RESEARCH ARTICLE OPEN ACCESS

Assessment of Active Queue Management algorithms by using NS2 simulator

Kamal Preet Kaur*, Navdeep Kaur**, Gurjeevan Singh***

*(Department of Electronics and Communication Engg., PTU, Punjab
Email: kamalsandhu2788@gmail.com)
** (Department of Electronics and Communication Engg., PTU, Punjab
Email: navdeepkaurjhaj213@gmail.com)
*** (Department of Electronics and Communication Engg., PTU, Punjab
Email: gurjeevansandhu@gmail.com)

ABSTRACT
Network security has become very important and foremost issue for the personal computer users, organizations, business and military. With the advent of internet, security has become the major concern. The main objective of this research is to simulate and analyze the effect of queuing algorithms RED and DROPTAIL with CPR on the TCP targeted LDDoS attack flows. LDDoS attack is more vulnerable to the network traffic than the classic DDoS attacks as they are difficult to identify. We use network simulator ns-2 to implement the network and investigate the behaviors of queuing algorithms in the network. The performance metrics of the comparison are average delay and packet drop. CPR based approach is used to detect and filter attacks. The test-bed experiments are conducted to analyze the performance of this approach which is compared to the existing DFT approach.

Keywords: DROPTAIL, RED, REM, NS2, QUEUE MANAGEMENT ALGORITHMS.

1. INTRODUCTION

1.1 DOS ATTACK:

The denial of Service (DOS) attack continues to be the major threat and hardest security problem to the network [3]. This attack tends to make a user incapable of using the machine or service by making it unavailable to them. It is the major problem to the today's internet. In DoS attacks there is no major benefit to the attacker except for the user's pain. The DoS attacks can detach the network from the internet. Thus prevents the information exchange.

1.2 DDOS ATTAKS:

A DDoS attack can be defined as an attack which uses a large number of computers to launch a synchronized Denial of Service (DoS) attack against a single machine or multiple victim machines. Using client/server technology, the executor is able to multiply the effectiveness of the DoS attack significantly by harnessing the resources of multiple unaware assistant computers, which serve as attack platforms [2].

1.3 LDDOS ATTACKS:

Traditional flooding-based DDoS attacks employ a ''sledge-hammer'' approach of high-rate transmission of packets, which obviously distinguishes themselves from normal data flows in statistical characteristics. Many of the proposed approaches for detecting DDoS attacks have been based on these statistical characteristics. LDDoS attacks are quite different from the traditional flooding-based DDoS attacks as they exploit the vulnerabilities in TCP's congestion control mechanism. Instead of sending continuous network traffic, an LDDoS attacker sends periodically pulsing data flows, which may dramatically reduce the average rate of attack flows. LDDoS attacks have already been observed in the Internet2 Abilene backbone, thus presenting a new challenge to the security of the Internet. [1]

2. RELATED WORK:

The work done by given authors which is related to our research work is studied and related information is given as under;

Mohit Agrawal et.al, (2011) this paper presents that, in the field of computer networks the implementation, management and performance analysis of queues is one of the foremost issues. The selection of the various queues is totally depends upon the need of transmission of data. Safe and Reliable propagation of data is a basic requirement of any computer network. In present scenario, there is a strong requirement of standardization, testing, and widespread deployment

of active queue management [AQM] in routers, which is further responsible for the improvement of performance of today's Internet. Queues performance assessment requires a concrete research effort in the measurement and deployment of router mechanisms, which advances to protect the Internet from flows that are not sufficiently responsive to congestion notification. In this paper, we evaluate the performance of Drop tail, DRR, RED, SFQ, and FQ by varying the number of hops. We are representing the detailed performance analysis & comparison of the various queues in terms of parameters like throughput, average delay and packet loss. These queues have been analyzed on various traffics like FTP and CBR, by varying the number of hops and the various conclusions have been drawn accordingly [4].

Santosh Kumar et.al, (2011) this paper present that Distributed Denial of Service (DDoS) attack is one of the biggest threats now days. This paper aims at providing the simulation results of buffer size and attack intensities effect on various queuing algorithms such as DropTail, Fair Queuing (FQ), Stochastic Fair Queuing (SFQ), Deficit Round Robin (DRR) and Random Early Detection (RED) using ns-2 as a simulation environment. The results in this paper indicate that Stochastic Fair Queuing is the best algorithms in terms of providing maximum bandwidth to legitimate users against various attack intensities. It is also cleared from simulation results that there is no effect of variation in buffer size on queuing algorithms such as Fair Queuing, Stochastic Fair Queuing and Deficit Round Robin while DropTail and Random Early Detection algorithms are giving the best performance on buffer size 60 against various attack intensities. This paper also covers the basic overview of Denial of Service Attack (DoS), Distributed Denial of Service attack (DDoS), attacking methods, DDoS defense approaches and Queuing Algorithms. [5]

Saman Afrasiabi et.al, (2013) this paper aimed to evaluate the computer networks behaviour by NS simulator version 2 (NS-2) and implementation of the network by this simulator and the investigation of the effect of queuing systems in the network performance. Thus, various queuing systems such as CBQ, SFQ, DRR, FQ, RED and Drop Tail are implemented by the purpose simulator. In an elementary scenario are compared with each other and throughput of the network is calculated for each of them. It can be said that the purpose of this paper is depicting the effect of queuing disciplines in the network and selecting a good system and as the selection of the type of optimized queue discipline depends upon the network topology, the results are dedicated for special topology of the network in this paper and is not generalized [6].

Mengke Li et.al, the paper presents that the focus of this work is to study the behaviors of varies queue managements, including RED (Random Early Detection), SRED (Stabilized-RED), and BLUE. The performance metrics of the comparison are queue size, the drop probability, and link utilization. The simulation is done using NS-2. The results of this work shows that different from the RED, SRED and BLUE, which use the available queue length as the indicator of the severity of congestion, they use packet loss and link idle events to manage the congestion. Thus SRED and BLUE achieve significant better performance in terms of packet loss rates and buffer size requirement in the Network. Finally we report a new queue management, SBQ (Stochastic Blue Queue management), which enforce fairness among a large number of flows [7].

3. ACTIVE QUEUE MANAGEMENT ALGORITHMS:

The active queue management algorithms allows to manage the access to fixed amount of bandwidth by distinguishing which packet should be transferred and which one should be dropped when queue limit is fully occupied. There are many queue management algorithms which can be used for the balance between complexity, control and fairness. The main reason for the complexity is when more number of packets arrive then the capacity. The main motive of queue management algorithms is to minimize the congestion and provide the required bandwidth to the traffic. In our simulation we are using RED and DROPTAIL. [2][5]

RED:

(Random Early Detection) works by randomly (based on certain probability) discarding packets at the nodes of the network, before the occurrence of congestion, when the average queue length exceeds the predefined minimum threshold. When the average queue length exceeds the maximum threshold, the probability of rejection becomes equal to 1. RED monitors the average length of the queues by discarding or ECN-marking packets based on statistical probability. If the buffer is nearly vacant, all incoming packets are received. As there is increase in use, the probability of discarding recently arrived packet also increases. When the buffer is occupied, all incoming packets are deleted. RED has no QoS differentiation in the basic version. The versions WRED (Weighted RED) and RIO (RED with In and Out), which consider the QoS into account [1].

DROPTAIL:

Drop Tail is a simple queue management algorithm: it sets a predefined value for the maximum length of the queue and when this value is reached, new packets are discarded, until the next vacant buffer space to accept new packets .When using the Drop Tail mechanism, all the packets in the traffic are treated identically, regardless of the type of traffic which it belongs to. Packet loss will cause the transmitter to reduce the number of TCP packets sent before receiving the acknowledgment. The throughput of the given TCP session will then reduce, until the transmitter start again to receive acknowledgments and begin increasing the size of its congestion window.

REM:

REM differs from RED only in the first two design questions; it uses a different definition of congestion measure and a different marking probability function. The first design of REM is to stabilize both the queue around a small target and the input rate around link capacity, regardless of the number of users sharing the link. Each productivity queue that implements REM maintains a variable which is called 'price' as a congestion evaluation measure. The second idea of REM is to use the addition of the link prices along a path as a measure of congestion in the path, and to implant it into the end-to-end marking probability that can be observed at the source. [9]

4. PERFORMANCE PARAMETERS:

The performance parameters used in this study are packet delivery ratio, minimal delay, maximal delay, packet drop, packet lost and end-to-end delay between the REM, RED and DROPTAIL algorithms.

4.1 **End-to-end delay**: it is referred to as the time taken for a network to reach from one end of a network to the other [1].

4.2 **Minimum end-to-end delay**: The delay specifies the minimum time it takes for a bit of data to travel across the network from one node or endpoint to another.

4.3 **Maximum end-to-end delay**: The delay specifies the maximum time it takes for a bit of data to travel across the network from one node or endpoint to another.

4.4 **Packet drop**: it occurs when the router which is supposed to relay packets actually discards them [1].

4.5 **Packet loss**: packet loss occurs when one or more packets fail to reach the destination and are lost on the way [1].

5. SIMULATION SETUP

Dumbbell network topologies are commonly used in congestion control studies. Network topology consists of two routers (R0, R1, 30 users (User1-----User30), 20 attackers (Attacker1------Attacker20), 30 servers (Server1-----Server30), and a victim server (Victim Server). The link between two routers is the bottleneck link with a bandwidth of 5 Mbps and one-way propagation delay of 6 ms. All the other links have a bandwidth of 10Mbps and a one-way propagation delay of 2 ms. In this topology, User i communicates with Server i (i = 1------30) using FTP, and 20 attackers send UDP packets to attack the Victim Server. The queue size of the bottleneck link is 50. A RED based on packet count is deployed at router R0 on the queues of the bottleneck link. Other links use Drop Tail queues. A CPR-based detection module is installed at router R0 where most normal TCP packets are dropped when an LDDoS attack is present. For comparison, we also install a module based on Cumulative Amplitude Spectrum (CAS) at R0; CAS uses Discrete Fourier Transform (DFT) to locate disturbances caused by LDDoS flows. Simulation time period is 240s and the LDDoS traffic begins at 120s and ends at 220s. And the frequency is 1000 Hz.

5.1 SIMULATION RESULTS

5.1.1 Minimal delay:

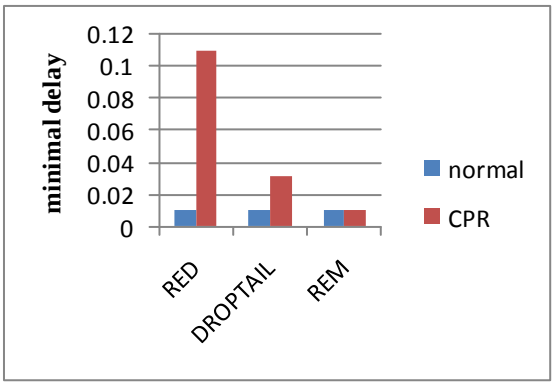

Fig 1: minimal delay in RED and DROPTAIL using CPR and without using CPR

The graph shows the comparison between REM, RED and DROPTAIL queue management algorithms on the basis of minimal delay. If we compare individually, RED shows more minimal delay when used with CPR and DROPTAIL also shows more minimal delay when used with CPR, REM shows same results with CPR approach as well as with normal approach. With CPR approach RED shows largest minimal delay when used with CPR approach when compared with each other.

But with using normal approach the results are approximately same.

5.1.2 Maximal delay:

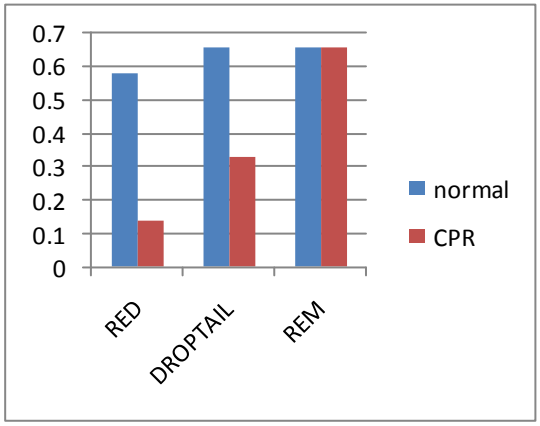

Fig 2: Maximal delay in RED and DROPTAIL using CPR and without using CPR.

The graph shows the comparison between the three queue management algorithms REM, RED and DROPTAIL with using CPR approach and without it on the basis of maximal delay. When compared individually, RED shows more maximal delay when while using normal approach and same is the case with DROPTAIL, but the REM shows approximately same results in both the cases. When compared to each other, REM and DROPTAIL shows large maximal delay then RED while using normal approach and REM shows largest maximal delay with CPR approach and RED has the minimum.

5.1.3 End-to-end delay:

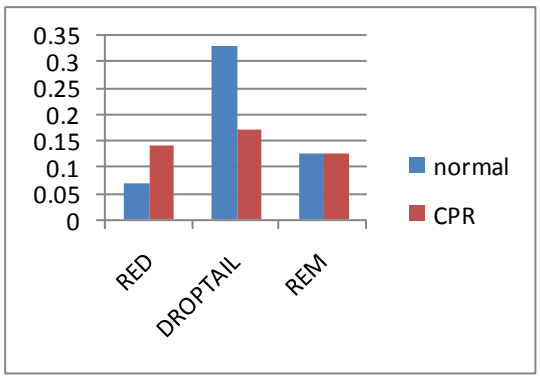

Fig 3: End-to-end delay in RED and DROPTAIL using CPR and without using CPR.

5.1.4 Packets dropped:

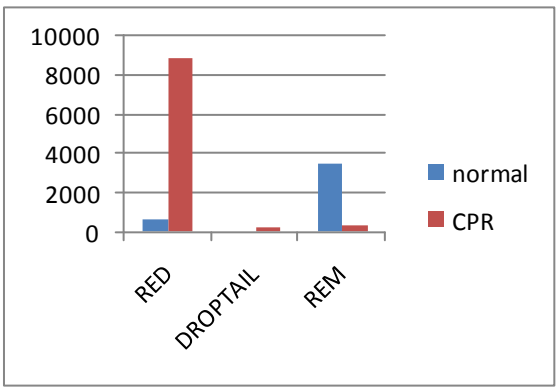

Fig 4: Packets dropped using RED and DROPTAIL using CPR and without using CPR.

The graph shows the comparison between the three queue management algorithms REM, RED and DROPTAIL with using CPR approach and without it on the basis of packets dropped. When compared individually, DROPTAIL shows negligible packet drop while using normal approach as well as CPR and RED shows very large number of packets dropped while using CPR approach, but the REM shows more number of packets dropped when using normal. When compared to each other, RED drops maximum and very large number of packets while using CPR approach and DROPTAIL and REM shows approximately negligible results as compared to RED. While using normal approach, REM shows maximum packet drop and DROPTAIL shows almost negligible result and RED drops very less number of packets.

5.1.5 Packet delivery ratio:

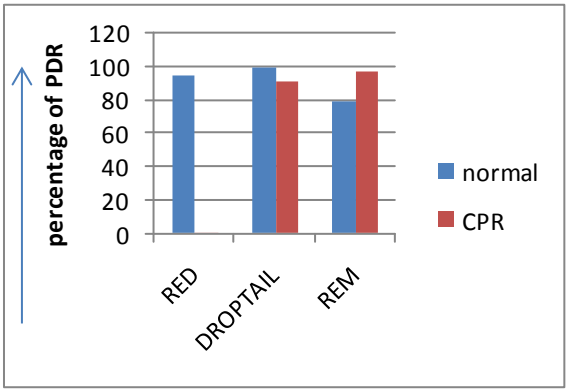

Fig 5: Packet delivery ratio for RED and DROPTAIL using CPR and without using CPR.

The graph shows the comparison between the three queue management algorithms REM, RED and DROPTAIL with using CPR approach and without it on the basis of packet delivery ratio. When compared individually, DROPTAIL shows more PDR while using normal approach and RED shows more PDR while using normal approach and shows almost negligible result with CPR approach, but the REM shows more PDR while using CPR approach then the normal approach. When compared to each other, DROPTAIL shows large PDR while using normal approach and REM shows minimum value of PDR but with very small difference and with CPR approach REM and DROPTAIL shows largest PDR as compared to RED which gives the minimum value.

Conclusion

In this paper, the comparisons are done between the three queuing management algorithms REM, RED and DROPTAIL**.** As the results shows minimal delay shown is more while using CPR approach and RED shows the largest minimal delay. For maximal delay, normal approach shows almost similar results and CPR shows maximum result in case of REM, in case of end-to-end delay DROPTAIL shows the maximum delay, RED drops the maximum number of packets and RED has the minimum PDR and REM has the maximum using CPR, DROPTAIL has the mixed response. So, in some cases REM is better than RED.

References:

Journal Papers:

[1] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, Jianping Yin, Flow level detection and filtering of low-rate DDoS, *Computer Networks 56 (2012) 3417–3431*

[2] Monowar H. Bhuyan, H. J. Kashyap1, D. K. Bhattacharyya and J. K. Kalita, Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, *The Computer Journal.*

[3] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, *Computer Networks 44 (2004) 643–666* .

[4] Mohit Agrawal,Navneet Tiwari,Lalla Atul Singh Chaurasia and Jatan Saraf, Performance Analysis and QoS Assessment of Queues over Multi-Hop Networks, *International Symposium on Computing, Communication, and Control (ISCCC 2009) Proc .of CSIT vol.1 (2011)*

[5] Santosh Kumar, Abhinav Bhandari, A.L. Sangal and Krishan Kumar Saluja, Queuing Algorithms Performance against Buffer Size and Attack Intensities, *Global Journal of Business Management and Information Technology. Volume 1, Number 2 (2011), pp. 141-157*

[6] Saman Afrasiabi , Farzaneh Abazari, The evaluation of the behavior of computer networks by NS simulator and the effect of queuing systems in the performance of especial networks, *Life Science Journal 2013;10(1)*

[7] Bin Xiao, Wei Chen ,Yanxiang He, A novel approach to detecting DDoS attacks at an early stage, *J Supercomput (2006) 36:235–24*

[8] Ningning Hu, Liu Ren, Jichuan Chang, Evaluation of Queue Management Algorithms, C*omputer Networks 15-744.d44*

[9] Sanjeewa Athuraliya and Steven H. Low, Victor H. Li and Qinghe Yin, REM: Active Queue Management, *IEEE Network, May/June 2001(0890-8044)*

[10] Wu Zhi-jun , Zhang Hai-tao , Wang Ming-hua , Pei Bao-song, MSABMS-based approach of detecting LDoS attack, computers & security 31(2012)402-417.

[11] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013*

[12] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim, DDoS attack detection method using cluster analysis, *Expert Systems with Applications 34 (2008) 1659–1665*