Comparative Analysis of various Active Queue Management Algorithms under Flooding based LDDoS Attack

Bhavya Jain
Department of Computer Science
Punjab Technical University, Punjab, India

Sanjay Madan
Cyber Security Technology Division,
Center for Development of Advanced Technology, Mohali, India

Abstract- Because of the growing popularity of Internet and the use of Internet is increasing in the organizations, the threat of different types of Denial of Service (DoS) attacks is increasing as well. As different types of DoS attacks are increasing, it is slightly difficult to mitigate these types of DoS attacks. So, instead of mitigating the DoS attacks, congestion controlling techniques are used with the help of different Active Queue Management (AQM) techniques. Here, we introduce the congestion handling techniques at the edge routers using Active Queue Management (AQM). The purpose of AQM techniques is to provide required bandwidth and identify attack flows so that mitigation steps can be explicitly taken against them to further mitigate the DoS attacks. LDDoS attacks are a type of DoS attack that is more vulnerable to the network traffic than the DDoS attacks as they are difficult to identify. Here, we use different queuing algorithms using network simulator (ns-2) to implement the network and diagnose the behavior of queuing algorithms. Performance metrics for the comparison are Packet Delivery Ratio (PDR), end-to-end delay, routing overhead and number of packets dropped.

Keywords – PI Controller, GK, DRR, LDDOS, NS2

I. INTRODUCTION

It has been widely noticed that Denial of Service (DoS) as well as Distributed Denial of Service (DDoS) is one of the prominent attack mechanisms on the Internet. In general, DoS attacks can be classified into two categories depending on the layer of the OSI model they target i.e. infrastructure-based attacks and application-based attacks. The former targets the layer 3 and 4 (i.e. network and transport layers) and the latter targets the application layer. Infrastructure-based attacks include SYN floods, UDP floods, ICMP floods and IGMP floods, while application-based attacks include HTTP/SSL GET and POST floods and NTP floods.
Congestion based attacks still dominate the denial of service attacks. Different academic institutions have performed significant amount of work towards understanding and mitigating network congestion based DoS attacks. In this paper, Active Queue Management (AQM) techniques are used for congestion control. Further, comparison of different AQM algorithm is done to find which algorithm is more suitable than other on basis of different parameters.

1.1 DoS Attack –

Many problems have been resolved in the field of network security using different tools and techniques. A DoS attack is a malicious attempt which makes users unavailable to use intended services they want to use. DoS attack make a server or a network resource unavailable for their users by suspending the services of a host connected to the Internet. However, DoS attack is still a problem in this field as different type of DoS takes place now a day like DDoS, LDDoS. DoS attacks cannot provide too much harm but only makes user unavailable from using the intended services.

1.2 DDoS Attack –

A Distributed Denial of Service (DDoS) attack is largescale, coordinated attack on the availability of services of a victim system or network resources launched indirectly through many compromised computers on the Internet. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more difficult to track down the original attacker connections with legitimate (non-malicious) clients.

1.3 LDDoS Attack –

Traditional flooding-based DDoS attacks employ a "sledge-hammer" approach of high-rate transmission of packets, which obviously distinguishes themselves from normal data flows in statistical characteristics. Many of the proposed approaches for detecting DDoS attacks have been based on these statistical characteristics.

LDDoS attacks are quite different from the traditional flooding-based DDoS attacks as they exploit the vulnerabilities in TCP's congestion control mechanism. Instead of sending continuous network traffic, an LDDoS attacker sends periodically pulsing data flows, which may dramatically reduce the average rate of attack flows. LDDoS attacks have already been observed in the Internet2 Abilene backbone, thus presenting a new challenge to the security of the Internet.

II. LITERATURE SURVEY

There are lot more research is going on in this direction and work done by various authors which is related to our work is studied and related information is given as under:

Minjuan Cheng, Xiaoming Ma,[1] focuses on RED and proposes a Real-time Dynamic RED (RDRED) algorithm, which modifies the static probability function to an adaptive nonlinear function, and uses instantaneous queue length as the congestion indicator instead of average queue size. Then the paper compares the proposed RDRED scheme with RED and its different variants, such as Adaptive RED (ARED), Nonlinear RED (NLRED), Dynamic RED (DRED) and Improved RED (IRED). The performance evaluation is done by using the Network-Simulator-2, which provides a convenient and reliable platform for simulating large-scale networks. It is demonstrated that the RDRED algorithm achieves the best performance among all the tested AQM algorithms. It can stabilize the queue length very well while keeping the queuing jitter very small. The simulation results also provide insights into the AQM design, e.g. the importance of congestion indicator, adaptive and nonlinear mechanism being suitable for time-varying TCP dynamics.

ArkaitzBitorika, Mathieu Robin, Meriel Huggard, Ciar´an Mc Goldrick,[2]. Much recent function has devoted to improving AQM efficiency as a result of alternative strategies. This research specifics the simulation primarily based analysis as well as contrast of a subset of such plans. The particular plans preferred have been created to accommodate setup as well as incremental deployment with routers in the existing World-wide-web architecture. The particular analysis strategy implemented permits the particular primary contrast involving AQM plans, definitely showcasing his or her similarities as well as dissimilarities. Like function ought to promote faster ownership involving increased AQM protocol inside World-wide-web routers. On this papers nine AQM plans are generally chosen intended for comprehensive analysis. The primary qualification useful for selection of these plans could be the alleviate using which often they are often implemented inside existing best-effort systems. The particular analysis can be accomplished using a specially created platform which often uses the particular NS2 simulator.

G.F.AliAhammed, ReshmaBanu,[3] Congestion can be an significant matter which usually experts focus on within the Indication Management Process (TCP) community environment. In this report that they analyzed various effective queue supervision algorithms with respect to their own abilities of preserving excessive useful resource operation, pinpointing and confining extraordinary bandwidth application, and their own deployment difficulty. The particular assessment from the overall performance of JOHN, GLOWING BLUE, SFB, and CHOKe determined by simulation results, employing REDDISH and Lower Trail as the evaluation baseline. The particular features of unique algorithms are reviewed and when compared. Simulation is performed through the use of Community Simulator (NS2) plus the equity graphs are drawn employing X- graph. Regarding all these algorithms, three facets are reviewed: (1) useful resource operation (2) fairness among unique traffic flows and (3) implementation and deployment difficulty.

Xiapu Luo, Rocky K. C. Chang, and Edmond W. W. Chan,[4]In this paper, the author investigate how the functionality connected with TCP streams can be afflicted with denial-of-service (DoS) attacks within the Decrease

Pursue and a variety of AQM techniques. Particularly, they will look at 2 kinds of DoS attacks—the conventional flooding-based DoS (FDDoS) attacks and the recently suggested Pulsing DoS (PDoS) attacks. The Decrease Pursue interestingly outperforms this RED-like AQMs once the router can be under a PDoS episode, in contrast to this RED-like AQMs execute superior under a significant FDDoS episode. In contrast, this Adaptive Exclusive Queue protocol may preserve a higher TCP throughput while in DDoS attacks when compared with the RED-like AQMs. This particular paper's primary aim is always to evaluate the effect connected with DoS attacks about the TCP functionality within the Decrease Pursue system and some various other well-known AQM techniques: RED, PI, REM, and AVQ. They look at 3 kinds of DoS attacks: the original flooding-based DoS episode and the growing intelligent DoS attacks, electronic. gary the gadget guy. Shrew, RoQ, and PDoS. The results obtained from this research are extremely revealing.

Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, Jianping Yin[5] The focus of this work is to propose a novel metric – Congestion Participation rate(CPR) - and a CPR-based approach to detect and filter LDDoS attacks by their intention to congest the network. Simulation conducted using ns-2 simulations, test-bed experiments, and Internet traffic trace analysis to validate analytical results and evaluate the performance of the proposed approach.

III. PERFORMANCE PARAMETERS

The number of parameters used in this study is packet delivery ratio, end-to-end delay, number of packet drop, routing overload and throughput between DRR, PI Controller and GK algorithms.

3.1 Packet Delivery Ratio: The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

3.2 Average End-to-end delay: It includes all possible delays caused by buffering during queuing at the interface queue, retransmission delays and propagation and transfer times of data packets.

3.3 Packet Drop: It occurs when the router which is supposed to relay packets actually discards them.

3.4 Routing Overhead: It is defined as ratio of total number of routing and reputation related packets and total number of data packets [6].

IV. SIMULATION SETUP

Dumbbell network topologies are commonly used in congestion control studies. Network topology consist of two routers (R0, R1, 30 users (User1 to User30), 20 attackers (Attacker1 to Attacker20), 30 servers (Server1 to Server30), and a victim server. The link between two routers is the bottleneck link with a bandwidth of 5 Mbps and one way propagation of 6 ms. All the other links have a bandwidth of 10 Mbps and a one-way propagation delay of 2 ms. In this topology, User I communicates with server I (where I = 1..30) using FTP, and 20 attackers send UDP packets to attack the victim Server. The queue size of the bottleneck link is 100. A DRR based count is deployed at router R0 on the queues of the bottleneck link. Other links used GK Controller queues. A CPR-based detection module is installed at router R0 where most normal TCP packets are dropped when an LDDoS attack is present. For comparison, we also install a module based on Cumulative Amplitude Spectrum (CAS) at R0; CAS uses Discrete Fourier Transform (DFT) to locate disturbances caused by LDDoS flows. Simulation time period is 220s and the LDDoS traffic begins at 120s and ends at 220s. And the frequency is 1000 Hz.

IV. SIMULATION SETUP

4.1 Packet Delivery Ratio –

As shown in Figure 1, the comparison between DRR, GK and PI Controller by using CPR based approach and without it on the basis of Packet Delivery Ratio. From the graph, algorithms shows higher PDR while using CPR approach when compared with normal approach. However, when compared individually GK shows the highest PDR while using CPR approach and lowest PDR while using normal approach. When we compare DRR it has been noticed that there is negligible difference in terms of PDR. And while comparing PI Controller, it reflects that there is much big difference when CPR approach is compared with normal approach.

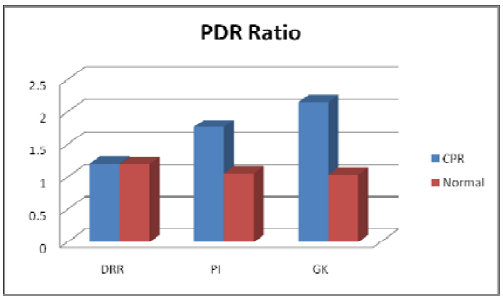

Figure 1. Packet Delivery Ratio for DRR , PI Controller and GK using CPR and without using CPR.

4.2 Packets Dropped –

As shown in Figure 2, the comparison between three queue management algorithms DRR, GK and PI Controller with using CPR approach and without using it on the basis of packets dropped. The graph shows that the packet dropped is maximum in GK while using CPR approach and is minimum as well with normal approach. Same way if we look for PI Controller algorithm, packet dropped are still high but less than GK when CPR approach is used and low when using normal approach. But in case of DRR algorithm, there is negligible difference in terms of packet dropped while comparing CPR based approach and normal approach.

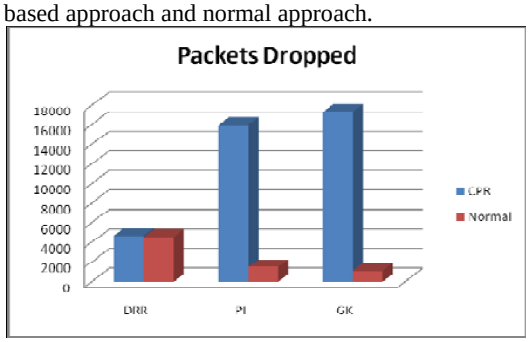

Figure 2. Packets dropped for DRR, PI and GK algorithm using CPR and without using CPR.

4.3 Average End-to-End Delays –

As shown in Figure 3, the comparison between three queue management algorithms DRR, GK and PI Controller with using CPR approach and without it on the basis of average end-to-end delay. Graph shows that GK and PI controller have equal ratio of highest and lowest end-to-end delay while using CPR approach and with normal approach. In case of DRR algorithm, average end to end delay is same in both the scenario.

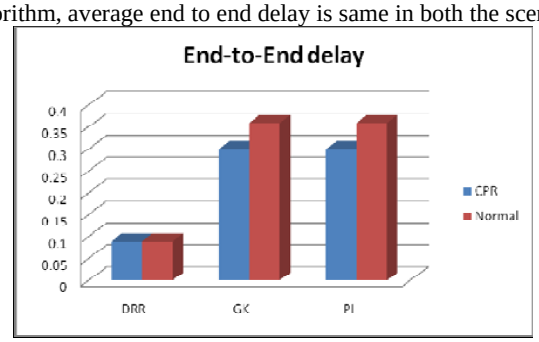

Figure 3. Average End-to-End delay in DRR, GK and PI Controller using CPR and without using CPR.

4.4 Routing Overhead –

As shown in Figure 3, the comparison is done on the basis of Routing overhead. From this graph, it is concluded that the routing overhead is near about equal in case of DRR by using CPR and without using CPR approach. However, in case of GK and PI Controller it make a huge difference, as we see that the routing overhead is much less while using CPR approach and on the peak when not using CPR approach.

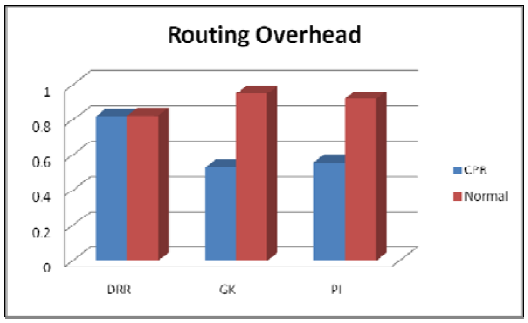

Figure 4. Routing overhead in DRR , GK and PI Controller using CPR and without using CPR.

IV.CONCLUSION

In this paper, comparisons are done between three queue management algorithms DRR, GK and PI Controller. It is concluded that average end to end delay is minimum for DRR and maximum for GK and PI Controller while using CPR approach, GK dropped the maximum number of packets while using CPR approach and minimum number of packets dropped with normal approach as compared with DRR and PI controller which has minimum number of dropped packets both in case of CPR approach and with normal approach as well. Further, when it comes to PDR, DRR has the minimum PDR and GK has the maximum PDR when CPR approach is used, PI controller lies in between of both queuing algorithm i.e. DRR and GK in terms of PDR. In terms of Routing Overhead, DRR algorithm does not make huge impact when using CPR and normal approach, but GK and PI Controller have low routing overhead while using CPR approach and high routing overhead while using normal approach. So, we conclude that in all the simulation parameters DRR results does not vary while simulating using CPR and normal approach and in the cases of GK and PI controller, both algorithm have same type of impact when using CPR and normal approach. So, it is stated from the results that DRR is the most effective algorithm and better than GK and PI controller algorithm.

REFERENCES

[1] Minjuan Cheng, Xiaoming Ma, "Performance Evaluation of Queue Management Methods for Congestion Control", Journal of Information & Computational Science 9:6 (2012) pp. 1599–1608.

[2] Arkaitz Bitorika, Mathieu Robin, Meriel Huggard, Ciaran McGoldrick, "A Comparative Study of Active Queue Management Schemes". In Proceedings of IEEE ICC 2004.

[3] G.F.Ali Ahammed, ReshmaBanu, "Analyzing the performance of Active Queue Management", Journal of Information & Computational Science Vol.2, No.2, March 2010.

[4] XiapuLuo, Rocky K. C. Chang, and Edmond W. W. Chan, "Performance Analysis of TCP/AQM Under Denial-of-Service Attacks", 13th International Conference on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2005.

[5] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, Jianping Yin, "Flow Level detection and filtering of low-rate DDOS", Computer Networks 56 (2012) pp. 3417-3471.

[6] Arvind Sharma, Dr. Neeraj Kumar, "Comparative Analysis of Low Rate Denial of Service Attack in MANETs*", IJARCSSE, vol. 3, Issue 7, July 2013*.

[7] A. Kuzmanovic and E. W. Knightly, "Low-rate tcp-targeted denial of service attacks and counter strategies", IEEE/ACM Trans. Netw., vol. 14, no. 4, pp. 683–696, 2006.

[8] A. Shevtekar, K. Anantharam, and N. Ansari, "Low rate tcp denial-of-service attack detection at edge routers*", Communications Letters, IEEE, vol. 9, no. 4, pp. 363–365, april 2005*.

[9] Wu Zhi-jun, Zhang Hai-tao, Wang Ming-hua, Pei Bao-song, "*MSABMS-based approach of detecting LDoS attack"*, Computer & Security 3I(2012), pp. 402-417.

[10] Harkeerat Bedi, Sankardas Roy, Sajjan Shiva, "Mitigation congestion based DOS attacks with an enhanced AQM technique", SEPTEMBER, ELSVIER 2014.

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