A Dynamic Bandwidth Assignment Approach Under DDoS Flood Attack

Raman Singh
UIET, Panjab University, Chandigarh, India
Email:chauhan4u.p@gmail.com

Amandeep Verma
Asistant Professor, UIET, Panjab University, Chandigarh, India
Email: verma_aman81@yahoo.com

***Abstract*—Distributed denial-of-service (DDoS) attacks are a major threat to the Internet. A lot of research is going on to detect, prevent and trace back DDoS attacks. Most of researchers are busy in post attack forensics which comes after the attack has been occurred but nobody is talking about how to design a system which can tolerate such attacks. In this paper we have suggested a approach for dynamic assignment of bandwidth in order to sustain the server. Basic idea is to examine genuine IP user's traffic flow based on volume. Divide traffic in two categories of genuine traffic and malicious traffic and assign bandwidth as per category. The idea is to design a system which can give services even when the server is under attack. However some performance will degrades but overall Quality of services will be acceptable. A new formula also has been derived for dynamic bandwidth assignment which is based on number of genuine users and traffic volumes of users and attackers.**

***Index Terms*— Bandwidth Management, Dynamic Bandwidth Assignment, QoS Controlling Factor**

I. INTRODUCTION

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource [1]. A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. As defined by the World Wide Web Security FAQ: A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms [2].

These unsecured computers, which were secretly broken into with a DDOS tool, are remotely controlled by the intruder. At the intruder's signal, all compromised "agent" systems simultaneously send a flood of packets to the victim. The results can be devastating [3]. Figure 1 shows how attacker uses unsecured computers to make them zombies and then these thousands zombies floods the bandwidth of victim server.

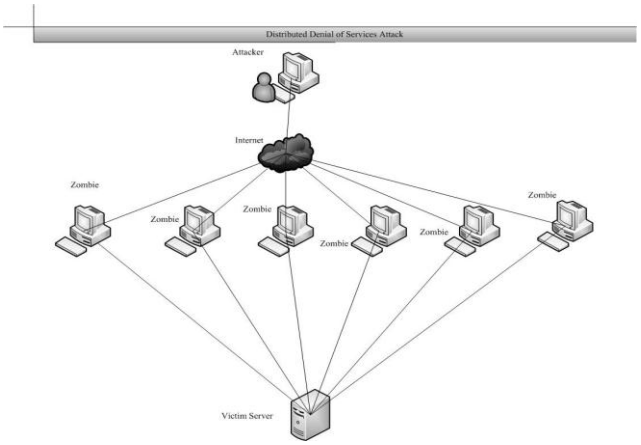

Figure 1. Distributed Denial Of Service Attack

A series of DDoS attacks blocks several e-commerce websites, like Yahoo, Ebay, and CNN. In January 2001, Microsoft's name server infrastructure was disabled by a similar attack. It is publicly recognized that DDoS attacks are some of hardest problems for the Internet. How to defend against DDoS attacks has become one of the extremely important research issues in the Internet community. The server can be effectively saved from being down by DDoS attack by proactive scheme which can effectively distinguish traffic from genuine and malicious users. Once the genuine and malicious users are defined, bandwidth can be effectively assigned in order to prevent server from flood attack. Droptail queue cannot distinguish between packets and treat all packets with same priority In this paper, bandwidth are assigned as per user groups and based on number of genuine and malicious user a new formula for dynamic assignment of bandwidth is suggested.

Manuscript received February 3, 2011; revised July 6, 2011;
Raman Singh is pursuing Ph.D in CSE from UIET, Panjab University, Chandigarh(India) (e-mail: chauhan4u.p@gmail.com).
Amandeep Verma is with the Department of Information Technology, UIET, Panjab University, Chandigarh, India (e-mail: verma_aman81@yahoo.com).

doi:10.4304/jait.3.2.120-129

This paper is divided into six sections. Section II describes the related work and gap of research for the quality of service and management of bandwidth under DDoS attack. Literature survey is done in this section. Section III explains the proposed approach of dynamic bandwidth management and QoS analysis. Section IV explain the implementation of proposed method. In section V, experiments and their results are discussed. In section VI paper is concluded and future scope is also suggested.

II. QUALITY OF SERVICE ISSUES

Most recent research in DDOS has taken place in the following areas:

A: Detection of DDOS: In this various methods and algorithms are developed in order to detect Distributed DOS Attack. For example using MIB (Management Information Base) groups: ip, icmp, tcp, udp and snmp in order to detect and mitigate DDOS. [7][21]. Prediction of numbers of zombies in DDoS attack by using polynomial regression model is suggested by B. B. Gupta, R. C. Joshi, and Manoj Misra [24].

B: Prevention: Need of preventing from DDOS attack arise after detection of attack. Researcher suggests various methods to prevent from DDOS attack. For example filtering each packet some traffic pattern and IP history and reject suspected packets. [12][13][14][15]. Trust based model to mitigate active attacks is suggested by N. Bhalaji, Dr. A. Shanmugam [25].

C: Traceback: After the detection and prevention of DDOS attack a need is arise to know the exact location of attacker I order to block those routers which are being used by attacker. Generally attacker use IP Spoofing and DNS Spoofing to hide their identity. IP packet filtering can be used to trace back the attacker. [16][17][18][19]

Now fourth area/phase in the research of DDOS attack is suggested: DDOS Attack Tolerance.

When DDOS attack occurs although detection, prevention and trace back mechanism are there but the service on which attack performed falls very dramatically and quality of service decrease under attack. So there should be some methods which may be used to tolerate attack so that the service quality doesn't fall below some standard level. The main problem is how to manage bandwidth of particular service like web service under attack and ensure standard quality of services (QOS) and tolerance under DDoS attack.

If we are able to manage bandwidth dynamically for some particular users (say priority users) the we will can control there QoS by controlling bandwidth of genuine and malicious users.

III. PROPOSED APPROACH

The proposed method for guaranteed QoS and availability of services depends on bandwidth management of victim server.

If attacker uses it's genuine IP address then guaranteed availability of service can be offered by Traffic Isolation. The basic idea is to divide traffic into two groups say one is genuine users and other group is malicious users. QoS of genuine user group can be controlled and guarantee of QoS can be offered to this group. The idea is to add priority users into genuine users groups, then divide users into these groups on the basis of many factors depending on type of service offered by server, number of users or any other relevant factor. Two factors are taken into consideration in this experiment; these are size of packets and rate at which packets are sent.

According to Campos F.H., Jeffay Kevin, Smith F.D. [22] in 1999 traces about 47% of responses were 1000bytes or smaller while in the 2003 traces, about 59% of the responses were 1000 bytes or less. It means that average packets sent by genuine users are 1000 bytes or below. So threshold of packets size 1000 bytes and rate of packets 1 MBPS to decide the group of users are decided. The users sending packets of size 1000 bytes or below with rate of 1 MBPS or below are put in the genuine users group and all other users are put in the malicious users group.
So the specified algorithm as:

Step 1: At the core router scan for each user the size of packets sent and rate at which packets are sent.

Step 2: On the basis of threshold of packet size and rate divide users into genuine users and malicious users groups.

Step 3: For the genuine users group assign full bandwidth available.

For the malicious users group assign bandwidth as per Dynamic Bandwidth Assignment Formula as per section V and subsection D.

Figure 2 shows the flow chart of the basic idea about bandwidth management of both groups of users' i.e. genuine users and malicious users. The Researcher have developed many methodologies till now to prevent the DDoS attack in which they either drop packets from malicious users or block them to further accept their packets. But a new approach of not to drop packets from malicious users but assign a very low bandwidth to them is suggested . The reasons for this new approach are:

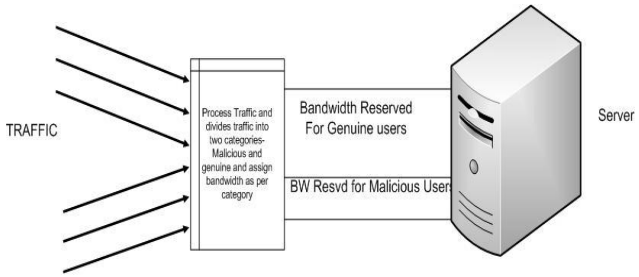

Figure 2. Basic idea of bandwidth management

a. First reason is to develop a methodology which can survive under heavy DDoS attack like situation which sometime caused due to users itself for example unintentional attack. Blockage of users is not suggested in this scenario because once a user is blocked in Intrusion Detection System (IDS), they are no longer use service further because their Internet Protocol (IPs) has been blocked by IDS. By the use of proposed methodology server can be saved to become unavailable for all users. QoS can be controlled for some users and provide good standard QoS for specified users and once these users use service of server and they withdrew and another set of users can get standard QoS and so on.

b. The Second reason is that if attacker is blocked he/she may know that he has been blocked and then change its location, IP, types of attack and can start new attack on victim server. However by assigning low bandwidth, good QoS for set of genuine user can be guaranteed while attacker believes he/she is still attacking victim server.

So proposed method of bandwidth assignment can work on both conditions when unintentionally DDoS type attack occur, when some server suddenly become popular and unexpected high number of users start browsing and using service of that servers or attacker intentionally attack on victim server by using its genuine IP, because if he/she use any fake IP or other fake identity method he/she will surely got caught cause in these days a number of methods are in use to prevent such type of DDoS attack as Wang H., Jin C., Shin K.G.[14] and Takemori Keisuke, Nishigaki Masakatsu [10] and Wang Shen, Guo Rui [23] suggests some methods.

If the attacker intentionally attacks on victim server, it is sure that he/she will sends packet at higher rate with larger size packets in order to choke the core router bandwidth. So, on core router, division of users is done into two groups of genuine users and malicious user because packets sent can be differentiate by genuine users and malicious attacker.

If the attack occurs unintentionally like when unexpected number of users suddenly starts requesting service of particular server then all users may send packets almost same size of packets but their rate may vary. So groups can be divided only on the basis of rate of packets or type of users or location of users like geographic location in order to sustain server under this unintentional attack and to facilitate server to continue provide standard QoS to some set users.

Flow chart of the proposed methodology are shown in figure 3.

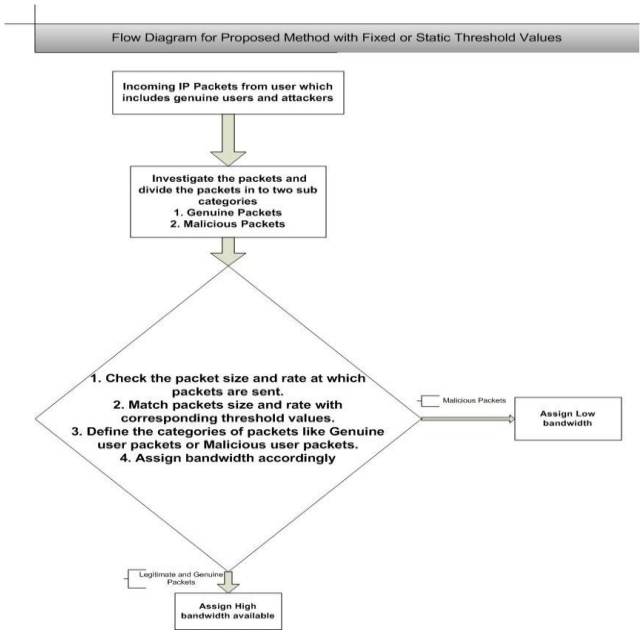

Figure 3 Flow chart

IV. IMPLEMENTATION

The proposed methodology of bandwidth assignment will be implemented on core router as shown in figure 4.

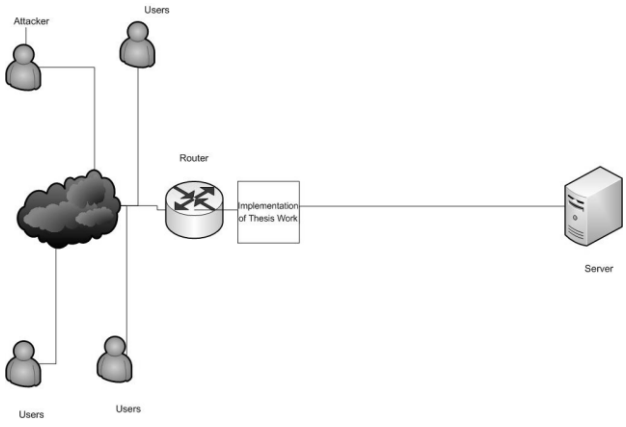

Figure 4. Network diagram for implementation of proposed methodology

Simulation study with three experiments using Network Simulator-2 (NS2 version 2.34) is performed.
These are:

1. Bandwidth and QoS Analysis with traditional drop tail Queue widely used in routers.
2. Bandwidth and QoS Analysis with proposed methodology and compare it with Drop tail Queue.
3. On the basis of experiment 1 and 2 and a Dynamic Bandwidth Assignment formula is proposed.

To perform these three experiments different topologies are used like 3/10/20 node topology with different attack intensity like 50%/ 100% /150%/200%/ 300% and 400%

TABLE I
DYNAMIC BANDWIDTH ASSIGNMENT OF MALICIOUS USER ON THE BASIS OF NUMBER OF GENUINE USERS

Attack Intensity	Total No. of Nodes	Malicious Nodes	Genuine Nodes	Limited Bandwidth assigned in mbps to Malicious user if Genuine user sends packets at the rate of 1 mbps
50	10	1	9	0.9
100	10	2	8	0.8
150	10	3	7	0.7
200	10	4	6	0.6
300	10	6	4	0.4
400	10	8	2	0.2

attack intensity. Attack Intensity is calculated as below:
If capacity of link between core router and victim server is C mbps (say 5 mbps)

50% Attack Factor = (50/100)*C say (50/100)*5 =2.5 mbps. So 50% Attack Intensity = C + 2.5= 5+2.5= 7.5 mbps. It means 50% attack Intensity means flooding packets in 5 mbps link with the rate of 7.5 mbps. Attack factor and Attack traffic is shown in table II.

For all topologies the link capacity are taken as below:
Capacity of link between core router to Victim server = 5 mbps.
Capacity of link of genuine users to core router = 5 mbps.
Capacity of link of malicious users to core router = 5 mbps.

Size of packets sent by genuine users = 1000 byte.
Size of packets sent by malicious users = 4000 bytes.
Rate of packets sent by genuine users = 1.0 mbps.
Rate of packets sent by malicious users = 2.5 mbps.

Number of genuine users and number of malicious users with attack intensity and proposed bandwidth to be assigned to malicious users are shown in table I.

Various topologies are used with different attack intensity with different number of genuine users and malicious

TABLE II
ATTACK FACTOR AND ATTACK TRAFFIC FOR DIFFERENT INTENSITIES OF ATTACK

Attack Intensity	Attack Factor in mbps	Total Traffic in mbps
50%	2.5	7.5
100%	5.0	10.0
150%	7.5	12.5
200%	10.0	15.0
300%	15.0	20.0
400%	20.0	25.0

users in the simulation. The different topologies used are shown in different figures.

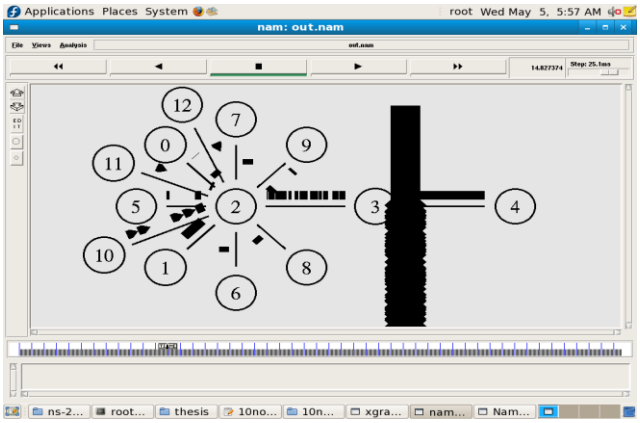

Figure 5: 10 node topology with 200% Attack Intensity

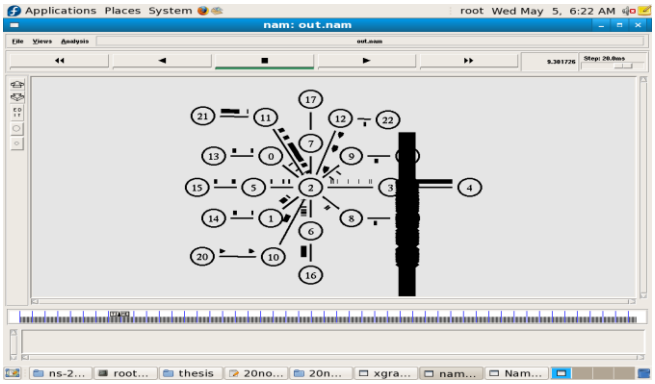

Figure 6: 20 Node topology with 500 % Attack Intensity

Figure 5 shows the 10 node topology which has been used in simulation to generate attack of 200% intensity.
Figure 6 shows the 20 node topology which has been used in simulation to generate attack of 500% intensity.

V. EXPERIMENTS, RESULTS AND DISCUSSION

A. *Experiment 1: Performanceanalysis and QoS analysis of traditional drop tail queue.*

Drop tail queue are in use widely in today's routers. So it becomes necessary to analyze its performance under normal condition and under different attack intensities.

Experiments are performed for the drop tail queue performance under different attack intensities.

Firstly implementation of drop tail queue on 3/5/10 node topology with no attack is done, it means on the link of core router and victim server of capacity of 5mbps packets are sent at the rate of less than or equal to 5 mbps and hence no packet lost and QoS is maximum as expected i.e. QoS =1.0

The attack is performed at different intensities like 50% /200% /500% attacks, and bandwidth utilization and packet loss with QoS are measured.
When the attack occurs, congestion increases, bandwidth degrades and QoS decreases. In the figure 7 it can be seen that degradation of bandwidth is occured. The Blue line is the bandwidth under normal condition while line in Red are bandwidth under attack. It can clearly be seen that bandwidth degradation from the graph.

In the figure 8 it can be seen that the QoS degrades after attack occur. In the normal condition with no attack, the QoS was 1.0 while when attack is performed with 50% intensity the QoS decrease to 0.94.

Further Drop Tail Queue is nalyzed with different attack intensities of 50% 200%/500%.

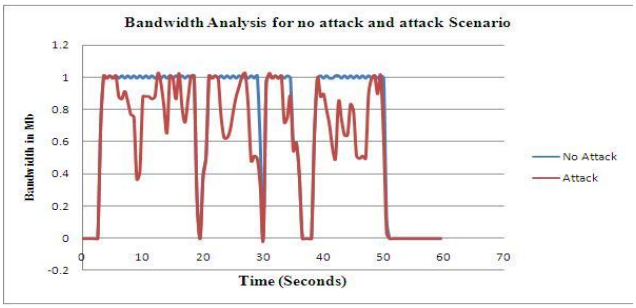

Figure 7. Bandwidth Analysis of Drop Tail Queue with Normal Condition and In Attack environment

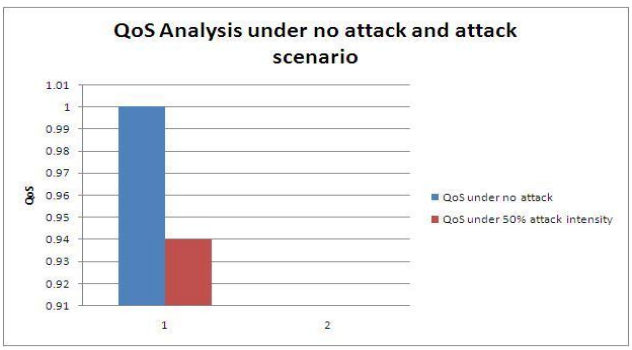

Figure 8: : QoS Analysis of Drop Tail Queue under 50% Attack Intensity

From the figure 9 performance of drop tail queuecan be seen. It has been observed that up to 50 to 75% of attack intensity, performance of drop tail queue is acceptable but beyond this limit QoS degrades too much and so drop tail queue fails if attack is performed by heavy intensity.

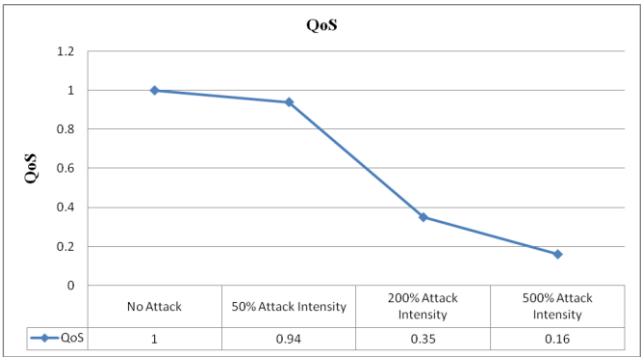

Figure 9: QoS analysis of Drop Tail queue under different attack intensity

CONCLUSION ABOUT DROPTAIL:
From the various attack intensities simulation, it is analyzed that implementation of simple Queue such as Drop Tail Queue on router is not the best practice when traffic is increased above the level of maximum limit. Droptail can tolerate attack up to 50% of Attack Intensity and if Attack further increases Drop Tail fails to maintain QoS. So, no guarantee of QoS. Further in drop tail queue QoS cannot be controlled.

B. Experiment 2: Performance analysis and QoS analysis of the proposed method of bandwidth assignment as per users group.

In the experiment 2, proposed methodology of assignment of bandwidth as per the users group is implemented. For example for genuine users full bandwidth is assigned but for malicious users only limited bandwidth is assign. For this experiment full bandwidth for genuine users is set but less bandwidth for malicious users and analyze its performance, bandwidth and QoS under different intensities of attack. Then comparison of bandwidth utilization and QoS of the proposed method with traditional drop tail queue.

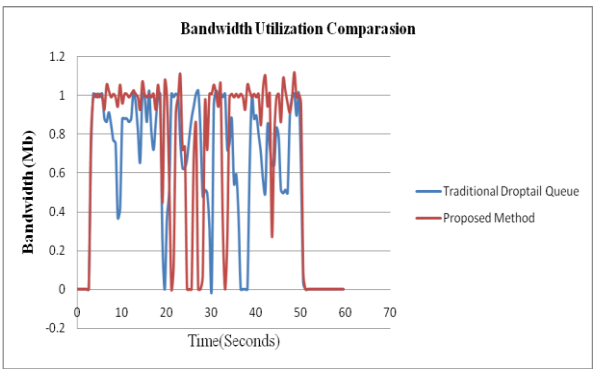

Figure 10. Bandwidth utilization comparisons between the proposed

In the figure 10, blue line shows the bandwidth utilization for traditional drop tail while red line shows the bandwidth utilization for the proposed methodology. Slightly improvement of bandwidth with the proposed method can be seen. Figure 11 and figure 12 shows the

slightly improvement of bandwidth for genuine users with the proposed bandwidth assignment method.

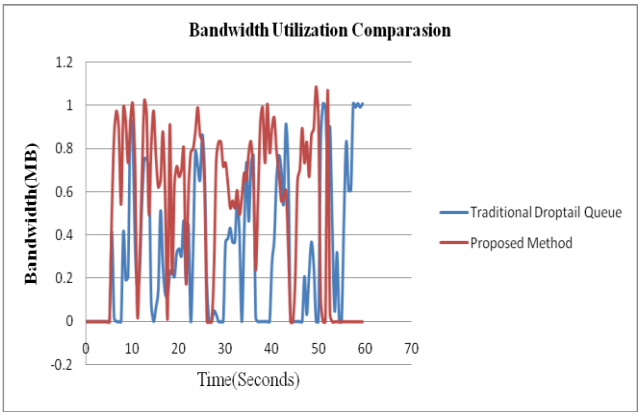

Figure 11. Bandwidth utilization comparisons between the proposed method and drop tail queue from node 2 to destination

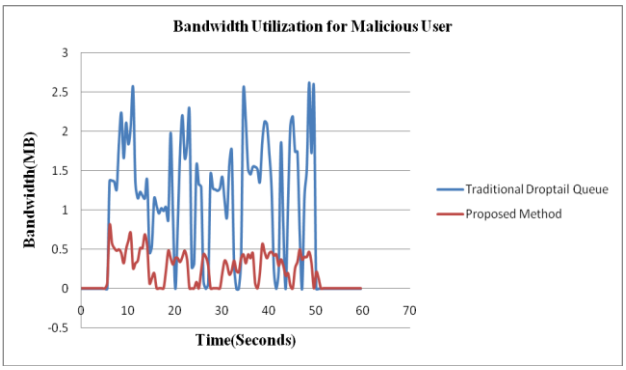

Figure 12. Bandwidth utilization comparisons between the proposed method and drop tail queue from node 1 (A Malicious User) to destination

If comparison of bandwidth assigned to malicious user is done, it can be seen that malicious users bandwidth is limited. From figure 12, it can be seen with drop tail queue that malicious users are enjoying full bandwidth utilization at which the rate attacker send packets but with the proposed method bandwidth is limited for malicious users. So he/she is no longer enjoying full bandwidth and does not degrades QoS of genuine users.

Now if the comparison of QoS of drop tail and the proposed method of bandwidth assignment is done then improvement of QoS can be seen.

In the figure 13, increment in overall performance can be seen with the proposed method. The QoS of users with the proposed method of bandwidth assignment is increased. If we assign bandwidth dynamically enhancement of QoS is guaranteed.

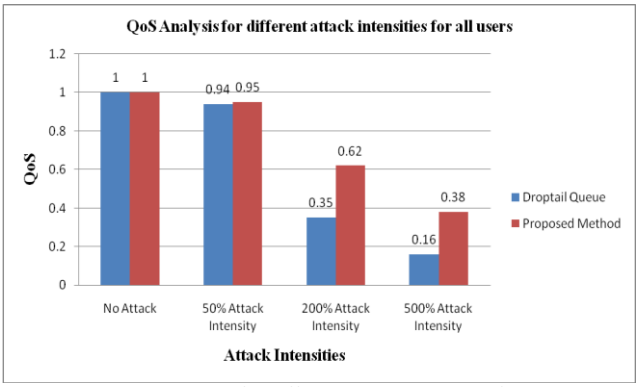

Figure 13. QoS analysis for different attack intensities for all users, genuine and malicious users

From figure 14 it can be seen that for genuine users QoS increases and from the proposed method the tolerance of attack for genuine users increase from 50% of drop tail to 200%.. But still beyond 200% attack intensity QoS of genuine users are not under acceptable limit.

Figure 15, shows the QoS for all users which includes malicious users and genuine users and comparison of QoS with drop tail queue.

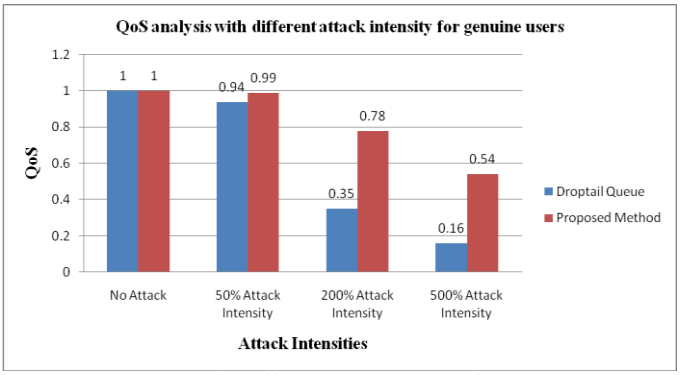

Figure 14. QoS analysis for different attack intensities for genuine users

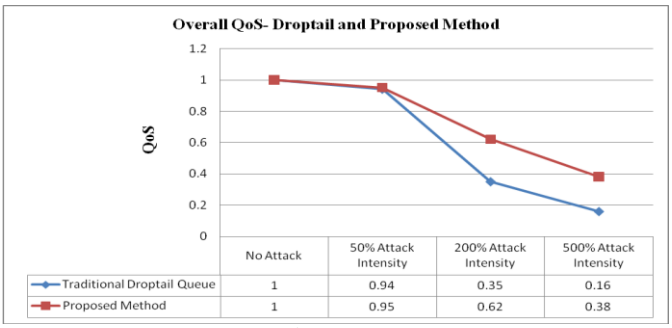

Figure 15. QoS Comparison of drop tail queue with the proposed method for all users

Figure 16, shows the QoS comparison for genuine user with the proposed method and traditional drop tail queue.

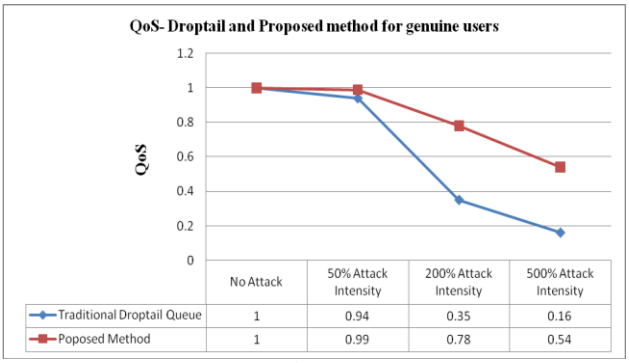

Figure 16. QoS Comparison of drop tail queue with the proposed method for genuine users

CONCLUSION OF EXPERIMENT 2:

Implementation of proposed method of dividing users into two groups- Genuine users and Malicious users and then assign Bandwidth to as per user group is performed. As per Bandwidth analysis and QoS analysis it is concluded that overall performance increased to some acceptable level while performance for Genuine users greatly enhanced. QoS is acceptable up to 200% Attack but beyond this it is not acceptable.

So further advancement of proposed method to keep QoS for genuine users acceptable is suggested. Enhanced Approach is that, Bandwidth should be assigned dynamically as per attack intensity.

C. *Experiment 3: Performance analysis and QoS analysis of the proposed method of Dynamic Bandwidth Assignment as per users group.*

If it is required to keep genuine user's QoS at constant acceptable level then the bandwidth assigned to genuine users and Malicious users should be dynamically assigned according to attack intensity. As the attack intensity increases Bandwidth must be adjusted to keep genuine users QoS at constant and acceptable level.Bandwidth of malicious users should decrease dynamically as the attack intensity increases.

So a new methodology of dynamic bandwidth assignment for malicious user as per bandwidth usage of genuine users is suggested.

Figure 17, shows the bandwidth analysis for traditional drop tail queue and dynamic bandwidth assignment methodology for user under 300% Attack.

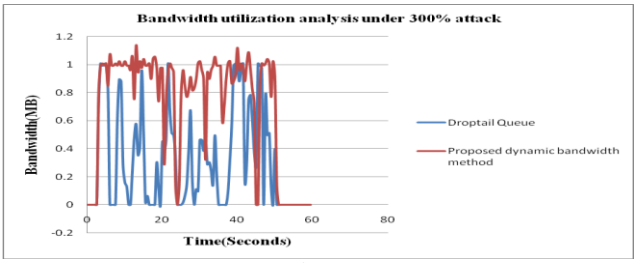

Figure 17 Bandwidth Analysis for Traditional drop tail queue and dynamic bandwidth assignment methodology for a genuine user under 300% Attack

Figure 18, shows the bandwidth utilization for a malicious user for dynamic Bbandwidth assignment.

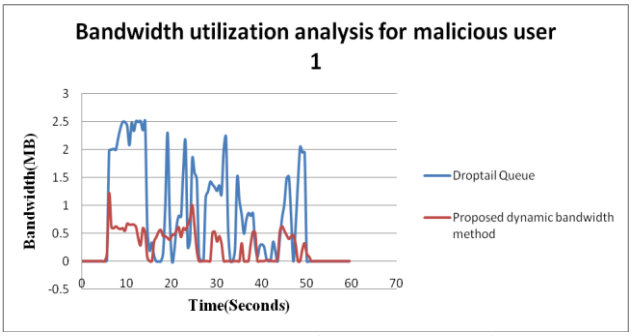

Figure 18 Bandwidth utilization for a malicious user for dynamic Bandwidth Assignment

From the figure 17, it can be said that bandwidth availability and bandwidth utilization of genuine users increases effectively from the proposed method of dynamic bandwidth assignment.

Figure 19, shows the QoS analysis for predefined bandwidth assignment method and dynamic bandwidth assignment method for all users and genuine users. From this figure it can be clearly said that for all users overall performance does not have effective change with dynamic bandwidth assignment but for genuine users i.e. group 1, QoS increases very effectively and genuine user will enjoy high level QoS irrespective of high congestion and heavily attack. So by using dynamic bandwidth assignment technique for genuine users and malicious users, a high level of QoS can be guaranteed for at least some set of users (say genuine users) under heavy attack or under heavy congestion due to suddenly popularization of victim server.

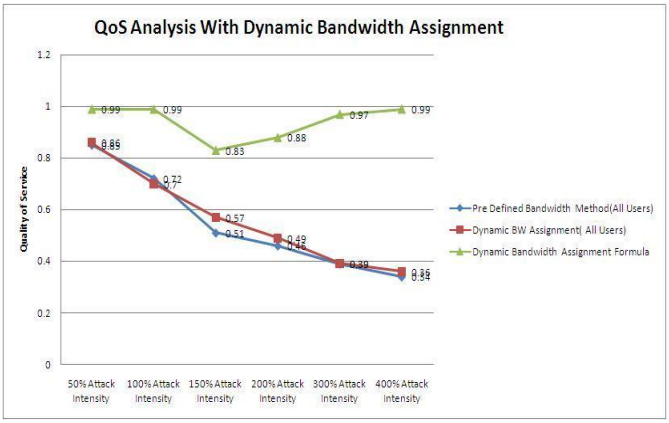

Figure 19 QoS analysis for predefined bandwidth assignment method and dynamic bandwidth assignment method for all users and genuine users

D. *Dynamic Bandwidth assignment Formula:*

Based on the experiment 1, 2 and 3 a new formula for dynamically bandwidth assignment is derived for malicious user as per increase of attack intensity in order to achieve controlled and guaranteed QoS for genuine users.

This formula is named as Dynamic Bandwidth Assignment (DBA) Formula. This formula is based on number of users i.e. number of genuine users, number of malicious users, total number and average rate at which genuine users are sending packets to the server.
From this formula calculation is performed for bandwidth of malicious users to be assigned according to number of malicious user, number of genuine users and bandwidth of genuine users.

Calculation of number of genuine users and malicious users can be performed by using two methods. One method is from user session. Every user has its own session when users want to use some server's service. So from server can calculate total number of users. Further genuine users and malicious users can be differentiate by using this approach.

Second method is to count source IP addresses from headers of packets. Every packets sent by some user whether packet is TCP, IP or UDP packet. Each have source and destination address header, so calculation of number of users can be performed. The derived formula is as below:
BMU = Bandwidth assigned to Malicious users
NGU = Numbers of Genuine Users
Total Users = Total Genuine users + Total Malicious Users
BGU = Average B/W at which Genuine users sent packets. Then

BMU = (NGU/Total Users)*BGU

E. QoS Controlling Factor:

From experiment 3 by using dynamic bandwidth assignment a new fact is discovered, that for genuine users when attack intensity increase, QoS decrease usually but at a point, when attacker further increase the attack, instead of decreasing QoS, the QoS of genuine users start increasing while QoS of total users(genuine plus Malicious) decreases as attack increases as expected.
In figure 19 it is analyzed that, from 50% attack to 200% attack QoS for genuine users decreases up to a point but if attacker further increase its attack to beyond 200% it can be seen that the QoS of genuine users start increasing instead of further decreasing.

The reason behind this is very interesting. From experiment 3 it is analyze that:
Suppose total traffic of genuine users at any time t is GT
And total traffic of malicious users at any time t is MT
Then while at any time t MT<GT
Then QoS of genuine users keeps decreasing until MT become equals to GT.

Further when MT over cross GT i.e. when MT>GT then at that time QoS of genuine users start increasing.

So from this fact controlling factor of QoS of genuine user can be derived. From this controlling factor the number of genuine user and malicious user can be adjusted and QoS for genuine users can be controlled. This technique can be very useful under situations which arise due to suddenly increase of user requests to the server like declaration of result or sudden popularity of a website.

VI. CONCLUSION AND FUTURE SCOPE

Three experiments are performed. First experiment shows the performance analysis of drop tail queue which is widely used in routers. Conclusion of first experiment is that implementation of simple Queue such as Drop Tail Queue on router is not best practice when traffic is increased above the level of maximum limit. There is no guarantee of QoS. In the second experiment proposed approach of dividing users in to two groups of genuine users and malicious users and then assign high bandwidth to genuine users and low bandwidth to malicious users is performed. Performance analysis shows that this approach gives better result than traditional drop tail queue but in the absence of effectively and logically assignment of bandwidth guaranteed QoS is only up to some particular attack intensity. The results shows that this approach can give good QoS up to 200% attack intensity. And hence no guarantee of QoS beyond this limit. In the third experiment a formula for dynamic bandwidth assignment is derived. This formula assigns bandwidth to malicious user according to attacker traffic. This formula is named as Dynamic Bandwidth Assignment Formula. Performance analysis shows that from this formula QoS of genuine users can be controlled and This formula gives guaranteed QoS for genuine user under heavy attacks.

There should be up gradation on Routers BIOS/Application level so that routers can sense attack traffic intensity level and then decide whether drop tail queue should be used (If attack intensity is less than 50%) or should invoke the proposed method with dynamic Bandwidth Assignment Formula.
In future there should be implementation and testing of Dynamic Bandwidth Assignment Formula in routers with actual networks. This dynamic bandwidth assignment method may be further enhanced based on type of traffic under normal and malicious behavior.

REFERENCES

[1] Yuval, Fledel. Uri, Kanonov. Yuval, Elovici. Shlomi, Dolev. Chanan,. "Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy (IEEE) (in press). doi:10.1109/MSP.2010.2. ISSN 1540-7993.
[2] Paul J. Criscuolo. "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319". Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-

ID-136939, Rev. 1., Lawrence Livermore National Laboratory.
[3] Boyle Phillip "Distributed Denial of Services" http://www.sans.org/y2k/DDoS.htm.
[4] Barros C. "ICMP Trace back message" http://research.att.com/~smb/talks.
[5] Senie Ferguson, D. "Denial of Services tools" http://www.cert.org/advisories/ca-98-13-tcp-denial-of-service.html.
[6] Mirkovic Jelena, Hussain lefiya, Reiher Peter, " Accurately Measuring Denial of Service in Simulation and Testbed Experiments", IEEE Transactions on Dependable and Secure Computing, Vol 2 No.2, April-June 2009. Pg. No. 81-95.
[7] Li Ming, Li Jung, zhao Wei," Simulation Study of Flood Attacking of DDoS", International Conference on Internet Computing in Science and Engineering, IEEE 2008. Pg no. 286-293.
[8] Khazan Golriz, Azgomi M.A., " A Distributed Attack Simulation for Quantitative Security Evaluation using SimEvents", IEEE 2009 Iran university of Science and technology,Tehran.
[9] Harada Shigeaki, Kawahara Ryoichi, " A Method of Detecting Network Anomalies In Cyclic Traffic", IEEE GLOBCOM 2008.
[10] Takemori Keisuke, Nishigaki Masakatsu, " Detection of Bot Infected PCs Using Destination based IP and Domain Whitelists during a Non-Operating Term", IEEE GLOBCOM -2008.
[11] Goldstein Markus, Reif Matthias, Stahl armin, Breuel Thomas," Server Side Protection of Source IP Address using Density Estimation", International Conference on Availability, Reliability And Security. IEEE 2009.
[12] Tupakula U.K., Varadharajan Vijay, Vuppala S.K., " SBAC : Service Based Access Control", 14th IEEE International Conference on Engineering of Complex Computer Systems, IEEE 2009.
[13] Swain B.R., Sahoo B.S., " Mitigating DDos attack and Savin Computational Time using s Probabilistic approach and HCF method", Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Orissa.2009 IEEE International Advance Computing Conference(IACC 2009).
[14] Wang H., Jin C., Shin K.G., " Defence Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM Transactions On Networking, Vol 15, No. 1, February 2007.
[15] N. Venkatesu, Chakravarthy Deepan, " An Effective Defence Against Distributed Denial of Service in Grid", International Conference on Emerging Trends in Engineering and Technology, IEEE2008.
[16] Stefanidis K., Serpanos D.N., " Implementing Filtering and Traceback Mechanism for Packet – Marking IP- Trace back Schemes against DDoS Attacks", 2008 International Conference " Intelligent Systems".
[17] Kumar Sanjeev, " Smurf Based Distributed Denial of Service Attack Amplification in Internet", Second International Conference on Internet Monitoring and Protection (ICIMP 2007) IEEE 2007.
[18] He Li, Tang Binhua, " Available Bandwidth Estimation and its Application in Detection of DDoS Attacks", ICCS 2008.
[19]] Paruchuri Varnsi, Durresi Arjan, Chellppan Sriram, " TTL Based Packet Marking for IP Traceback", IEEE GLOBCOM 2008.
[20] Clark C. "Insertion, evasion and denial of service : eluding network detection" http://clark.net/~roesch/idspaper.html.
[21] Evans John, Filsfils, Clarence, "Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice" Morgan Kaufmann, 2007.
[22] Campos F.H., Jeffay Kevin, Smith F.D., " Tracking the Evolution of Web Traffic: 1995-2003", IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systeem(MASCOTS), Orlando FL, October 2003, Page 16-25.
[23] Wang Shen, Guo Rui, " GA- Based Filtering Algorithm to Defend against DDoS Attack in High Speed Network", International Conference on Natural Computation IEEE 2008.
[24] B. B. Gupta, R. C. Joshi, and Manoj Misra, "Prediction of Number of Zombies in a DDoS Attack using Polynomial Regression Model", Journal of advances in information technology, Vol 2, No. 1, FEBRUARY 2011, pp 57-62.
[25] N. Bhalaji, Dr. A. Shanmugam, "Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET", Journal of advances in information technology, Vol 2, No. 2, MAY 2011, pp 92-98
[26] Eddaoui Ahmed, Mezrioui Abdellatif, " Defeat the Network Attack by Using Active Network Approach", IEEE 2006.
[27] Gao Zhiqiang, Ansari Nirwan," Differentiating Malicious DDoS Attack Traffic from Normal TCL Flows by Proactive Tests", IEEE Communication Letters, Vol 20 No. 11, November 2006.
[28] Paruchuri Vamsi, Durresi Arjan, Barolli Leonard, " FAST : Fast Autonomous System Traceback", International Conference on Advanced Networking and Applications(AINA 2007).
[29] Shevtekar Amey, Ansari Nirwan, " Is It Congestion or a DDoS Attack" IEEE Communication Letters, Vol. 13, No. 7 , JULY 2009.
[30] Hasan Muhhamad, Nadeem Kamran, Khan Shoab, " Optimal Placement of Detection Nodes against Distributed Denial of Service Attack", International Conference on Advanced Computer Control, IEEE 2008.
[31] Li Ming, Li Jung, zhao Wei," Simulation Study of Flood Attacking of DDoS", International Conference on Internet Computing in Science and Engineering, IEEE 2008. Pg no. 286-293.
[32] Liu Chung-Hsin, Lo Chun-Lin," The Simulation for VOIP DDoS attack", International Conference on MultiMedia and Information Technology, IEEE 2008. Pg. No. 280-283.
[33] Fu Zhang, Tsigas Philippas," Mitigating Distributed Denial of Service Attacks in Multyparty Applications in

the presence of Clock Drifts", Symposium on Reliable Distributed Systems, IEEE 2008. Pg no. 63-72.

Raman Singh born in Yamuna Nagar on April 12, 1984. He completed his B.Tech(CSE) from Haryana Engineering College, Jagadhri. After his degree he joined Karman Infotech Pvt. Ltd. As a Technology Specialist. His work was to deploy Microsoft's Latest technologies like Directory services, Firewall, Email Server, Backup server etc. Currently he is pursuing Ph.D in CSE and completed Master of Engineering(M.E.) in IT from Panjab University Chandigarh. His area on interest includes Computer Networks and Network Security.

Amandeep Verma born on November 22, 1981, received her B. Tech. (Computer Science & Engineering) from Punjab Technical University, Jalandhar , Punajb ,in the year 2002. She obtained her M. Tech. (Computer Science and Engineering) from Punjabi University ,Patiala,Punjab in 2004 with specialization "Multistage Interconnection Networks".

Presently, she is working as Assistant Professor in the Department of Information Technology, U.I.E.T, Panjab University, Chandigarh. Her fields of interest lie in Information Security, and Distributed Systems.