ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 3, March 2014**

# Detection and Controlling of DDoS Attacks by a Collaborative Protection Network

Anu Johnson[1], Bhuvaneswari.P [2]

PG Scholar, Dept. of C.S.E, Anna University, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu,India [1]

Assistant Professor, Dept. of C.S.E, Hindusthan Institute of Technology. Coimbatore,Tamil Nadu,India [2]

**ABSTRACT:** Distributed denial-of-service (DDoS) attacks remain a major security problem and the mitigation of which is very hard . In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.The early discovery of these attacks, although challenging, is necessary to(IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information.The evaluation of this work using extensive simulations and a real dataset is presented, showing its effectiveness and low overhead, as well as its support for incremental deployment in real networks.As an enhancement to this work the controlling of DDoS attacks are also included by constructing Inter Domain Packet Filters protect end-users as well as the expensive network infrastructure resources. Here, address the problem of DdoS attacks and present the theoretical foundation, architecture, and algorithms of detecting DDoS attacks. The core of this work is composed of intrusion prevention systems.

**KEYWORDS**: DDoS attacks; intrusion prevention systems; Internet service providers; Inter Domain Packet Filters

## I. INTRODUCTION

Distributed denial-of-service (DDoS) attacks still constitute a major concern [1] even though many works have tried to address this issue in the past. As they evolved from relatively humble megabit beginnings in 2000, the largest DDoS attacks have now grown a hundredfold to break the 100 Gb/s, for which the majority of ISPs today lack an appropriate infrastructure to mitigate them [1].Most recent works aim at countering DDoS attacks by fighting the underlying vector, which is usually the use of botnets [3]. A botnet is a large network of compromised machines (bots) controlled by one entity (the master). The master can launch synchronized attacks, such as DDoS, by sending orders to the bots via a Command & Control channel. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself [4], which raises important ethical issues, or to first detect botnet-related malicious activities (attacks, infections, etc.), which may delay the mitigation.

To avoid these issues, this paper focuses on the detection of DDoS attacks and *per se* not their underlying vectors. Although nondistributed denial-of-service attacks usually exploit a vulnerability by sending few carefully forged packets to disrupt a service, DDoS attacks are mainly used for flooding a particular victim with massive traffic as highlighted in [1]. In fact, the popularity of these attacks is due to their high effectiveness against any kind of service since there is no need to identify and exploit any particular service-specific flaw in the victim. Hence,this paper focuses exclusively on flooding DDoS attacks. A single intrusion prevention system (IPS) or intrusion detection system (IDS) can hardly detect such DDoS attacks, unless they are located very close to the victim. However, even in that latter case, the IDS/IPS may crash because it needs to deal with an overwhelming volume of packets (some flooding attacks reach 10–100 Gb/s). In addition, allowing such huge traffic to transit through the Internet and only detect/block it at the host IDS/IPS may severely strain Internet resources.

Here presents a new collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level. It relies on a distributed architecture composed of multiple IPSs forming overlay networks of protection rings around subscribed customers.

This system is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging *belief*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

*scores* on potential attacks.The IPSs form virtual protection rings around the host they protect.The virtual rings use horizontal communication when the degree of a potential attack is high. In this way, the threat is measured based on the overall traffic bandwidth directed to the customer compared to the maximum bandwidth it supports. In addition to detecting flooding DDoS attacks, *system* also helps in detecting other flooding scenarios, such as flash crowds, and for botnet-based DDoS attacks.

Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, proposes an inter domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. In this paper, proposes an inter domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. In this paper, proposes an inter domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of this scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers.

## II. RELATED WORK

The previous paper[1] describes a preliminary architecture of this paper with initial simulations. In this paper, these are substantially extended by enhancing and detailing the communication algorithms. A mitigation technique is provided as well as a detailed investigation of configuration in [2]. Experimentation with a real dataset and different traffic patterns was also performed, as well as an analytical analysis of the complexity.Even though a publicly available dataset was used, this does not ease the quantitative comparison to related work. Unlike packet-based methods, false and true positives are computed globally taking into account each router and each time window in [3].This is why the focus of the comparison needs to be on qualitative aspects.Bellovin proposes in the use of distributed firewalls, which is implemented in [4] . However, only firewall rules are exchanged, and each firewall must detect the attacks on its own.The authors of propose a similar solution where a Gateway is requested to block the traffic of an attack. In[5], only the DDoS mitigation of the attacks is distributed, but the detection is located very close to the victim. Unlike this paper, all previously mentioned solutions do not exploit effective use of collaboration.

## III. PROPOSED SYSTEM

A. *Ring-Based overlay Protection:*

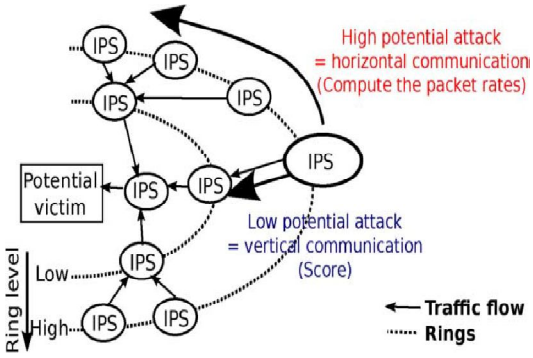


Fig 1:Horizontal and vertical communication

The system maintains virtual rings or shields of protection around registered customers. A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer .Each IPS instance analyzes aggregated traffic within a configurable *detection window*. The *metrics manager* computes the frequencies and the entropies of each rule . A rule describes a specific traffic instance to monitor and is essentially a traffic filter, which can be based on IP addresses or ports.Following each detection window, the *selection manager* measures the deviation of the current traffic profile from the stored ones, selects out of profile rules, then forwards them to the *score manager*. Using a decision table, the *score manager* assigns a score to each selected rule based on the frequencies, the entropies, and the scores received from upstream IPSs(vertical collaboration/communication). Using a threshold, a quite low score is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

marked as a *low potential attack* and is communicated to the downstream IPS that will use to compute its own score. A quite high score on the other hand is marked as *high potential attack* and triggers ring-level (horizontal) communication (Fig. 2) in order to confirm or dismiss the attack based on the computation of the *actual packet rate* crossing the ring surpasses the known, or evaluated, customer capacity. As can be noticed, this detection mechanism inherently generates no false positives since each potential attack is checked. However, since the entire traffic cannot be possibly monitored, we promote the usage of multiple levels and collaborative filtering described previously for an efficient selection of rules, and so traffic, along the process. In brief, to save resources, t he *collaboration manager* is only invoked for the few selected candidate rules based on resource-friendly metrics.

B. *Subscription Protocol:*

This system protects subscribers (i.e., potential victims) based on defined rules. A rule matches a pattern of IP packets.Generally, this corresponds to an IP subnetwork or a single IP address. However, the rule definition can include any othermonitorable information that can bemonitored, such as the protocols or the ports used.

This system is an added value service to which customers subscribe using the protocol. The protocol uses a trusted server of the ISP that issues tokens. When a customer subscribes for the system protection service, the trusted server adds an entry with the subscribing rule along with its subscription period (TTL) and the supported capacity. The server then issues periodically a corresponding token to the customer with a TTL and a unique ID signed using its private key. All communications between subscribers and the server are secured a using private/public key encryption scheme.

The ring level of a *system*-enabled router (IPS) is regularly updated based on the degree of stability of IP routing. This is done using a two phase process. First, the router sends a message *RMsg* to the protected customer containing a counter initialized to 0. The counter is incremented each time it passes through a *FireCol*-enabled router. The customer (or first-level *FireCol* router) then replies to the initiating router with the value of its ring level. This procedure is optimized through aggregation when several routers are requesting a ring-level update.

## III. EVALUATION

The objective of the experiments is to evaluate the accuracy of *system* in different configurations. Furthermore, the robustness of system is evaluated in abnormal situations such as the existence of noncooperative routers or configuration errors.

A. *Simulations*

Although obtaining real router traces is possible, getting synchronized traffic and host states of a real network along with its detailed topology is quite difficult for security, privacy, and legal reasons. Thus, we mainly used a simulation-based approach for the evaluation of the system.

B. *Metrics*

The true positive rate (TPR) measures the proportion of rightly detected attacks. The false positives (FPs) counter represents the amount of benign traffic wrongly flagged as malicious. As previously described, horizontal communication discards all of them by computing the real packet rates. However, the number of rules to analyze the traffic has to be as low as possible, and so we will consider the misselected rules as false positives. From a practical point, this corresponds to taking the output of the *score manager* (Section III) as the final result.

C. *Ring Levels of the Attack*

The previous experiment assumes attacks come from beyond outer rings. A skilled attacker, however, might launch an attack from within the vicinity of the victim, hence avoiding high-order rings. The extreme case corresponds to a single ring. However,this rare case implies that the attack is no more distributed and can be detected without collaboration since its traffic is more concentrated and distinguishable. For instance, using only one or two rings is not efficient because all traffic, including benign one, is also analyzed by only these rings and so is not really distinguishable from attack traffic. However, by using a five-rings topology with attacks injected at the first or the second rings, the benign traffic is also analyzed by the upper rings, which helps in distinguishing it from the malicious ones.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 3, March 2014**

## IV. ENHANCEMENT

The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, proposes an inter domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that, even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks. Credible BGP calls for a modification to the standard BGP route selection algorithm such that it takes into account validity state of routing updates. These two scores are defined as follows: Route origination validation score is derived based on the ability of a route receiving node to determine whether the AS originating the route actually is authorized to do so. Route AS-Path validation score is derived based on the ability to which the node is able to determine whether the received update actually traversed the ASs listed in the AS Path. There are number of types of attacks that successfully employ IP spoofing. So it is mandatory for today's network scenario that there must be some mechanism present to avoid IP spoofing which ultimately causes different kinds of network and resource attacks. Many attempts are made to prevent from such attacks at router or network level. We employ an approach to control IP spoofing at Autonomous System (AS) level or at inter domain level by making use of implicit information contained in border gateway protocol (BGP) messages transferred between border routers of different ASes

## V. CONCLUSION AND FUTURE WORK

This system proposed, a scalable solution for the early detection of flooding DDoS attacks. Belief scores are shared within a ring-based overlay network of IPSs. It is performed as close to attack sources as possible, providing a protection to subscribed customers and saving valuable network resources. Experiments showed good performance and robustness of system and highlighted good practices for its configuration. Also, the analysis of system demonstrated its light computational as well as communication overhead. Being offered as an added value service to customers, the accounting for system is therefore facilitated, which represents a good incentive for its deployment by ISPs. As a future work, plan to extend this system to support different IPS rule structures.

## REFERENCES.

1. A. Networks, Arbor, Lexington,MA, "Worldwide ISP security report," *IEEE/ACM Trans. Netw.*, vol. 4, no. 5, pp. 601–615, Oct. 2010.
2. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense countering the DoS and DDoS problems," *Comput. Surv.*, vol. 39, no.4,pp.306-315,Apr. 2007, Article 3.
3. V. Paxson, "End-to-end routing behavior in the Internet," *IEEE/ACM Trans. Netw.*, vol. 5, no. 5, pp. 601–615, Oct. 1997.
4. T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm,", *IEEE/ACM Trans. Netw.*, vol. 2, no. 3, pp. 201–215, Oct. 2008, Article no. 9.
5. A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, "Locating Internetrouting instabilities," *Comput. Commun. Rev.*, vol. 34, no. 4, pp. 205–218, 2004.

## BIOGRAPHY

She received the B.Tech degree in Computer Science & Engineering from Jyothi Engineering College, Cheruthuruthy, Kerala in 2012. She is currently doing the Post graduation in Hindusthan Institute of Technology, Coimbatore,Tamil Nadu, now working on the research project in Network Security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 3, March 2014**

**Ms.Bhuvaneshwari.P** was born in Pollachi, Tamilnadu,India on March 13,1988. She obtained her B.E. (CSE) from Anna University, Chennai , India in 2010 and received her Master of Computer Science and Engineering from Anna University,Chennai, India in 2013.She is currently a assistant professor in Hindusthan Institute ofTechnology, Coimbatore, India.