DDOS Attacks Router Throttling Mitigation Technique

DHWANI GARG

Department of Computer Science and Engineering, Delhi Technological University (formerly Delhi College of Engineering), Shahbad Daulatpur, Main Bawana Road, Delhi – 110042, India

e-mail: dhwanigupta@gmail.com

Abstract

Distributed Denial of Service (DDOS) is now on of the most significant kinds of security threats in the internet. Through this form of attack the available resources are engaged to such a level that it ceases to provide service to the legitimate users. Internet services have been the major victim of various forms of this attack with complete network faces sharp reduction in performance. In a coordinated manner sheer volume of packets are being sent from a distributed set of locations with sole purpose being the consumption of both computational or communication resources of the network resulting graceful degradation of network performance. In this paper, an overview of the DDOS problem attack, defense principle and how the gap between the problem and possible mitigation could be resolved through the application of queuing mechanism over optimum throttle algorithm has been proposed.

Keywords: Internet security, Denial of Service, Distributed Denial of Service, Queuing approach, throttle algorithm.

1 INTRODUCTION

Network security breaches have now become a major threat to businesses and institutions providing online services and in the end costs in the tune of billions of dollars every year. As per statistical details by CERT [1], the rate of network attacks have gone up from a mere 171 vulnerabilities in 1995 to 7236 in 2007, and the attacks reached a staggering level of 4110 in the first half of 2008 [2]. The list might not represent the actual number of breaches as most of them go unreported. Denial-of-service or DOS attacks are among the various forms of attacks with possibilities of highest level of harm in simplest possible form. This "Denial of Service" could impact the network in following forms [3]:

- Occupying the already scarce resources of network further limiting its availability for legitimate users.
- Damaging the network configuration through overloading resulting malfunctioning of various software and hardware components of the network.
- The extent of damage of could extent to the damage of electronic as well as network line resulting loss of physical information.

Hence, this DOS attacks is basically a set of events which hinders legitimate users from various online services due to lack of network connectivity [4]. Therefore, rehearsing it detail a DOS attack attempts.

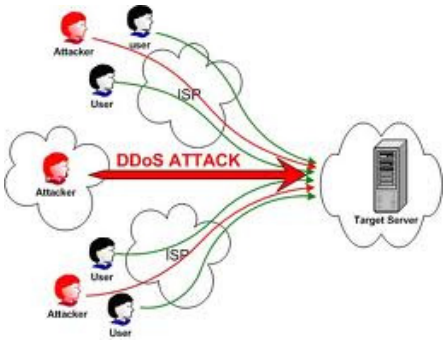
1. To grade the performance of the network for legitimate user by coordinated flooding of the network.
2. To disable the ability of the service provider through planned disruption of connections between two parties.
3. To systemically restrict the access of a particular individual to a service.
4. To interrupt a specific service or the system that provides that service.

Hence, the main motive of all such attacks is to obstruct the functioning of a service provider as a potential competitor in online business or preventing an individual from getting the benefits of a given service [5].

Distributed DOS is a variant of DOS in which attacks are induced through deployment of program on a number of host compromised over security features [4]. Technically the attack involves breaches network in two forms. The first being the compromised units which are used as attack units and the other forms is that of enabling DOS through jamming the network with useless traffic. Hence, the mitigation of DDOS attacks requires reinforced nature of defense mechanisms with implementation is necessitated over both phases. As, the DDOS attacks can be enabled two modality with first being the brute force attacks and the second one as logical attacks. The brute force DDOS attacks, the victim is flooded with useless data packets resulting unnecessary traffic with bandwidth for legitimate users reduces to

the level of non-usability and preventing access to a service. DDOS through Logical attacks is the result of some bug coming into existence during the implementation of some protocol or application installed at the victim or the target and later unknowingly used for eating into the resources [5]. The consequence of DDOS attacks can easily be figured out with shutting down of some high profile websites [6] and in some recent surveys of FBI and other supporting agencies, DOS attacks have now become second most rampant after virus infection.

The design of the internet makes it more vulnerable and hence a heaven for DDOS attacker. As per design this internet is quite simple in architecture at intermediary level so that packet movement could be made as fast as possible. Hence, the complex part of this network falls at the two end with one being the server and other being the client. So, the misbehavior at one end could easily affect the other end as the intermediate entities would do almost nothing to protect them from further damage. Tools like firewall can protect the victim but still it has to respond to the requests that is being sent from various units that includes both legitimate as well as attackers [7]. And here DDOS attackers make their impact as this form of attack relies on intermediate component of the internet and hence easily impact the internet [8]. As the internet resources is already a limited resources, hence the DDOS attackers can make significant change in the performance of the net as a whole. The lack of any globally deployed security mechanism makes this more favorable for attackers [7].



Figures 1: Illustration of DDOS attack scenario[21]

This paper concentrates on the fundamental understanding of router throttling as a mechanism against DDOS attacks. Further advancement has been made over control- theoretic model that makes it useful for better understanding of the system behavior under a medley of limits as well as operating conditions. The implementation of an adaptive throttle algorithm that can enhance the security feature of the server as well as protect it from further resources overload and makes it free enough for further requests from legitimate users. The paper extends to the implementation of max-min fairness throttle algorithm and how this throttling could impact real application performance in case of a DDOS attack.

2 RELATED WORK

2.1 Countermeasures a bandwidth- exhaustion attacks

It is a mechanism that enables the system to counter DOS yielded bandwidth-exhaustion attacks through the concepts of aggregate-based congestion control [9], trace back [10] and filtering [12]. Another mechanism being the Aggregate-based congestion control (ACC) that extends its scope to traditional flow based so that data packets could be managed to finer granules. An aggregate is defined as a collection of packets that share some property (signature). ACC provides mechanisms for detecting and controlling aggregates at a router using an attack signature, and a *pushback* mechanism to propagate control requests (and the attack signature) to upstream routers. ACC critically depends on the mechanism by which attacks are detected and an attack signature is formulated, and this can be a source of difficulty against an intelligent adversary that varies its traffic characteristics over time. A goal of Congestion Puzzles (CP) is to avoid the need to formulate attack signature.

A related congestion control mechanism is level-k max-min fair throttles. The mechanism differs from ACC in that a congested server is responsible for issuing congestion-control requests to routers k hops away(denote the set of these routers by R(k)) to help maximize the bandwidth allocated to those receiving the smallest allocation (max-min optimization). This approach does not depend on formulating attack signatures, but offers fairness only to the extent that the routers in R(k) can provide it. With the low deployment depth (small k), it is possible that 'legitimate clients' flows may aggregate to a relatively high bandwidth flow before reaching a router in R(k),thus being subjected to rate limiting. Another limitation of the mechanism is the assumption that all routers are trusted, which makes it vulnerable to attacks from compromised routers. Several methods focus primarily filtering or tracing spoofed traffic, such as ingress filtering, hop count filtering, and numerous works on trace back. These approaches are of less utility against non-spoofed traffic, and thus permit DDOS attacks from zombies using their real source addresses. In addition, many of these schemes rely upon some way of distinguishing attack packets from legitimate ones, thereby again raising the difficulties of generating attack signatures. Finally, some filtering schemes consider coordination among routers. Our approach also supports such coordination within the context of the CP mechanism. Recently, an approach that uses overlay network to protect web servers from congestion based DDOS attacks. An overlay network is composed of a set of nodes across the internet. A client who wants to connect to the web server has to first pass a reverse Turing test posed by an overlay node, which then tunnels the client's connection to an approved location so as to reach the web server. This approach

however does not solve the general bandwidth-exhaustion problem: First, adversaries might still be able to use other protocols or the traffic addressed to a less sensitive server to congest routers on paths to the web server. Second, this solution is tailored to protocols driven by human users, who can be called upon to pass a reverse Turing test. Third, once adversaries have implemented zombies at overlay nodes or routers, they might circumvent the defense mechanism.

2.2 Client Puzzles

Client Puzzles have been proposed to defend against denial of service attacks in the context of TCP. To our knowledge, no puzzle protocol has been proposed to defend against DDOS attacks on IP layer. *Furthermore our mechanism is compatible with existing network protocols and can operate in a decentralized way, so that multiple upstream routers can cooperate to defend against a bandwidth- exhaustion attack.
Whereas most puzzle proposals impose a number of computational steps to generate a solution, there exists other type of puzzles. Another proposal has been about a "memory bound "puzzle that accesses upon clients in an effort to impose similar puzzles solving delay even on different hardware. Reverse Turing test also presents an attractive approach as puzzles prevent automated flooding in network protocols that should be driven by humans. A similar approach also offers insightful comments on the weaknesses of computation-based puzzles in providing guaranteed access for end to end services during DDOS attacks. At the IP layer, however, service is characterized by "best effort" delivery, with the goal of max-min fairness in bandwidth allocation. Computation-based puzzles do have the potential to achieve this goal coarsely, and offer various pragmatic benefits: such puzzles are easier to generate and require less state in comparison to other types of puzzles.

2.3 Aggregate Increase Multiplicative Decrease

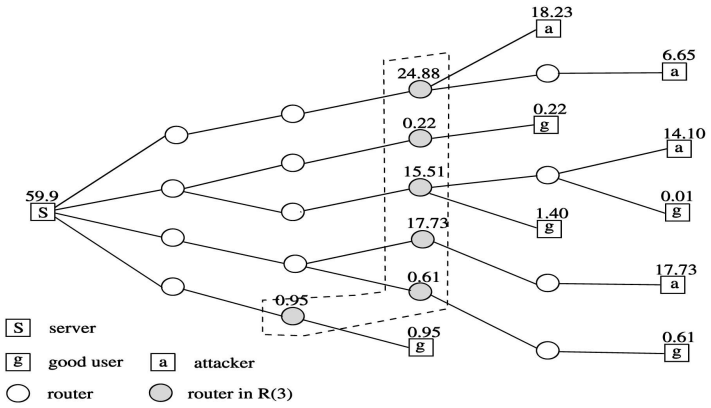


Figure 2: Network Topology illustrating R(k) deployment points of router throttle. [19]

As DDOS attacks has been a resource management problem and the server system is being protected from scenario that might require it to deal with excessive service request arising out of the global network. The solution provided by researchers propagates a proactive approach. It involves the installation of router based throttle mechanism which actually regulates the traffic along the path to the server with contribution in form of managing the rate of incoming packets to moderate levels. This regulatory mechanism ultimately forestalls an attack that might have affected the performance of the server and have hurt the service provider as well as the client. The victim server would be made capable enough to install a router throttle at an upstream router thereby limiting the rate of throttle at which the packets that are destined for server router will be forwarded by the router. The limit is now the deciding factor for dropping, rerouting or continuing the traffic heading for the given server.

The throttle should be a factor of current demand distributions and requires dynamic negotiation between the server and the global network that includes the client. The base for the initiation of the router throttle by the server is based on the load it is observing. In case the load is below the designated limit, the server doesn't need to install any router throttle. But the same server would install as well as activate the router throttle at upstream routers with traffic increasing beyond the load limits 'Us'. If the current throttle doesn't bring down the load rate to below Us, then the extent of throttle is increased through the reduction in the throttle rate. The throttle is removed in case there is no further increase in server load. This algorithm is effective in various attack scenarios but it requires a careful estimation of step size (δ).

In the next section we have proposed a new algorithm that can effectively handle this problem.

3. PROPOSED ALGORITHM

In the proposed approach we have tried to reduce the search range by half at every iteration. It uses the concept of aggregate rate (ρ) to determine the direction of adjustment. When the aggregate rate is more than Us, Rs is reduces by half.
Now, to simulate the proposed solution, the paper relies on a network model with a connected graph G= (V,E), where V is the set of nodes and E is the set of edges. As the leaf nodes have been considered the host, it can be considered as a traffic source. The internal node is a router with the role as an intermediary between the two peers or hosts and forwarding from one end to other. Routing nodes are denoted by R which is the set of internal routing nodes. All routers are assumed to be trusted. The set of hosts, H = V-R, is portioned into the set of ordinary "good" users,

Hg and the set of attackers Ha. E models the network links, which are assumed to be bi-directional. Since our goal is to investigate control against server resource overload, each link is assumed to have infinite bandwidth. The assumption can be relaxed if the control algorithm is also deployed to protect routers from overload.

In the network, we designate a leaf node in V as the target server S. A good user sends packets to S at some rate chosen from the range [0, Rs]. An attacker sends packets to S at some rate chosen from the range [0, Ra]. In principle, while Rs can usually be set a reasonable level according to how users normally access the service at S(and we assume Rs<<Us), it is hard to prescribe constraints on the choice of Ra. In practice it is reasonable to assume that Ra is significantly higher than Rs. This is because if every attacker sends at a rate comparable to a good user, then an attacker must recruit or compromise a large number of hosts to launch an attack with sufficient traffic volume. The paper here presents an algorithm that installs at each router in R(k), a uniform leaky bucket rate(i.e the throttle rate) at which the router can forward traffic for S. In the specification, Rs is the current throttle to be used by S. It is initialized to (Ls + Us)/f(k), where f(k) is either some small constant ,say 2, or an estimate of the number of throttle points typically needed in R(k). Algorithm tries to reduce the time required to calculate the value of Rs

Algorithm

```
1.  ρ last :  = -∞;
2.  Hv    :  =  Us;
3.  Lv    :  =  0;
4.  Rs    :   = (Ls + Us)/f(k) ; /*initialize throttle rate*/
5.  While(1)
6.        If (ρ >= Us)
7.          Hv  : =  Rs;
8.           If (ρ last - ρ < €)
9.             Lv  := 0;
10.           end if
11.    else if (  ρ <= Ls)
12.           Lv  := Rs ;
13.            If (ρ  - ρ last < €)
14.                Hv  : =  Us;
15.            end if;
16.      end if;
17.      ρ last :  = ρ;
18.      Rs  :  = (Hv + Lv)/2);
19.      end while;
```

TABLE 1

Iteration	Rs	ρ
1.	11	34.78
2.	5.5	18.38
3.	14.7	45.88
4.	7.3	24.68
5.	6.4	20.98

Ls = 20, Us = 24

4 ANALYSIS

Router throttling is a feedback control strategy. To better understand its stability and convergence behavior, we formulate its control theoretic model. Using the model, we explore how delays, the hysteresis control limits, and the number and heterogeneity of traffic sources, can impact system performance. We point out that our mathematical model can also provide a general framework for studying various multisource flow control problems. Comparing with the earlier AIMD algorithm it has been calculated that it is near optimal for certain reasonable cost functions of overshooting and undershooting. The algorithm detects the situation that shrunken search range for Rs, can no longer deal with changed traffic conditions. In the above table it can be observed that we have initialized the Ls and Us values to 20 and 24. We calculate the value of ρ. When the value of ρ reaches between 20 and 24 the algorithm terminates and the throttle rates of all the routers are adjusted to that particular value whose throttling rate has earlier been adjusted to a value greater than the present rate.

5 DISCUSSION

Several observations are in order about the practical deployment of our defense mechanism. First, we must achieve reliability in installing router throttles. Otherwise, the throttle mechanism can itself be a point of attack. To ensure reliability, throttle messages must be authenticated with the server sites that desire protection have to do authentication. Other edge routers can just drop throttle requests unconditionally. Also, throttle requests must be efficiently and reliably delivered from source to destination, which can be achieved by high network priority for throttle messages and retransmissions in case of loss. Since throttle messages are infrequent and low in volume, the cost of authentication and priority transmissions should be acceptable.

Second, because of the feed back nature of the control strategy, it is possible that the server will transiently experience resource overload. To ensure that the throttle mechanism remains operational during these times, we can either use a coprocessor on the server machine that it is not concerned with receive-side

network processing, or deploy a helper machine, whose job is to periodically ping the server, and initiate defense actions when the server is not responsive.

Third, the throttle mechanism may not be universally supported in a network. Our solution remains applicable provided at least one router supports the mechanism on a network path that sees substantial attacker traffic. Depending on the position of such a router, the feasible range of k may be more restricted.

Fourth, we have adopted a generic notion of max-min optimization in our study, which makes it easy to manage and deploy. As observed, however, it is also possible to have a policy-based definition of max-min limit in practice. The policy can refer to different conditions in different network regions, in terms of traffic payments, network size, susceptibility to security loopholes etc.

6 CONCLUSION

We presented a server-centric approach to protect a server system under DDOS attacks. The approach limits the rate at which an upstream router can forward packets to the server, so that the server exposes no more than its designed capacity to the global network. In allocating the server capacity among the upstream routers, we studied the notion of level- _max-min fairness, which is policy-free and hence easy to deploy and manage.

In addition, we evaluated algorithm effectiveness using a realistic global network topology, and various models for attacker and good user distributions and behaviors. Our results indicate that the proposed approach can offer significant relief to a server that is being flooded with malicious attacker traffic. First, for aggressive attackers, the throttle mechanism can preferentially drop attacker traffic over good user traffic, so that a large fraction of good user traffic can make it to the server as compared with no network protection. Second, for both aggressive and meek attackers throttling can regulate the server load to below its design limit.

Our focus in the paper has been upon reducing the searching time for the routers to decide upon the appropriate throttle rate for attacks caused due to flooding of the server. However other forms of attacks are present that do not depend on volume of attack traffic. More analysis is required to deal with these other types of attacks.

7 REFERENCES

[1] Raktim Bhattacharjee, S. Sanand, and S.V. Raghavan. “Path Attestation
Scheme to avert DDoS Flood Attacks” International Federation for Information Processing,2010.

[2] Biswa Ranjan Swain, Bibhudatta Sahoo “Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method”
IEEE International Advance Computing Conference, March 2009.

[3] Palvinder Singh Mann, Dinesh Kumar “A Reactive Defense Mechanism based on an Analytical Approach to Mitigate DDoS Attacks and Improve
Network Performance”
International Journal of Computer Applications, January 2011.

[4] Yinghong Fan, Hossam Hassanein and Patrick Martin “Proactive Control
of Distributed Denial of Service Attacks with Source Router Preferential Dropping” IEEE,2009.

[5] Nicholas A. Fraser, Douglas J. Kelly, Richard A. Raines, Rusty O. Baldwin and Barry E. Mullins “Using Client Puzzles to Mitigate Distributed
Denial of Service Attacks in the Tor Anonymous Routing Environment” ICC,
2007.

[6] Fasheng Yi, Shui Yu, Wanlei Zhou, Jing Hai and Alessio Bonti,”Source
based Filtering Scheme Against DDOS Attacks” International Journal Database
of Theory and Application

[7] Gal Badishi, Amir Herzberg, Idit Keidar, Oleg Romanov, Avital Yachin
“An Empirical Study of Denial of Service Mitigation Techniques” IEEE 2008.

[8] W.J. Blackert, D.M. Gregg, A.K. Castner, E.M. Kyle, R.L. Hom, R.M.
Jokerst “Analyzing Interaction Between Distributed Denial Of Service Attacks
and Mitigation Technologies” IEEE 2003.

[9] Ruiliang Chen, Jung-Min Park “Attack Diagnosis: Throttling Distributed
Denial of Service Attacks Close to the Attack Sources” IEEE 2005.

[10] Abraham Yaar, Adrian Perrig, Dawn Song “Pi: A Path Identification Mechanism to Defend against DDOS Attacks” IEEE 2003.

[11] Yinan Jing, Xueping Wang, Xiaochun Xiao, Gendu Zhang”Defending
Against Meek DDOS Attacks By IP Trace-back based Rate Limiting”IEEE
2006.

[12] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry "A
Survey of DDOS Defense Mechanisms"

[13] Ping Du, Akihiro Nakao "Mantlet Triology: DDOS Defense Deployable
with Innovative Anti-Spoofing, Attack Detection and Mitigation" IEEE 2010.

[14] Antonis Michalas, Nikos Komninos, Neeli R. Prasad, Vladimir
A. Oleshchuk"New Client Puzzle Approach for DoS Resistance in Ad hoc
Networks" IEEE 2010.

[15] Ruiliang Chen, Jung-Min Park, Randolph Marchany "A Divide – and-
Conquer Strategy or Thwarting Distributed Denial-of-Service Attacks" IEEE
2007.

[16] Ping Du, Akihiro Nakao "DDoS Defense Deployment with Network Egress and Ingress Filtering" IEEE 2010.

[17] V.Praveena, N.Kiruthika "New Mitigating Technique to Overcome DDOS Attack" World Academy of Science, Engineering and Technology 2008.

[18] Xiuli wang "Mitigation of DDOS Attacks through Pushback and Resource Regulation" International Conference on Multimedia and Information Technology 2008.

[19] David K.Y Yau, John C.S Lui, Feng Liang and Yeung Yam, "Defending Against Distributed Denial-of-Service Attacks With Max-Min Fair Server-Centric Router Throttles" IEEE Transactions on Parallel and Distributed Systems, July 2001

[20] Rajesh Sharma, Krishan Kumar, Kuldip Singh, R.C. Joshi "Shared Based
Rate Limiting; An ISP level Solution to deal DDOS Attacks" IEEE 2006.

[21] Palvinder Singh Mann, Dinesh Kumar "A Reactive Defense Mechanism
based on an Analytical Approach to mitigate DDoS Attacks and Improve
Network Performance" International Journal of Computer,2011

[22]http://t0.gstatic.com/images?q=tbn:ANd9GcTj--soxy3_JK7asVro37G69dr3NPxZ9h0N6jVDKn72Hmp2G7vg