Advanced Engineering Forum *Online: 2011-09-09*
ISSN: 2234-991X, Vol. 1, pp 315-319
doi:10.4028/www.scientific.net/AEF.1.315

Half-Droptail: Algorithm to Mitigate LDoS Attacks*

Jing Zhang[1, a], Huaping Hu[1,b] , Bo Liu[1,c] and Lin Chen[1,d]

[1]School of Computer, National University of Defense Technology, Changsha, Hunan, China

[a]jingzhang132@gmail.com, [b]howardnudt@yahoo.com.cn, [c] boliu615@yahoo.com.cn,

[d] leeyon@yahoo.cn

Keywords: Low-Rate Denial-of-Service, Droptail, NS2, Mitigate.

Abstract. Low-Rate Denial-of-Service (LDoS) attack was a new type of denial-of-service attack, the queue management algorithm were found valuable to this attack, especially Droptail. In this paper, based on the impacts of the parameter setting of the Droptail on the LDoS attack, we proposed the Half-Droptail algorithm by changing parameter on the queue management algorithm. We made a set simulation of this algorithm, and the results show that the algorithm can effectively improve the defense performance of algorithm itself.

1. Introduction

The algorithm of Droptail was a simple FIFO (First In First Out) queue. The arriving packet which will be dropped was decided by whether exceeds upper limit length of queue or beyond the capacity of buffer. The mechanism of dropping packet was valuable to LDoS (Low-rate Denial-of-Service) attacks [1]. The LDoS attack made use of the self-adaptive mechanism which was used on the network or end-system to attack. TCP congestion control mechanism got universal concern in low-rate denial-of-service attacks. This attack was that it does not have to send a high rate of continuing attack traffic streams, instead of that, it periodically send a short time high-rate pulse. Compared with flooding attacks, LDoS attack was a low-rate attack, making the attack stream more subtle, which made the DoS attacks difficult to detect by traditional DoS detection methods.

In this paper, we propose Half-Droptail algorithm to mitigate the LDoS attacks based on the analysis of attack model. This algorithm makes some change on traditional Droptail Algorithm. Based on the size of attack packet impacts on the attack, the basic idea of algorithm is to let the buffer of router hold more packets. We make a set of simulations to evaluate the algorithm, the results shows that the Half Droptail can largely reduce the attack performance.

2. Related Work

2.1 LDoS Attacks

LDoS makes use of the self-adaptive mechanism which is used on the network or end-system to attack. TCP congestion control mechanism gets universal concern in low-rate denial of service attacks. This attack is through the router queue management algorithm to expire TCP timeout retransmission mechanism. LDoS attack stream, which is periodically sending short high-rate pulses, makes attacks on stream periodically take up the router's resources or reach the max length of the queue, resulting in dropping packets, and causing all affected normal TCP streams to enter the retransmission state, it will eventually make a significant reduction the servicing capability of router to achieve the attack purpose.

Based on the attack way impacts on the attack [2], we let the attack stream like as Fig.1. In this paper we describe the attack using four parameters (T, L, R, N, M). T represents the attack period, L represents the attack burst length, R represents the attack rate, N represents the number of normal TCP connection and M represents the number of attack stream.

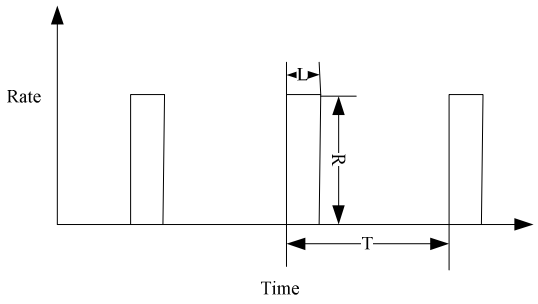

Fig.1 LDoS Attack Stream

2.2 Counter-LDoS Techniques

To mitigate the LDoS attack, 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 this method has to change the internet protocol, cannot be implemented. Sarat S [3] 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 an easy detect, but is not effective to mitigate the LDoS attack.

For the detection, HAWK(Halting Anomaly with Weighted Choking) [4] 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 mistake the normal TCP flow for the attack stream which let the method have high wrong alarm [5]. The RRED (Robust RED) algorithm [6] drop the arrived packet according to the short time gap by calculating arriving packet after a packet is dropped for the attack flow which is different with TCP flow. But if the LDoS attack launched by MANLCA [7], the method may lose the result. Sun H at al. [8] 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 [5]. Chen Yu [9] develops a distributed CDF(Collaborative Detection and Filtering) 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 [5] 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 transform 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.

2.3 Metrics

Under normal circumstances, the packets which are totally sent are $Num\_Normal(Packet)$. In case of attack, the number is $Num\_Attack(Packet)$. The relationship between the two values is $Num\_Normal(Packet) \geq Num\_Attack(Packet)$. So we have the following definition about defense performance about the queue management mechanism.

Definition1: $Defense\_Performance = \frac{Num\_Attack(Packet) - Num\_Normal(Packet)}{Num\_Normal(Packet)}$

In this paper, we use this metric to estimate the defense performance of queue management mechanism to counter LDoS attack. As can be seen from the definition, the best defense performance is 0. In the best case, the attack does not have any effect on the normal TCP connection. The worst defense performance is -1. In this case normal TCP connection cannot get any services from the affected router.

2.4 Simulation Settings

In this paper, we use NS2 [10] simulation environment to build simulation network based on the Fig. 2. In Fig. 2, Noamal-1 to the Normal-N is the normal TCP connection, using the FTP data in NS2 to simulate; Attacker is attack traffic stream, using the CBR [3] to simulate attack traffic in NS2. The max length of Router queue is 100. And the size of attack packet is 40 bytes.

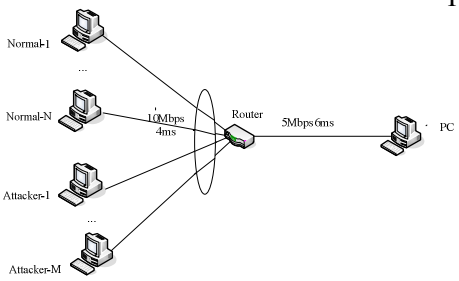

Fig.2 Network Toplogy

Table 1 Experment Parameter

T	L	R	N	M
1s	200ms	5Mbps	50	1

3. Half-Droptail

Consider the bottleneck queue shared by TCP flow and DoS flow every T seconds bursts at a constant rate. During the burst length time L in one period, suppose that: (a) $Length$ denotes the maximum length of bottleneck queue which shared by TCP flow and attack traffic stream, (b) n_{LDoS} denotes the number of arrived attack packet, (c) n_{TCP} denotes the number of arrived TCP packets, and (d) n denotes the number of packet transferred by router.

The max time of first packet dropped by router can be calculated as $t = (Length / n_{\mathrm{LDoS}} + n_{\mathrm{TCP}} - n) * L$. Suppose n_{Attack} denotes the number of attack stream, given the rate of attack stream for each node is r, the size of attack packet is given by $Size$, the number of packet which attack stream will be send in each attack period is computed by $\lceil r * L/(8 * Size) \rceil * n_{Attack}$. So, we can know that the smaller size of attack packet, the larger number of attack packets, the less value of t. After time t the queue reaches its maximum length. And the queue remains this state for time $t_1 = L - t$. The attack will have impacts on the TCP flow only if $n_{\mathrm{LDoS}} + n_{\mathrm{TCP}} - n > Length$. If we increase the value of $Length$, so makes the value of t become large which also reduce the impact of attack on TCP flow.

As we know, The Droptail which is one mode queue management of router will set an upper limit q_lim for the queue. The purpose is to limit the length of the queue. Therefore, if the packet arrives at the router meet $q\_len\_current + 1 > q\_lim$ or $byte\_of\_queue\_current + byte\_of\_packet > buffer$, this packet will be dropped. But this setting becomes a weakness which used by the LDoS attacks.

In this section the focus is on how the defense performance is impacted by the length of queue if with the fixed router buffer size, as shown in Fig.3. From Fig.3, we learn, as the queue length increases, the defense performance of Droptail will drastically improve, but not well enough.

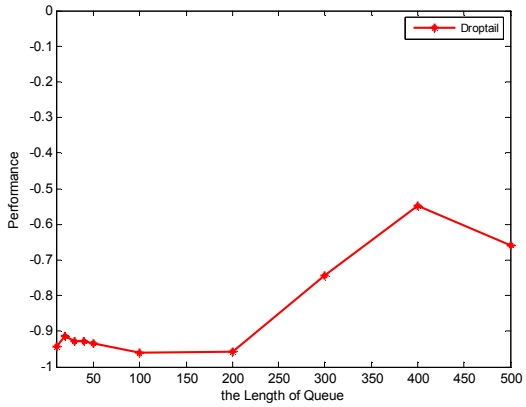

Fig.3 The length of queue impacts on the attack

Table 2 Compasion of Droptail and Half-Droptail

Droptail	**Half-Droptail**

Receive (P)
If ($q\_len\_current+1>q\_lim$ ||
$byte\_of\_queue\_current+byte\_of\_packet>buffer$)
{Drop (P);}
Else {Enque (P)}
	Receive (P)
	If ($byte\_of\_queue\_current+byte\_of\_packet>buffer$)
	{Drop (P);}
	Else
	{Enque (P)}

So, we know that LDoS attack is to meet the upper limit length of queue in a short time by sending a large number of small packets in order to drop subsequent packets from normal connection. In the case of subjected by attack, the length of queue reaches its upper limit in short time, but the buffer of router only occupying little. May be the attacker can send large size of attack packet in order to occupy larger buffer, but this method may have impact on the attack, shown as Fig.4. So, we can get a conclusion that the attack must use small size packet to attack in order to make good attack effect. This is the basic idea of Half Droptail algorithm. The Half Droptail algorithm is very simple. It only changes the packet drop condition from traditional to $byte\_of\_queue\_current+byte\_of\_packet>buffer$, shown as Table 2.

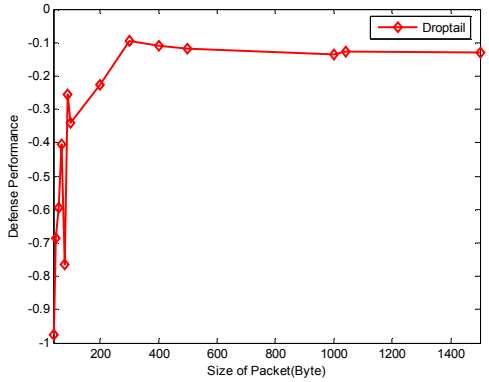

Fig.4 Size of attack packer impact on the attack

4. Performance Evaluation

In this section, we will make a set of experiments to evaluate the performance of Half Droptail. From the introduction of LDoS attacks, we know that the attacker my increase the attack rate in order to make the attack have a good effect. And we know that the number normal connection is a variable in the internet. How the number of normal connection changes impact the performance of Half Droptail. We will discuss in this section.

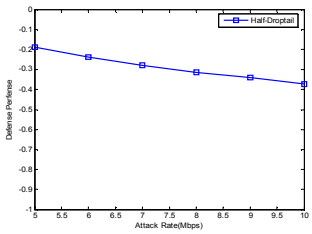

Fig.5 Attack Rate [5Mbps, 10Mbps]

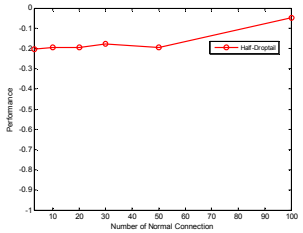

Fig.6 Number of Normal Connection [3,100]

Fig.5 depicts the degree of Half Droptail algorithm sensitive to the attack rate. From Fig.5 we know that, with the increase of attack rate, the defense performance of Half Droptail reduces. We can get that in the case of 10Mbps' attack rate, the defense performance becomes -0.37. Although the defense performance still good, how to counter this occasion, we think the method is to limit the sending rate of each node, let is below the capability of bottleneck link.

As shown in Fig.6, with the increasing number of the normal connection, the defense performance of Half Droptail will improve. So the next step we can change the mechanism of TCP retransmission timeout to improve the performance of Half Droptail algorithm.

5. Conclusion

We propose Half Droptail algorithm to counter the LDoS attacks in this paper, and simulation show that the algorithm can effectively counter LDoS attacks. We also know that only small change of Droptail can get very well performance in countering attacks. But the performance of Droptail is not good enough, how to improve the performance is the next step work.

This work is supported by the High Technology Research and Development Program of China (863 Program) under Grant No. 2008AA01Z414.

References

[1]. Kuzmanovic A, Knightly E W. Low-rate TCP-targeted denial-of-service attacks[C]. Proceedings of ACM SIGCOMM 2003，Kadsruhe, Germany, 2003:75-86.

[2]. Jing Zhang, Bo Liu, Huaping Hu, Lin Chen. Simulation and Analysis of LDoS Attacks [C]. 2010 International Conference on Multimedia Information Networking and Security (MINES'2010), Nanjing, China.

[3]. Sarat S, Terzis A. On the effect of router buffer sizes on low-rate denial of service attacks[C]//San Diego, CA, United States: Institute of Electrical and Electronics Engineers Inc, Piscataway, NJ 08855-1331, United States, 2005.

[4]. Kwok Y K. HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks[C]//Zhangjiajie, China. Springer Vedag, Heidelberg, D-69121, Germany, 2005.

[5]. He Yanxiang, Cao Qiang, Liu Tao, Han Yi, Xiong Qi. A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform. Journal of Software, 2009(4): 930-941

[6]. Changwang Zhang, Jianping Yin, Zhiping Cai, Weifeng Chen. Robust RED Algorithm to Counter Low-rate Denial-of-Service Attacks [J]. IEEE Communication Letter,2010,5

[7]. Huaping Hu, Jing Zhang, Bo Liu, Lin Chen, Xin Chen. Simulation and Analysis of Distributed Low-rate Denial-of-Service Attacks. ICCIT'2010, Seoul, Korea.

[8]. Sun H, Lui J, Yau D. Defending against low-rate TCP attacks: dynamic detection and protection[C]//Proceedings of ICNP'04: the 12th IEEE International Conference on Network Protocols, Berlin, Germany, 2004.

[9]. Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis [J]. Journal of Parallel and Distributed Computing, 2006, 66(9):1137-1151.

[10]. S. Mc Canne and S. Floyd, "The network simulator: ns-2", 2010