Design of Low-rate DoS Attack Detection in Robust WRED

Daisuke Sato†, Hiroshi Inamura*, Shigemi Ishida*, Yoshitaka Nakamura‡,

†Graduate School of Systems Information Science, Future University Hakodate, Japan
‡Faculty of Engineering, Kyoto Tachibana University, Japan
* School of Systems Information Science, Future University Hakodate, Japan

Abstract - Low-rate DoS attacks degrade TCP transmission performance by exploiting a vulnerability in TCP's RTO mechanism. Since the average attack traffic is small, it is difficult to detect it with conventional DoS attack method. One of the problems in existing mechanisms are their low resistance to miss-detections. Based on the characteristics of low-rate DoS attacks, we designed a Robust WRED algorithm as a mitigation mechanism with improved resistance to detection errors.

Keywords: DoS, Low-rate DoS, WRED, Network Security

1 Introduction

Denial of Service (DoS) attacks and Distributed DoS (DDoS) attacks are one of the major threats in the network security field. DDoS attacks are more large-scale attacks than DoS attacks and are a bigger threat. Examples of large-scale DDoS attacks include the world's largest bps (bits per second) type DDoS attack [1] targeting GitHub in 2018, which recorded a maximum of 1.35Tbps; One example is the pps (packets per second) type DDoS attack [2], which was the largest in history, targeting a major European bank. In both cases, service denial was successful by generating a large amount of attack traffic, but it was restored in about 10 minutes by Akamai's response[1][2]. This indicates that DDoS attacks have a large amount of attack traffic, so capturing and detecting the characteristics is easy. Low-rate DoS (LDoS: Low-rate DoS, also known as Low-rate Shrew DoS) attacks[3] can block TCP flow with a low average attack traffic volume[3][4]. Since LDoS attacks have a low average attack traffic volume, detection methods based on traffic volume for DoS attacks and DDoS attacks are difficult to detect[5]. Therefore, research on detection methods of LDoS attacks is required.

RED (Random Early Detection) and WRED (Weighted RED), which are representative algorithms of AQM (Active Queue Management), are widely used on the Internet[6]. However, existing research indicates that RED is vulnerable to LDoS attacks[4][7]. RRED (Robust RED) has been proposed as a method to eliminate the vulnerability of RED to LDoS attacks[8]. RRED protects network resources from LDoS attacks and stabilizes flow by installing detectors and detecting and discarding LDoS attack traffic before queuing by RED. However, the detection conditions for LDoS attacks in RRED's detectors are high in false positives, and there is a possibility that normal flow other than LDoS attack traffic will also be suppressed[8].

While there are efforts to improve the detection accuracy of LDoS attack detection methods, we believe that it is necessary to propose a defense mechanism that assumes that detection results include unconfident results. The degree to which a given traffic is the optimal pulse waveform shape for LDoS attacks can be used to identify and mitigate attack traffic. We propose Robust WRED (RWRED), a multi-class RED that can identify and mitigate attacks using WRED. We conducted simulation experiments and confirmed that the proposed Robust WRED successfully divided bandwidth based on the degree of LDoS conformance.

The remainder of this paper is organized as follows. Section 2 describes the basics of LDoS attack and RED algorithm as well as related work. Section 5 presents the design of our Robust WRED (RWRED), followed by simulation evaluations in Section 6. Finally, Section 7 concludes the paper.

2 LDoS Attack and RED

This section describes the following related techniques necessary for the discussion: Low-rate Shrew DoS attacks intentionally cause continuous TCP retransmission timeouts. This study utilizes RED and its derivative algorithm, WRED.

2.1 TCP Retransmission Time Out

In TCP communication, a retransmission timer is started each time a packet is sent. If no response is received from the receiver within *minRTO* of the minimum RTO (Retransmission Time Out), which is the maximum waiting time of the retransmission timer, the packet is considered to be lost and the packet is retransmitted. The initial value of RTO is determined by the formula (1).

$$\begin{aligned} RTO = \quad & \max \quad \{minRTO, SRTT \\ & + \quad \max(G, RTTAVR \times 4)\} \end{aligned} \tag{1}$$

$$minRTO > SRTT + \max(G, RTTAVR \times 4) \tag{2}$$

where *minRTO* is the minimum value of *RTO*, *SRTT* is the smoothed round trip time (RTT), *G* is the operating system-dependent clock granularity, and *RTTAVR* is the mean deviation of *RTT*. *RTO* is recommended by the IETF to be set to a minimum value of 1s[9]. In many cases, the initial value of RTO is set to minRTO as in the formula (3) because the formula (1) holds in many cases. The initial value of RTO is generally set to minRTO, as in the formula (3).

$$RTO_1 = minRTO \tag{3}$$

$$RTO_{\mathrm{i}} = RTO_{\mathrm{i}-1} \times 2 \tag{4}$$

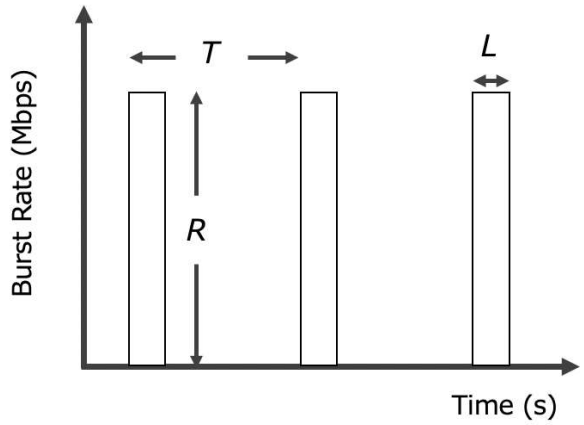

Figure 1: Attack Parameter

In TCP, RFC 6298[10] defines the specification that when it is judged that the same packet has been dropped consecutively, the RTO is retransmitted with the RTO increased by a factor of two. If no response is received from the receiver within *RTO* of a packet sent *RTO* times consecutively, the RTO_i of the packet is set by the expression (4). However, RFC 6298 indicates that the maximum value of *RTO* shall be 60s or longer. If the packet is successfully transmitted, *RTO* is reset to its initial value *minRTO*. This is called Karn's algorithm and is implemented as a retransmission control algorithm in most TCP implementations[11].

2.2 Low-rate Shrew DoS Attack

The LDoS attack was demonstrated in 2003 by Kuzmanovic and Nightly[3]. the LDoS attack consists of three parameters $\langle R, L, T \rangle$, as shown in Figure1. where R is the burst rate, L is the burst length, and T is the burst interval. LDoS attacks are stealthy DoS attacks because they achieve DoS attacks with low average traffic volume and are difficult to distinguish from the general traffic. LDoS attacks are attacks against transport layer protocols that exploit the retransmission timeout mechanism of the TCP retransmission control algorithm. TCP detects a packet loss if no ACK is returned from the destination after waiting *RTO*. If packet loss occurs continuously, *RTO* is set by the formula (4) and increases periodically.

We explain the specific attack method by assuming that the bandwidth and buffer size of the bottleneck link in the network over which the target TCP is communicating is C and B, respectively. First, a target TCP packet is lost by sending enough attack traffic to satisfy C and B. The target TCP packet is continuously lost by sending the attack traffic again at the time when the packet retransmits. The LDoS attack can be considered as a packet that sends attack traffic with a parameter R of C, L long enough to fill B or R long enough to fill C, L long enough to fill B, and L long enough to fill C. If the length of the traffic parameter R is set to *RTT* of the target TCP or T is set to *minRTO* of the target TCP, the TCP flow will be more suppressed[12].

2.3 RED Algorithm

The RED algorithm is a buffer management technique[13] proposed as a congestion avoidance strategy for TCP networks. The main design goal of the RED algorithm is to provide congestion avoidance to the network by monitoring and controlling the average queue size. The RED algorithm provides early congestion detection by monitoring the average queue size, notifying hosts by marking packets to control the average queue size and dropping packets early. When a sender is notified of early congestion, it can reduce the amount of traffic, thereby reducing network performance degradation.

Initial congestion detected by the RED algorithm is notified to the host by either dropping packets or marking packets. Packets are divided into three categories based on the average queue size, which is divided into two thresholds, the maximum threshold, and the minimum threshold, and each category is processed differently. If the average queue size is less than the minimum threshold, the packet is enqueued without packet marking or packet discarding. When the average queue size is greater than the minimum threshold and less than the maximum threshold, packet marking and discarding are performed based on the packet marking probability, which increases proportionally to the average queue size. If the average queue size is greater than the maximum threshold, packet marking or packet discarding is performed for all packets.

2.4 WRED

The WRED (Weighted RED) algorithm can run the RED algorithm separately for each traffic class. [14][15]. The WRED algorithm integrates the functionality of the RED algorithm with the Precedence functionality to achieve preferential traffic processing for packets with high Precedence[6]. Here, the WRED algorithm can set minimum and maximum thresholds based on Precedence, and the thresholds are generally set higher for higher priorities[13]. The WRED algorithm refers to the precedence when discarding packets and can manipulate the discard probability using thresholds by precedence. Since the maximum and minimum thresholds can be set for each precedence, packets with higher precedence can be enqueued preferentially.

3 Related Study

LDoS attacks are difficult to detect using volume-based detection methods for DoS and DDoS attacks because LDoS attacks succeed with low average attack traffic by generating attack pulses in RTO cycles. Therefore, various approaches have been studied for the detection of LDoS attacks, and some of them are based on the attack parameters such as burst length L and burst interval T to detect the attacking traffic. [16]. The method detects LDoS attack traffic as 1-second bursts whose burst length L is greater than or equal to the RTT of other flows connected to the same server and whose burst interval T is *minRTO*. This detection method is a basic detection method for detecting pulse-wave attack traffic, which is a characteristic of LDoS attacks. This LDoS attack detection method is referred to as the attack parameter-based LDoS attack detection method and the conventional LDoS attack detection

method. The conventional LDoS attack detection method assumes only optimized attack pulses, and it is believed that manipulating the attack parameters of LDoS attacks and changing them from the optimal parameter values can avoid detection.

As one of the defense methods against the LDoS attack proposed by Kuzmanovic et al.[3], we investigate attack mitigation by detection and throttling at routers. RED-PD (RED with Preferential Dropping)[17] or RED is applied to routers to verify the identifiability of attack flows for LDoS attacks by comparing the target TCP throughput. RED-PD detects LDoS attack traffic by setting a target bandwidth, but its performance is shown to be insufficient as a detection method. PD could be improved by applying strong bandwidth limiting only to flows with high potential for LDoS attack traffic, instead of bandwidth limiting all flows fairly.

There is an existing detection method[16] that uses burst length (L) and burst interval (T) as detection criteria. This detection method measures the length of burst transmission time and the time interval between burst transmission in the flow to be detected and detects attacks based on the similarity between the optimal values of burst length (L) and burst interval (T). Flows with high similarity are judged as attack flows, and those with low similarity are judged as normal flows. The optimal values of burst length (L) and burst interval (T) are the same as the recommended values of L for 2RTT-3RTT and 1-second burst interval (T) for other flows connected to the same server. Thus, the optimal value of the attack parameter is used for detection.

However, existing detection methods may falsely detect attack flows as normal flows. Since the optimal values of burst length (L) and burst interval (T) are used as the detection criteria, LDoS attacks that manipulate burst length (L) may be falsely detected as normal flows. For example, consider the case of an attack in a network where the bandwidth of the bottleneck link is C. If the optimal attack parameters for detection are $R = C$, $L = 200$ms, and $T = 1000$ms, and the attack parameters set for the attack flow are $R = C$, $L = 100$ms, and $T = 1000$ms, the attack If the attack parameters are set to $R = C$, $L = 100$ms, and $T = 1000$ms, the attack flow is mistakenly judged as a normal flow and false detection occurs.

4 Research Goal and Proposed Method

The objective of this study is to improve the immunity to miss-detection of existing suppression mechanisms. The existing suppression mechanism, Robust RED[8], has a low tolerance to miss-detection, and when a miss-detection occurs, it may protect attacking flows and deter normal flows. The reason for the low immunity to positive in existing suppression mechanisms is that they deter attacks by processing only two types of flows: 100 % attacking flows and 100 % normal flows.

We propose a method of suppression based on the *degree* of LDoS attack flow, instead of classifying it in two ways: attack flow or normal flow. In addition to discarding and queuing, we also provide multiple partial discards. Specifically, we construct an attack detection and mitigation mechanism based on the RED algorithm for LDoS attacks. Based on the existing Robust RED algorithm, our method is multi-classed by replacing the queuing mechanism from RED to WRED and mitigates LDoS attacks, and protects TCP flows by prioritizing traffic according to the probability of the traffic being LDoS attack traffic as identified by the attack detection part. The proposed method is called Robust WRED. The proposed method is called Robust WRED (RWRED).

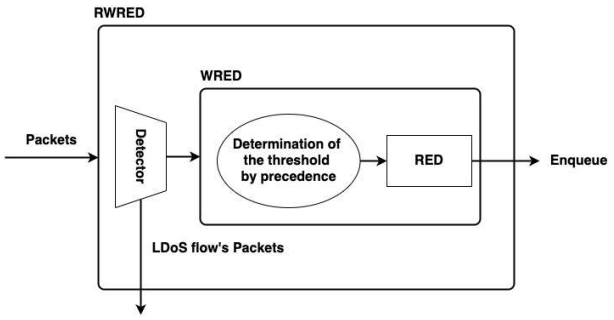

Figure 2: RWRED system

5 Design of Robust WRED

5.1 Overview of RWRED

The RWRED is designed based on the RRED[8] and has a Detector block in front of the WRED block as shown in Figure 2. The Detector block identifies incoming packets by the flow and calculates the probability of LDoS attack traffic for each flow. The Detector block identifies each input packet and calculates the probability that the packet is LDoS attack traffic for each flow. The packets are identified by source IP address, destination IP address, source port number, destination port number, and flow protocol, which are obtained from the header of the input packet. Depending on the calculated probability of the packet being LDoS attack traffic, the Detector block either drops the packet or marks it as a Precedence (IP Precedence). Packets with a high probability of being LDoS attack traffic are queued inferiorly, and packets with a low probability of being LDoS attack traffic are queued preferentially. It behaves as if bandwidth is reserved for the flow with a low probability of being LDoS attack traffic.

Since the RWRED mechanism can prioritize LDoS attack traffic according to its probability of being LDoS attack traffic, it is thought to be able to detect and deter LDoS attack traffic while protecting normal traffic.

5.2 LDoS Conformance Index for Attack Detection

We define the LDoS Conformance Index (LCI), which indicates the degree to which a given flow is a malicious LDoS/LDDoS traffic, as the basis for Robust WRED priority control. We apply an existing detection method[16], to define LDoS Conformance Index for detection based on attack parameters. Since existing detection methods use the optimal values of burst length (L) and burst interval(T) as criteria for detection, we define LDoS Conformance by the similarity between burst length (L) and burst interval(T). From the above, we define

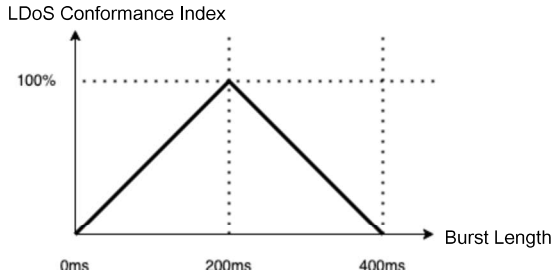

Figure 3: LCI for Burst Length(L)

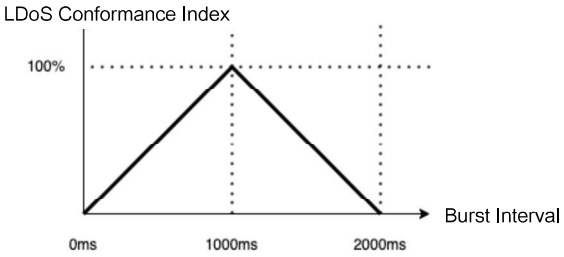

Figure 4: LCI for Burst Interval(T)

the Overall LDoS Conformance Index as the product of the LDoS Conformance Index of burst length (L) and the LDoS Conformance Index of burst interval (T).

Since the optimal attack parameters for detection are L = 200ms and T = 1000ms, burst length (L) takes values in the range of 0ms-400ms based on 200ms. The definition of the LDoS Conformance Index for burst length (L) is shown in Figure 3. For example, if the length of the burst transmission in the flow to be detected is 0 ms and 400 ms, the LCI of the burst length (L) is 0.0 percent. When the length of burst transmission in the flow to be detected is 100ms and 300ms, LCI of the burst length (L) is 50.0%.

LCI for burst interval (T) is similar to that of the burst length (L), taking values in the range of 0ms-2000ms with 1000ms as the reference. Figure 4 shows the definition of LCI for burst interval (T). Thus, we define the LDoS Conformance Index for attack parameter-based detection as the product of the LCI for burst length (L) and the LCI for burst interval (T). To reproduce the conventional detection method, 50% LCI is used as the decision threshold.

5.3 Link Share and RED Threshold derived from LCI

Set the threshold value to be given to the WRED queue control from the ideal bandwidth share in order to split the flow according to the LDoS Conformance Index.

In order to suppress LDoS attack traffic and allow normal traffic to pass, the appropriate bandwidth to be given to the flow in question using the LDoS conformance is considered to be $LinkBandwidth \propto (1 - LCI_i)$. To express the per-flow share of the link bandwidth, we define the per-flow Normalized Flow Share (NFS), which is normalized with respect

Table 1: Ideal Link Share and LCI

	LCI	ideal Link Share
TCP Sender 1	0.00(0%)	100[Mbps]×0.250=25.0[Mbps]
TCP Sender 2	0.10(10%)	100[Mbps]×0.225=22.5[Mbps]
TCP Sender 3	0.20(20%)	100[Mbps]×0.200=20.0[Mbps]
TCP Sender 4	0.30(30%)	100[Mbps]×0.175=17.5[Mbps]
TCP Sender 5	0.40(40%)	100[Mbps]×0.150=15.0[Mbps]

to the link bandwidth, as follows

$$NFS_i = \frac{(1 - LCI_i)}{\sum_{f \in AllFlowintheLink}(1 - LCI_f)} \quad (5)$$

$$FS_i = \text{(Link-bandwidth)} \times NFS_i \quad (6)$$

Ideally, link bandwidth should be divided according to the LDoS Conformance Index for each flow. Equation (5) is a formula for calculating the ideal bandwidth partition for each flow, and equation (6) is a formula for calculating the ideal acquisition bandwidth for each flow. Table reftab:ideal shows the relationship between the ideal acquired bandwidth and LDoS conformance calculated using the formula (6) . As described above, the ideal link bandwidth share according to LDoS Conformance Index is defined by (5).

$$Max\_thresh_i = \text{(Upper limit of threshhold)} \times NFS_i \quad (7)$$

To achieve bandwidth partitioning according to LDoS conformance, the threshold is optimized. The ideal bandwidth allocation is given by the formula (5), and the queue control parameter Max_thresh_i for each flow given to WRED is determined using the formula (7).

5.4 Handling Non-Adaptive Protocols

In order to treat non-adaptive protocol flow fairly with adaptive protocol flow, the minimum and maximum thresholds of the RED algorithm are set to the same value and a process such as Tail Drop is performed. Non-adaptive flows are trasmitted by UDP protocols, while adaptive flows are transmitted by TCP in this paper. There is a difference between TCP and UDP in whether or not the amount of data sent is reduced when packets are dropped. This difference may cause non-adaptive flow to occupy undue bandwidth. The proposed mechanism solves this problem by limiting the queue lengths available for non-adaptive flow for providing extra resources for adaptive flow. For the non-adaptive flow, we apply a Tail Drop-like process by setting the minimum and maximum thresholds to the thresholds calculated by the minimum threshold, thus, the suppression is stronger than for the non-adaptive flow.

6 Evaluation Plan of RWRED performance

6.1 Overview of Experiments

The purpose of the evaluation simulation is to clarify that the proposed mechanism, Robust WRED, is more tolerant to miss-detection than the existing mechanism, Robust RED.

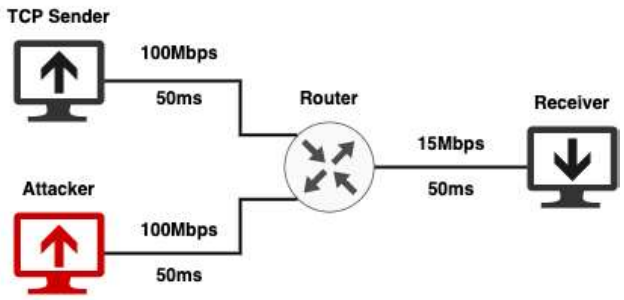

Figure 5: Simulation Scenario for Evaluation 1

We evaluate the resistance to miss-detection of the proposed mechanism and the existing mechanism.

Existing detection mechanisms are likely to cause detection errors. Based on the simulation results of the validation in Section 6.2, the existing detection has a high likelihood of overlook LDoS attacks with burst length (L) set outside of the optimal value, as normal flows, and a high likelihood of falsely detecting TCP flows with RTT set close to the optimal burst length (L) as attacking flows. (L) is more likely to be miss-detected as an attack flow than a TCP flow whose RTT is set close to the optimal value of burst length (L).

6.2 Experiment Setting

Figure 5 shows the evaluation simulation environment used in Evaluation 1. The evaluation system was constructed using ns-3[18], a discrete event network simulator. The network consists of four nodes: TCP Sender, which sends TCP packets, Attacker, which is the LDoS attack node, Router, which is the intermediate node, and Receiver, which is the receiving node. The bandwidth of the links between the TCP Sender and Router and between the Attacker and Router is 100 Mbps, the propagation delay is 50 ms, and the bandwidth of the link between the Router and Receiver is 15 Mbps. The bandwidth and propagation delay of the links between the Router and Receiver are set to 15 Mbps and 50 ms, respectively. The bottleneck link of the evaluation network for the proposed mechanism in this time domain detection is the link between the Router and Receiver, and the bottleneck queue is the output queue of the Router. The bottleneck queue is queue-controlled by RED, and other queues are queue-controlled by Tail Drop, with the minimum threshold of RED set to 225 and the maximum threshold set to 450, and queue control is set on a per-packet basis. TCP packet size is set to 1400Byte.

6.3 Miss-detection in Attack Parameter based Detector

Possible miss-detections in detection based on attack parameters are illustrated below.

Example.1 A false negative occurs when the configuration values deviate from the optimal attack parameters in the LDoS attack model. For example, consider the case of an attack on a network where the bandwidth of the bottleneck link is C. If the optimal attack parameters for detection are $R = C$, $L = 200$ ms, and $T = 1000$ ms, and if the attack parameters set for attacking flows are $R = C$, $L = 100$ ms, and $T = 1000$ ms, the attack If the attack parameters are set to $R = C$, $L = 100$ms, and $T = 1000$ms, the attack flow is mistakenly judged as a normal flow and miss-detection occurs.

Example.2 A false positives occurs when the length of time of bursts of normal flow and the time interval between bursts of normal flow are similar to the optimal attack parameters in the LDoS attack model. False positives occur when the RTT of normal flow is similar to the optimal attack parameters in the LDoS attack model. For example, if the normal flow is TCP and the RTT is set to 200 ms, false positives occur because the length of the burst transmission time is similar to the attack flow $L = 200$ ms in terms of waiting for ACKs. If the normal flow is assumed to be a TCP flow and the RTT is set to 1000 ms, false positives occur because the time interval between burst transmission is similar to $T = 1000$ ms.

7 Conclusion

In this paper, we proposed Robust WRED as a mitigation mechanism with improved resistance to detection errors in attack parameter based detection.The proposed mechanism introduces the per-flow LDoS Conformance Index and divides the link bandwidth according to the LDoS Conformance Index for the flow. The proposed mechanism will be effective suppression and mitigation mechanisms for LDoS/LDDoS attacks, which are difficult to detect.

REFERENCES

[1] Sam Kottler. February 28th ddos incident report. available from ⟨https://github.blog/2018-03-01-ddos-incident-report/⟩, 2018.

[2] Tom Emmons. Flargest ever recorded packet per second-based ddos attack mitigated by akamai. available from ⟨https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html⟩, 2020.

[3] Aleksandar Kuzmanovic and Edward 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*, number 12 in SIGCOMM '03, pages 75–86, 2003.

[4] Aleksandar Kuzmanovic and Edward W Knightly. Low-rate tcp-targeted denial of service attacks and counter strategies. *IEEE/acm transactions on networking*, 14(4):683–696, 2006.

[5] Wu Zhijun, Li Wenjing, Liu Liang, and Yue Meng. Low-rate dos attacks, detection, defense, and challenges: A survey. *IEEE Access*, 8:43920–43943, 2020.

[6] Inc. Cisco. Qos: Congestion avoidance configuration guide, 2017.

[7] Mina Guirguis, Azer Bestavros, and Ibrahim Matta. Exploiting the transients of adaptation for roq attacks on in-

ternet resources. In *Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004.*, pages 184–195. IEEE, 2004.

[8] Changwang Zhang, Jianping Yin, Zhiping Cai, and Weifeng Chen. Rred: robust red algorithm to counter low-rate denial-of-service attacks. *IEEE Communications Letters*, 14(5):489–491, 2010.

[9] IETF. Transmission control protocol. available from⟨https://tools.ietf.org/html/rfc793⟩, 9 1981.

[10] IETF. Computing tcp's retransmission time. available from ⟨https://tools.ietf.org/html/rfc6298⟩.

[11] Tanenbaum Andrew S. and Wetherall David J. Computer networks fifth edition, 2011.

[12] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu, Jian Sun, and Keping Long. On a mathematical model for low-rate shrew ddos. *IEEE Transactions on Information Forensics and Security*, 9(7):1069–1083, 2014.

[13] Sally Floyd and Van Jacobson. Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on Networking*, 1(4):397–413, 1993.

[14] Mark Wurtzler. Analysis and simulation of weighted random early detection (wred) queues. *Diss., University of Kansas*, 2002.

[15] R. Makkar, I. Lambadaris, J.H. Salim, N. Seddigh, B. Nandy, and J. Babiarz. Empirical study of buffer management scheme for diffserv assured forwarding phb. In *Proceedings Ninth International Conference on Computer Communications and Networks (Cat.No.00EX440)*, pages 632–637, 2000.

[16] A. Shevtekar, Karunakar Anantharam, and N. Ansari. Low rate tcp denial-of-service attack detection at edge routers. *IEEE Communications Letters*, 9(4):363–365, 2005.

[17] R. Mahajan, S. Floyd, and D. Wetherall. Controlling high-bandwidth flows at the congested router. In *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, pages 192–201, 2001.

[18] nsnam.org. ns-3 — a discrete-event network simulator for internet systems. available from⟨https://www.nsnam.org/⟩.