International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25589-25598

http://www.ripublication.com

Mitigating Congestion Based DoS Attacks By Using Weighted Fair Queuing With An Enhanced AQM Technique

A.Sreeja and Mr.M.Ganesh Karthik

M.Tech 2nd year Computer Science and Engineering
Sree Vidyanikethan Eng.College Tirupati,AP
sreeja.alinedi@gmail.com
M.Tech., Assistant Professor
Dept. of CSE Sree Vidyanikethan Eng.College Tirupati,AP
ganeshkarthik16@gmail.com

ABSTRACT

Denail of service (DoS) attacks are one of the biggest problem in an organization. The organizations can connect the internet can face these types of attacks. In Active queue management(AQM) scheme should ensures that (a)Each flow gets its fair bandwidth for all incoming packets.(b)Identify attack flows and then correct them. Recently coming AQM do not satisfy the above two goals. So here it proposes the concept of Deterministic fair sharing (DFS) for using the fair bandwidth. The DFS can allocate the bandwidth in per-flow basis. The DFS can share the bandwidth equally to all incoming flows. So here the congestion problem occurs. So we can avoid those problems we can propose the concept of weighted fair queueing (WFQ) for mitigating those drawbacks. Here it allocates the weights for all flows and also allocates the buffer by varying their packets.

Keywords: Congestion control, Active Queue Management, Deterministic Fair Sharing, Denial of service, Weighted Fair Queueing

1. INTRODUCTION:

A Foreswearing of Administration attack (DoS attack) or DDoS is an endeavor to make a PC asset distracted to its proposed users. DoS assaults ordinarily target sites or services facilitated on high. Profile web servers such as, credit card installment doors and even root name servers. One basic system for assault includes suturing the target machine with outer communications requests, such that it can't react to genuine

movement or reacts so gradually as to be rendered viably inaccessible. In general terms, DoS assaults are executed by either implemented by the target PCs to reset, or devouring its resources. So that it can no more give its planned administration that the correspondence media between the expected clients and the exploited person so they can no more impart adequately. DoS assault is an endeavor to avoid true blue clients of an administration or system or resource. DoS assaults for the most part make utilization of programming bugs to crash or stop an administration or system resource, or data transfer capacity restricts by making utilization of a surge assault to soak all data transmission.

DoS assaults for the most part attain to their objective by sending extensive volumes of bundles that possess a critical extent of the accessible bandwidth. Hence DoS assaults are likewise called data transfer capacity attacks. The point of the data transmission assault is to expend basic sources in a system service. Possible target assets may incorporate CPU limit in a server, stack space in system convention software, or web join limit. The urgent highlight of data transmission assaults is that their quality lies in the volume instead of the substance of the assault traffic. This needs to real ramifications.

- Attackers can send a mixture of packets. The assault movement can be made subjectively like genuine traffic, which enormously confounds resistance.
- The volume of movement must be sufficiently vast to expend the target's resources. The aggressor for the most part needs to control more than one PC to create the assault traffic. Bandwidth assaults are in this manner regularly DoS assaults.

Refusal of administration is a standout amongst the most unmistakable assault systems on the internet. In a late study led by Radware and wonder Organization that comprised of looking over 705 IT practitioners, it was watched that 65% of the spoke to associations experienced DoS assaults. DoS assaults can be characterized into two classes relying upon the OSI model: infrastructure-based assaults and application-based attacks. The previous focuses on the system layer and transport layer and recent focuses on the application layer. Infrastructure-based assaults incorporate HTTP/SSL GET and POST surges and NTP surges.

Secure correspondence has some attractive security perspectives, for example, confidentiality, authentication, message respectability and non denial. Furthermore, as of late more individuals are mindful that accessibility and access control are likewise earnest necessities of secure correspondence in light of the infamous Dissent of Administration (DoS) assaults that render by the illegitimate clients into a system, host, or other bit of system base to damage them, particularly it is done against the as often as possible went to sites of various prominent organizations or government sites. DDoS (Appropriated Dissent of Administration) assault uses sufficient manikin PCs to make measure of information bundles, the assaults gets to be composed and originate from different manikins in the meantime therefore are notwithstanding pulverizing. An average DDoS assault contains two stages, the first stage is to trade off defenseless frameworks that are available in the Web and introduce assault devices in these bargained frameworks. This is known as transforming the PCs into

"zombies." In the second stage, the assailant sends an assault charge to the "zombies" through a safe channel to dispatch a transfer speed assault against the focused on victim(s). The current assaults on popular sites like Amazon, Yippee, e-Sound and Microsoft and their resultant disturbance of administrations have revealed the shortcoming of the Web to Conveyed Disavowal of Administration (DDoS) assaults. It has been seen through reports that more than 85% of the DoS assaults use TCP. The TCP SYN flooding is the most usually utilized assault. It comprises of a surge of parodied TCP SYN bundles coordinated to a listening TCP port of the exploited person. The Web servers as well as any frameworks associated with the Web giving TCP-based system administrations, for example, FTP servers or Mail servers, are helpless to the TCP SYN flooding assaults.

1.1 Types of Dos Assaults:

Before characterization of DDoS assaults, we portray a common DDoS assault situation. At that point we present why it is so pervasive, and its inherent reasons why it is so natural to dispatch. Figure (1) demonstrates a various leveled model of a DDoS assault. DDoS assault partition into 2 sorts. One is data transfer capacity consumption. This technique is to clog the system, gigantic utilization of the transfer speed then lead the system breakdown. The other sort is asset exhaustion. Assailant exhausts the key assets, for example, CPU, memory etc. At that point break the server. The assault more often than not begins from various sources to go for a solitary target. Numerous target assaults are less regular; notwithstanding, there is the likelihood for aggressors to dispatch such kind of assault Mock, changed, or replayed directing data

1.1.1 SYN surge assault:

Any framework giving TCP-based system administrations is possibly subject to this assault. The aggressors utilize half-open associations with reason the server fume its asset to keep the data portraying every pending association. The outcome would be framework accident or framework broken.

1.1.2 TCP Reset Assault:

TCP reset likewise use the qualities of TCP convention. By listening the TCP associations with the victimized person, the aggressor sends a fake TCP RESET parcel to the victimized person. At that point it causes the victimized person to incidentally end its TCP association.

1.1.3 ICMP assault:

Smurf assault sends produced ICMP reverberation demand parcels to IP telecast addresses. These assaults lead a lot of ICMP reverberate answer bundles being sent from a delegate site to a victimized person, as needs because system blockage or blackouts. ICMP datagram can likewise be utilized to begin an assault by means of ping. Aggressors utilize the ping Order to build larger than average ICMP datagram to dispatch the assault.

1.1.4 UDP tempest assault:
This sort of assault cannot just disable the hosts. Administrations additionally clog or back off the predominant system. At the point when an association is built between two UDP administrations, each of which delivers an extremely immense number of bundles, accordingly cause an assault.

1.1.5 DNS appeal assault:
In this assault situation, the assault sends an expansive number of UDP-based DNS appeals to a name server utilizing a parodied source IP address. At that point the name server, going about as a middle gathering in the assault, reacts by sending back to the ridiculed IP address as the victimized person destination. In view of the enhancement impact of DNS reaction, it can bring about genuine transfer speed assault.

1.1.6 CGI appeal assault:
By just sending different CGI solicitation to the target server, the aggressor devours the CPU asset of the victimized person. At that point the server is compelled to end its administrations.

1.1.7 Mail bomb assault:
A mail bomb is the sending of a colossal measure of email to a particular individual or framework. An enormous measure of mail may essentially top off the beneficiary's plate space on the server or, sometimes, may be excessively for a server to handle and may bring about the server to quit working. This assault is likewise a sort of surge assault.

1.1.8 ARP tempest assault:
Amid a DDoS assault, the ARP asks for volume can get to be extremely enormous, and after that the victimized person framework can be adversely influenced.

1.1.9 Spam Attack:
This sort of assault is utilized for focusing on the different mail administrations of corporate and additionally open clients. DDoS assault through spam has expanded and bothered the mail administrations of different associations. Spam enters through all the channels to make DDoS assaults, which causes genuine inconvenience to clients and the information. Anyhow, these mail administrations are regular focus of programmers and spammers.

A refusal of administration assault (DOS) is any kind of assault on a systems administration structure to handicap a server from overhauling its customers. Assaults range from sending a huge number of solicitations to a server trying to ease it off, flooding a server with extensive bundles of invalid information, to sending appeals with an invalid or mock IP address.

In AQM [1] the DoS attacks is one of the major problem. The organizations can face these types of problems when connected to the internet .Based on their DoS attacks the congestion problem is occurred in edge routers. In the networks the attackers can send the duplicate packets or data to the routers because of the

authorized data will be captured or destroy. The main aim of the attackers is to destroy the authorized data.

2. RELATED WORK:

Jarvinen & Kojo (2014) [2] assessed CoDel (Controlled Delay) and PIE (Proportional Integral controller Enhanced), both being new AQM recommendations, and look at the execution against a forceful RED (Random Early Detection) variation called HRED (Harsh RED). Likewise centered around AQM conduct amid burden drifters ordinarily happening at the system edge with the basic activity sorts of today, for example, Web exchanges. It found that CoDel auto-tuning does not scale well with the heap.

Nagarjun et al., (2013) [3] broke down RTS/CTS assault which abuses the medium reservation system of 802.11 systems through length of time field. Likewise proposed variations of RTS/CTS assaults in remote systems. It reenacts the assaults conduct in ns2 reproduction environment to show the assault practicality and in addition potential negative effect of these assaults on 802.11 based systems. It examined conceivable methods for identifying and alleviating such Low rate DoS assaults in remote systems.

Dissent of Service (DoS) assault is a suite of assaults comprising of assaults like Blackhole, Grayhole assault and so on in which the system activity is caught and sent to a pernicious hub or a gathering of working together noxious hubs in the system in order to hamper real interchanges in the system. Das & Taggu (2014) displayed an investigation of the impacts of Blackhole, Grayhole, Rushing and Sleep Deprivation assaults in Adhoc On-Demand Distance Vector (AODV) based MANETs. Different execution measurements have been utilized to study the impacts of diverse DoS assaults in MANETs and an exhaustive examination is displayed. NS-2.35 has been utilized widely to mimic these assaults.

Oktian et al., [5] made an application on the highest point of Beacon controller to alleviate the DoS assaults in the OpenFlow systems. The assaults incorporate IP/MAC Spoofing and Bulky/Garbage Message. Likewise dispatch the DoS assaults towards the system and examine the execution of the application. These assaults, Beacon, and OpenFlow are executed in the system reproduction environment Mininet.

Random early detection (RED) [4] is used to avoid the congestion. Drop tail is one of the concept is used to identify the attack flows. In this concept the packets can send the edge routers. The flows or networks can send the packets to the edge routers. If suppose at a time more than one network can send the packets. The packets can use more than their output bandwidth so the drop-tail concept can drop the excess packets. It identified those excess packets had attack packets.

3. PROBLEM STATEMENT:

In the existing paper the recent Active Queue Management (AQM) cannot satisfy these goals:

1. It cannot share the fair bandwidth to the packets.

2. Do not identify the attack flows.

So we can mitigate these two concepts here it proposes deterministic fair sharing (DFS).DFS use the concept of weighted fair sharing. The DFS also cannot provide the fair bandwidth to the packets. So we can propose the concept of weighted fair queueing for mitigate the fair bandwidth allocation and also avoid the congestion based on their DoS attacks by using this concept.

4. PROPOSED WORK:

In Active queue management (AQM) proposes the concept of deterministic fair sharing (DFS) for fair bandwidth allocation. The DFS having without knowledge about the incoming packets whether the incoming packet is from the attacker or not. It can allow all the packets to the edge routers. If suppose the networks or flows can send the packets to the edge routers. The attackers can add the packets to the incoming packets or flows. The attackers can use the available bandwidth. So they have no space can use their legitimate packets.

The deterministic fair sharing (DFS) can send the packets on per-flow basis. The packets can enter the buffer and after it leaves. By using the enque and deque operations.

1. Enqueue Operation: They can send the packets to the buffer. If the packets are less than the buffer space it can enqueue the buffer. For example:

$$F_1 < R \quad \rightarrow \quad (1)$$

Where

F_1: packets which is in the flow1
R: Buffer capacity

2. Dequeue Operation: If suppose they have no space or else the packet size is more than the buffer space. It can automatically drop or dequeue the packets.

$$F_2 > R \quad \rightarrow \quad (2)$$

where

F_2: Packets which is in the flow2
R: Buffer capacity

The Active queue management (AQM) having to share the buffer fairly to all incoming packets by using the weighted fair sharing. The WFS can share the buffer fairly to all incoming flows based on their scaling factor. The WFS can allocate the buffer dynamically to the all incoming flows and also do not overflow the buffer usage. In DFS the fair bandwidth is the problem so we can overcome this problem by using the weighted fair queuing (WFQ) [6].The WFQ is the packet scheduling process for a wireless network. In Weighted fair queueing is used the concept of Generalized

processor sharing(GPS).The fair queueing concept can group the packets into classes and service these classes to the edge routers based on their weights. This weight is calculated by the concept of generalized processor sharing.GPS can share the packets based on their fixed weights.

In GPS, the N flows (classes or sessions) are arranged with weight w_1 for each for each flow. Based on their weights to service the packets to the queue. The WFQ supports large number of flows or classes. It allocates the fair bandwidth to the queues by varying the packet size so by using this concept there is no wastage of bandwidth.

4.1 Problem Formulation:

For example: The buffer capacity is 16 it is denoted by R. The flow1 can send the packets to the buffer which is 8.Then flow2 can send the 2 packets, flow3 sends the 3 packets and flow4 and 5 sends the 1 packet to the buffer.

Calculate the weight based on their packets. Which flow can send the highest packets or else which flow uses the highest buffer space.

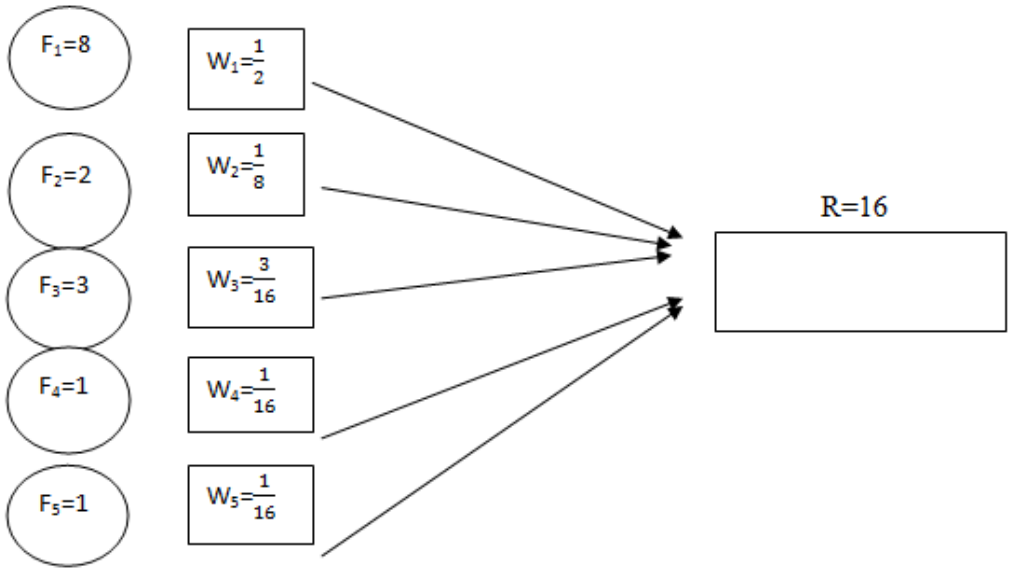


Fig 1: The conceptual model of flows

There are 5 flows F1……F5 sharing a buffer capacity R=16 based on their weights they can utilize the buffer as shown in Fig 1.

Flow1=8packets
Weight $w_1=\frac{1}{2}$
Flow2=2packets
Weight $w_2=\frac{1}{8}$
Flow5=1packet

Weight $w_5=\frac{1}{16}$

The weight w_1 of flow f_1 is defined by reserved buffer space with respect to the available buffer space.

$W_1=\frac{F_1}{R}$

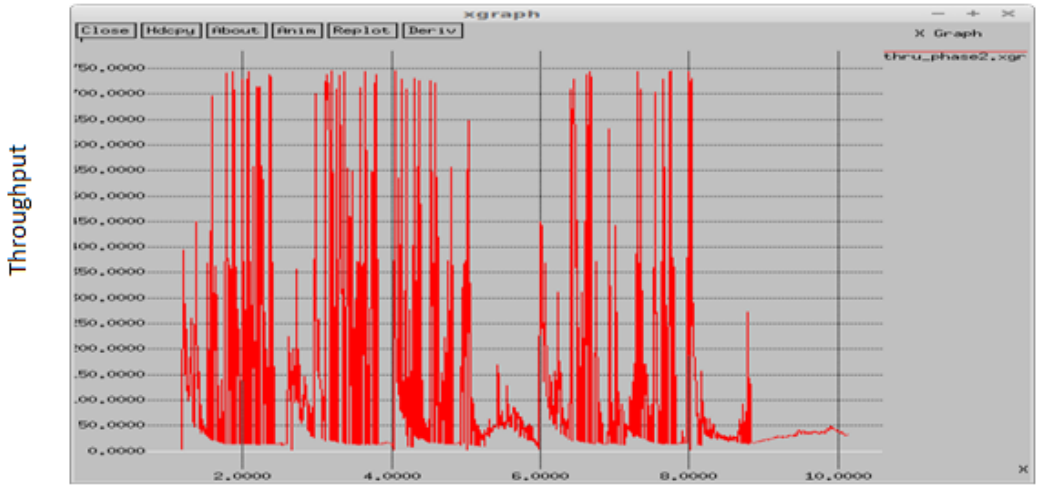
4.2 Simulation Parameters:

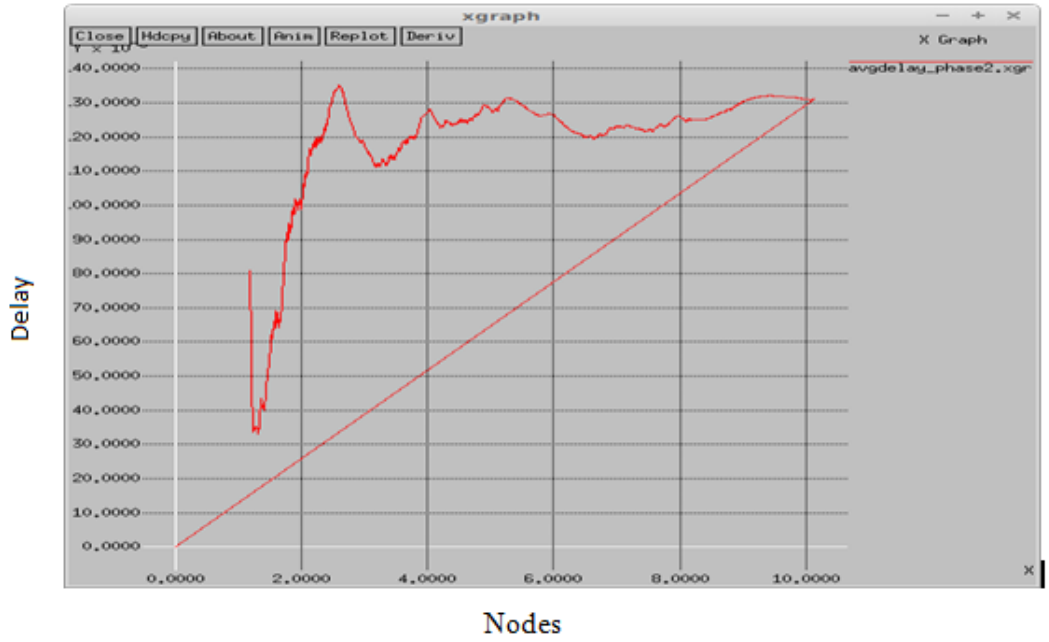
In this experiment we are setting different nodes to analyze the performance of the system. Here we consider 30 nodes; we configure the nodes with wireless network properties.

Channel	Wireless channel access
Propagation	Two ray Ground
Physical layer	Physical/Wireless physical Layer
MAC Layer	MAC/802.11
Queue	Droptail
Antenna	Omni-Antenna/Antenna
Protocol	AODV
Number of nodes	30-35
Simulation Time	1000sec
Simulation Environment	1000*1000
Transmission Range	2Mb/s
Slot Time	9ms

5. RESULTS:

To overcome the drawbacks of the existing paper. To increase the throughput and delay when compared the existing paper and we got that the throughput and delay is greatly increased.





6. CONCLUSION:

In this work, the AQM can avoid the congestion based on their DoS attacks with edge routers. The AQM proposes the concept i.e., DFS for fair bandwidth. The DFS can send the packets to per flow basis.DFS can use the concept of weighted fair sharing. The WFS can allocate the buffer fairly with all incoming flows. It can allocate dynamically to all flows. The DFS can share the bandwidth equally to all incoming flows. Some flows having less space and some flows having more space. So we can avoid this drawback we can propose the concept of weighted fair queueing. It allocates, how much of space having their flows only that much of space they can assign based on their weights.

References:

[1] **Mitigating congestion based DoS attacks with an enhanced AQM technique.** Harkeerat Bedi, Sankardas Roy, Sajjan Shiva., Elsevier trans. Networking(2014).

[2] **The new AQM kids on the block: An experimental of CoDel and PIE.** Jarvinen and kojo. In IEEE/ACM trans. Networking(2014).

[3] **Comparing the impact of blackhole and grayhole attacks in moble adhoc networks**. Nagarjun et al.,. IEEE trans.Networking(2013).

[4] **Random early detection gateways for congestion avoidance.** S.Floyd., V.Jacobson, IEEE/ACM trans. Networking(1993).

[5] **The BLUE active queue management algorithm .**Oktian et al.,IEEE trans. Networking(2002).

[6] **HP 12500 switch series: QOS solution brief.** April(2014).