An Efficient Dynamic Router Approach to Defeat DDOS Attacks

S S NagamuthuKrishnan[1] *V. Saravanan*[2]

Abstract

Denial-of-service attacks represent a major threat to modern organizations that are increasingly dependent on the integrity of their computer networks. Recently many prominent web sites face so called Distributed Denial of Service Attacks (DDoS). Even there are many approaches to avoid DDOS attacks no approaches completely satisfies the protection yet.

A new approach to combating such threats introduces dynamic routers into the network architecture. These dynamic routers offer the combined benefits of intrusion detection, and work collaboratively to provide a distributed defense mechanism. The paper provides a detailed description of the design and operation of the algorithms used by the dynamic routers and demonstrates how this approach is able to defeat the attacks. It is proposed that the adoption of a dynamic router approach in protecting networks overcomes many of these weaknesses and therefore offers enhanced protection.

This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DDoS attacks which use forged IP addresses to be propagate from 'behind a nearest router aggregation point.

Keywords : DDOS Attack, Time slot, Transfer Rate, Signature of a Packet, Security, Incentive, Economical.

1. Introduction

Internet-enabled business, or ebusiness, has mushroomed into a significant part of the US economy, yet further advancement of e-business is plagued by various Quality-of-Service (QoS) and security problems. One of the worst is the Distributed Denial-of-Service (DDoS) attack, which aggregates junk data traffic from up to thousands of computers into a formidable volume and floods and effectively blocks a certain victim website. DDoS attacks have drawn a lot of media attention since the landmark attacks on a large portfolio of famous e-business websites including Yahoo!, Amazon, CNN, eBay, and E*Trade, in early 2000 [Klein bard 2000]. Cavusoglu et al. [2002] estimate that the firms involved lost more than 2.8% of their market capitalization. Academic discussion also quickly followed up with proposals that can be broadly classified into two categories: technological solutions [Wang and Reiter 2004; Badishi et al. 2004; Xiang et al. 2004; Mirkovic et al. 2005 Chapter 7], and economic solutions [Geng and Whinston 2000; Geng et al. 2002].

Figure 1 illustrates the mechanisms of a DDoS attack. There are two separate stages of DDoS attacks: recruiting zombies and flooding the victim [Chang 2002]. In the recruiting stage (steps 1 and 2), security flaws are used to break into master computers and a large set of zombie computers is established. In the flooding stage, a direct attack or a reflector attack is launched and synchronized traffic with IP spoofing [Geng and Whinston 2000] disables the services of the victim (steps 3 and 4).

[1] Ph.D. Research Scholars, Assistant Professor, Thiagarajar School of Management, Madurai, Bharthathiar University, Coimbatore – 641 146, Tamilnadu, India, Email : ssnkrishnan@gmail.com

[2]Professor & HOD, Department of Computer Application, Karunya University, Coimbatore – 641 114, Tamilnadu, India. Email : tvsaran@hotmail.com

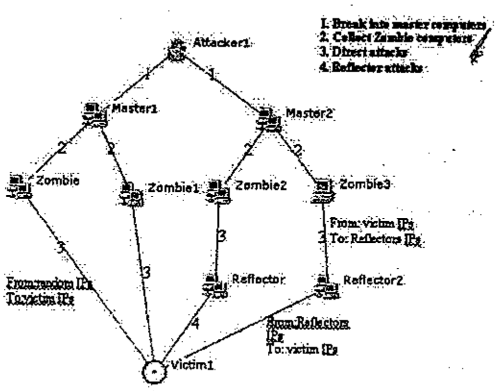

Figure 1 : The Mechanism of DDOS attacks

It is now well-understood that several cooperative technological solutions including cooperative filtering and cooperative traffic smoothing by caching (as we will shortly discuss) will be quite effective against DDoS attacks but some of those cooperative technological solutions were proposed as early as in 2000 (e.g. RFC 2827—ubiquitous ingress filtering), they are clearly not effectively deployed.

But the drawback of this method is that, the traffic is found through out the path from source to destination. Hence the bandwidth of the network is not utilized properly and also affects economy of ISPs and ICPs. Since there is traffic the service for the request is delayed for long time. So here we propose a new solution called Dynamic router approach which works based on the conditions –Ip-address, request parameters. In order to identify the attackers 'request first Ipaddress of the source is verified whether it is from a known source or not. Then the parameter types are compared. When the request is found to be the attackers request then the request will be blocked.

2. The Cooperative Technological Solutions To Ddos Attacks

2.1 Cooperative Filtering

Cooperative filtering is the first cooperative technological solution. Cooperative filtering works in three steps: alarming, tracing, and filtering (illustrated in Figure 2). By analyzing the pattern of network traffic, Intrusion Detection Systems (IDS) identify suspicious traffic and send out alarms. Following the alarms, a tracing mechanism kicks in to track back each attack path as far as possible. Finally, a series of filters along every attack path are configured to filter out attack traffic. In the best scenario, a tracing mechanism may find the computers (zombies) that are initiating attack traffic, and may inform the responsible ISPs to take them offline.

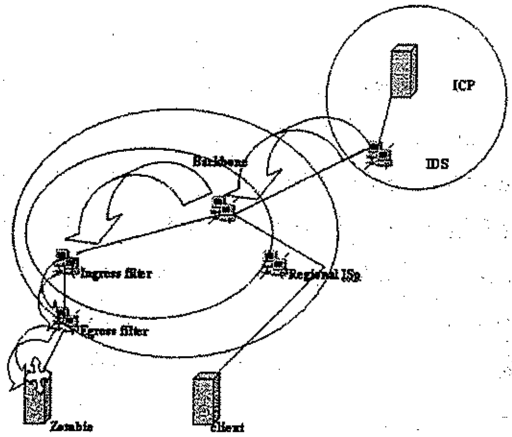

Figure 2 : The Process of Co-operative Filtering

2.2 Cooperative Caching

Cooperative caching is an effective solution to DDoS attacks when cooperative filtering is costly to implement, or when attack traffic is well concealed in legitimate data requests such that pattern recognition is technically difficult. Cooperative caching and filtering can also be jointly deployed so that attack traffic is both reduced and diverted, resulting in a more effective defense. One important technological issue in using cooperative caching to defeat DDoS attacks is the fact that only relatively static content can be cached. If a DDoS attack targets dynamic content or protocols (such as ICMP ECHO, SYN floods, BGP floods), and traditional caching solutions cannot divert it. This issue is now partially addressed in two ways. First, standards like Edge

Side Include (ESI, see www.esi.org) enable caching of dynamic content. Second, more ISPs start screening and restricting control packets. For example, the attacks using ping commands are no longer effective when ICMP traffic is restricted.

2.3 The Broken Incentive Chain

Despite the fact that cooperative filtering and cooperative caching are two effective technological solutions against DDoS attacks, to date they have rarely been deployed on the Internet because of incentive chain.

There are two major sources driving the flow of digital content on the commercial Internet: end users' demand to consume digital content and ICP's demand to publish digital content. As shown in Figure 3, while both end users and ICP's only pay directly to their ISPs for Internet connections, those regional ISPs in turn pay larger regional ISPs and backbone ISPs for the connectivity to the core of the Internet. We call this series of payments the "incentive chain," which acts as glue to link all parties together in the end-to-end transmission of digital content.

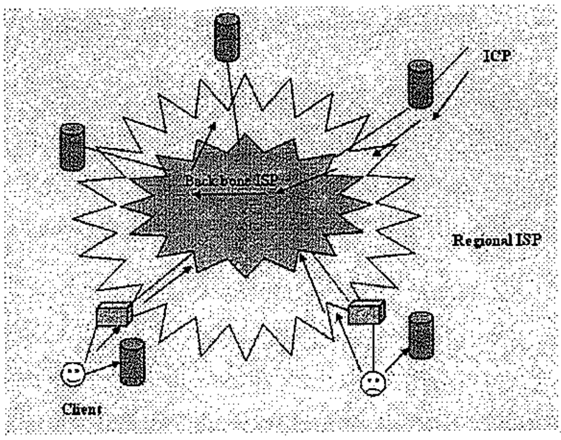

Figure 3 : Incentive Chain

2.4 Lack Of Incremental Payment Structure And The Failure Of Co-operative Filtering

One important implication of this conservative practice in uplink planning is that most of the time ISPs have abundant unused residue bandwidth that they have already paid for to the upper-level ISPs. ISPs are willing to provide such an unused resource for better consumer retention, and on the surface it appears not to hurt anybody else. However, it actually leads to devastating consequences on cooperative filtering against DDoS attacks, once we look at the question: what are the costs and benefits for an ISP to engage in cooperative filtering? While the cost side includes the administrative work in setting up and maintaining filters, and the reduction of transmission performance due to filtering overhead; the benefit side often includes little to nothing as long as DDoS attacks only consume some of the residue bandwidth, which is unused anyway.

The inability of victims in DDoS attacks to motivate ISPs who are in the best position to filter attack traffic is the direct result of the lack of incremental payment structures on the Internet. By selling and buying Internet access on a subscription basis, ISPs have little incentive to control traffic volumes as long as it does not create congestion in their own neighborhoods, simply because the marginal cost for transmitting additional data packets is zero. Additional bandwidth may be used to initiate DDoS attacks and harm ICPs far away. However, this does not provide any incentive for local ISPs to take any action. Clearly, when it comes to a DDoS attack, the incentive chain is broken.

2.5 Caches On The Edge Of The Internet: Inaccessible Treasures

The optimization of an incentive chain is all about the tradeoffs between the costs and benefits of various possible incentive schemes. As we noted before, cooperative filtering is actually costly to ISPs because of administrative costs and performance reduction. Alternatively, if DDoS attack traffic can be diverted to a lot of cache servers through cooperative caching, it can be an effective solution, as it prevents the accumulation of traffic from happening. Since cache servers already exist, as long as cooperative caching only uses redundant cache capacity, it incurs little cost to any party involved, and thus is more cost efficient than cooperative filtering. Nevertheless, as shown in Figure 3, ISPs' caches only serve their local users who pay for connections. Congestion at the ICP's website does not provide any payment for cache servers on the demand side to engage in cooperative caching. Therefore, the resource is inactive for defending DDoS attacks, and again the incentive chain is broken.

3. Existing Solution

3.1 Fixing The Incentive Chain Capacity Provision Network

A Capacity Provision Network (CPN), which would be a network of cache servers owned, operated and coordinated through capacity trading by different ISPs. A CPN is initially proposed for demand-side cache trading, the usefulness of which is supported by the fact that there exist positive network externalities across individual ISPs who provide caching services to their respective local users: when some ISPs are experiencing high demand for caching, other ISPs' cache capacity may be idling. Therefore, by sharing the idling cache capacity with busy ISPs, total welfare increases. Cache trading is operated in a CPN market, which is organized by a market owner. We propose that the owner of the CPN market fits well in the intermediary's role as we described it: the owner specializes in dealing with large numbers of ISPs who own cache servers, and the owner is a single entity that can deal with outside organizations on behalf of its participating ISPs. Figure 4 illustrates an incentive chain for CPN owner-intermediated cooperative caching. An ICP initiates the incentive chain by contracting with and paying the CPN owner for cooperative caching against any possible DDoS attacks. When a DDoS attack happens, the CPN owner decides which cache server is in the best position to dilute the traffic and then pays relevant ISPs to start cooperative caching, which completes the incentive chain. Of course, how much the ICP pays the CPN owner depends in turn on how much the owner pays ISPs.

4. Proposed Solution

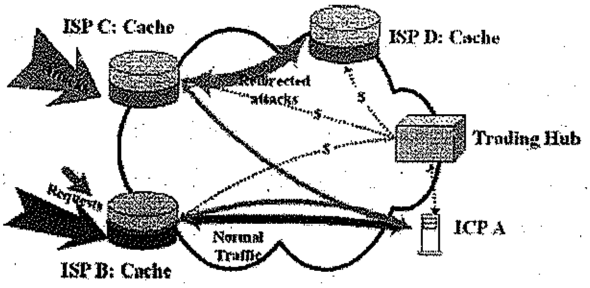

Figure 4 : Capacity Provision Network

The attacks are generally conducted by sending packets to the victim at a higher rate than they can be served, causing the Denial of legitimate service requests. In distributed Denialof service (DDoS) attacks, the aggregate traffic from several different sources is responsible for disabling the services provided by the victim.

The limitation of IP trace back problem is that identified machines might not be the actual attack sources. In fact only Zombies may be recognized and, therefore, more sophisticated schemes are required to locate the true origin of the attack.

Before seeing the solution in detail the things to be kept in mind are the maximum request size is 2GB, maximum number fields to be in the request is 100 (normally the users use only up to 20 fields).

In this solution using header information of packets - size of packets and number of fields and IP address we are able to find out the attack in the first router itself. It avoids more traffic which penetrates through network. So this approach will save the time, and the network bandwidth is utilized properly. "Time Slot" is maintained for each request. The nearest router will check each request to see whether the request is legitimate or not. If there is more number of requests immediately one after other with packet size nearer to maximum then it is considered to be attack request and the request is dropped. The number of request arrived from unique IP address corresponding to particular router can be found from the router's database.

If the request is attack request, the transfer rate of the network is very low and the network bandwidth is blocked. Hence the service for the legitimate users is also denied. If the illegitimate request is identified in the first router itself, there is no need to find the source of the attack. Trace back is not at all needed.

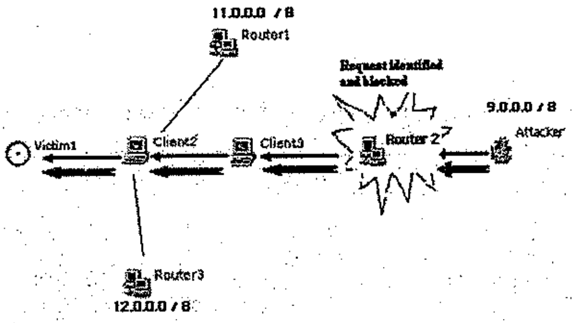

Figure 5 : Restricting Fake Packet

In the example above, the attacker resides within 9.0.0.0/8. An input traffic filter on the ingress (input) link of "router 2", which provides connectivity to the attacker's network, restricts traffic to allow only traffic originating from source addresses within the 9.0.0.0/8 prefix, and prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range.

In other words, the ingress filter on "router 2" above would check. If the address also would have been same then the packet signature such as request size, the number of fields in each packet will be checked. If it is an attacker's request then it will be blocked and so the traffic will be reduced.

Sample Data and Results

Nodes in the Network	Time Taken
100	0.078125
200	0.109375
300	0.109375
400	0.15625
500	0.15625
600	0.15625
700	0.171875
800	0.234375
900	0.234375
1000	0.265625

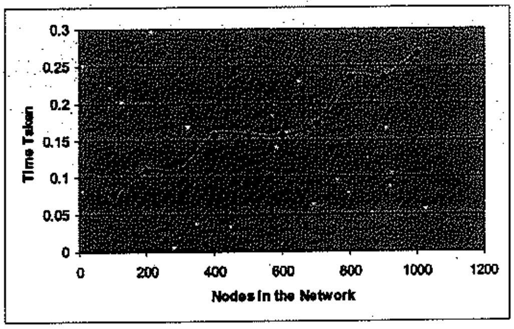

Figure 6

[YUN HUANG., 2007]The above graph depicts the CPN method. In that, Time taken for reaching the victim based on the network path is shown for the sample data.

Nodes	Time taken
100	0.078125
200	0.078125
300	0.5
400	0.078125
500	0.078125
600	0.078125

700	0.078125
800	0.078125
900	0.078125
1000	0.078125

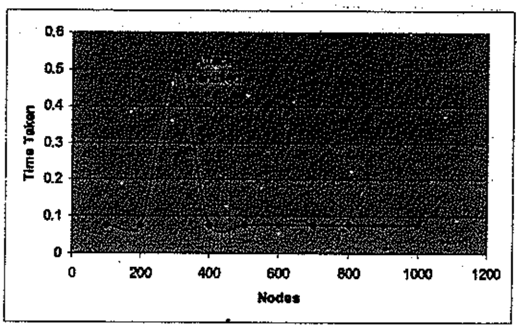

Figure 7

In our proposed solution the time taken to reach the victim is avoided. Since the attack is identified in the first router itself.

No of Packets(No's)	Transfer Rates (Mbps)
100	100
200	96
300	84
400	77
500	55
200	90
210	96
220	94
215	98
225	100

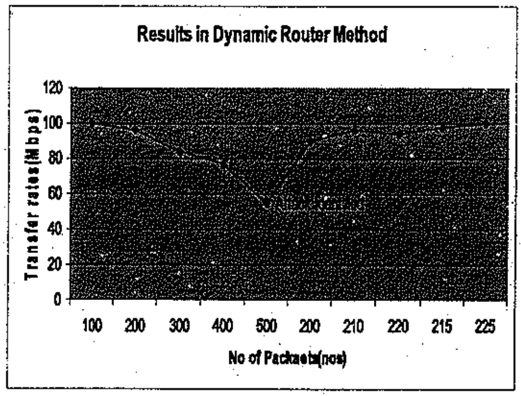

Figure 8

When compared to CPN, this method is cost effective because in CPN the attack request is not identified just when there is more network traffic the traffic is spitted and distributed to the near cache server to serve the request. In our solution, the request whether is attack request or a legitimate one is identified in the nearest router (first router the request passes through from the sender) and only the attacker's LAN traffic gets affected and not the traffic through out the network is avoided. Hence the cache can be used efficiently to provide service for the legitimate requests.

5. Conclusion

Denial-of-services attacks can cause significant damage to web service providers. Currently, the Internet routing infrastructure does not provide means of locating the attacker nor avoiding such attacks. The rapid growth of denial-of-services attacks has led to a great number of proposed solutions. All the previously proposed methods concentrated mostly on determining the attack path. However, with our proposed solution we can easily safeguard any network from attack. While implementing this within LAN congestion may occur. Additional functions should be considered for future platform implementations, such as the implementation of multiple cache servers on the network in order to avoid the congestion with in the network facilitated by some complex congestion control algorithm.

References

[1] Kleinbard, D. 2000. More sites hacked in wake of Yahoo! CNN Money News (Feb. 8), Published on the <http://money.cnn.com/2000/02/08/technology/yahoo>.

[2] Cavusoglu. H, Mishra. B. K and Raghunathan. S, *"The effect of internet security breach announcements on market value of breached firms*

and internet security developers", Workshop on Information Systems and Economics Program, Barcelona, Spain, December, 2000.

[3] Wang. X and Reiter. M. K, *"Mitigating bandwidth-exhaustion attacks using congestion puzzles",* In Proceedings of the 11thACM Conference on Computer and Communications Security, Washington, DC (October), PP. 257–267, 2004.

[4] Badishi. G, Keidar. I and Sasson. A, *"Exposing and eliminating vulnerabilities to denial of service attacks in secure gossip-based multicast",* In Proceedings of the International Conference on Dependable Systems and Networks (DSN'04), Palazzo dei Congressi, Florence, Italy, June, PP. 223–232, 2004.

[5] Xiang. Y, Zhou. W and Chowdhury. M, *"A survey of active and passive defense mechanisms against DDoS attacks",* Tech. Rep., TR C04/02. School of Information Technology, Deakin University, Australia (March), 2004.

[6] Mirkovic. J, Dietrich. J. S, Dittrich. D and Reiher.P, *"Internet Denial of Service: Attack and Defense Mechanisms",* Prentice Hall PTR, Indianapolis, IN, 2005.

[7] Geng. X, and Whinston. A. B, *"Defeating distributed denial of service attacks",* IEEE IT Professional 2, 36–41, 2000.

[8] Chang. R. K. C, *"Defending against flooding-based distributed denial-of-service attacks a tutorial",* IEEE Comm. Mag. 40, 42–51, 2002.

[9] Geng. X and Whinston. A. B, *"Defeating distributed denial of service attacks",* IEEE IT Professional 2, 36–41, 2000.

[10] Defeating DoS Attacks with IP Trace back Rafael P.Laufer* - Pedro B.Velloso** - Otto Carlos M. B. Duarte 2005*

[11] *"Defeating Ddos Attacks By Fixing The Incentive Chain",* Yun Huang., University Of Texas At Austin., Xianjun Geng., University Of Washington And Andrew B. Whinston University Of Texas At Austin, february 2007.

Author's Biography

Mr. S S Nagamuthu Krishnan has got his Bachelor's degree in Physics from Madurai Kamaraj University during the year 1995 and MCA degree from Bharathiar University during the year 1998. He has obtained his MPhil in Computer Science from Bharathiar Universitym in the year 2007. He has got more than 9 years of academic experience. His areas of interest are Object Oriented Analysis and Design, Computer Security, Data Structures & algorithms and Networking. He is also pursuing his research leading to Ph. D. in Network Security.

Dr. V Saravanan obtained his Bachelor's degree in Mathematics from University of Madras during 1996 and Masters Degree in Computer Applications from Bharathiar University during 1999. He has completed his PhD in Computer Science in the Department of Computer Science and Engineering, Bharathiar University during 2004. He specialized on automated and unified data mining using intelligent agents. His research area includes data warehousing and mining, software agents and cognitive systems. He has presented many research papers in National, International conferences and Journals and also guiding 3 researchers leading to their PhD degree. He has totally 10 years experience in teaching including 3 years as researcher in Bharathiar University. He is the member of Computer Society of India, Indian Association of Research in Computing Sciences and many professional bodies.