Analysis of Detection Mechanism of Low Rate DDoS Attack Using Robust Random Early Detection Algorithm

[1]Shreeya Shah, [2]Hardik Upadhyay
[1]Research Scholar, [2]Assistant Professor
[1]IT Systems & Network Security, [2]Computer Engineering
[1]GTU PG SCHOOL, Gandhinagar, Gujarat, India [2] Gujarat Power Engineering and Research Institute, Gujarat, India

***Abstract*— The entire world is associated with each other through web, utilizing the different gadgets. Such an enormous Network gets influenced by various digital attacks day by day. Appropriated Denial of Service Attack is one in all the real security attack over the web. At the point when the Distributed Denial of Service Attack is performed for bringing the target down discreetly by Attacker, is considered as a Low Rate Distributed Denial of Service attack and it is difficult to characterize the legitimate traffic and malicious traffic. Low Rate Distributed Denial of Service Attack is often simply evading through the traditional detection techniques, therefore the effective and economical detection and mitigation technique is needed for the Low Rate Distributed Denial of Service Attack. Robust Random Early Detection (RRED) Algorithm with different parameters have been utilized to identify the Low Rate Distributed Denial of Service Attack. This paper has included review of those detection methods of Low Rate Distributed Denial of Service Attack.**

***Index Terms*— Low Rate DDoS, RED, Robust RED, Detection and Mitigation of Low Rate DDoS Attack**

I. INTRODUCTION

The most important characteristics of the Low Rate DDoS (distributed denial of service) attack is that it doesn't send a high rate of attack packets over traffic streams, but it is sent on a short period of time for low rate, but with the regular time period to overflow the average queue of the router and cause the packet loss of the normal traffic. A better TCP source will come back off to recover from the packet congestion and retransmit after one Retransmission Timeout (RTO). [1] The existing Random Early Detection (RED) algorithm was found vulnerable to emerging attacks, especially the Low Rate Distributed Denial-of-Service attacks. [1] So that the improvement over that algorithm came up with the Robust Random Early Detection Algorithm. Attack with the high rate for short time can be consider as a Low rate DDoS. It has periodic cycles. So that attack can be either constant or pulsing. A Low Rate Distributed Denial of Service (DDoS) attack has the significant ability to disguise its traffic because it is somehow similar to normal traffic and can't be detected using traditional detection mechanism of DDoS attack. Therefore, effective and efficient detection mechanism is required to secure the network from a Low Rate Distributed Denial of Service attack. This paper analyzes the detection mechanism used by Robust Random Early Detection algorithm over Low Rate Distributed Denial of Service attack.

II. OVERVIEW OF LOW RATE DDOS ATTACK

Low-rate DDoS attacks are quite different from the traditional DDoS attacks, as their traffic is similar to legitimate traffic. A low-rate DDoS attacker exploits the vulnerability of TCP's congestion-control mechanism by periodically sending burst attack packets over short periods of time repeatedly (pulsing attack) or continuously launching attack packets at a constant low-rate (constant attack). [8] The Low Rate Distributed Denial of Service Attack is just an another form of the DDoS in which high rate of data is pushed to network for very short period of time and this process repeats over intervals which corresponds to the retransmission time out period of TCP. [4] Therefore this attack reduces the TCP throughput near to zero. Attacks can be in many forms. Some of them are like a giant elephant, such a thundering while others are like tiny shrew, such a silent and difficult to detect. Distributed Denial of Service Attack at a Low Rate is working like a tiny shrew in a network. It effects the network silently. Being such a silent and similar to normal flow, it is very difficult and challenging to detect it. Only few mechanisms are there to detect such attack. The below figure illustrates a Low rate attack stream.

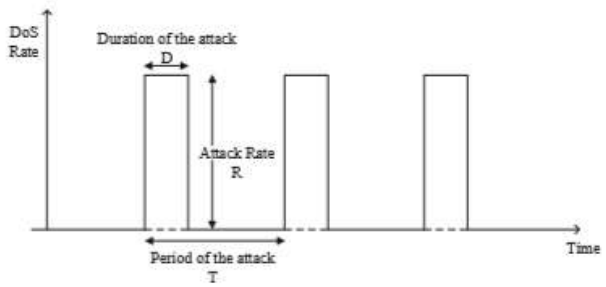

Fig 1 Attack stream of Low Rate Distributed Denial of Service Attack [9]

The attack stream of Distributed Denial of Service Attack at a Low Rate can be define by 3 different parameters.
As presented in fig. 1, R represents the attack rate
D represents the attack duration
T represents the period of attack.

III. DETECTION AND PREVENTION MECHANISMS OF LOW RATE DDOS

Routers on the internet has a queue to manage the upcoming packet to handle them while the network is busy. When the queue is filled to its maximum size, the new arriving packets are discarded. Thus, the simplest technique to limit the queue is tail drop. But because of this, the global synchronization occurs, as to manage the queue size, when router sends the acknowledgement to the TCP senders, all the senders enter into the slow-start state. Here, the tail-drop algorithm discards one segment from each connection rather than discarding many segments from one connection. Therefore, tail-drop leads to TCP global synchronization as all TCP connection hold back simultaneously, and then step forward simultaneously. Thus, the network become under-utilized.
Then, Floyd and Jacobson proposed the Random Early Detection (RED) as an efficient congestion avoidance mechanism for network routers which helps to prevent the global synchronization in the TCP connections [6]. RED was an improvement over tail drop algorithm.

Random Early Detection. (RED)

This algorithm use probabilistic discard methodology of queue fill before overflow conditions are reached. By detecting congestion early and to convey congestion notification to the end-hosts, allowing them to decrease their transmission rates before queues in the network overflow and packets are dropped. For this, RED gateway has two separate algorithms. One of those computes the average queue size while other determines the packet marking probability. The goal of RED is to make the packets fairly, to avoid biases and global synchronization. And also to control the average queue size. Though, RED cannot detect congestion occurred by short-term traffic load changes [6]. Still, the existing RED algorithm and its variants found vulnerable to the low rate DDoS. Due to the oscillating TCP queue size caused by the attacks. Thus, to improve the TCP application throughput, RRED was proposed.

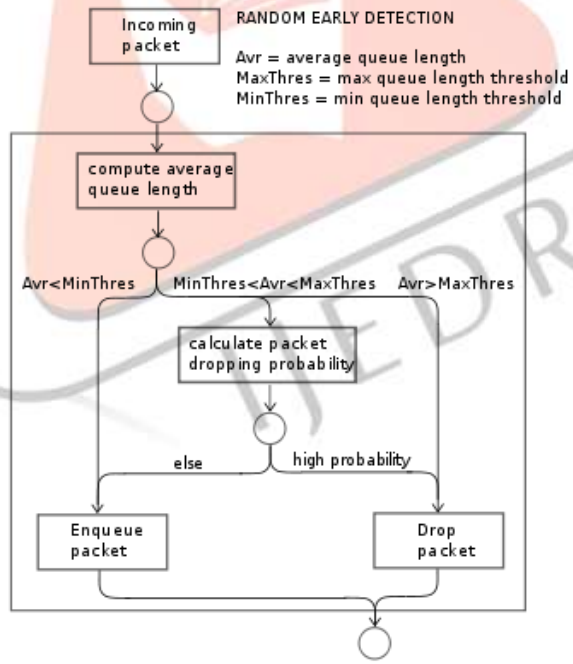

Fig 2 Random Early Detection algorithm

Robust Random Early Detection. (RRED)

Zhang, C., Yin, J., Cai, Z., & Chen, W. (2010) proposed the Robust RED to overcome the problems of RED algorithm.
In RRED, a detection and filter block is added in front of a regular RED block on a router. The basic idea behind the RRED is to detect and filter out Low Rate DDoS attack packets from incoming flows before they feed to the RED algorithm. In RRED, the packet is confirmed as an attacking packet if it is sent within a short-range after a packet is dropper. [1][6] RRED obviously performs better than existing RED algorithm against LDDoS attack. [1]

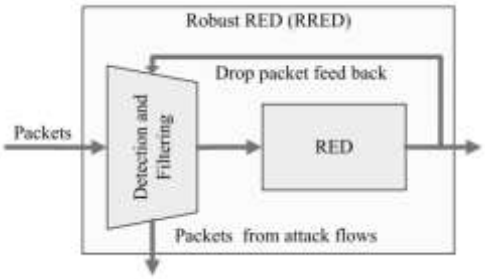

Fig 3 Architecture of RRED algorithm [1]

Improved RED Algorithm

Ma, Li, Jie Chen, and Bo Zhang (2012) proposed the improvement over the existing RED algorithm. As low rate distributed denial of service attack stream has two characteristics. The first one is that the strength of each attack is very high and the second is attack pulse has cycles. Improvement was based on these two characteristics to identify the low rate distributed denial of service attack and be able to take appropriate action. For the improvement, here, the time of queue length exceeds, is being considered. And thus the router take appropriate measures when it identify the Low rate DDoS attack stream. The research to the LDDoS was just beginning, the further researches was required. [3]

Robust Preferential Dropping RED

In 2012, Mohan, Lija, M. G. Bijesh, and Jyothish K. John proposed another mechanism that removes LDDoS attack from initially identified high bandwidth consuming flows. By using partial flow analysis it is able to prevent the attack. [10]

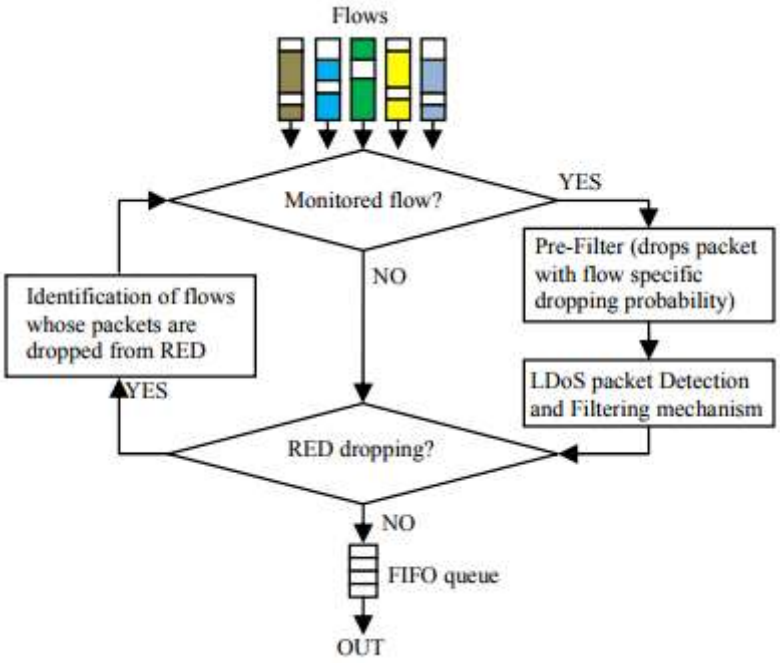

Fig 4 Proposed Methodology to prevent LDDoS attack [10]

In order to prevent the LDDoS attack, here the modification to RED presented as Preferential Dropping-RED with a filter to detect and prevent the LDDoS packets. Simulation results shows that there is no change in throughput and average queuing delay of the system if no attack takes place. At the time of attack, this proposed system shows better characteristics.

Fair Robust Random Early Detection. (FRRED)

Lin, J., Zhang, C., Cai, Z., Liu, Q., & Yin, J. (2016) proposed the fair robust random early detection as an improvement over RRED algorithm. Here, the flow is only attacking, if it arrives within a short-range after a packet from the same flow that is dropped by the detection and filter block or after a packet from any flow that is dropped by the RED block [6]. For Fair RRED, a detection and a filtering block is added to detect and filter out LDDoS attack packets from incoming flows before they feed to the RED block. The structure of Fair RRED is a space-efficient, counting bloom filter, to efficiently maintain the statistical records of incoming

flows. To overcome the problems of RRED, Fair RRED introduced a novel hash function named 'protocol-based hash partitioning' which maps flows of different protocols into segregated sets of bins at the first level of the counting bloom filter. Theoretical analysis and simulations results show that the Fair RRED algorithm can easily effectively preserve the throughput and fairness among TCP flows and mitigate the address-spoofing LDDoS attacks. [6]

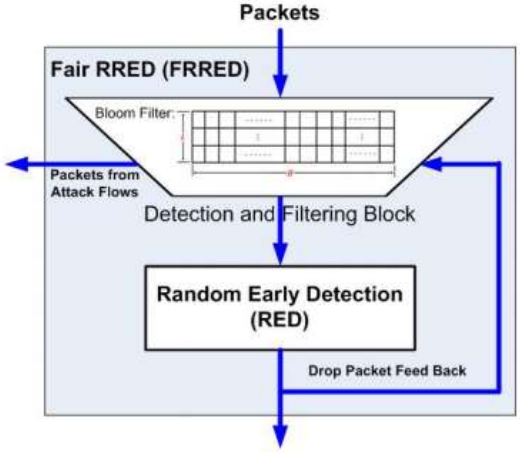

Fig 4 Architecture of Fair RRED algorithm [6]

Fourier Robust Random Early Detection.

As described above in II section, by ending periodic packet bursts to bottleneck routers, Low Rate Distributed Denial-of-Service (LDDoS) attack can degrade the throughput of TCP applications while being so hard to detect. Thus, Chen, Z., Pham, T. N. D., Yeo, C. K., Lee, B. S., & Lau, C. T. (2017, May) introduced power spectrum density entropy (PSD-entropy) to detect LDDoS attack. They proposed the Fourier transform based algorithm, using which the suspicious attack packets detects first based on PSD-entropy. To overcome the traditional RED algorithm, here the PSD-entropy filtering block is added so that the FRRED (Fourier Transform based RRED) can further determine whether this upcoming packet is from an attack flow or not. Based on the entropy ratio the packet is analyzed. The simulation result of this algorithm, show that the FRRED is a better choice over RRED when countering the LDDoS attack. By FRRED (Fourier Transform based RRED) the dropping rate of normal TCP packets reduces and the output of normal users improves. [7]

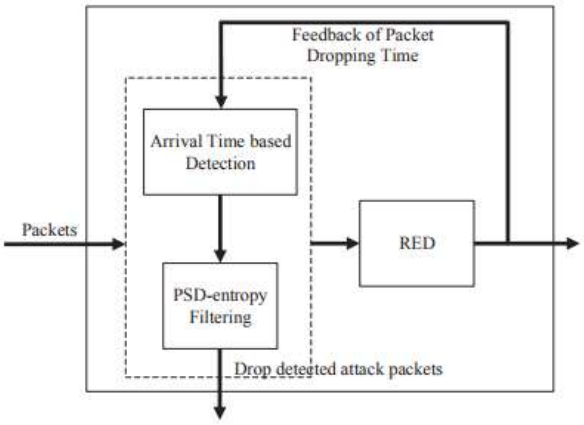

Fig 5 Architecture of Fourier RRED algorithm [7]

IV. CONCLUSION

The world is increasing digitally day by day. Everyday devices are connected more and more with the Internet. In such a way, the network security becomes more important feature. As network might can get affect by different types of attacks. DDoS at a low rate attack damage the network in a silent manner without getting any notification to the user. It affects the output of TCP

applications. And in a network, many applications run within the TCP protocol. This papers describes the techniques of detecting the LDDoS using the RRED algorithm.

REFERENCE

[1] Zhang, Changwang, et al. "RRED: robust RED algorithm to counter low-rate denial-of-service attacks." IEEE Communications Letters 14.5 (2010).
[2] Xiang, Yang, Ke Li, and Wanlei Zhou. "Low-rate DDoS attacks detection and traceback by using new information metrics." *IEEE Transactions on Information Forensics and Security* 6.2 (2011): 426-437.
[3] Ma, Li, Jie Chen, and Bo Zhang. "Improved RED Algorithm for Low-Rate DoS Attack." *Advances in Electronic Commerce, Web Application and Communication* (2012): 311-316.
[4] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.
[5] Arora, Arsh, and Lekha Bhambhu. "Performance Analysis of RED & Robust RED." International Journal of Computer Science Trends and Technology (IJCST) 2.5 (2014): 51-55.
[6] Lin, Jiarun, et al. "A TCP-friendly AQM algorithm to mitigate low-rate DDoS attacks." International Journal of Autonomous and Adaptive Communications Systems 9.1-2 (2016): 149-163.
[7] Chen, Zhaomin, et al. "FRRED: Fourier robust RED algorithm to detect and mitigate LDoS attacks." Zooming Innovation in Consumer Electronics International Conference (ZINC), 2017. IEEE, 2017.
[8] Zhou, Lu, et al. "Low-Rate DDoS Attack Detection Using Expectation of Packet Size." Security and Communication Networks 2017 (2017).
[9] Zhang, Changwang, et al. "Flow level detection and filtering of low-rate DDoS." Computer Networks 56.15 (2012): 3417-3431.
[10] Mohan, Lija, M. G. Bijesh, and Jyothish K. John. "Survey of low rate denial of service (LDoS) attack on RED and its counter strategies." In Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, pp. 1-7. IEEE, 2012.
[11] Wu, Zhijun, Limin Liu, and Xingchen Liu. "The approach of detecting LDoS attack based on correlative parameters." Multimedia Technology (ICMT), 2011 International Conference on. IEEE, 2011.
[12] Yang, Jin-Seok, Min-Woo Park, and Tai-Myoung Chung. "A Study on Low-Rate DDoS Attacks in Real Networks." Information Science and Applications (ICISA), 2013 International Conference on. IEEE, 2013.
[13] Sujatha, P., and J. Kalaivani. "Survey On Detection Of Low Rate Denial Of Service Attack."
[14] Wu, Zhijun, Liyuan Zhang, and Meng Yue. "Low-rate DoS attacks detection based on network multifractal." IEEE Transactions on Dependable and Secure Computing 13.5 (2016): 559-567.