ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

RI-MADA: AN EFFECTIVE RING MODEL APPROACH TO DEFEND DISTRIBUTED-DOS ATTACK

M.Thanjaivadivel, M.Viswanathan, R.Ganesan, P. Suresh
Department of Computer Science and Engineering, Vel Tech University, Chennai, Tamil Nadu, India.
Department of Computer Science and Engineering, Vel Tech University, Chennai, Tamil Nadu, India.
Department of Computer Science and Engineering, Vel Tech University, Chennai, Tamil Nadu, India.
Department of IT, VelTech Multi Tech Dr.Rangarajan Dr.Sakunthala Engg College,
Chennai, Tamil Nadu, India.
Email: thanjaivadivel@gmail.com

Received on: 04-02-2017 *Accepted on: 11-03-2017*

Abstract

DDoS in other words distributed-denial of service is the most common attack model in the networked system where a single system will be the victim but unfortunately the other systems are also illegally controlled by the Trojan virus. In this paper we are discussing on the various attack models such as, Direct DDoS attack, Reflector based attack, and bandwidth and resource based attack. The proposed solution happens to be the most efficient because it uses, ring model approach and different algorithms for finding and defending the Distributed-DoS attack. Also we can have a detailed knowledge on the various approaches used to detect the D-DoS. The performance evaluation results show us the difference between the other solutions and our proposed solution.

Keywords: D-DoS, Ring model, finding, defending, CBR

1. Introduction

Distributed – DoS attack is the type of attack, where a Trojan is used to infect the series of the networked systems. But the target will be mostly a single system; also the networked systems are controlled and infected by the adversary. So this makes the entire network to cripple. In Distributed-DoS the inward bound traffic causes the overflow the targeted system that starts off from the various numbers of systems that ranges from hundreds and thousands of the systems. This effectively makes it impossible to stop the attack simply by blocking a single IP address, plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin. In order evade these problems we concentrate on the finding of the Distributed-DoS and not the principal vectors itself. Normally in the single

system model the DoS will try packet forging method to distort the data. So our understanding on the DDos and Dos will be, it concentrates the particular node and tries to overflow the traffic data.

The effect of DoS lies on its unique quality of attacking any kind of environment without hassle. Because it doesn't want to utilize any service based flaws of the end node which happen to be the victim. In this paper we are discussing about the most commonly used preventive techniques namely, Intrusion prevention (IP) and Intrusion detection (ID). But it has its own limitation like detecting the adversary when lies closer.

The IP/ID systems may collapse whenever it happens to meet the packets sizes crosses 100's of GB/s. the depletion of resources happen when huge transition of traffic will take place via internet.

2. Background And Literary Work Involved

2.1 Various approaches to find Distributed-Dos

Ever since the DDoS attacks showed up, there have been various approaches to solve the problem. Each approach has its merits and demerits. In this section, we will discuss about the two most prominent approaches.

2.2 Fighting the underlying vectors

This approach aims at curbing the menace at the very sources. The solutions built on this approach proposed anti-malwares and anti-virus solutions to prevent Trojans, thereby stopping the births of botnets themselves [1]. The intriguing part is that the potential victim, which in this case is a server up in the Internet, has no part to play. The administrators of these potential victims would not have much control on the attack prevention system. Another variant of this approach is, counter-attacking the attack sources. When a victim receives more traffic that it can handle, and if it can be established that it is an attack scenario, the anti-malware systems can kick in and check for infections and possible commands from a remote botnet controller. This is very ineffective and tends to delay the mitigation.

There cannot be specialized solutions protecting potential victims. The security infrastructure is 'toothless'. Detecting bot nets is hard and efficient solutions require the presence of the solutions in these hosts, which may raise important ethical and privacy issues. Mitigation is usually much delayed and much damage would have already been done.

2.3 Single IPS approach

Another approach in stark contrast to the approach described in section 4.1.1 is the single IPS/IDS (Intrusion Prevention System/Intrusion Detection System) approach. This is very popular in research circles. The solutions derived using this

approach usually consist of a single IPS located very close to the server being protected. All the requests to the server pass through the IPS, which acts as a filter which filters out detected attacks and sends the server only legitimate requests. The IP/ID systems may collapse whenever it happens to meet the packets sizes crosses 100's of GB/s. The depletion of resources happen when huge transition of traffic will take place via internet. The cost of the solution is usually very high, as each of the server needs to have a dedicated IPs, which can lead to huge maintenance costs, especially if there are standby IPs.

2.4 Literary work involved

In [5], Gil et al proposes, abnormality detection using the volume of the traffic. In here a novel method is implemented using multi level tree for online packet statistics algorithm. It uses a hierarchical level of tree structure which uses statistical data of the packet rate. Usually traffic pattern will be of relatively combination of host and the neighbor nodes. So the attacker will be detected whenever the traffic pattern will go deviated from certain path.

In [6], L. Feinstein et al describe an arithmetical method to shield the Distributed-DoS by studying the entropy and determining the chi square stats of the prevention data. This method separates the source node address in to several containers based on the transmission mode. The chi square algorithm is used to find the source node address where as the transmission methods are kept intact. Now a filter is used to take out the needed packet from the containers. The major drawback we can state in this is, it will not protect when there are any fake packets, because these attacks have a small node address differentiation.

In [7] Lee et al proposes a proponent technique to guess the traffic pattern and the mean deviation value to find out the abnormal changes in the pattern of the traffic. The problem arises whenever any huge and dynamic pattern happens the proponent technique is less effective in terms of accuracy.

In [8] Jiang et al proposes an attacker withstanding technique which will be also forecast the moving traffic pattern. The study on the overall traffic is been made and find out for the deviation occurs in the traffic. So using the forecasting technique it is easier to predict the deviant occur in the pattern of the traffic. Sometimes the real accurate systems are not useful in the real time forecasting because of its working out complexity. However the existing studies will be helpful for detecting the attacker of the cumulative traffic pattern. Whenever a small change occurs it is impossible to study the same.

3. Attack Models of Distributed-DoS

3.1 Direct and Reflector-based Attacks

During a direct attack, spoofed IP addresses are usually involved to prevent attackers from being discovered. As shown in the figure, the attacker directly sends packets with forged source IP addresses to the victim side and tries to periodically establish connections with the victim to exhaust the victim's resources. Such kind of attacks utilizes the inherent weaknesses of some communication protocols, which require the receiver to send feedback to the sender side when it receives packets from senders. The attacker can take advantage of such feedback mechanism to launch an attack. One of the most prevalent DDoS attacks in the past decade is SYN flood attack which belongs to direct attacks.

According to the three-way handshake mechanism of TCP initialization process, the victim server needs to send an acknowledge packet to the sender side. Since source IP addresses of malicious packets are spoofed, the server will never get responses from sender's side. At the same time, the victim server still keeps a large amount of memory and CPU resources for those broken connections. By exhausting the resources of the server, legitimate users cannot access normal services. Compared with the direct attack, the attackers do not send packets directly to the victim but to some reflectors. Both routers and DNS servers can be utilized as the reflectors. The attacker sends packets, which are required to be responded to the reflectors. However, those packets which are sent to the reflectors contain the victims' IP addresses. The reflectors will then send a large number of packets to the victims. The large number of packets will saturate the ingress link of the victim. Such kind of attacks is more dangerous since all the responding packets have no difference compared with legitimate packets and thus it is more difficult to detect[11].

3.2 Bandwidth and Resource Attacks

The DDoS attacks can also be divided as bandwidth attacks and resources attacks in terms of the target of DDoS attacks. For the bandwidth attack, there are usually two types of DDoS attacks, namely, denial of edge service and denial of network service attacks. For the former type, the attackers usually try to saturate the ingress bandwidth of the victim side. The reflector attack belongs to the former type, which can render normal users not able to receive responses from the server on time. During a resource attack, the attacker mainly tries to send a large number of virtual connections in order to exhaust CPU and memory resources of the victim. Since the resource of the host is limited, a large number of broken connections will result in the disability of the server to respond to legitimate users.

Proposed Network Model

3.1 Virtual ring model

The virtual ring gives us the protection shield across the neighboring nodes. Every ring comprised of set of IP's lies equally at the similar distance from each node. Every ip occurrence calculates the cumulative traffic pattern in a certain range.

There are few managers who manages the entire process namely, selection, store and metrics manager. The metrics-manager will follow a simple rule to calculate the frequency. Similarly the detection range's values are being collected by the selection-manager for the sake of variation in the traffic pattern and send it to the store-manager. The store manager will allot the score based on the decision-table. Using an entry level score is taken as the low scale on the potentiality of the attack and will be sent to the downstream IP's so that it will calculate its own score. Similarly the mean score will be taken as the high score and taken as the high risk attack and starts ring level transmission to make sure the attack is calculated based on the real packet rate travelling across the ring. The calculation is based on the node travelling across, known node, evaluated node and the final capacity of the network. The detection technique of the ring based method does not produce any fake results even after the attacker has been detected. Since the whole traffic monitoring is highly impossible the usage of hierarchical level rings and the combination filtering is being suggested.

4. Algorithm used for Attack Detection and Attack Mitigation

The collaboration manager who calculates the respective packet using some predefined rule by calculating the consumption of bandwidth at the last transmission. If the calculated rate ig higher than the predefined higher rate than the alert will be given else it will be sent to the next IP's across the ring. The final step in the process of detecting the attack is the collaboration manager.

The detection of the most anticipated flood attack will be confirmed only whenever the traffic is higher than the network designated capacity. To trigger an alert the capacity has to be calculated between the predefined typical traffic and the actual traffic occurred along the network. Whenever an IP's gets a communication to compute the accumulated packet value for the setoff rules. It will check whether the request came from the same originator. If yes, then that particular communication won't be a possible attack. On the other hand it calculates a new value by adding the self rate to check whether the minimum capacity is reached or not.

```
checkRule (IPS_id, i, rate_i, cap_i)

 1: if b_i ∧ (IPS_id ≠ null) then
 2:     if IPS_id == myIDthen
 3:         b_i = false;
 4:         return
 5:     else
 6:         rate_i ← rate_i + F_i
 7:         if rate_i > cap_i then
 8:             b_i = false;
 9:             raise DDOS alert;
10:             return
11:         else
12:             nextIPS.checkRule(IPS_id, i, rate, cap_i)
13:         end if
14:     end if
15: else
16:     b_i = true;
17:     nextIPS.checkRule(myID, i, 0, cap_i)
18: end if
```

Fig5.1 Algorithm Used for Attack detection.

```
mitigate (r_i, firstRing)

 1: for all ips ∈ upstreamIPSs do
 2:     ips.mitigate(r_i, False)
 3: end for
 4: for all a ∈ getAddr(r_i) do
 5:     block_IPs(a)
 6: end for
 7: if firstRing = True then
 8:     nextIPS.mitigate(r_i, True)
 9: end if
10: setCautiousMode(r_i)
```

Fig 5.2 Algorithm Used for Attack Mitigation.

5. Evaluation environment and Result analysis

The environment is created and simulated in network simulator 2 (NS-2) to evaluating the performance of the algorithm used in this paper. The experimental setup includes source node, intermediate routers and destination nodes. The numbers of the above nodes used are 3,2 and 1 respectively.

The traffic flow of 40 Constant Bit Rate (CBR) at an interval of 0.20 seconds and the attacker starts his attack flow literally every micro second. The result set will be compared based on efficiency of the packet received at particular interval.

Entropy Calculation is based on the following:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

Where P (xi) = (Number of attack or normal packet)/ Total No of packet.

Trace Data:

Time Interval	Normal Packet			Attack Packet			Normalize Entropy
	M1	M2	M3	M1	M2	M3	
0 - 0.5	25	38	32	91	78	101	1.54
0.5 - 1.0	38	29	4	131	148	431	0.98
1.0 – 1.5	39	31	8	104	126	396	1.03
1.5 – 2.0	27	32	29	132	112	142	1.32

Metrics:

The True positive Value(TPVs) will check for the attack detected at the time of the simulation similarly the False Positive Values (FPV) are the right nodes which is wrongly marked as attacker. The factor involves is the number of rules applied should be minimum and the horizontal check will rule out the possibility of being the false positive values. So the entire process will works on the two values.

6. Conclusion and Future Enhancements

The proposed solution is happens to be scalable and it does the detection at the early level of the network flooding. This paper details about the various attack models and the current approaches to detect the Distributed-DoS attacks. The working style of the ring level approach and the various algorithms are as below. The hierarchical ring level proven to be efficient to shielding the nodes and protect the same. Separate algorithms are written to detect and mitigate the attacks and give us the desired performance and clarity in the nodes and works well over ISPs.

The future enhancement will lies without disturbing the architecture of the proposed solution and can be enhanced using more levels of the IPs rule and further addition to the existing rules can be a great upgrade.

References

1. Yang-Seo Choi, et al., “Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention. Information Technology Convergence and Services (ITCS)," 2010 2nd International Conference, pages 1 - 6, 23 September 2010.
2. Yao Chen, et.al “Detecting and Preventing IP spoofed Distributed DoS Attacks” International Journal of Network Security,Vol.7(1), pages 70 - 81, July 2008.
3. M.Viswanathan, et.al., “Document Detection of flood attacks in DTN using rate limiter technique” Journal of Computer Science, Vol.10(7), Pages 1216-1221, 2014.

4. Mopari, I.B.et.al., "Detection and defense against DDoS attack with IP spoofing". Computing, Communication and Networking, 2008. ICCCN 2008. International Conference, pages 1 – 5, 24 February 2009.
5. T.T. Gil and M. Poleto, "Multops: A Data-Structure For Bandwidth Attack Detection," in Proceedings of 10th Usenix Security Symposium, 2001, pp. 23-38.
6. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response." in Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, April 2003, pp. 303-314.
7. S. Lee, H. Kim, J. Na, and J. Jang, "Abnormal traffic detection and its implementation," Advanced Communication Technology, vol. 1, February 2005, pp. 246-250.
8. J. Jiang and S. Papavassiliou, "Detecting network attacks in the internet via statistical network traffic normality prediction," Journal of Network and System Management, vol. 12, no. 1, 2004, pp. 51-72.
9. Jieren Cheng; Jianping Yin ; Yun Liu ; Zhiping Cai ; Chengkun Wu. "DDoS Attack Detection Using IP Address Feature Interaction". 2009 International Conference on Intelligent Networking and Collaborative Systems, pages.113 - 118, 4-6 Nov. 2009.
10. El Defrawy et.al., "Optimal Allocation of Filters against DDoS Attacks" . Information Theory and Applications Workshop, 2007, pages 140 - 149, Jan. 29 - 2 Feb. 2007.
11. Tao Peng, et.al., "Protection from distributed denial of service attacks using history-based IP filtering" 2003 IEEE ICC '03, Vol.7, No.1, pages 482-486, May 2003.