Detection and Mitigation of Low Rate Distributed Denial of Service attack using Robust Random Early Detection

Shreeya Shah[1], Hardik Upadhyay[2]

[1] Research Scholar, Computer Engineering, GTU PG SCHOOL, Gujarat, India
[2] Assistant Professor, Computer Engineering, Gujarat Power Eng. & Research Institute, Gujarat, India

ABSTRACT

The whole world is connected with the technological devices. Human beings are also connected through those devices with each other. Such devices are connected within the network. Connectivity can have personal to professional data. Thus this connectivity needs better security. As the current lifestyle contains much digitalization, security becomes the major prospect. The traditional Distributed Denial of Service attack has already been mitigated and detected. But such techniques are not working for the Low-rate Distributed Denial of Service attack.. Random Early Detection and Robust Random Early Detection algorithms are used for Low Rate Distributed Denial of Service attack [6]. Compared to Random Early Detection, Robust Random Early Detection algorithm is more efficient to TCP throughput for Low Rate Distributed Denial of Service attack. Improvement over Robust Random Early Detection algorithm, suggested in this paper, has the low false positive rate and can improve TCP throughput.

Keyword: - *Low Rate Distributed Denial of Service attack, Random Early Detection, Robust Random Early Detection, Network Simulator-2*

1. Introduction

Low Rate Distributed Denial of Service attack is different from traditional Distributed Denial of Service attack, as it sends periodic short duration attack packets, which exploits TCP's congestion control mechanisms degrading the Quality of Service of TCP applications [9]. In such kind of scenarios, buffers in the bottleneck routers overflow quickly and start dropping the packets. So that the valid information might cannot be reached to the destination router. The communication between sender and receiver drops because of packet dropping. Random Early Detection algorithm already has been found vulnerable to Low rate Distributed Denial of Service attack [1]. Robust Random Early Detection algorithm consist new detection block to filter the Low rate Distributed Denial of Service attack packets. Many improvements over Robust Random Early Detection algorithms has been proposed to detect the Low rate Distributed Denial of Service attack. Simulation result with Random Early Detection and Robust Random Early Detection show that the Robust Random Early Detection algorithm is highly robust and it also improve the performance of normal TCP traffic under Low Rate Distribute Denial of Service attack [6]. Here, in this paper Improvement over Robust Random Early Detection algorithm has been suggested. Experiment results shows that at the same time, the packet dropping ratio has been improved. The TCP throughput has also been maintained.

2. Low Rate Distributed Denial of Service attack

Low rate Distributed Denial of Service attack is new threat to the internet. It is different from traditional Distributed Denial of Service attack. Thus traditional mitigation and detection techniques cannot be useful for Low rate Distributed Denial of Service attack. When the attacker sends the periodic packets with the same time amount of time, can be consider with the Low rate Distributed Denial of Service attack. Low rate Distributed Denial of Service attack can be collaborate with the pulsing attack and constant attack as well [10]. When the attack packets sending over short time periodically it can be considered as pulsing Low rate Distributed Denial of Service attack, while the constant Low rate Distributed Denial of Service attack have attack packets at a constant low rate on a continuous

base. Thus, such attack flow is similar with normal legitimate flow. So that low rate Distributed Denial of Service attack is hard to detect from the normal packet flow.

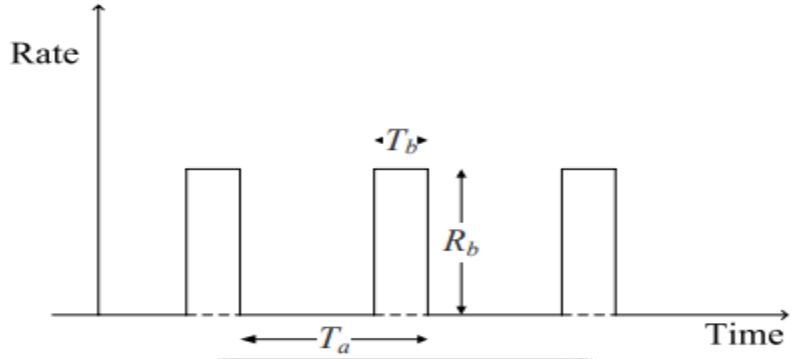

Fig -1: Low Rate Distributed Denial of Service Attack Stream [1]

As shown in figure above, Low rate Distributed Denial of Service attack stream can be define with Ta, Tb and Rb parameters, where Ta stands for attack period, Tb stands for attack burst width and Rb stands for attack burst rate[1][5]. An attacker can cause the TCP retransmission application by sending high rate packets for the short period of time periodically.

3. Robust Random Early Detection

Robust Random early detection is the improvement over the Random Early Detection used for congestion control. But the Random Early Detection does not provide Quality of Service differentiation as well it is vulnerable to Low Rate Distributed Denial of Service Attacks [4]. Thus, the Robust Random Early Detection introduced as a variant of RED that can efficiently detect the Low Rate Distributed Denial of Service Attack. It has packet detection and filtration block before the RED block to provide the better detection. Incoming flow will be attacking flow if arrives within the short-range of time after a packet being dropped by the detection and filtering block and also repeated for several times [6]. Result analysis of RED and RED in NS2 simulator shows that the Robust Early Detection algorithm is highly robust and can improve the performance of normal TCP traffic under the Low Rate Distributed Denial of Service Attack [6].

4. Proposed System: Improved ROBUST RANDOM EARLY DETECTION algorithm

Robust Random Early Detection algorithm is efficient then RED algorithm, still improvement over such algorithm is still continue to lower the false detection of the attacking flow. Whether the upcoming flow is attacking flow or normal TCP flow, Congestion Participation Rate is being used [5]. Congestion Participation Rate is the ratio of the incoming packets into the congestion to the total number of packets from the flow. Once the flow is detected as attacking flow it will be blocked or the packets will be send to the detection block. At the detection block the time interval between the packets will be count and if within the short amount of time, packet resend after being dropped, it might can consider as a Low Rate Distributed Denial of Service attack flow. So that from the detection block, the flow will be blocked else it will be redirected to the RED block for further detection and filtration.

4.1 Algorithm

1. The coming flow f is calculated and compared with the CPR (Congestion Participation Rate) value of it.
2. If the CPR value is greater than the decided threshold value. The flow is considered for the detection block else it will diverted to the RED block.
3. At the detection block the detection will be done by the arrival timings of packets. tp1 – tp2 = T1 tp2 – tp3 = T2 tp3 – tp4 = T3 And so on … It will be consider for number of packets np.
4. If the T1* = T1 = T2 = T3 = T4 = T5, T2* = T1 = T2 = T3 = T4 = T5, T3* = T1 = T2 = T3 = T4 = T5 and if the T1* = T2* = T3* happens, the flow will be declared as attacking flow and the alarm will be generated for that.
5. But if the T1*, T2*, T3* will not be equal, then the flow f will not be consider as attacking flow and redirected to the RED block.

5. Simulation and Result Analysis

To simulate the Random Early Detection NS2 simulator is being used. To implement the Random Early Detection, the below mentioned topology is used.

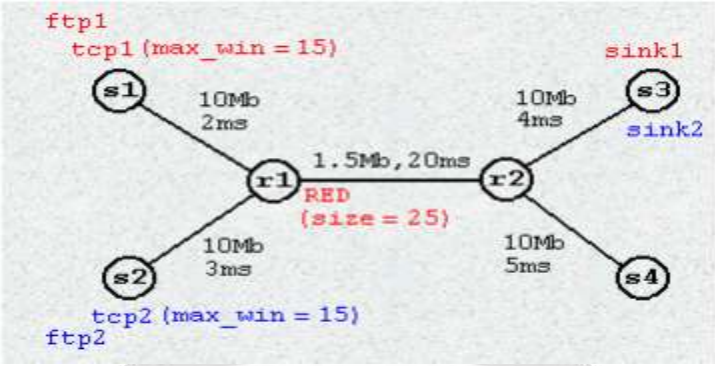

Fig-2: Topology of RED [19]

Here, the TCP window size is 15 and the link between routers contain the 25 packet size.
With this topology, the xgraph shows the below result.

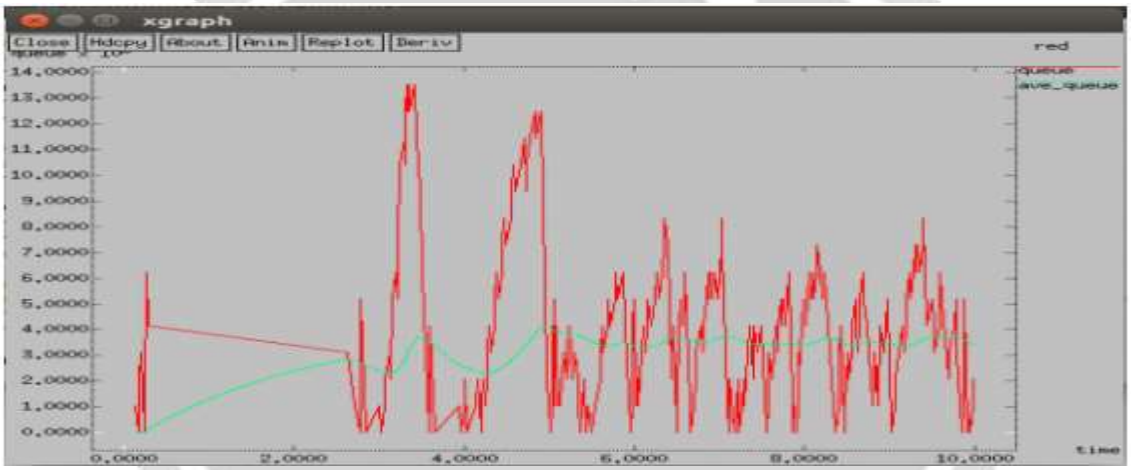

Fig-3: Xgraph of RED

Here, the topology has been modified with the below mentioned details.

Channel	Wired
NS Version	Ns-2
CBR Packet Size	50 Bytes
Interface Queue	RED
Queue Length	100
No. of Nodes	13
Simulation Area Size	800*600
Simulation Duration	60 Seconds

Table-1: Simulation Parameters

With the use of ns-2 simulator to simulate the bottleneck network topology, here is the evaluation results shown. Based on this topology, extensive simulations have been conducted to verify the results of proposed system in mitigating the low rate Distributed Denial of Service attack. Two different AQM algorithms are implemented here.

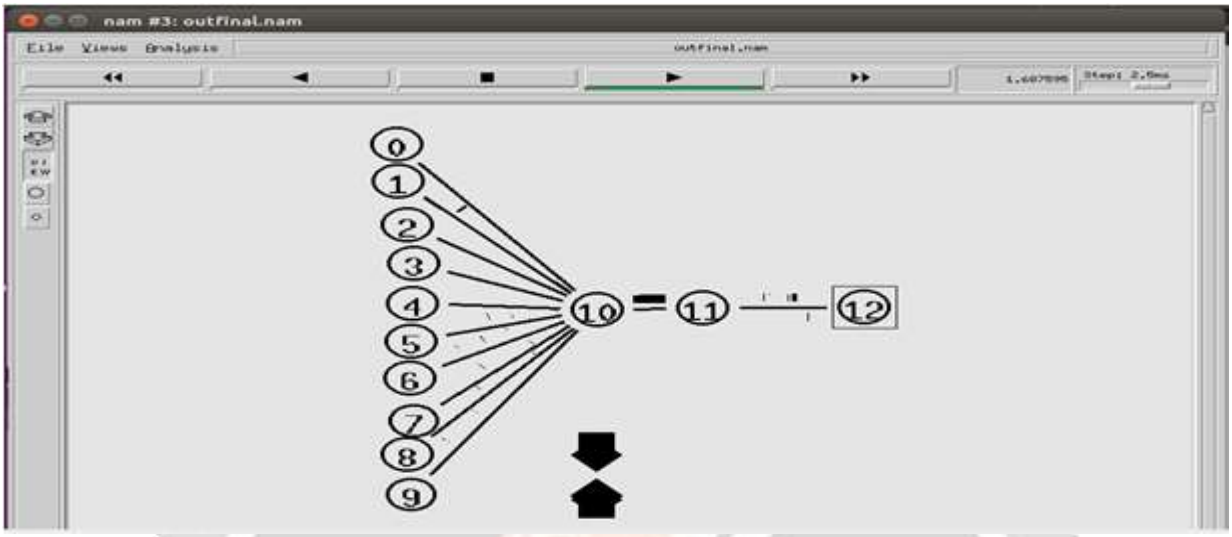

Fig-4: Simulation with proposed system

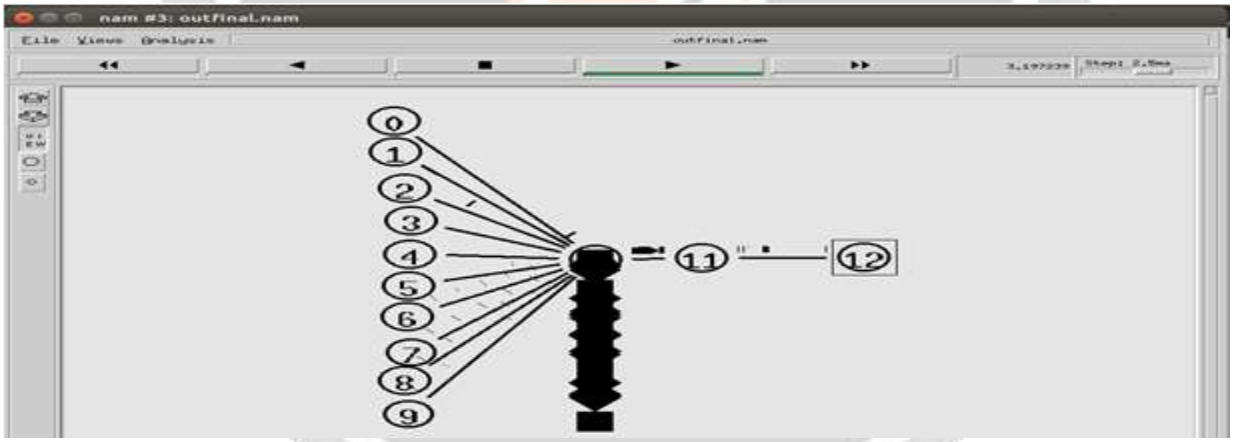

Fig-5: Simulation with proposed system

The Above shown figure shows the bottleneck network topology. In this simple topology, 5 node are working as attacker and five normal TCP users are connected to the bottleneck router with a link rate of 100 Mbps, while the bottleneck link between the two routers has a bandwidth of 10 Mbps. Two different AQM algorithms are applied to the bottleneck queue in Router 1 (node 10). The queue size is set to 100 packets.

Normal Users are communicating with the server using TCP flow (TCP newreno) with the packet size of 1500 bytes. The attacker nodes generates Low rate Distributed Denial of Service traffic by sending UDP packets with the packet size of 50 bytes.

The sending rate of Low rate Distributed Denial of Service packet is set to 10 Mbps to be equal to the bottleneck bandwidth, which is good enough to suppress the normal TCP flows.

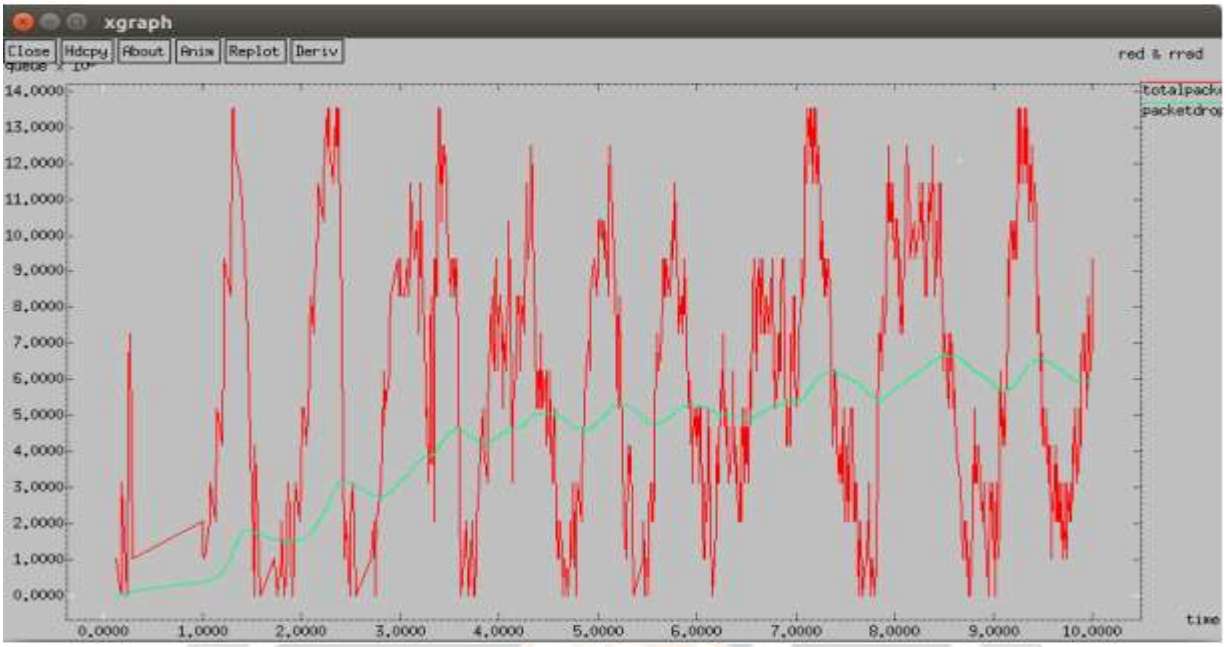

Fig-6: xgraph with proposed system

After implementing proposed system, the results of the xgraph shows the increasing of the packet flow with the time simultaneously. Implementing the two different AQM algorithms and having below mentioned parameter shows the above mentioned results with the derived bottleneck topology.

6. Conclusion

The distributed denial of service attack at low rate can damage the network on a secret base as it happens on the low rate and on a short period of time with the regular basis, so that the differentiation between the normal traffic and attack traffic is tough to get. After implementing proposed system, the packet dropping ratio with the two different AQM algorithms are maintained with the time at simultaneous time rate. The future work with the packet arriving timing can be done by having the filtration with the UDP packet and the time difference between those packets.

7. References

[1] Zhang, Changwang, Jianping Yin, Zhiping Cai, and Weifeng Chen. "RRED: robust RED algorithm to counter low-rate denial-of-service attacks." *IEEE Communications Letters* 14, no. 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, no. 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] 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.

[5] Zhang, Changwang, Zhiping Cai, Weifeng Chen, Xiapu Luo, and Jianping Yin. "Flow level detection and filtering of low-rate DDoS." *Computer Networks* 56, no. 15 (2012): 3417-3431.

[6] Arora, Arsh, and Lekha Bhambhu. "Performance Analysis of RED & Robust RED." *International Journal of Computer Science Trends and Technology (IJCST)* 2, no. 5 (2014): 51-55.

[7] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." In Contemporary Computing (IC3), 2014 Seventh International Conference on, pp. 80-84. IEEE, 2014.

[8] Lin, Jiarun, Changwang Zhang, Zhiping Cai, Qiang Liu, and Jianping Yin. "A TCP-friendly AQM algorithm to mitigate low-rate DDoS attacks." International Journal of Autonomous and Adaptive Communications Systems 9, no. 1-2 (2016): 149-163.

[9] Chen, Zhaomin, Thi Ngoc Diep Pham, Chai Kiat Yeo, Bu Sung Lee, and Chiew Tong Lau. "FRRED: Fourier robust RED algorithm to detect and mitigate LDoS attacks." In *Zooming Innovation in Consumer Electronics International Conference (ZINC), 2017*, pp. 13-17. IEEE, 2017.
[10] Gu, Q. and Liu, P., 2007. Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, pp.454-468.
[11] Mathew, 2013, *Low rate Denial of Service (LDoS) Attack Detection*, Gyandhara International Academic Publication, Thane, India
[12] "Low rate TCP attack" *https://reproducingnetworkresearch.wordpress.com/2017/06/05/cs244-17-low-rate-tcp-dos-attacks/* Accessed: 2017-10-10
[13]"DDOS ATTACKS*"* *https://www.incapsula.com/ddos/ddos-attacks/*
Accessed: 2017-10-10
[14]"TCP-ACKTimeout" *https://commons.wikimedia.org/wiki/File:TCP_ACK_Timeout.png*
Accessed:2017-10-10
[15] "Security + technotes"
http://www.techexams.net/technotes/securityplus/attacks-DDOS.shtml
Accessed: 2017-10-10
[16] "How to Stop a DDoS Attack in Its Tracks (Case Study)"
https://kinsta.com/blog/ddos-attack/
Accessed: 2017-10-10
[17] Lin, Dong, and Robert Morris. "Dynamics of random early detection." In ACM SIGCOMM Computer Communication Review, vol. 27, no. 4, pp. 127-137. ACM, 1997.
[18] "Random Early Detection"
https://en.wikipedia.org/wiki/Random_early_detection
Accessed: 2017-10-10
[19] "Random Early Detection in NS2"
http://nile.wpi.edu/NS/queuemon.html
Accessed: 2017-10-10
[20] "Low rate attack"
https://security.radware.com/ddos-knowledge-center/ddospedia/low-rate-attack/
Accessed: 2017-10-10
[21] "NS2 Simulator"
https://ns2blogger.blogspot.in/
Accessed: 2017-10-10