Volume 6, Issue 5
October 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Distributed DoS Attack Detection using IP Addresses

[1] A. Saraswathi, [2] Dr.K.Thangadurai

[1] Research Scholar & Assistant Professor, P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur, Tamil Nadu, India.

[2] Assistant Professor, P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur, Tamil Nadu, India.

E-mail: [1]asaraswathi.mscphd@gmail.com, [2]ktramprasad04@yahoo.com

ABSTRACT

It is now more than a decade since the first full-scale High-Rate Flooding (HRF) DDoS attacks were unleashed on the Internet community. The vector for that attack was a set of compromised machines (bots), controlled by an attacker (bot-master), and used to direct high volumes of unwanted network traffic towards a target host. Even after a decade, and notwithstanding their conceptual simplicity, HRF DDoS attacks in various guises continue to constitute a pernicious threat within the Internet community. However, an efficient and timely detection of such attacks, combined with the formulation and implementation of an effective attack mitigation strategy, remains a challenging problem. This paper attempts to provide a solution to the DDoS attack detection problem, and outlines the design of a corresponding lightweight mitigation strategy and this paper describes an approach based on the source IP address of the incoming packets, and demonstrates how that simple network traffic feature, coupled with a change-point analysis of the rate of arrival of new IP addresses, is sufficient in some circumstances to detect the onset of a DDoS attack. Finally concludes by presenting a scheme to download the legitimate IP addresses identified by the above detection strategy to an application firewall to provide a mitigation facility.

Keywords:*DDos, Intrusion detection, IP Address, Data transfer, Network Security.*

1. INTRODUCTION

The onset of a HRF DDoS attack is typically accompanied by an increase in the number of unsolicited packets originating from previously unseen or new source IP addresses arriving at the target host. A real-world example of a DDoS attack with this characteristic is the CAIDA DDoS Attack 2007 dataset – a popular dataset used by DDoS researchers containing approximately one hour of pseudonymised traffic traces from a DDoS attack. The characteristics of this attack in terms of the rate of incoming traffic (left y-axis) and previously unseen or new source IP addresses (right y-axis). This characteristic feature of a HRF DDoS attack forms the basis of the proposed DDoS attack detection approach, namely, to analyze the incoming traffic in terms of the source IP addresses of the packets received, and to reliably determine if the current incoming network traffic represents a DDoS attack. The proposed DDoS attack detection approach, cooperatively developed and it consists of two high-level functions. They are ipac and ddos.

- ipac function for classifying the source IP addresses of the packets received
- ddos function for identifying an attack

2. RELATED WORK

The ipac or IP address classification function first extracts the IP addresses of the incoming network traffic. It determines whether the source IP address has been seen previously or is new (Not Seen Previously – NSP). The resulting time series of the rate of previously unseen or new IP addresses is then is analysed by the ddos function to identify whether the system is under attack. The system being protected against DDoS attacks is represented in terms of two independent states: NA (not under attack), which is the system state when receiving nonattack or normal traffic, and A (under attack), the system state when receiving DDoS attack traffic. In order to learn the network behaviour under normal (non-attack) conditions, the ipac function is first applied to normal network traffic without the activation of the ddos function. After the training period, the ddos function is invoked at regular intervals (1 to 10 seconds), and based on the rate of arrival of packets from previously unseen IP addresses (as calculated by the ipac function), the ddos function then determines if the system is under attack.

A transition from state NA to A signals that an attack has been identified, and the ddos function then generates a 'white list', which can then be used for mitigation, for example, by only allowing traffic from IP addresses within the white list. On the other hand, a transition from state A to NA is indicative of the end of an attack, and can be the prompt for the relaxation of the mitigation strategy. In order to perform the source IP address classification of the incoming packets, ipac maintains two data structures representing the IP addresses of the packets received: W (White-list) and R (Recent). The data structure W is initialized with the source IPs of known attack-free or normal traffic i.e. legitimate clients.

The data structure R is initialized to be empty at system start-up, and is used to temporarily hold the source IPs of the packets arriving from new (NSP) IP addresses. Only once the ddos function has recently determined that the system is not under attack can those addresses be copied to the white-list the data structure W. This avoids polluting the white-listed (legitimate) source IPs stored in W. If, on the other hand, the ddos function determines that the system was recently under attack, then the data structure R is discarded. The ipac function (described in Algorithm) analyses the source IP address of an incoming packet, and if the ip address is new or has not been seen previously, it updates the data structure R.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Algorithm: ipac function for classifying IP addresses.

Input: Source IP address (ip) of the incoming packets.
Output: Previously unseen or new source IP addresses (newIP).

```
if NOT ((ip in W) OR (ip in R)) then
        INC (newIP) /* increment the counter for new IPs */
        add ip to R /* update data structure R */
end
```

The ddos function (described in Algorithm) is periodically invoked, at 1 to 10 second intervals, to analyze recent changes in the arrival of packets from NSP IP addresses, as calculated by the ipac function. The ddos function calls the State Change function, which in turn uses a change detection technique to detect abrupt changes in the rate of arrival of packets from NSP IPs, specifically in the change from the state NA to A.

Algorithm: ddos function for identifying attacks.

Input: Time series of the rate of new source IP addresses.
Output: System State – A or NA

```
if (in state NA) then
        if NOT (StateChange(NA)) then /* no state change */
                add R to W /* add IP addresses to white-list */
                else /* state change to A */
                state = A
                send white-list to the application firewall
                R = empty
        end
end
else if (in state A) then
if StateChange(A) then /* change state to NA */
        state = NA
        inform the application firewall to stop using the white-list
end
end
```

There are a few limitations to this approach. The first is that whenever the system is deemed under attack, new IP addresses are treated as malicious. This can give rise to false positives. Proposed ensemble-based DDoS detection technique aims to limit these false positives by extending the rejection criterion of the incoming packets beyond the simple property of NSP IP addresses. It does this by making use of additional network-based parameters such as traffic volume, traffic volume per IP address, along with server-load based parameters such as CPU and memory utilization, in tandem with NSP IP addresses to improve the identification of malicious traffic.

A second limitation concerns the malicious IP addresses observed during normal network operations. This can be addressed not only by using the additional network and server-load based features described above, but also by using smaller historical time periods. An additional limitation concerns the time taken by the execution of the ipac and ddos functions. The intention is to keep these two functions small and efficient. However, if they are slow, incoming packets may not be properly processed. The implementation of the NSP algorithm using bit vectors: a data structure that compactly stores the IP addresses as a bit-array.

3. IMPLEMENTATION OF AN IP-BASED DDOS DETECTION STRATEGY:

This section describes the implementation details of the main components of the IP-based DDoS attack detection technique – IP addresses classification, and DDoS attack detection.

3.1 IP ADDRESS CLASSIFICATION

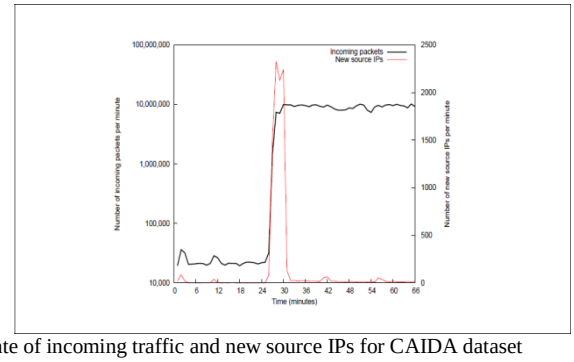
Using the change in rate of new source IP addresses as the primary feature to detect the onset of a DDoS attack requires keeping track of source IP addresses already seen in the network under normal, non-attack network conditions. At these times, the rate of arrival of new source IP addresses is relatively low, i.e. the target server experiences a small number of previously unseen (new) sources IPs. On the other hand, the onset of a DDoS attack is generally marked by a substantial increase in the rate of arrival of new source IP addresses. Therefore, the implementation of the IP address classification function (ipac) requires the use of a compact and efficient data structure.

3.2 BIT VECTOR IMPLEMENTATION

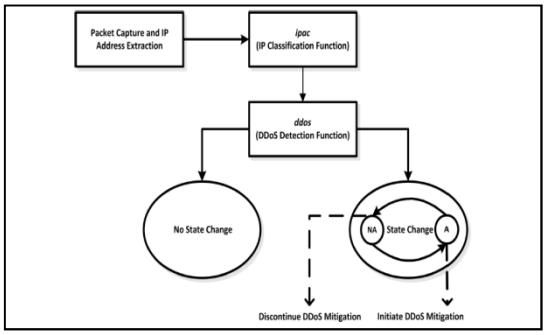
In order to accommodate all the IP addresses in the IPv4 address space, a bit vector can be used as the data structure to represent W (White-list) and R (Recent) in the implemented NSP algorithm. In the IPv4 address space, in order to accommodate all of 232 IP addresses using a bit vector, 0.5 GB of space is required. In contrast, a bit vector in IPv6 address space needs to represent 2128 IP addresses. This increase in the address size from 32 bits in IPv4 to 128 bit in IPv6 significantly increases storage requirements. One possible solution to the scaling problem in the ipac function would be to accommodate the larger IPv6 address space by using a more efficient data structure such as a bloom filter. In the IP address classification function (ipac), whenever an incoming packet is received, a bit at a specified position in the bit vector is set to indicate the presence of a given IP address. A separate counter is then used to calculate the number of new source IP addresses observed during an interval, resulting in a time series of the rate of previously unseen or new IP addresses. This implementation via bit vectors allows for a number of optimizations to the proposed NSP algorithm. In the ddos function, the step ‘add R to W’ can be optimized by modifying the ipac function so that at the time of setting the appropriate bit in the data structure R, a temporary copy of the IP address value, or better still, a copy of the address of the bit being set can be kept. This optimization allows the ‘add R to W’ step to be implemented as a series of bit operations rather than as an OR operation between the entire bit vectors R and W. Another similar optimization relates to the step ‘R = empty’ in the ddos function. This step is optimized by unsetting the relevant bits rather than zeroing the entire bit vector R.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



Rate of incoming traffic and new source IPs for CAIDA dataset



DDoS Detection using NSP source IPs

3.3 DDOS ATTACK DETECTION

The onset of a HRF DDoS attack is typically accompanied by an increase in the number of unsolicited packets arriving at the target host from previously unseen or new IP addresses. In such attacks, an increase in the number of unsolicited packets usually results from a large number of compromised hosts (bots), controlled by a bot master, which send a high volume of traffic to the target host. As a result, the target host not only experiences an increase in incoming traffic volume but also an increase in the number of sources sending such traffic. Thus, the problem of identifying the onset of a DoS attack can be formulated as a change detection problem. This involves detecting changes in the statistical properties of the incoming traffic parameters of interest, such as the change in rate of new source IP addresses.

The IP address classification function (ipac) identifies the number of new source IP addresses within a given measurement interval. It then calls the ddos function (change detection algorithm) to identify the onset of a DDoS attack. For detecting abrupt changes in the parameter under investigation i.e. the rate of new source IP addresses, a change detection technique called Exponentially Weighted Moving Average (EWMA) has been used.

3.4 DATASETS USED

In order to experiment with and evaluate the proposed DDoS attack detection technique it is important to have a dataset with two distinct components, viz., normal (background) traffic and the anomalous traffic. The normal traffic component is drawn from the data collected by the University of Auckland (Auckland VIII dataset) [1] and the anomalous (attack) traffic component is constructed using the fudp3 utility.

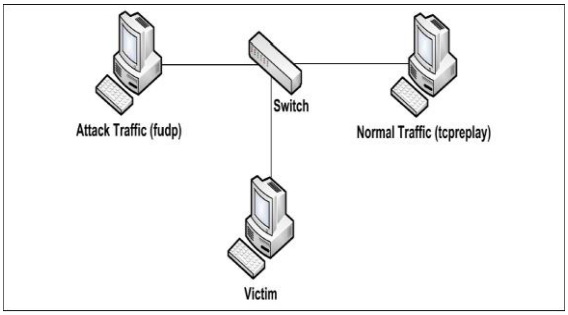
3.5 BACKGROUND TRAFFIC

The Auckland VIII dataset GPS synchronized IP header trace collected using a DAG3.5E Ethernet network measurement card. The entire trace consists of only TCP, UDP, ICMP based traffic, and all the non-IP traffic has been discarded. All TCP and UDP packets have been truncated to 20 bytes after the start of transport header.

To ensure anonymity and privacy, the IP addresses in the captured traffic trace have been mapped to 10.*.*.* using a one-to-one hash mapping. The one-to-one mapping is performed sequentially so that the first real IP address observed is replaced by 10.0.0.1, and the next new IP address is mapped to 10.0.0.2, and so on. The sequential mapping pattern is preserved across the entire traffic trace. For the purpose of experimentation, a subset of the entire dataset was used, comprising nearly 1 hour of continuous bidirectional real-world network traffic collected. Before using this data, it was pre-processed. The dataset was analysed to extract traffic destined for the busiest web-server (destination IP address 10.0.0.63). The selected traffic was then processed to remove TCP SYN attacks, which were the most common type. In order to achieve this, TCP flows with less than 3 packets were considered malicious and were removed. TCP flows with no data from the web-server were also ignored. The processed data was then converted into a one-way incoming traffic target at the destination web-server 10.0.0.63. The cleaned data was reproduced over the test bed using the TCP replay utility. The cleaned network traffic trace was replayed at around 300 packets per second.

Number of Unique Source IP's	Number of Packets	Attack Duration (Seconds)	Traffic Rate(Mbps)
35	342,141	134.38	1.01
40	328,579	129.35	1.01
45	321,433	129.29	1.01
50	313,747	123.23	1.01
100	237,831	93.49	1.01
150	201,020	86.83	1.01

Table 1: Statics of the Attack Traffic



The test bed architecture for evaluating the NSP algorithm

3.6 ATTACK TRAFFIC

The attack traffic, superimposed on the cleaned background traffic. It was used to flood the target host with UDP packets having between 35 and 150 different source IP addresses. The rationale for using this variation was to analyse the proposed algorithm under different attack conditions. It is acknowledged that attacks with a large number of different source IP addresses are relatively easier to detect compared to those with a small number of different source IPs. The average packet rate for the attack traffic is approximately 3000 packets per second. The attack traffic used for experimentation is summarised in Table 1.

4. CONCLUSION

Notwithstanding the research conducted in DDoS attack detection over the past decade, timely and reliable detection of such attacks remains a challenging problem. So too does the formulation and implementation of an effective attack mitigation strategy. The main contribution of the design of a DDoS attack detection technique based on new or NSP source IP addresses and its proof-of concept implementation and evaluation. The technique exploits a key characteristic of DDoS attacks, viz., a marked increase in the number of new source IPs accompanying the onset of a HRF DDoS attack than can transcend protocol specific defenses, such as those that protect against specific types of flooding attacks, such as SYN flood. The current implementation of the detection technique, although post hoc, uses a single network traffic feature and a lightweight data structure, and thus facilitates the detection of DDoS attacks at 'wire speed', compared to computationally intensive machine learning-based models such as Hidden Markov Models (HMMs) and Artificial Neural Networks (ANN). Finally, this paper has presented the conceptual design of a mitigation strategy, which can employ the various detection strategies designed and developed, including that presented.

5. REFERENCES

[1] E. Ahmed, G. Mohay, A. Tickle, and S. Bhatia, "Use of IP Addresses for High Rate Flooding Attack Detection", Security and Privacy–Silver Linings in the Cloud, PP: 124–135, 2010.

[2] L. V. Ahn, M. Blum, and J. Langford, "Telling Humans and Computers Apart Automatically", Communications of the ACM, 47(2), PP: 56–60, 2004.

[3] I. Ari, B. Hong, E.L. Miller, S.A. Brandt, and D.D.E. Long, "Managing Flash Crowds on the Internet", In Proceedings of 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems (MASCOTS), PP: 246–249, IEEE, 2003.

[4] W.J. Blackert, D.M. Gregg, A.K. Castner, E.M. Kyle, R.L. Hom, and R.M. Jokerst, "Analyzing Interaction Between Distributed Denial of Service Attacks and Mitigation Technologies", In DARPA Information Survivability Conference and Exposition, Proceedings, volume 1, PP: 26–36, IEEE, 2003.

[5] C. Bo, B.X. Fang, and X.C. Yun, "A New Approach for Early Detection of Internet Worms Based on Connection Degree", In Machine Learning and Cybernetics, Proceedings of 2005 International Conference on, volume 4, PP: 2424–2430. IEEE, 2005.

[6] G. Carl, G. Kesidis, R.R. Brooks, and S. Rai, "Denial-of-service Attack detection Techniques", Internet Computing, IEEE, 10(1), PP: 82–89, 2006.

[7] J. Cheng, J. Yin, Y. Liu, Z. Cai, and M. Li, "DDoS Attack Detection Algorithm Using IP Address Features", Frontiers in Algorithmics, PP: 207–215, 2009.

[8] D. Gavrilis, I. Chatzis, and E. Dermatas, "Flash Crowd Detection Using Decoy Hyperlinks", In Networking, Sensing and Control, IEEE International Conference on, PP: 466–470. IEEE, 2007.

[9] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of service Attacks", ACM SIGCOMM Computer Communication Review, 31(3), PP:38–47, 2001.

[10] V.A. Siris and F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, Computer Communications, 29(9), PP: 1433–1442, 2006.

[11] X. Xu, Y. Sun, and Z. Huang, "Defending DDoS Attacks Using Hidden Markov Models and Cooperative Reinforcement Learning", In Intelligence and Security Informatics, PP: 196–207, Springer, 2007.

[12] J. Yu, H. Lee, M.S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB using SVM", Computer Communications, 31(17), PP:4212–4219, 2008.

[13] B. Zhang, A. Iosup, J. Pouwelse, and D. Epema, "Identifying, Analysing, and Modeling Flashcrowds in Bittorrent", In Proceedings of Peer-to-Peer Computing (P2P), IEEE International Conference on, PP: 240–249, IEEE, 2011.

Authors Profile:

A.Saraswathi is presently doing Ph.D in P.G. and Research Department of Computer Science, at Government Arts College (Autonomous), Karur, Tamilnadu, India. She has received her B.Sc(Computer Science) degree from Vellalar College for Women, Erode, Tamilnadu, India. She has received her M.Sc degree from Navarasam Arts & Science College for Women, Tamilnadu, India. She has published number of papers in esteemed national/international conferences and journals. Her interests are in Network security and Ad hoc networks.

Dr.K.Thangadurai is presently working as Assistant professor in research and PG Department of Computer science, Government Arts College (Autonomous), Karur. He has Fourteen years of rich teaching experience with 10 years of Research experience in the field of Computer Science. He has worked as the HoD of PG Department of Computer Science at Government Arts College (Autonomous), karur. He has published technical papers in many National and International Conferences and Journals. His areas of interests are Software Engineering, Network Security, Data Mining, etc.,