Active Queue Management based Solution for Improving Performance under DDOS Attacks

Shivani Mishra
Research Scholar YCoE
Punjabi University, Patiala
India

Ashok Kumar Bathla
Asst. Prof. in CE, YCoE
Punjabi University, Patiala
India

ABSTRACT
Effectively and fairly allocating resources to the competing users in a network is a major issue to meet the demand for higher performance nowadays. How to provide better congestion control for network emerges as a major issue. The problem of congestion control is reduced with the help of active queue management techniques. The main objective of this research is to simulate and analyze the effect of 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. It is an approach in developing a comparison on congestion avoidance algorithms for router-based communication and conclude that Stochastic fair queuing give better performance among all and provides an effective way to insulate users from ill behaved sources and improve the drawback of the queuing algorithm. Stochastic Fair Queuing algorithm can give fair allocation of bandwidth to each source nodes and packet loss can be minimized and dropped packets can be retransmitted and network congestions can be managed in efficient way. The results also indicate that UDP type attack traffic is more powerful as compared to TCP type attack. The performance metrics of the comparison are average delay and packet drop and throughput The algorithms are tested in terms of delay , throughput fairness, utilization and packet loss rate by applying various number of flows under TCP, and TCP/UDP traffic..

Keywords
Queuing Algorithms, AQM, packet Drop, ns2

1. INTRODUCTION
Today's Internet only provides best effort service in which traffic is processed as quickly as possible but there is no guarantee as to timeliness or actual delivery. DDoS attacks often take the form of flooding the network with unwanted traffic. Network Congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical effects include queuing delay, packet loss or the blocking of new connections. The cooperation of distributed sources makes DDoS attacks hard to combat or trace back Two approaches are used to implement the DoS and DDoS attacks, exploiting the vulnerabilities available on the target or sending a vast number of messages to overwhelm the target. First type of attack is called vulnerability attack and another one is known as flooding attack.

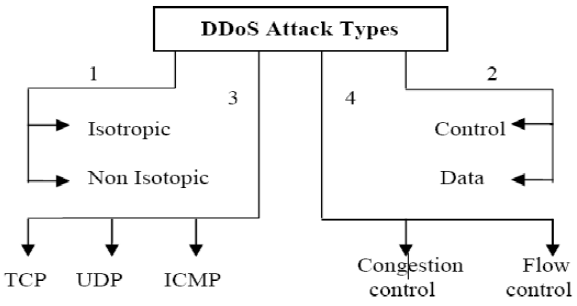

Fig 1

The Internet traffic generates stream of data packets in the network with different traffic rate and leads to congestion. During congestion, the network throughput drops whereas end to end delay increases. Congestion is an important issue which researchers focus on in the TCP network environment**.** Most used protocols on internet are UDP and TCP. Queue management algorithm by the routers is one of the important issues in the congestion control study. These routers are augmented to monitor traffic and grant requests for rate-limiting of the streams they deliver to their peers .These algorithms are evaluated on router architecture for their practical feasibility and these mechanisms are evaluated for various quality metrics such as throughput, packet loss, transportation delay. Improving the congestion control and queue management algorithms in the Internet has been one of the most active areas of research in the past few years.

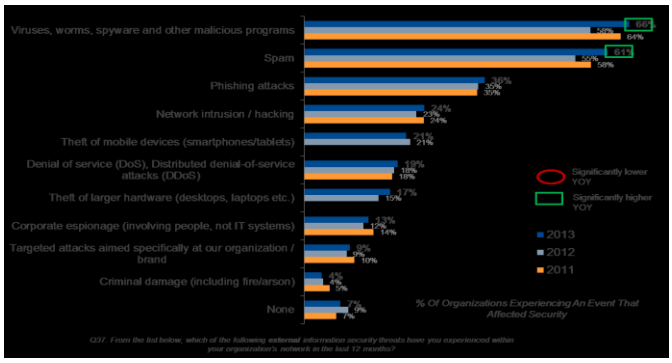

Fig. 2 IT Security threats according to KASPERSKY LAB survey

2. ACTIVE QUEUE MANAGEMENT

To keep the stability of the whole network, congestion control algorithms have been extensively studied. Queue management method employed by the routers is one of the important issues in the congestion control study. Active Queue Management (AQM) has been proposed as a router-based mechanism for early detection of congestion inside the network. The definition of too much depends on the Quality of Service (QoS) to be delivered by the network. Congestion reactive protocols such as TCP and AQM strategies have done a lot of interesting research during the last decade. For our purposes, AQM strategies can be classified into two types: oblivious (stateless) and stateful . An AQM scheme does not inspect packets to determine which flow they belong to. Hence it cannot perform differential marking or scheduling for different flows. Stateful schemes such as fair queuing offer good performance on a variety of metrics. Most of this misbehaving traffic does not use TCP. . Thus, it seems important to study scenarios where end-points are greedy and selfish, and do not follow socially accepted congestion control mechanisms. Of course, one could use stateful schemes such as fair queuing to guard against selfish users.

2.1 Benefits of AQM

AQM disciplines are able to maintain a shorter queue length than drop-tail queues.

1. Reducing number of packets dropped in routers: Keep average queue size small,

hence leaving enough space for bursts.

2. Providing lower-delay interactive service by keeping average queue size small,

end-to-end delays will be shorter.

3. Avoid bias against low bandwidth and bursty flows.

4. Guarantee that a newly arriving packet 'almost always' finds a place in the buffer

It also furnishes protection between different services on outputport, so that poorly behaved service in one queue can not impact the bandwidth delivered to the other services. In our simulation we are using the DropTail, Fair Queuing (FQ), Stochastic Fair Queuing (SFQ),Deficit Round Robin (DRR) and Random Early Detection (RED) available in ns-2.

3. QUEUING ALGORITHMS

3.1 Droptail

Drop Tail is a Passive Queue Management (PQM) algorithm which only sets a maximum length for each queue at router. It is based on first in first out (FIFO) queue policy. The entire incoming packets are stored in a buffer or queue of limited size. It introduces global synchronization in several connections, when the packets are dropped.

3.2 Random Early Detection

Among various active queue management schemes (AQM), random early detection (RED) is probably the most extensively studied. it monitors the average queue size to find out whether it lies between some minimum threshold value and maximum threshold value. If it is true then the arriving packet is marked or dropped with some probability that is increasing function of average queue size. All the arriving packets are dropped when the variable does not lie between minimum and maximum threshold values.

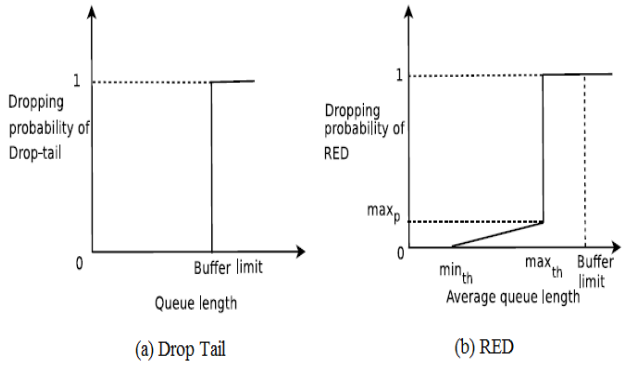

Fig. 3 Dropping probability of Drop Tail and RED.

- min_{th} determined by the utilization requirement, Needs to be high for fairly bursty traffic
- max_{th} set to twice min_{th}

3.3 Calculating Average Queue Size

Avg. = (1 – Weight) * Avg + Weight * Actual Queue Length, , where 0 < Weight <1

$$P = \max\_P \frac{\text{avg\_len - min\_th}}{\text{max\_th - min\_th}}$$

Fine tuning minQ, maxQ, maxP and weight needed for optimum performance. RED needs to be deployed at the edge of the network

3.4 Defict Round Robin

Deficit Round Robin (DRR) like scheduling algorithms is their ability to provide guaranteed service rates for each flow (queue). DRR services flows in a strict round-robin order. It has complexity *O*(1) and it is easy to implement. Deficit Round Robin uses three parameters, weight, DeficitCounter and quantum [18]. Weight decides percentage of output port must be allocated to the queue. Deficit Counter decides whether a queue is permitted to send data packet or not. Quantum is proportional to the weight of a queue and also represented in terms of bytes [19]. The value of the Quantum is added to the Deficit Counter associated with that queue and will be used in the next service round

$$quantum_i = \frac{r_i}{C} \times F$$

Wherer i is the rate allocated to flow i, C is the link service rate, and F is the frame size that represents the summation of Quantum's for all fows. DRR only considers whether a packet could be sent out in a round and does not care for their eligible transmission sequence.

3.5 Stochastic Fair Queuing

Fair queuing (FQ) was proposed by John Nagle in 1987. FQ is the foundation for a class of queue scheduling disciplines that are designed to ensure that each flow has fair access to network resources and to prevent a bursty flow from consuming more than its fair share of output port bandwidth. Stochastic Fair Queuing is an implementation of Fair Queuing. Because it is not practical to have one queue for each conversation SFQ employs a hashing algorithm which divides the traffic over a limited number of queues .Due to the hashing in SFQ multiple sessions might end up into the same bucket. Because there is the possibility for unfairness to manifest in the choice of hash function, this function is altered

periodically. The key word in SFQ is conversation (or flow), which mostly corresponds to a TCP session or a UDP stream.. Traffic is then sent in a round robin fashion, "giving each session the chance to send data in turn. This leads to very fair behavior and disallows any single conversation from drowning out the rest.

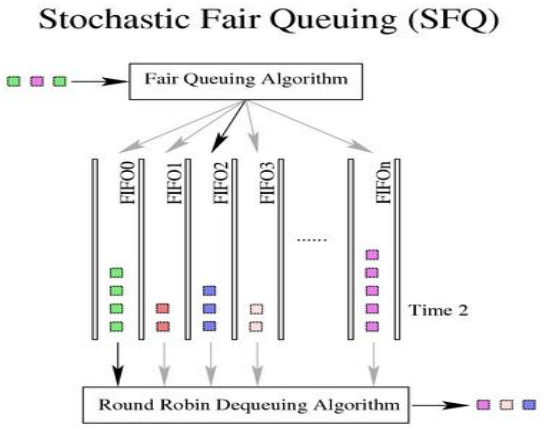

Fig. 4 SFQ

SFQ has also been claimed to be the first queuing algorithm focusing on handling both CBR and VBR traffic, and thus has benefits when applying on modern networks where VBR traffic is common.

4. EFFECT OF DDOS ATTACKS ON VARIOUS QUEUING ALGORITHM

A Internet like topology of comprising of the attackers, legitimate users, router and the destination node is put through the flooding based DDOS attack and different AQM techniques(Droptail, RED, DRR and SQF) are implemented on the router one by one to study their impact on the different parameters like Throughput , Delay and Packet loss. An attempt has been made to Mitigate the effect of DDoS attack by applying diffrent time rates of each sender node, and setting threshold value and evaluate performance.

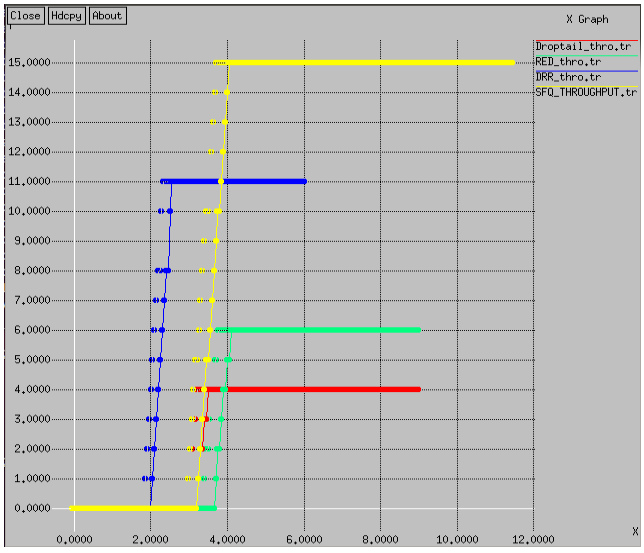

Fig. 4 Throughput of various queuing algorithms

Throughput = Packets Sent/ Time

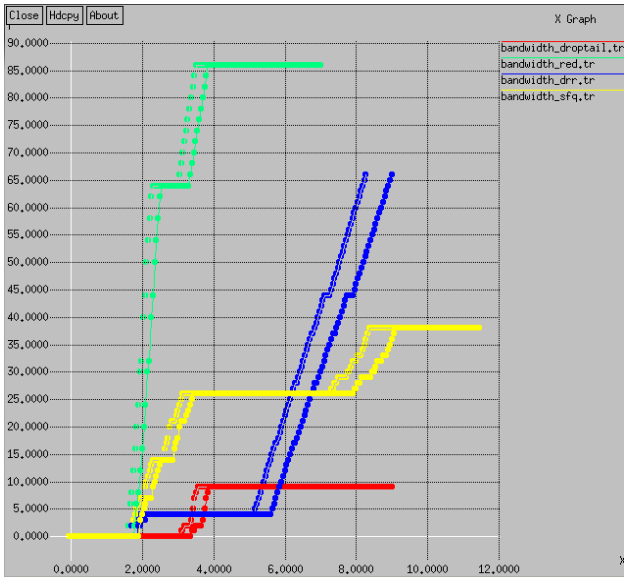

Fig. 5 Bandwidth graph of the AQM techniques

The effect on the Bandwidth by the different AQM techniques, directly showing the effect on link utilization in topology.Allocation Of Resources = Bandwidthh of legitimate traffic / bandwidth of attack traffic

5. STOCHASTIC FAIR QUEUING PERFORMANCE

This fairness-queuing algorithm operates by maintaining a separate first-come-first-served (FCFS) queue for each conversation. Since the queues are serviced in a bit-by-bit round-robin fashion ill-behaved conversations that attempt to use more than their fair share of network resources will face longer delays and larger packet-loss rates than well-behaved conversations that remain within their fair share. The major differences are that the queues are serviced in strict round-robin order and that a simple hash function **is** used to map from source destination address pair into a fixed set of queues. Global synchronization and bias against bursty traffic is the major problem which is faced by almost all the algorithms. So for this we can pace the sender to send at approximately the rate it can deliver data to receiver. Each Flow is assigned a rate in bytes per interval. The flow entry maintains a point in time the next packet in the flow should be scheduled. Similarly we can set the set time rate according to the delay experienced by the packet can be used to guess the rate available at the given time on the path even though the characteristics of the path and the competing traffic remain unknown. The receiver sends the acknowledgement after getting data, so the arrival of acknowledgement at the sender paces the sender at approximately the average rate it is able to achieve through network.

Evaluation

- Congestion → Good
- Bias Against Burst Traffic → Good
- Global Synchronization → Good
- Link Utilization → Good

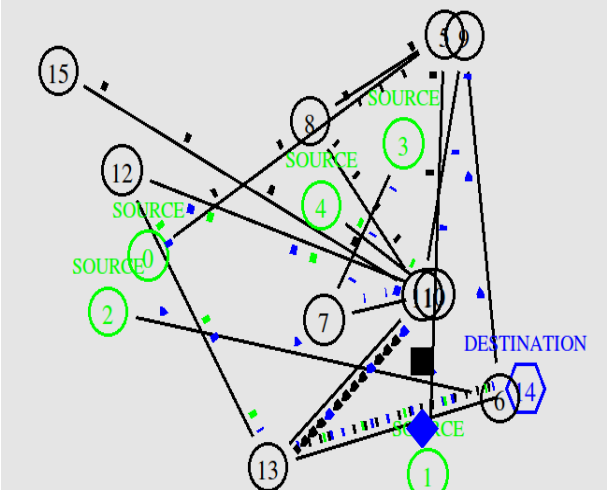

Fig. 6 Simulation Structure

6. FINDING THE MOST POWERFUL ATTACKS AMONG TCP AND UDP ATTACKS

According to the consideration node is representing a system in the internet; node 0, node 1, node 2, node 3 and node 4 represent the legitimate UDP user, legitimate TCP user, attacker, router and receiver respectively. Link bandwidth for node 0, node 1, node 2, node 3 and node 4 is 1Mbps with 100ms of propagation delay. Drop Tail is used as queuing algorithm. Most used protocols on internet are UDP and TCP. First of all we have perform UDP flood attack and TCP attack to find out which one is more powerful attack in terms of affecting the legitimate users and consuming the more bandwidth as much as possible. We consider node 0 sends 50% data that means it will occupies 0.5Mbps bandwidth. Therefore, concurrently if node 0 sends the 30% data to node 4, and node 2 sends 30% data to node 4 and node 2 sends 60%data to node 4, the total coming traffic at node 3 is 140 % means coming traffic will use 1.3Mbps bandwidth but here we have 1Mbps link between node 3 and node 4. So data capable of 1Mbps can be transferred by node 3 therefore 40% data will be dropped and also called 40% attack intensity. These data may belong to any of users, may be of TCP user, UDP user or attacker. So finally attacker gets success in consuming the bandwidth.To meet the objective three criteria has been taken:

5.1 Performance Legitimate TCP and UDP Users In Case Of Attack Free Traffic

In this case both legitimate TCP and UDP users get the desired bandwidth 0.4Mbps and 0.3Mbps respectively in case of no attack traffic.

5.2 Effect on Legitimate TCP and UDP Users during TCP Type Attack Traffic

Legitimate TCP and UDP users are sending data respectively on their specified rate and attacker is sending data on varying rate. Result shows that TCP attack traffic does not have any effect on legitimate UDP user. It affects only legitimate TCP user.

5.3 Effect on Legitimate TCP and UDP Users during UDP Type Attack Traffic

Legitimate TCP and UDP users are sending data respectively on their specified rate and attacker is working with varying attack intensities .Simulation results shows that UDP attack traffic has greater effect on both users as compared to TCP type attack traffic. TCP user is being affected much as compared to UDP user.Therefore it is analyzed that there is more packet loss, delay and lesser throughput is achieved in TCP type of attack Traffic. TCP has no explicit congestion signal defined.

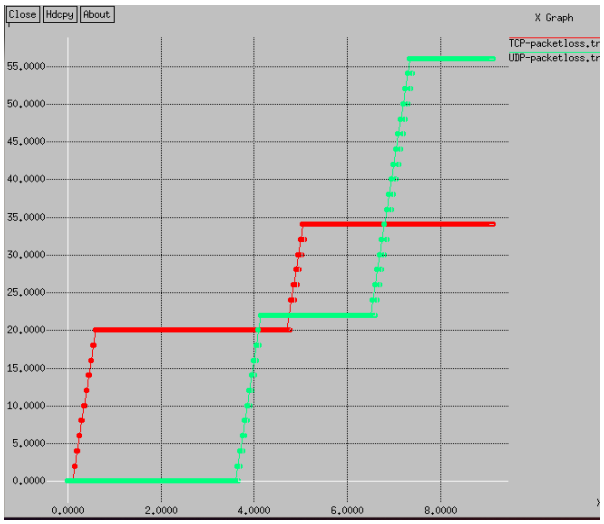

Fig. 7 Packet drop rate

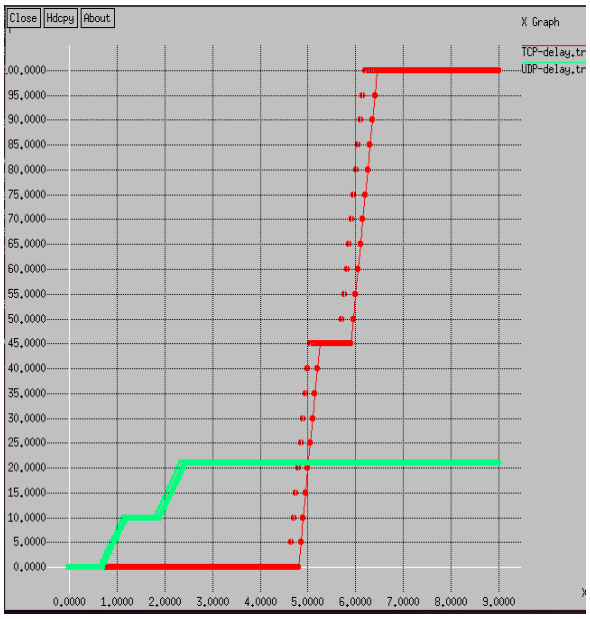

Fig 8 representing the considerable rise in the delay parameter of TCP user

Average end to end delay = ∑ Packet arrival time – Packet Start Time

7. CONCLUSION AND FUTURE WORK

DDoS attacks often take the form of flooding the network with unwanted traffic. In this paper We have explained about Queuing algorithms including DropTail, Stochastic Fair Queuing, Deficit Round Robin and Random Early Detection. We have calculated the different performance parameters for each algorithm of considered network configuration. On comparing the performance of different queuing algorithms we found that Stochastic Fair Queuing is best algorithm among all algorithms. The result of simulation suggests that UDP type attack is more powerful attack as compare to TCP type one. We have also proposed an approach that how the problems of global synchronization can be lessen in Stochastic Fair Queuing algorithm so that there is fair allocation of bandwidth to each source nodes and packet loss can be minimized and dropped packets can be retransmitted. The detection of the attack is not completely reliable, and misclassification of normal flows is still possible. The distributed denial of service is the critical problem which is not solved yet. There is no complete solution existing of the DDoS attacks. For future work, we plan to extend the simulation for the new algorithm which would comprise all the advantage of each algorithm The algorithm can be further enhanced with incorporation of traffic management algorithms. Further studies may produce more meaningful characterization of AQM algorithm performance in the real-world network**.**

8. REFERENCES

[1] Distributed Denial of Service Prevention Techniques B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE[9]A Taxonomy of DDoS Attacks and DDoS Defense Mechanism Jelena Mirkovic, Janice Martin and Peter Reiher Computer Science Department University of California, Los Angeles Technical report #020018

[2] Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1 and J. K. Kalita2

[3] Denial of Service Attacks Qijun Gu, PhD. Assistant Professor Department of Computer Science Texas State University – San Marcos San Marcos, TX, 78666 Peng Liu, PhD. Associate Professor School of Information Sciences and Technology Pennsylvania State University University Park

[4] Stochastic Fairness Queuing' Paul E. McKenney Information and Telecommunications Sciences and Technology Division SRI International Menlo Park

[5] Queuing Algorithms Performance against Buffer Size and Attack Intensities Santosh Kumar, Abhinav Bhandari, A.L. Sangal and Krishan Kumar Saluja Computer Science and Engineering, Dr. B. R. Ambedkar NIT, Jalandhar, India

[6] Jain, R., "A Delay based approach for congestion avoidance in interconnected heterogeneous computer networks", Computer communication review, V.19 N.5, october 1989, pp. 56-71.

[7] The Effects of Active Queue Management andExplicit Congestion Notification on Web Performance Long Le Jay Aikat Kevin Jeffay F. Donelson Smith Department of Computer Science University of North Carolina at Chapel Hill http://www.cs.unc.edu/Research/dirt

[8] Implementation of Deficit Round Robin Scheduling Algorithm Amir Hosain Jodar Communication Networks Laboratory http://www.ensc.sfu.ca/research/cnl School of Engineering Science Simon Fraser University