An Approach to Increase Bandwidth Utilization under Suspected Flood Attack

Raman Singh
University Institute of Engineering and Technology
Panjab University
Chandigarh

Harish Kumar
University Institute of Engineering and Technology
Panjab University
Chandigarh

R.K. Singla
DCSA,
Panjab University
Chandigarh

ABSTRACT
Bandwidth is very crucial and limited resource available, so it should be properly utilized. Network congestion occurs when a link or node is carrying large amount of data in case of flood attack and quality of service deteriorates. Effects of flood attack include queuing delay, packet loss or the blocking of new connections. As a consequence incremental increases in offered load leads to either small increase in network throughput, or to an actual reduction in network throughput. Modern networks use congestion control and avoidance techniques to avoid such congestion collapses. One of widely used queuing algorithm is Drop Tail which is used in most of the routers to avoid congestion and to encourage smooth flow of packets. In this paper we propose a technique to better utilize bandwidth under flood attack. Simulations of the proposed technique have been carried out to compare it with the DropTail. Ns-2 is used as the simulation tool. In this simulation experiment, different types of traffic like tcp, udp are considered. Routers are attacked with different attack intensities to determine the effect of proposed method under various circumstances.

General Terms
Bandwidth Management

Keywords
Network Congestion, Bandwidth Management, Drop Tail Queue, Queuing Algorithms.

1. INTRODUCTION
Bandwidth management is the process of measuring and controlling the communication parameters like traffic, number of packets etc. on a network link, to avoid network congestion and poor performance [1]. Drop-Tail is a simple queue management algorithm used by Internet routers to decide about dropping packets during trouble time. In contrast to other algorithms like Random Early Detection (RED) and Weighted Random Early Detection (WRED), in Tail Drop all the traffic is not differentiated. Each packet is treated identically. With tail drop, when the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept incoming traffic. Once a queue has been filled, the router begins discarding all additional datagrams, thus dropping the tail of the sequence of datagrams.

This paper is organized into six sections. Section-2 discusses the suspected flood attack and bandwidth management. Section-3 explains about the proposed bandwidth management method under suspected flood attack. Section-4 describes about the simulation setup and parameters used. In section-5, results have been presented and explained. Finally, section-6 sets the conclusion and future work.

2. SUSPECTED FLOOD ATTACK AND BANDWIDTH MANAGEMENT
Flood attack is the denial of service (DoS) attack in which large amount of traffic from distributed agents/bots are flooded to the victim server in order to bring down the network services of that server. The flooded traffic can be of any types like TCP/IP, UDP, ICMP, ECHO traffic etc. The DoS attack floods the target system by sending bogus requests, and the target system become unable to provide normal services [2].

Suspected flood attack is a type of attacks in which there is no surety that whether the attack is intentional or un-intentional. An example of un-intentional flood attack is sudden popularity of a website like if some result is declared and millions of candidates login to see details. Another can be very interesting news published and everyone wants to read that news. Sometime it happens that some event/tragedy occurs in anywhere in world and Internet users all over the world start to search for that event/tragedy. These types of traffic surges are un-intentional. Due to the growth in Internet traffic and variety of applications, it is difficult to characterize the traffic patterns on an IP network in advance. Network traffic can be classified by using some parameters like port, payload classification and classification based on statistical traffic properties [3]. The anomalies which are produced by some worms or DoS attack can be detected or classified by traffic classification [4]. A technique which is based on self-similarity to detect low rate ICMP based Distributed Denial of Service (DDoS) attack is suggested in [5].

In [6] a model is proposed which is capable of collecting data for detecting malicious packets then examining protocol features to detect and validate attack. This model is designed specifically for detection of attacks on ICMP protocol. A database of encapsulated headers of packets is maintained and then rule applies on this to detect possible attacks. In order to save the company's servers, routers or network link from exhaustion of bandwidth an approach which is based on Hidden Markov Model (HMM) is proposed to maintain the dynamics of Access Matrix (AM). This approach has higher attack detection rate with lower false positive rate [7]. An approach by combining pattern based and anomaly based detection is suggested. It has good detection rate and low false alarm rate. It also simplifies feature selection which plays major role in anomaly detection.

Pattern language for modeling state machine is also proposed to deal with higher layer or lower layer protocols issues in anomaly detection [8]. Researchers have suggested many techniques to classify malicious behavior from genuine behavior. Review of soft computing in order to detect or classify malicious activities is provided in [9].

In order to trace back DDoS attack, entropy variation based trace back mechanism is suggested in [10]. This is different from packet marking schemes. This method use features which cannot be altered by hackers. This method utilizes less memory as well as scalable, robust, and doesn't have effects on changing patterns of traffic. A real time attack detection technique is presented which is based on per-IP traffic behavioral analysis. It can be deployed on leaf node in order to detect attack in real time. It has low computation overhead and is capable in self-immunization. Sending and receiving packet is inspected for synchronization TCP and UDP behavior to know whether it is synchronized or not. Then CUSUM algorithm is applied to detect SYN attack [11]. An approach is also suggested to prevent whole network from attacker by installing a puppet computer and allow hacker to attack that puppet computer [12]. In [13] a method is proposed to detect TCP SYN flood attack. If the behavior of attack is known, by analyzing every packet of TCP/IP header, TCP-SYN flood attack can be easily detected. The parameters like CPU utilization time and file download rate is also taken into consideration to detect TCP-SYN attack. A detection of DoS/DDoS attack on entropy-based input-output traffic mode detection is proposed. Packet size and packet content entropy-based technique is used in [14]. In [15] parameters are suggested to distinguish between DoS attack and similar looking Flash Events (FE) generated by genuine users. The various parameters which can be used to distinguish DoS attack and FEs are Change in Rate of Incoming Traffic, Change in Rate of New Source IP Addresses, and Distribution of Requests among Source IP Addresses. FOSEL (filtering with the help of an overlay security layer) is proposed to protect network-based control systems (NBCS) from DDoS attack. It is a defense technique which drops excessive packets effectively and reduces the overhead at victim. It is constructed using a combination of access point proxies, packet authentications, secret green nodes, routing via onion tunnels, rate limiter routers and a selective filter [16]. The demand for networks that provide guaranteed level of Quality of Service (QoS) is increasing consistently. For the cost effective construction and operation of such networks, we need traffic engineering methods that efficiently utilize the bandwidth of links while satisfying bandwidth requirements [17]. Bandwidth management mechanisms can be used to enhance performance. Following are some of categories for bandwidth management:

2.1 Traffic Shaping / Rate Limiting [1]:

The traffic shaping is the control of computer network traffic in order to optimize or guarantee performance, increase latency, and/or increase usable bandwidth by delaying packets that meet certain criteria [18]. It is also known as Internet Traffic Management Practices (ITMP). It is any action on a set of packets which imposes additional delay on those packets such that they conform to some predetermined constraint like traffic profile [19]. It provides a means to control the volume of traffic being sent into a network in a specified period (bandwidth

throttling), or the maximum rate of sending the traffic (rate limiting) etc.

There are many ways to accomplish traffic shaping, but most of the times delaying packets is the mechanism used for this purpose. Traffic shaping is commonly applied at the network edges to control traffic entering into a network, but can also be applied by the traffic source (for example, computer or network card or by an element in the network. Traffic policing is the distinct but related practice of packet dropping and packet marking [20]. Some of the uses of traffic shaping are:

- Applied by traffic sources to ensure that the traffic sent should comply with a contract enforced in the network by a police.
- It is widely used for network traffic engineering, and appears in domestic ISPs' networks.

2.2 Scheduling Algorithms [1]:

A scheduling algorithm is the method by which threads, processes or data flows are given access to system resources like processor time, communications bandwidth etc.. This is usually done to load balance a system effectively or achieve a target quality of service. The need for a scheduling algorithm arises from the system requirements to perform multitasking and multiplexing. Some of algorithms are: Weighted fair queuing (WFQ), Class based weighted fair queuing, Weighted round robin (WRR), Deficit weighted round robin (DWRR), Hierarchical Fair Service Curve (HFSC).

2.3 Congestion Avoidance [1]:

It is the technique to regulate the traffic by rate limiting the senders. Some of the methods are:

- RED/WRED - Lessens the possibility of port queue buffer tail-drops and this lowers the likelihood of TCP global synchronization
- Policing (marking/dropping the packet in excess of the committed traffic rate and burst size)
- Explicit congestion notification
- Buffer tuning

2.4 Bandwidth Reservation Algorithms [1]:

Resource reservation protocol (RSVP), Constraint-based Routing Label Distribution Protocol (CR-LDP), Top-nodes algorithms are some of the examples of bandwidth reservation protocols.

3. BANDWIDTH UTILIZATION APPROACH UNDER SUSPECTED FLOOD ATTACK

Proposed method for bandwidth utilization depends on bandwidth management of victim server. If attacker uses its genuine IP address then we can guarantee availability of service by Traffic Isolation. There is a lot of research occurred for intentional flood attack like black listing of attacker's IP, but in case of unintentional suspected flood attack we cannot perform those method which are used for intentional flood attack. Blacklisting the IP addresses is not better method due to the reason that these systems may not be the attackers. The basic idea is to divide traffic into two groups: One is genuine users

and other group is suspected malicious users. QoS of Genuine user group can be controlled and guarantee of QoS to this group may be granted. Also priority users can be added into genuine users groups. A division of users into these groups is possible on the basis of many factors depending on type of service offered by server, number of users etc. Two factors have been considered in this experiment: Size of packets and rate at which packets are sent. For genuine users assign at least 80% of available bandwidth, while if the users seems to be suspected malicious, assign this group the bandwidth of not more than 20 %. In this way the attacker still get some

responses from victim server and will thought the attack is successful and will not further increase attack intensity while groups of genuine users still enjoys acceptable QoS.

According to [21] about 59% of the packet sizes are 1000 bytes or less on the Internet. It means that average packets sent by genuine users are 1000 bytes or below. So a threshold of packets size 1000 bytes and rate of packets 1 Mbps have been considered to decide the group of users. 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 suspected malicious users group. The proposed approach is:

Step 1: At the core router scan for each user the size of packets 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 suspected malicious users groups depending on rate of packets and size of packets.

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

For the suspected malicious users group assign bandwidth as not more than 20% of bandwidth assigned to genuine users.

4. SIMULATION SETUP

Large numbers of simulators are available for simulating various network conditions. Ns-2 [22] is widely used and open source simulator for this purpose. For these simulations ns-2 has been used as the simulator.

4.1 Simulation Parameters

Different topologies with 3, 10 and 20 nodes with varying attack intensity like 50%/ 100% / 150% / 200% / 300% / 400% are used. For all topologies the link capacity are taken as below:

- Between core router to Victim server as well as between genuine users to core router is 5 Mbps.
- Between suspected malicious users to core router is 5 Mbps.

Drop Tail queue size for all nodes are 10. Packet Delay Time between nodes is 10 milli-second. Size of packets sent by genuine users is 1000 byte. Size of packets sent by suspected

malicious users is 4000 bytes. Rate of packets sent by genuine users is 1.0 Mbps and that of by suspected malicious users is 2.5 Mbps. Number of genuine users and suspected malicious users with attack intensity and proposed bandwidth to be assigned to malicious users are shown in table 1. 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.

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 2.

Table 1 Dynamic Bandwidth Assignment of suspected malicious user on the basis of number of genuine users.

Attack Inten-sity	Total No. of Nodes	Suspected Malicious Nodes	Genu-ine Nodes	Limited Bandwidth Assigned to Malicious (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

Table 2: 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
500%	25.0	30.0

5. RESULT AND DISCUSSION

This section discusses the results of experiment in which the proposed methodology of assignment of bandwidth on user's group basis has been implemented. For genuine user's full bandwidth is assigned but for suspected malicious users only limited bandwidth is assign. It is found that Quality of Service (QoS) improves using the proposed method as compare to drop-tail method. Figure 2 shows the QoS for all users including suspected malicious and genuine along with comparison of QoS with drop tail queue. Figure 3 shows the QoS comparison for genuine user of proposed method with traditional drop tail queue As per Bandwidth analysis and QoS analysis it can be concluded that overall performance increased to acceptable level while performance for genuine users greatly enhanced. QoS is Acceptable up to 200% Attack but beyond this it is not acceptable.

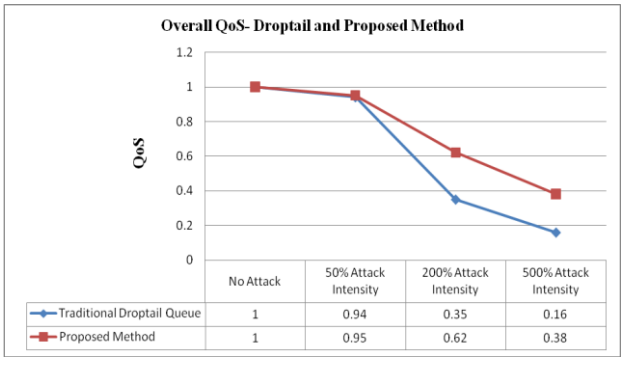

Fig 2 : QoS Comparison of drop tail queue with our proposed method for all users

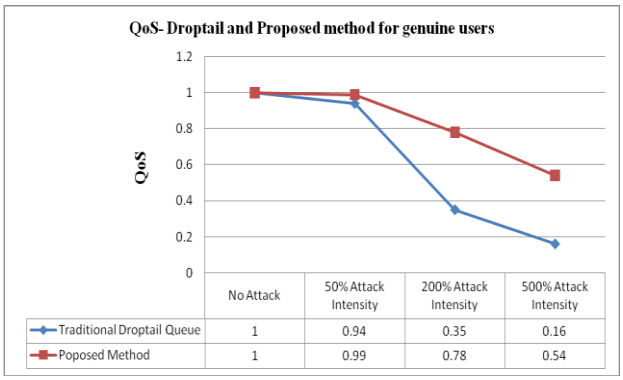

Fig 3 : QoS Comparison of drop tail queue with our proposed method for genuine users

6. CONCLUSION AND FUTURE SCOPE

Drop tail queue is widely used in routers in the Internet. The implementation of simple Queue such as Drop Tail Queue on router is not best practice when traffic is more than the maximum capacity of a link. QoS is minimal in such cases.

In this paper a method is proposed by dividing the users into two groups: Genuine and suspected malicious users. A high bandwidth is assigned to genuine users and low bandwidth to suspected malicious users. Performance analysis shows that this approach gives better result than traditional drop tail queue up to some particular attack intensity. Results show that this approach can give good QoS up to 200% attack intensity.

Further research can be carried out to assign bandwidth dynamically to the genuine users as per their requirements while assigning lower bandwidth to the user who seems malicious

The dynamic assignment of bandwidth may help to mitigate attack having intensity beyond 200%.

7. REFERENCES

[1] John Evans and Clarence Filsfils, "Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice", Morgan Kaufmann Publishers, 2007, ISBN 0-12-370549-5

[2] Won Kim , Ok-RanJeong, Chulyun Kim and Jungmin So, "The dark side of the Internet : Attacks, costs and responses", Journal of Information Systems, Vol. 36, No 3, May 2011, pp 675-705

[3] Thuy T.T. Nguyen and Grenville Armitage, "A Survey of Techniques for Internet Traffic Classification using Machine Learning", IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, 4th Quarter 2008, pp 56-76

[4] Arthur Callado, Carlos Kamienski, Géza Szabó, Balázs Péter Ger˝o, Judith Kelner, Stênio Fernandes and Djamel Sadok, "A Survey on Internet Traffic Identification", IEEE Communications Surveys & Tutorials, Vol. 11, No. 3, 3rd Quarter 2009, pp 37-52

[5] Zhang Sheng, Zhang Qifei, Pan Xuezeng and Zhu Xuhui, "Detection of Low-rate DDoS Attack Based on Self-Similarity", 2nd International Workshop on Education Technology and Computer Science (ETCS), March 6-7, 2010, Wuhan, China, pp 333–336

[6] Atul Kant Kaushik and R. C. Joshi, "Network Forensic System for ICMP Attacks", International Journal of Computer Applications, Vol. 2, No.3, May 2010, pp 14-21

[7] S. Prabha and R. Anitha, "Mitigation of Application Traffic DDoS Attacks with Trust and AM Based HMM Models", International Journal of Computer Applications, Vol 6, No. 9, September 2010, pp 26-34

[8] P. Rajapandian and K. Alagarsamy, "Intrusion Detection in Dos Attacks", International Journal of Computer Applications, Vol. 15, No. 8, February 2011, pp 33- 37

[9] Raman Singh, Harish Kumar and R.K. Singla, "Review of Soft Computing in Malware Detection", International Journal of Computer Applications, Special Issue on IP Multimedia Communications, October 2011, pp 55-60

[10] Shui Yu,Wanlei Zhou, Robin Doss and Weijia Jia, "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 3, March 2011, pp 412-425

[11] YiZhang and QiangLiu, "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), July 9-11, 2010, Chengdu, China, pp 163-167

[12] Xueping Chen, "Distributed Denial of Service Attack and Defense", International Conference on Educational and Information Technology (ICEIT), Sept. 17-19, 2010, Chongqing, China, Vol. 3, pp 318-320

[13] S.H.C. Haris, R.B. Ahmad and M.A.H.A. Ghani, "Detecting TCP SYN Flood Attack based on Anomaly Detection", 2nd International Conference on Network Applications Protocols and Services (NETAPPS), September 22-23, 2010, Alor Setar, Kedah, Malaysia, pp 240-244

[14] S. Tritilanunt, S. Sivakorn, C. Juengjincharoen and A. Siripornpisan, "Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks", International Symposium on Communications and Information Technologies (ISCIT), October 26-29¸ 2010, Tokyo, Japan, pp 804-809

[15] S. Bhatia, G. Mohay, A. Tickle and E. Ahmed, "Parametric Differences Between a Real-world Distributed Denial-of-Service Attack and a Flash Event", 6th International Conference on Availability, Reliability and Security, August 22-26, 2011, Vienna, Austria, pp 210-217

[16] Hakem Beitollahi and Geert Deconinck, "A dependable architecture to mitigate distributed denial of service attacks on network-based control systems", International Journal of Critical Infrastructure Protection, Vol. 4, No. 3-4, December 2011, pp 107-123

[17] Ryiochi Kawahara and Keiuski Ishibashi, "A method of bandwidth dimensioning and management for aggregated TCP flows with heterogeneous access links." 11th International Symposium on Telecommunications Network Strategy and Planning, Vienna, Austria, June 13-16, 2004, pp 15-20

[18] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss, "An Architecture for Differentiated Services", IETF RFC 2475, 1998, pp 17

[19] Eckberg, A.E., "B-ISDN/ATM traffic and congestion control", IEEE Journal of Network, Vol. 6, No. 5, 1992, pp 28-37

[20] Fraser K. and Pratt I., "Arsenic: a user-accessible gigabit Ethernet interface", Proceedings of 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), April 22-26, 2001, Anchorage, USA, Vol. 1, pp 67-76

[21] Campos F.H., Jeffay Kevin and Smith F.D., "Tracking the Evolution of Web Traffic: 1995-2003", 11th IEEE/ACM International Symposium on Modeling

[22] Analysis, and Simulation of Computer and Telecommunication System (MASCOTS), Orlando FL, October 12-15, 2003, pp 16-25

[23] The Network Simulator Website [Online] http://www.isi.edu/nsnam/ns/ns-documentation.html Last seen on October 30, 2011