online]. Available: https://datatracker.ietf.org/doc/draft-cardwell-iccrg-bbr-congestion-control

[14] Y. Cheng, N. Cardwell, N. Dukkipati *et al.*, "The RACK-TLP Loss Detection Algorithm for TCP," Internet Engineering Task Force, Request for Comments RFC 8985, Feb. 2021.