Robustness of RED in Mitigating LDoS Attack

Jing Zhang, Huaping Hu and Bo Liu
Computer School, National University of Defense Technology
Changsha, Hunan 410073-P.R.China
[e-mail: jingzhang132@gmail.com]
*Corresponding author: Jing Zhang

Received March 16, 2011; revised April 24, 2011; accepted May 9, 2011; published May 31, 2011

Abstract

The Random Early Detection algorithm is widely used in the queue management mechanism of the router. We find that the parameters of the RED algorithm have a significant influence on the defense performance of the random early detection algorithm and discuss the robust of the algorithm in mitigating Low-rate Denial-of-Service attack in details. Simulation results show that the defense performance can be effectively improved by adjusting the parameters of $Q_{\min}$ and $Q_{\max}$. Some suggestions are given for mitigating the LDoS attack at the end of this paper.

Keywords: Low-rate denial-of-service, mitigate, attack, defense performance

DOI: 10.3837/tiis.2011.05.012

1. Introduction

Kuzmanovic and Knightly proposed Low-rate Denial-of-service (LDoS) to exploit the TCP's retransmission timeout mechanism [1], which is followed by the RoQ (Reduction of Quality) attack [2] and the Pulsing attack [3]. The attack target router can impact significantly on the data transfer of the TCP flows while the TCP flows periodically enter retransmission timeout caused by dropping packets. Moreover, attacks on Border Gateway Protocol (BGP) which use TCP as its transport protocol can result in a serious influence on the internet [4]. The LDoS makes use of the self-adaptive mechanism of the network or end-system to launch the attack. The TCP congestion control mechanism gets universal concern in low-rate denial of service attack. The LDoS attack is to touch off the TCP timeout retransmission mechanism through the router queue management algorithm as showed in **Fig.1**. The congestion window will become one packet as soon as the TCP timeout retransmission mechanism is touched off.

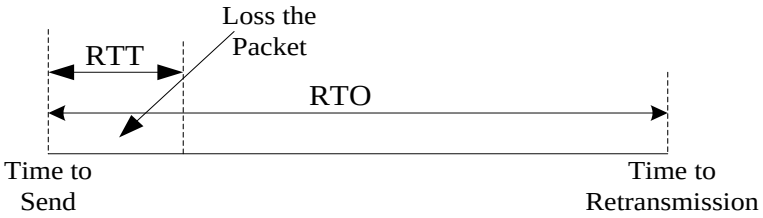


Fig. 1. TCP's Timeout Mechanism

The characteristics of the LDoS attack can lead to subtle attack traffic and a low average stream rate in a long time. The aggregated LDoS attack stream (showed in **Fig. 2**), periodically sends the short but high pulses. Acorrdingly, the attack stream may periodically take up the most buffer size of the router or reach the maximum length of the queue, which results in dropping packets and makes all the affected legitimate TCP flows enter the retransmission state. As a result, the throughput is severely depressed, and thus the attack is achieved. Suppose the rate after aggregation is R and the router's capability is C, the traditional relationship between them is $R \geq C$.

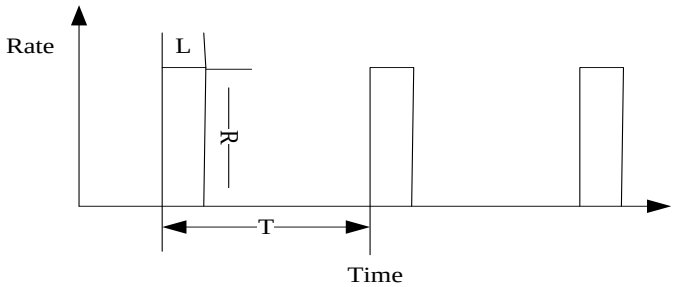


Fig. 2. Attack Traffic Stream

The LDoS attack has two ways to launch. One way is that only one of the all attack nodes

sends the attack stream in a period, which is known as the many attack nodes launch single attack (MANLSA). The other way is that every attack node sends the attack stream in a period, which is known as the many attack nodes launch cooperation attack (MANLCA) (showed in **Fig. 3**). In this paper, we use MANLCA to launch the LDoS attack.

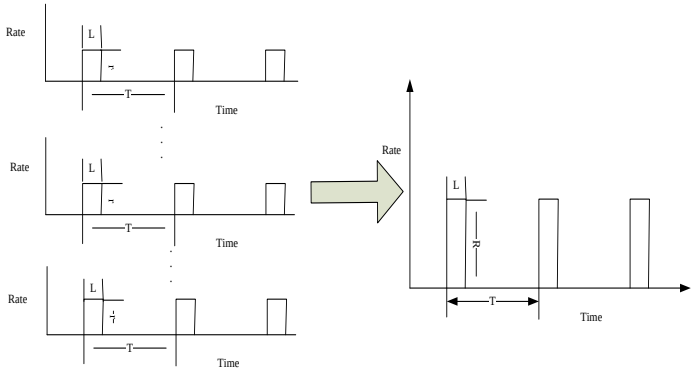


Fig. 3. Way for launching LdoS Attack

To study the robust of the Random Early Detection (RED) algorithm in mitigating LDoS attack, we analyze the RED algorithm and show the principle of the attack, and make the RED algorithm itself mitigate the attack by setting the suitable parameters. Symbols used in this paper are summarized in **Table 1**.

Table 1. Symbols Used in the Paper

Symbol	Meaning	Symbol	Meaning
MANLCA	way to launch attack	n_{LDoS}	denotes the number of arrived attack packet,
MANLSA	way to launch attack	n_{TCP}	denotes the number of arrived TCP packets
T	period of the attack	n	denotes the number of packet transferred by router
L	length of burst	n_{Attack}	denotes the number of attack stream
R	attack rate after aggregation	r	rate of pulse
C	the capability of bottleneck link	Size	size of attack packet
RED	Random early detection	RTT	round Trip Time
wq	the weight of current length of queue in calculating Q_{avg}	RTO	retransmission timeout
$Q_{\min}$	the threshold of RED	M	number of attack traffic stream
$Q_{\max}$	the threshold of RED	min_{RTO}	The minim value of RTO
$P_{\max}$	the max value of probability the packet to be dropped	max_{RTO}	The maxim value of RTO
Q_{avg}	the average length of the queue	SRTT	Smoothed round-trip time
$count$	the number of packets which have been dropped	RTTVAR	Round-trip time variation
$Length$	the maximum length of bottleneck queue		

The RED algorithm and its variants have been widely used to improve the TCP performance [5][6]. The basic idea of the RED queue management algorithm is to detect the incipient congestion early and convey the congestion notification to the end-hosts as early as possible, allowing them to reduce their transmission rates before the queues in the network overflow and the packets are dropped. The probability that an arrived packet will be dropped can be computed by:

$$Q_{avg} = (1 - wq) * Q'_{avg} + wq * Q_{cur} \tag{1}$$

$$P_b = \begin{cases} 0 & Q_{avg} < Q_{min} \\ P_{max} * \dfrac{Q_{avg} - Q_{min}}{Q_{max} - Q_{avg}} & Q_{min} \le Q_{avg} < Q_{max} \\ 1 & Q_{avg} \ge Q_{max} \end{cases} \tag{2}$$

$$P_d = \frac{P_b}{1\text{-}count * P_b} \tag{3}$$

The two thresholds Q_{min} and Q_{max} of the RED algorithm are used to keep the steady of queue length, which is a valuable weakness to launch the LDoS attack [1]. Q_{avg} is the average length of the queue, and wq is the weight of current length in calculating Q_{avg}. P_{max} is the maximum probability to drop the packet. P_d is the probability of the arriving packets to be dropped, and $count$ is the number of the dropped packets. It is easy to find that the bigger value of $count$ is, the more likely the arriving packet is to be dropped.

During the burst length time L in a period, suppose that: (a) $Length$ denotes the maximum length of the bottleneck queue which is shared by the TCP flow and the attack traffic stream, (b) n_{LDoS} denotes the number of the arrived attack packet, (c) n_{TCP} denotes the number of the arrived TCP packets, and (d) n denotes the number of the packets will be transferred by the router.

The maximum time of the first packet dropped by the router can be computed by $t = (Length * L)/(n_{LDoS} + n_{TCP} - n)$. Suppose n_{Attack} is the number of the attack streams, given the rate of the attack stream r and the size of the attack packet $Size$ for each attack node, the number of the packets that the attack stream will be sent in a period can be computed by $\lceil r * L/(8 * Size) \rceil * n_{Attack}$. So, we can know that if the smaller size of attack packet, then there is a larger number of attack packets, less time of t, and a bigger number of $count$. After the time t, the queue reaches its maximum length. Meanwhile, the queue will be in the state for the time of $t_1 = L - t$. The attack will impact on the TCP flow only if $n_{LDoS} + n_{TCP} - n > Length$.

In order to mitigate the attack, we must make the value of t as large as possble by making the $n_{LDoS} + n_{TCP} - n < Length$. Since the value of n_{LDoS} and n_{TCP} are kept steady during the attack, the value of n should be increased. It means that we need decrease the value of P_d by increasing the value of Q_{min} and Q_{max} or decreasing the value of P_{max} to drop less packet. In this paper, given the value of P_{max} does no change, we focus on the change of Q_{min} and Q_{max} impact on the attack. Since the size of the attack packet is usually small, the average flow can

be used to calculate the probability of dropping the arriving packet.

The rest of this paper is organized as follows. The related work of the LDoS attack is provided in Section2. In Section 3, the simulation environment is introduced. Then we show the robust of the RED algorithm in mitigating the LDoS attack in section 4. In section 5, we give the contributions of the paper and give the conclusion in Section 6.

2. Related Work

To mitigate or detect the LDoS attack, research so far has primarily focuses on prevention and detection.

For the prevention, one method is to stochastic minimum retransmission timeout time's value to destroy the consistent produced by the TCP retransmission timeout mechanism [1], which is used to prevent the LDoS attack. But it is impossible to realize the method by changing the internet protocol. Based on the behavior characteristic of the attack, the attack pulse can make arriving rate (or the packet) of the flow has a significant increase in a short time. To mitigate the attack, Kuzmanovic proposes the queue management algorithm to drop the packets of the flows with a high rate. Sarat S [7] proposed a moderate increase in buffer size over the Stanford model renders the shrew ineffective make the attack need to send faster to fill up the buffer, combined with the AQM (Active Queue Management) to filter the attack stream. This method can make the attack no longer with a low rate to get a easy detect, but is not effective to mitigate the LDoS attack.

For the detection, HAWK(Halting Anomaly with Weighted Choking) [8] by calculating the strength of attack flow, the attack burst time and the attack period, upgrade the existing queue management algorithm to realize filter the periodically high rate but short flow. But the method may mismake the normal TCP flow for the attack stream which let the method have high wrong alarm [9]. The RRED (Robust RED) algorithm [10] drop the arrived packet according to the short time gap by caculating arriving packet after a packet is dropped for the attack flow which is different from TCP flow. But if the LDoS attack is launched by MANLCA, the method may lose the result. Sun H at al. [11] suggests detecting the LDoS attack by matching the pattern with the prestored attack signatures. They use a deficit round robin (DRR) algorithm to allocate the bandwidth and protect the legitimate flows. However, their method has problem on the efficiency. Since the malicious flows cannot be distinguished from the legitimate ones, the legitimate flows have to suffer the rate-limit packet filtering process [9]. Chen Yu [12] develops a distributed CDF (Collaborative Detection and Fltering) scheme to detect and segregate the attack flow from legitimate the TCP/UDP traffic flow. The scheme uses the rate of arriving packet as the sample sequence of the time zone to get the time series after processing. With the aid of the discrete Fourier transform, the autocorrelated time series are converted to the power spectrum density (PSD) which is then matched with the database of the attack signature to detect the LDoS attack. If the attacker uses the IP spoofing technology, this method will cost a lot of space and time to compute which will induce the overflow. He Yanxiang [9] proposes a detection system DSBWA(detection system based on wavelet analysis) to detect the LDoS attack according to the characteristic of the periodicity and the short burst in the LDoS flows and uses wavelet thransform to extract the feature. The proposed system focuses on the number of the arriving packets at the monitoring node and extracts five feature indices of the LDoS flows using wavelet-based multi-scale analysis of the network traffic. Then a synthesis diagnosis is made by a trained BP neural network. But the system only focuses on the detection and has no response technology to mitigate the LDoS attack.

3. Simulations

3.1 Settings

We use NS2 [13] simulation environment to build the simulation network based showed in **Fig. 4**. Noamal-1 to the Normal-50 is the normal TCP connection with the FTP data in NS2. Attacker-1 to the Attacker-M is the attack traffic stream, with the CBR [13] to simulate attack traffic in NS2. The maximum length of the queue is 100(denoted by q_lim), and the default value of the attack packet size is 40 Bytes.

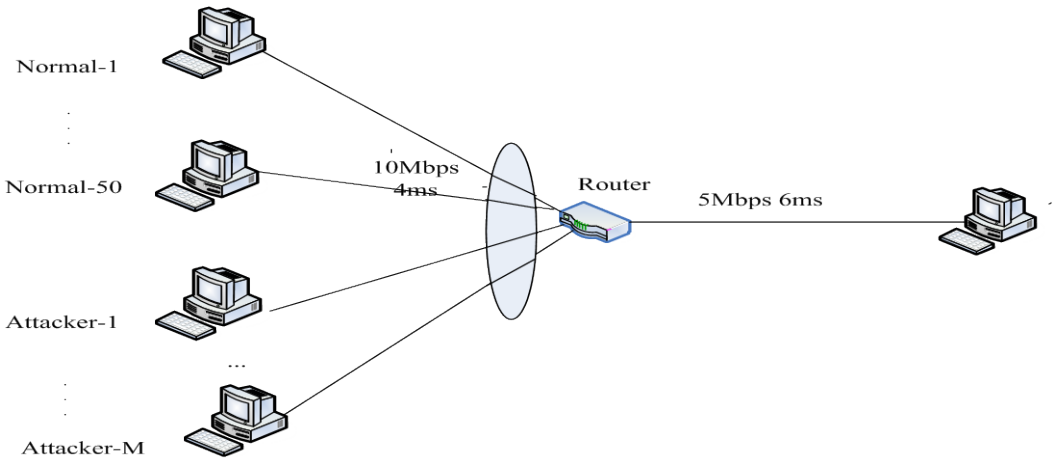


Fig. 4. Network Topology

The retransmission timeout mechanism has two important parameters min_{RTO} and max_{RTO}. The two parameters are set to the defaults of 1s and 64s using the TCP protocol respectively. From **Fig. 4** we can see that the one-way propagation delay is 10ms. It comes to the conclusion that the value of RTT varies from 20ms to 180ms which satisfies $min_{RTO} > SRTT + max(G, 4RTTVAR)$ with the aid of the queue parameter. In the following simulation, $RTO = min_{RTO}$ when it first starts retransmission timeout. Since the LDoS attacks only have impact on the TCP flows, the normal connection is default represents the TCP flow.

3.2 Metric

Under the normal circumstances, the packets totally sent by TCP are $Num\_Normal(Packet)$. Under the normal circumstances, the packets which totally sent by TCP are $Num\_Normal(Packet)$. The number is $Num\_Attack(Packet)$ ($Num\_Normal(Packet) \geq Num\_Attack(Packet)$) during the attack. So the defense performance of the RED algorithm can be described by the follow definition, which is first mentioned in [14].

Definition 1:

$$Defense\_Performance = \frac{Num\_Attack(Packet) - Num\_Normal(Packet)}{Num\_Normal(Packet)} \quad (4)$$

The best defense performance is 0. The attack does not have any effect on the TCP connection only in the best case. The worst defense performance is -1. In the best case, the affected TCP connection cannot get any services.

4. Experimental Results and Analysis

In this part, we discuss how the defense performance of RED can be improved by changing the values of $Q_{\min}$ and $Q_{\max}$ while other parameters of the RED algorithm use default values.

The parameters of the attack traffic stream include the Attack Period (T), the attack rate (r) and the burst length (L). Since $L > max_{RTT}$ [1], let $L = 200ms$. The attack rate is computed by $r = C/M$ according to the way of attacking, and the attack period is determined by the experiment.

4.1 Attack Period

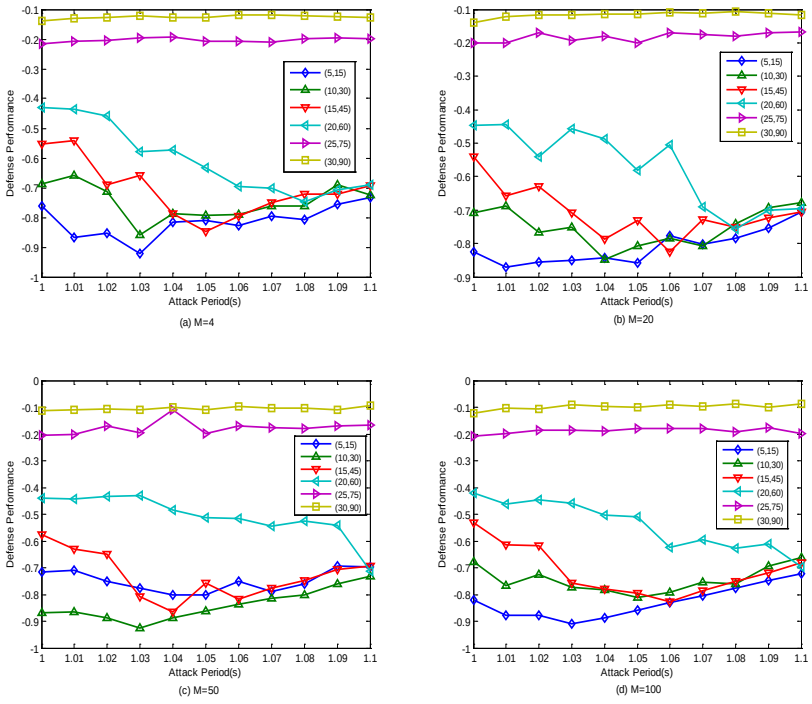


Fig. 5. Attack Period

Table 2. Best Attack Period

	M=4	M=20	M=50	M=100
(5,15)	1.03s	1.01s	1.07s	1.03s

(10,30)	1.03s	1.04s	1.03s	1.05s
(15,45)	1.05s	1.06s	1.04s	1.06s
(20,60)	1.08s	1.08s	1.1s	1.1s
(25,75)	1s	1s	1s	1s
(30,90)	1s	1s	1s	1s

To get an accurate conclusion, the attack traffic streams with different numbers ($M=4$, $M=20$, $M=50, M=100$) are discussed when changing the values of $Q_{\min}$ and $Q_{\max}$ with the restriction of $Q_{max}=3*Q_{min}, Q_{max}<q\_lim$. To choose the best attack period, the experiments are performed using the range of $[1s, 1.1s]$ where the best attack period is regularly distributed. The results are showed in **Fig. 5**.

The best attack period is different when changing the values of $Q_{\min}$ and $Q_{\max}$ as showed in **Table 2**. Moreover, with the increase of $Q_{\min}$, the best attack period becomes the same. This is not a good result, but the defense performance is high enough to counter the LDoS attack when the attack is launched by the attack traffic stream with various numbers.

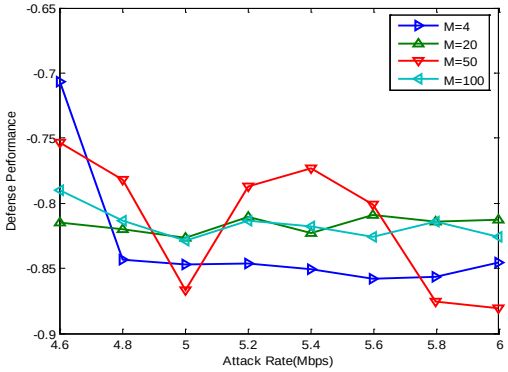


Fig. 6. Attack Rate [4.6Mbps, 6Mbps]

The attack rate after aggregation is set to 5Mbps which is the same to the capability of the bottleneck link. Whether this setting is the optimum value or not, we make simulation to evaluate the impacts of the attack rate on the LDoS attack to identify the optimum value. The result is showed in **Fig. 6**. The defense performance of RED is reducing while the attack rate is changing from 4.6Mbps to 5Mbps. After the attack reaches 5Mbps, the defense performance begins to increase. Considering the relationship between the defense performance and the attack rate, we can see that the defense performance reaches its minimum value when the attack rate is 5Mbps. So the attack rate after aggregation is set to 5Mbps in the following simulation.

4.2 Fixed Q_{max} , different Q_{min} impacts on RED

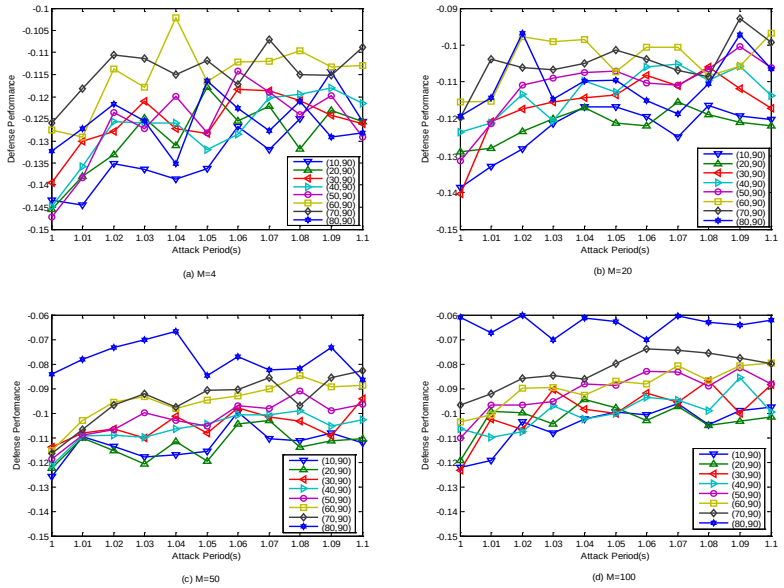
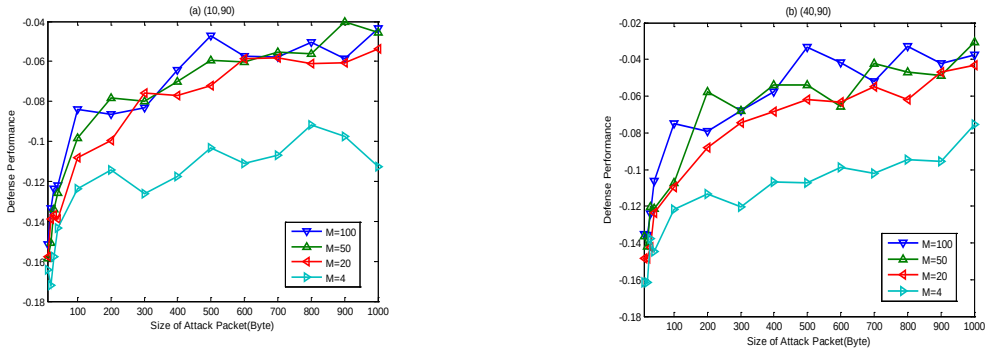


Fig. 7. Defense Performance

As mentioned above, a high defense performance can be achieved by increasing $Q_{\max}$ especially when $Q_{\min}$ =30 and $Q_{\max}$ = 90. To check the impact of $Q_{\min}$ on the defense performance, given we do the following simulations using various values of $Q_{\min}$ with a range from 10 to 80 and a fixed value 90 of $Q_{\max}$. The results are showed in **Fig. 7**.

It is easy to find that the value of $Q_{\min}$ has a marginal impact on the defense performance when $Q_{\max}$ =90. There's the largest defense performance gap of 0.06 between the best and the worst defense performances, with the least difference when $Q_{\min}$ =70. Since the stability of the queue plays an important role in the RED algorithm, the values of $Q_{\min}$ and $Q_{\max}$ should be set according to the queue management.

4.3 Size of Attack Packet



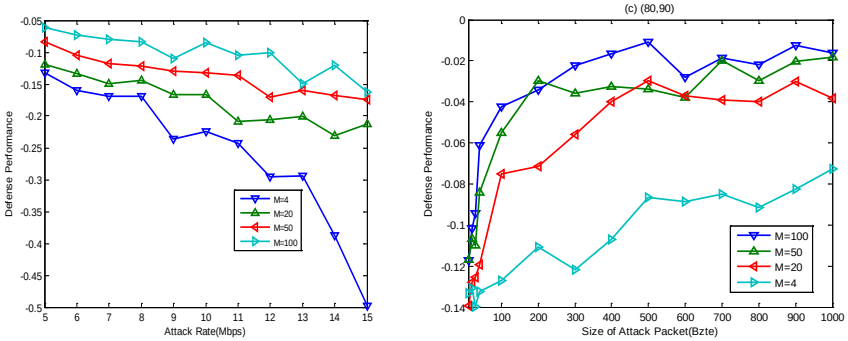


Fig. 8. Different value of packet size [10, 1000]

From the simulation above, we can see that the high defense performance of the RED algorithm can be achieved by the three pairs of values of $(Q_{\min}, Q_{\max})$. In fact, the size of attack packet can be changed by attacker, and what kind of impact will the change have on the defense performance? Given a fixed burst length of 200ms and the attack rate of 5Mbps after aggregation, the impacts of the attack packet size on the defense performance is disscussed as follows where (Q_{min}, Q_{max}) is set to (10,90), (40,90) and (80,90) respectivly. The results are showed in **Fig. 8**.

Fig. 8 shows that the larger size or the larger number of attack stream, the better defense performance. Given the rate of attack traffic stream after aggregation R and the number of attack stream M, the number of packet sent by each attack stream can be computed by $\lceil (R/M)*L/(8*Size) \rceil$ and the time gap between two consecutive packets can be computed by $L/(\lceil (R/M)*L/(8*Size) \rceil -1)$. **Fig. 8** shows the impact of M and *Size* on the defense perfomance when the values of R and L are fixed. For a fixed value of M, a small number of attack packets and a large time gap can be obtained by enhancing the value of *Size*, which leads to a high defense performance.

4.4 Attack Rate

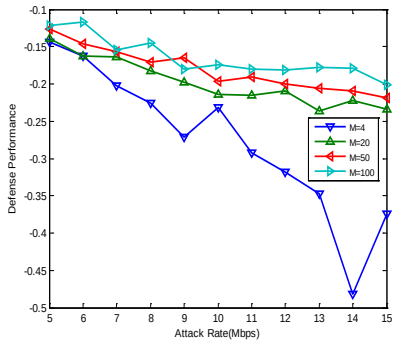


Fig. 9. (10, 90)

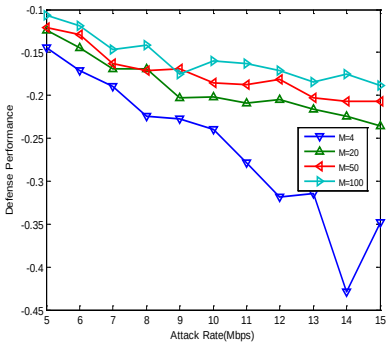


Fig. 10. (40, 90)

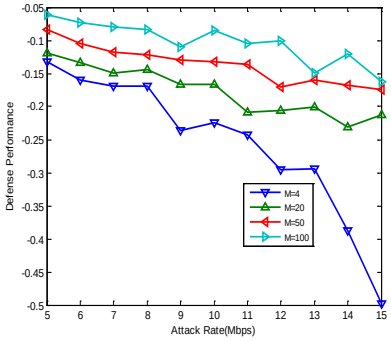


Fig. 11. (80, 90)

As mentioned above, the attack rate can be computed by $r = C / M$ and a high defense performance of RED can be achieved when $Q_{\max} = 90$. In fact, a increased attack rate may have an adverse impact on the defense performance, which is discussed in this section. Here , the values of L and $Size$ are set to 200ms and 40 Bytes respectively.

The three settings of ($Q_{\min}$, $Q_{\max}$) ((10, 90), (40, 90), (80, 90)) are consided in the section. The results are showed in **Fig. 9**, **Fig. 10**, and **Fig. 11** respectively. With the increase of attack rate, different number of attack traffic stream shows different trends. Moreover the defense performance will soon reduce rapidly with the increase the attack rate if the attacker uses four attack traffic streams to launch the attach. That is, the defense performance will be sensitive to the attack rate when there are few attack traffic streams. Here, the distance of defense performance becomes the largest value of 0.35 when the attack rate reaches 14Mbps after aggregation. Unfortunately, the time gap of two consecutive packet will become smaller and smaller with the increase of attack rate. The gap can be used to counter the LDoS attack on condition that the attack does not use IP spoofing technology.

In addition, given a fixed number of the attack traffic stream, the attack rate has the same impact on the defense performance no matter that the values of ($Q_{\min}$, $Q_{\max}$) are different. Therefore, the three pairs of values above can represent the most cases.

4.5 Different value of maximum length

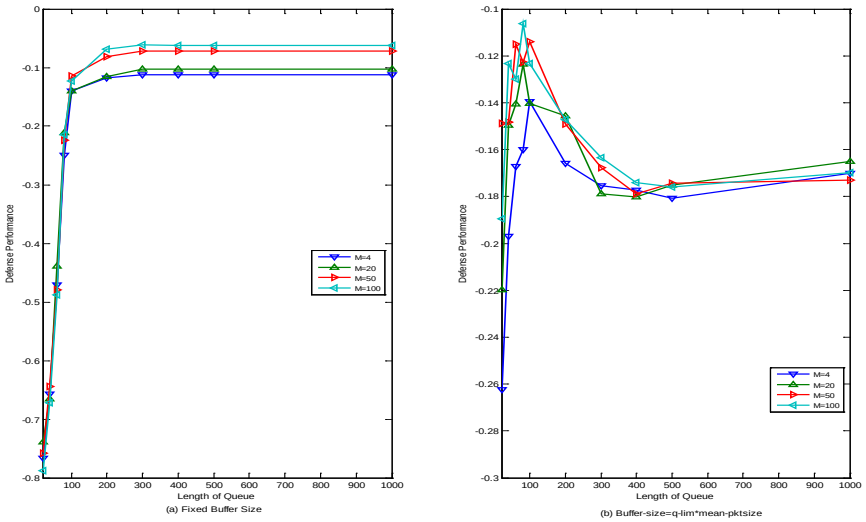


Fig. 12. Buffer Size Impacts on Defense Performance

In the simulation above, the defense performance of RED is weighed using 100 as the queue length, and the buffer size is determined by *q_lim*mean_pktsize* . In this section, we discuss the correctness of the conclusion above when the maximum queue length is changed.

Fig. 12 illustrates how the different length of queue impacts on the defense performance of the RED algorithm. **Fig. 12-(a)** is the case with a fixed buffer size of *100*mean_pktsize* and a variable value of *q_lim* . **Fig. 12-(b)** is the case with a buffer size of *q_lim*mean_pktsize* . Here, *mean_pktsize* uses the default value of NS2. The relationship between $Q_{\min}$ and $Q_{\max}$ is $Q_{\max} = 3 * Q_{\min}$, and $Q_{max} = 0.9 * q\_lim$.

From **Fig. 12-(a)**, we can see that suppose the size of buffer is fixed, with the increase of *q_lim* , the defense performance of RED improves until *q_lim* is large enough. So if we know the buffer size, we can choose a suitable value of *q_lim* to counter the LDoS attacks. **Fig. 12-(b)** shows that the size of buffer changes with the value of *q_lim* . If *q_lim* ranges from 20 to 80, the defense performance of RED will be improved If *q_lim* ranges from 100 to 1000, the defense performance will be depressed but still high.

So, we can effectively counter the LDoS attacks by using the suitable values of *q_lim* , $Q_{\min}$ and $Q_{\max}$.

4.6 Different capability of bottleneck link

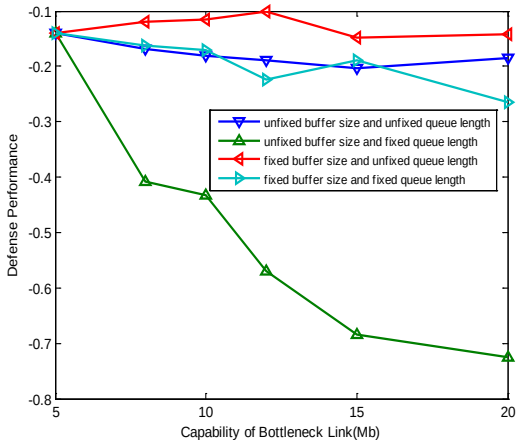


Fig. 13. Defense Performance

With the bottleneck link capabilityof 5Mbps, we make the simulation above. When the capability changes, how to set the parameter of RED to effectively mitigate the LDoS attack will discuss in this section.

Suppose the capability of the bottleneck link is $C^{'}$ and the values of the maximum queue length is $q\_lim^{'}$. Based on the conclusion above, the RED has a high defense performance when $Q_{\max} = 3 * Q_{\min}$ and $Q_{max} = 0.9 * q\_lim^{'}$. The maximum queue length is determined by $q\_lim^{'} = \lceil C^{'} / C \rceil * q\_lim$, and the buffer size is determined by $q\_lim^{'} * mean\_pktsize$. The four groups of simulations (unfixed length of queue and unfixed buffer size, unfixed length of queue and fixed buffer size, fixed length of queue and unfixed buffer size, fixed length of queue and fixed buffer size) were made. The fixed buffer size ($q\_lim * mean\_pktsize$, $q\_lim = 100$) means the buffer size does not increase with the bottleneck link capability. The unfixed length of queue means that the queue does not have the maximum length. Four groups of simutions are made whose results are showed in **Fig. 13**.

From **Fig. 13**, we can see that with the increasing capability of the bottleneck link, the defense performance will becomes poor if the buffer size is increasing with a fixed queue length limit. We can also get the point when the defense performance is always high in despite of the increasing capability of bottle neck link. With the fixed buffer size and the changed queue length limit, the defense performance is not sensitive to the bottleneck link capability.

4.7 Against MANLSA Attack

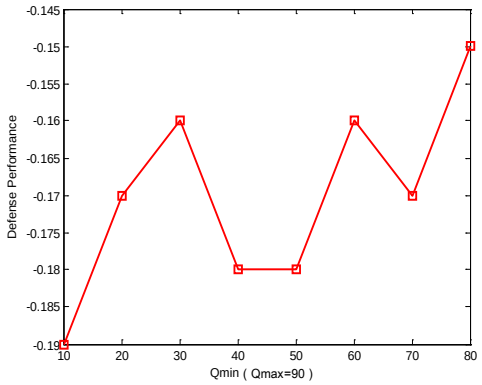


Fig.14. Defense Performance of RED Against MANLSA Attack

To testify whether the robustness of the RED algorithm whether still effective or not if the attacker launches the LDoS using MANLSA attack methodology, we make simulation in the case of M=1, Q_{max} =90 . The result is showed in **Fig. 14**.

Moreover, the RED can mitigate the LDoS attack no matter which attack methodology is used in launching the attack when the values of (Q_{min}, Q_{max}) are well set. With the setting of (80, 90), the RED can achieve the best defense performance, then (30, 90) and (60,90), the gap is 0.01. It comes to the conclusion that the RED is robust enough in mitigating the LDoS attack launched by MANLSA.

4.8 Comparative with other algorithm

The paper analyzes the robustness of RED algorithm in mitigating LDoS attack. There is also some other research work in mitigating LDoS attack, for example, stochastic minimum retransmission timeout time's value [1]. But this method can not be employed in the network since it has to change the TCP which is not able to make any change. The method proposed in [7] increases the buffer size also need make some change on the hardware of the router, and limited in mitigating the attack [12].

In this paper, we note that the RED algorithm is itself robust enough by adjusting the relevant parameters to sufficiently mitigate most of the LDoS attacks which only need minor modifications on the setting of the router.

5. Our Contributions

The mainly contributions of our work are:

- Provide a simple method which can make the minor modifications on the RED algorithm by adjusting the relevant parameters are sufficient to mitigate the most LDoS attacks.
- Idetify the robust of the RED algorithm in mitigating different attacks launched by LDoS.
- Give some suggestions on setting the parameters for different capabilities of bottleneck links to mitigate the LDoS attack.

6. Conclusion

The robust of RED in mitigating the LDoS attack is discussed in the paper. From the

simulation results, it comes to the conclusion that a suitable set of the maximum of the queue length (q_lim) and the values of $(Q_{\min}, Q_{\max})$ can effectively improve the defense performance of RED and mitigate the LDoS attack. Their relationship can be described by $(Q_{\min}, Q_{\max})$ $Q_{\max} = 3 * Q_{\min}$, $Q_{\max} = 0.9 * \text{q\_lim}$. Moreover, some suggestions are made to set the queue in different capabilities of bottleneck links. With the small change on the RED algorithm, let the algorithm can have a high defense performance.

References

[1] Kuzmanovic A and Knightly E W, "Low-rate TCP-targeted denial-of-service attacks," in *Proc. of Proceedings of 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp.75-86, Aug. 2003. Article (CrossRef Link).

[2] Guirguis M, "Reduction of Quality (RoQ) Attacks on Internet end-systems," in *Proc. of24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp.1362-1372, Mar. 2005. Article (CrossRef Link) .

[3] Luo X and Chang R, "On a new class of pulsing denial-of-service attacks and the defense," in *Proc. of 12th Annual Network & Distributed System Security Symposium*, pp.67-85, Feb. 2005. Article (CrossRef Link)

[4] Ying Zhang, Z. Morely Mao and Jia Wang, "Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing," in *Proc. of 14th Annual Network & Distributed System Security Symposium*, pp.1-15, 2007. Article (CrossRef Link)

[5] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Transactions on Networking*, vol. 1, no. 4, pp. 397-413, Aug. 1993. Article (CrossRef Link).

[6] Mahajan R, Floyd S and Wetherall D, "Controlling high-bandwidth flows at the congested router," in *Proc. of Ninth International Conference on Network Protocols*, pp.192-201, 11-14 Nov. 2001. Article (CrossRef Link).

[7] Sarat S, and Terzis A, "On the effect of router buffer sizes on low-rate denial of service attacks," in *Proc. of 4th International Conference on Computer Communications and Networks*, pp. 281-286, Oct. 2005. Article (CrossRef Link).

[8] Kwok Y K, "HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks," in *Proc. of International Conference on Computer Networks and Mobile Computing*, pp.423-432, Aug. 2005. Article (CrossRef Link).

[9] He Yanxiang, Cao Qiang, Liu Tao, Han Yi and Xiong Qi, "A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform," *Journal of Software*, vol. 20, no. 4, pp. 930-941, Apr.2009. Article (CrossRef Link).

[10] Changwang Zhang, Jianping Yin, Zhiping Cai and Weifeng Chen, "RRED: Robust RED Algorithm to Counter Low-rate Denial-of-Service Attacks," *IEEE Communication Letter*, vol. 14, no. 5, pp. 489-491, May 2010. Article (CrossRef Link).

[11] Sun H, Lui J and Yau D, "Defending against low-rate TCP attacks: dynamic detection and protection," in *Proc. of 12th IEEE International Conference on Network Protocols*, pp.196-205, Oct. 2004. Article (CrossRef Link).

[12] Chen Y and Hwang K, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1137-1151, Sep. 2006. Article (CrossRef Link).

[13] S. Mc Canne and S. Floyd, "The network simulator: ns-2", 2010 [Online]. Article (CrossRef Link)

[14] Usman Traiq, ManPyo Hong and Kyungsuk LHee, "PMS an expeditious marking scheme to combat with the DDoS attack," in *Proc. of 9th International Multitopic Conference*, pp.1-4, Dec. 2005. Article (CrossRef Link).

Jing Zhang received her M.S. degrees in Military Science from National University of Defense Technology, Changsha, China, in 2007, and is currently pursuing the Ph.D. degree in National University of Defense Technology. Her research interests include Network and information security, cryptography.

Huaping Hu received his Ph.D. degree in Engineering from National University of Defense Technology, Changsha, China, in 1995. He is currently a Professor with Computer School, National University of Defense Technology. His research interests include Network and information security, cryptography.

Bo Liu received his M.S. degrees in Engineering from National University of Defense Technology, Changsha, China, in 1997. He is currently an Associate Professor with Computer School, National University of Defense Technology. His research interests include Network and information security, cryptography.