Methodologies to prevent DDOS Attacks using Clustering algorithm during Peak Hours of Server – Probabilistic Packet Marking (PPM)

[1]M.Padmavathy M.Sc. (CS)., M.Phil., [2]Dr. M. Ramakrishnan, M.E., Ph.D., Ph.D.
[1]*Research Scholar, Department of Computer Applications, School of Information Technology, Madurai Kamaraj University, Palkalainagar, Madurai – 625021.*
[2]*Professor and Head Department of Computer Application, Chairperson - School of Information Technology Madurai Kamaraj University, Madurai – 625 021.*

Abstract:
In the tremendous growth of internet world, networking communications play an important role. Network communication is one of the sharing of information between server and clients. But in today fast technology, the number of clients has increased and consequently the server is unable to send the response to all the legitimate clients in time. It may also happen due to the attack of intruders. So the prevention of this kind of attacks is the important aspect throughout the network communication. Specifically, unsupervised data mining clustering techniques allow to effectively distinguishing the normal traffic from malicious traffic in a good accuracy. In this paper, a bird view for a set of probabilistic packet marking methodologies has been discussed to prevent the DDOS attacks using clustering algorithm during peak hours of server. These various methodologies are useful to find the IP address of clients and find the intruders among them depending upon the client's behavior. And also we envision DDoS attack starts when network traffic is more than our default threshold. In this type of packet marking protocol, packets are marked based on predefined probability.

Key words: *Server, DDOS attacks, Intruders, Probabilistic Packet Marking (PPM), Clustering, Peak hours.*

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are the important and oldest Internet threats and continue to be the top risk to networks around the world. As protections have evolved, the technology used by hackers has adapted and has become much more sophisticated. The financial services industry is one of the largest targets of cyber criminals for DDoS attacks followed closely by the government sector (4). Besides disrupting Internet operations through a brute-force data onslaught, DDoS attacks have recently been used to hide more sophisticated attempts to break into financial and e-commerce information. These attacks often have the intent of disrupting operations mostly through the destruction of access to information (7). Service providers are routinely expected to prevent, monitor and mitigate these types of attacks which occur daily on their networks. Packet marking is one of the classified methods of IP Trace back. Packet marking techniques allows router to inscribe their IP on incoming packets either deterministically or probabilistically. By collecting and analyzing the marked packets, victim should able to reconstruct the attack path leading back to the nearest source of attack. Identifying D(DoS) attacks and defending against them are one of the network security's gravest concerns to protect vital services and information. Recently, several schemes proposed to detect and/or prevent such attacks which are known as IP Trace back.

The majority organizations spend a lot of time and effort to choose a DDoS mitigation solution, however often they don't provide the same level of diligence in testing their defenses. Many approaches are used to choose various prevention methods (7). Whatever approach chooses, the most important element of testing is to create realistic scenarios based on your unique valid user traffic. Understanding what attacks are blocked is important only in the context of determining whether legitimate traffic gets serviced acceptably. Should the defenses block all traffic, good and bad, the DDoS attack might be stopped, but the end result to the company might be catastrophic losses (5). Expectation levels for service providers are also increasing as companies revenues are directly tied to having reliable connectivity to the Internet. The financial industry is especially susceptible to DoS/DDoS attacks as millions of consumers move

to electronic bill payments, purchases and on-line banking. DoS/DDoS monitoring and black hole filtering are becoming entry level requirements for service providers to sell Internet services in the financial industry.

The rest of the paper is structure as follows; section 1 provides internet security attacks and its basic information's. Section 2 embraces the various existing papers which are based on DDoS attacks mechanisms. It is followed by section 3 includes the various security issues and the general remedy solutions are also discussed in this section. The next section 4 contains the DDoS attacks preventing mechanisms depend upon its classification. Finally section 5 brings to a close with conclusion of the Distributed Denial of Service (DDoS) attacks and its simple remedies to solve the security issues due to its peak hours of internet processing.

2. RELATED WORKS

In 2014, Darshan Lal Meena and Dr.R.S.Jadon (2) has described the nature of the problem in DDoS attacks and look for its root causes, further presenting brief insights and suggested approaches for defending against DDoS. The authors point out both the positive and negative sides of each potential solution in DDoS. They also give a brief summary of what has realistically been achieved so far, as well as what the key missing components still. In this paper, they present a classification of available mechanisms that are proposed in literature on preventing Internet services from possible DDoS attacks and discuss the strengths and weaknesses of each mechanism. The authors say this paper provides better understanding of the problem and enables a security administrator to effectively equip the problem with proper prevention mechanisms for fighting against DDoS threat.

In 2013, Sreeja Rajesh (9) have captured a mechanism to the normal flash crowd event pattern is introduced and the App- DDoS attack monitoring, detection and then blocking of further attack is implemented. An effective method is introduced to identify whether the surge in traffic is caused by normal Web surfers or by App-DDoS attackers in this paper. Access Matrix (AM) is defined to detect App-DDoS attacks based on user logs and threshold value. Hidden Markov model is used to detect App-DDoS attack based on user behavior. The author says this method reveals early attacks merely depending on the threshold specified, user logs, user behavior and gives all the privilege for administrator who can effectively identify and block the connections for specified attacking host. Measures can be devised to check for IP spoofing as an additional detection process.

In 2013, John Burke (6) provided attacks methods for DDoS attacks and DDoS. Attacks are on the rise, with serious implications for any enterprise or entity connected to the Internet. The sophistication of the attacks evolves continually, and the thousands of botnets now in existence comprise millions of zombie systems. The intensity, scale, and scope of attacks can overwhelm and disable any size Web presence; no company or government is immune. The primary choice is whether to implement an on-premises DDoS defense (DIY) or to enroll in a cloud---based DDoS service. For organizations requiring DDoS protection, and barring specific strategic or other concerns, the unique nature of DDoS and the significant differences between DIY and cloud-based defense favors service in the cloud.

In 2013, Muhammad Aamir and Mustafa Ali Zaidi (8) have discussed a study which can be helpful for readers and researchers to recognize better techniques of defense in current times against DDoS attacks and contribute with more research on the topic in the light of future challenges identified in this paper. In this paper, the authors presented a review on Distributed Denial of Service attack and defense techniques with an emphasis on current DDoS defense schemes based on entropy variations and other traffic anomalies, neural networks and application layer DDoS defense. Some traditional techniques such as Traceback and packet filtering have also been covered in the discussions. They found that new attack techniques have been introduced with sophisticated DDoS attack tools such as botnet fluxing, GET floods and reflector attacks. With such enriched attacks, the defense is even more challenging especially in the case of application layer DDoS attacks where the attack packets are a form of legitimate-like traffic mimicking in the events of flash crowds.

3. SECURITY ISSUES IN DDoS ATTACKS

Current Internet design focuses on effectiveness in moving packets from the source to the destination. This design follows the end-to- end paradigm: the intermediate network provides the bare minimum, best-effort packet forwarding service, leaving to the sender and the receiver the deployment of advanced protocols to achieve desired service guarantees such as quality of service, reliable and robust transport or security (1). The end-to-end paradigm pushes the complexity to end hosts, leaving the intermediate network simple and optimized for packet forwarding. There is one unfortunate implication. If one party in two-way communication (sender or receiver) misbehaves, it can do arbitrary damage to its peer. No one in the intermediate network will step in and stop it, because Internet is not designed to police traffic. One consequence of this policy is the

presence of IP spoofing another one is DDoS attacks. The Internet design raises several security issues concerning opportunities for DDoS attacks (1).

The following security issues (9) are raised the internet design, the issues are as follows,

a. Internet security is highly interdependent - DDoS attacks are commonly launched from systems that are subverted through security-related compromises. Regardless of how well secured the victim system may be, its susceptibility to DDoS attacks depends on the state of security in the rest of the global Internet.

b. Intelligence and resources are not collocated - An end-to-end communication paradigm led to storing most of the intelligence needed for service guarantees with end hosts, limiting the amount of processing in the intermediate network so that packets could be forwarded quickly and at minimal cost. At the same time, a desire for large throughput led to the design of high bandwidth pathways in the intermediate network, while the end networks invested in only as much bandwidth as they thought they might need. Thus, malicious clients can misuse the abundant resources of the unwitting intermediate network for delivery of numerous messages to a less provisioned victim.

c. Accountability is not enforced - IP spoofing gives attackers a powerful mechanism to escape accountability for their actions, and sometimes even the means to perpetrate attacks.

d. Control is distributed - Internet management is distributed, and each network is run according to local policies defined by its owners. The implications of this are many. There is no way to enforce global deployment of a particular security mechanism or security policy, and due to privacy concerns, it is often impossible to investigate cross-network traffic behavior.

3.1 DDOS DETECTION USING CLUSTERING DATA MINING

All printed material, including text, illustrations, and charts, must be kept within the Firewall device may not detect and prevent many types of DDoS attack passing through the network traffic because of its security weakness. In DDoS attacking time, attacker may carry out the attack packet with genuine packets which cause more harmful to the victim and difficulty for firewall in detection for this type of attack. Moreover, the attacker uses spoofed IP causing the tracing process more difficult (7). DDoS attack can be implemented through many layers of TCP/IP layers. UDP/ICMP flooding attacks send a large number of UDP/ICMP packets to the victim who limits the communication link and make overall congestions. Web server may attack with HTTP GET flood attack which causes Denial of Service (DoS) attack by repeatedly request to download the web page (8). A little CPU consumption and space complexity is involved in this hybrid method by testing each testing data point with max-min rules to differentiate the legitimate and malicious traffic.

3.1.1 ASA

In DDoS attacks ASA is one of the types to protect some storage level encryption, it also reduce the bandwidth. Cisco provides Adaptive Security Appliance (ASA) firewall which is capable to use in packet filtering, packet inspection against the attacks like Access Attacks, Reconnaissance Attacks, and Denial of Service (DoS) attacks (10). Cisco ASA-5510 Intrusion Prevention System is one of the firewall mechanism to preventing DDoS attacks. This system provides security to the private networks from many threats on the Internet that already exist and also from the zero day threats. The Denial of Services attacks are over Internet from many years, and there is a lot of research work going on in defending against these attacks. It is hypothesized that mimicking natures principles, and is not its epiphenomena, leads to better algorithms. The popular Cisco ASA-5510 intrusion prevention system, which is a latest technology and has built in security features for Denial of Service attacks.

Cisco ASA threat detection consists of different levels of statistics gathering for various threats, as well as scanning threat detection, which determines when a host is performing a scan. Administrators can optionally shun any hosts determined to be a scanning threat.

Threat detection statistics can help administrators manage threats to the Cisco ASA; for example, enabling scanning threat detection provides statistics to help analyze the threat. Administrators can configure two types of threat detection statistics:

Basic threat detection statistics: Include information about attack activity for the system as a whole. Basic threat detection statistics are enabled by default and have no performance impact.

Advanced threat detection: Statistics track activity at an object level so the Cisco ASA can report activity for individual hosts, ports, protocols, or access lists. Advanced threat detection statistics can have a major performance impact, depending on the statistics gathered, so only the access list statistics are enabled by default.

3.2 GENERAL REMEDY APPROACHES IN DDoS

This section provides the general remedy approaches in DDoS attacks on internet system security. The remedy approaches (5) are as follows,

Allow connections to trusted clients only - This is clearly the most conservative approach to communication and as such it has the highest degree of averting security threats. Such a solution is justifiable for deployment only in closed and special-purpose (e.g. military) environments. It is inherently inapplicable and incompatible to an open communication system such as the Internet (5). A known problem with closed environments is that outside intrusions are both not expected and commonly not anticipated. So, the level of preparedness for a security breach, should it ever occur, is very low and the damage grows proportionally high.

Mitigating the effect of the attack on the victim - While the utmost goal is to avoid being attacked, when and if this happens it is highly desirable to be able to sustain some level of (degraded) performance during the high load, even prior to the actual detection of an attack (10). The following approaches try to achieve this goal in different ways.

Secure all computers on a network: Achieving that would render the existence of zombies impossible and hence an attacker would be reduced to being able to mount only a Unisource attack. In addition, IP trace back schemes would directly lead to the attacker's weapon machine, which in turn would both reduce the management overhead in the post-mortem tracing process and serve as a disincentive for the attacker to start in the first place (3).

Ingress filtering - This approach is describe details in next section targeted at reducing or completely eliminating the ability to forge source addresses, which if accomplished would ultimately result in much easier tracing back to the true source of an attack and as such would serve as a significant deterrent for attackers (5).

3.3 PROPOSED ALGORITHM FOR PROBABILISTIC PACKET MARKING

In this section, we present our new integrated algorithm which is efficient in reducing false positive ratio and convergence time. First, we explain the marking mechanism and pseudo code of the algorithm and then the reconstruction algorithm steps are as follows.

a. Marking algorithm

Based on previous researches fixed marking probability is the main problem of PPM. Different methods were introduced to fix this issue but unfortunately none of them could succeed to resolve the issue completely. According to, dynamic probability could somehow solve the problem of low accuracy (4). But it still needs improvement in other aspects. In simple terms, our aim is to design an approach, which would remarkably reduce the false positive rate in multi-source attacks using dynamic probability. We assume that not all incoming packed are marked probability. Instead, we consider routers to be marked either with p=1 or p=1/d . If it has been marked before then the marking probability will be changed to 1, this helps the prevention of being overwritten by downstream routers otherwise it should be marked with p=1/d. (note that d is the distance of router from victim (9).

In marking mechanism in spite of exploiting dynamic probability, we used another method to reduce the false positive rate. Because of the problem in addressing DDoS attacks and also adding authentication function, we suggest TTL coding which is discussed in (6). So, in case of receiving packets from the same distance we will consider TTL value which should be the same in all incoming fragments. The pseudo code of the scheme explained in following.

Marking Algorithm

Let x be a random number [0…1)
IP[c]={ip[0] , ip [1] , ip [2] , ip [3]}
If x < p & w.flag=0 then Write router‟ s address into w.start
TTL=f2 (IP)mod 256
If TTL<30 then TTL
w.flag=1 & p=1/d
w.start=c++(mod4)
Node[c] □ IP[c]
else
If w.flag=1 then P=1
endif d++
end if

b. Reconstruction procedure

The Second part of our method is to detect and reconstruct the attack path by collecting marked packets. So, in this step we have to reassemble these fragments to map the attack path. All incoming packets are clustered according to their distances (8). Also, Packets with same distances goes to the appreciate cluster based on their TTL.

Reconstruction Algorithm

Let Node.tb1 be a table of (node , distance , TTL)
For each packet w from attacker
Z:=look up w.node in node tb1
If Z<> null then
Insert tuble(w.node ,1) in node tb1
If TTL(w.node)mod 256 = TTL+d or ttl+d- 30
then
Sort node tb1 by distance and by TTL value Extract path (Ri ….R j) from ordered node fields in node tb1

4. DDoS ATTACKS PREVENTING MECHANISMS

Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes (9). Attack prevention schemes are not enough to stop DDoS attacks because there are always vulnerable to novel and mixed attack types for which signatures and patches are not exist in the database. It also provides to control the attacks on the system peak hours also.
The prevention of DDoS attacks techniques can be broadly divided into two categories (9) such as,
1. General techniques: These are some common preventive measures. For example, system protection, replication of resources etc. That individual servers and ISPs should follow so they do not become part of DDoS attack process.

1.1. Disabled unused services
The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks (10).
1.2 Install latest security patches
In today world, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system.

1.3 Global defense infrastructure
A global deployable defense infrastructure can prevent from many DDoS attacks by installing filtering rules in the most important routers of the Internet. As Internet is administered by various autonomous systems according their own local security policies, such type of global defense architecture is possible only in theory.
1.4 Disabling IP broadcast
Defense against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will be successful only if host computers and all the neighboring networks disable IP broadcast.
1.5 Firewalls
Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses.

2. Filtering techniques: which include ingress filtering, egress filtering, router based packet filtering, history based IP filtering, SAVE protocol etc (3).

2.1 Ingress/Egress filtering
A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge. One technique known as reverse path filtering can help to build this knowledge.

2.2 Router based packet filtering
It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated.
2.3 Capability based method
Capability based mechanisms provides destination a way to control the traffic directed towards itself. In this approach, source first sends request packets to its destination. Router marks (pre-capabilities) are added to request packet while passing through the router. The destination may or may not grant permission to the source to send (3). If permission is granted then destination returns the capabilities, if not then it does not supply the capabilities in the returned packet.

5. CONCLUSION

In network communication system DDoS attacks is the main attack to attempt the network processing and collapse or destroy the processing. So the entire processing is terminated, if it an important transaction the users losses their data and other things. So the prevention is the main to protect the network system throughout its processing. In this paper we contributed to the design and implementation of efficient and optimized Packet Making Algorithm. As mentioned previously, probabilistic packet marking (PPM) has a high false positive ratio and also does not perform well in the event of DDoS attacks. To overcome the limitations of PPM that we have mentioned, we used dynamic marking probability in order to reduce the convergence time and rate of false positive. In this paper, a security issues which are possible to attack the internet processing is also discussed. And also this paper offers a set of remedy solutions to protect the network communication system. This paper gives a bird view of the methodologies which are used to prevent the DDoS attacks during the peak hours of server. This study helps to presents a better way of remedy method to help the prevention of attack.

References

1. T. Anderson and T. Roscoe, "Preventing Internet Denial-of-Service with Capabilities," In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44.
2. Darshan Lal Meena and Dr.R.S.Jadon, "Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches", IJARCSMS,Volume 2, Issue 4, April 2014, pp. 183-197.

3. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Telecommunications Networking, vol. 44, no. 5, Apr. 2004, pp. 643– 666.
4. B. B. Gupta and R. C. Joshi et al. International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163.
5. Incident Note IN-2004-01 W32, Novarg. (2004). A Virus. CERT. [Online]. Available: http://www.cert.org/incident_notes/ IN-2004- 01.html.
6. John Burke, "Defense for Distributed Denial of Service Attacks", Nemertes Research, 2013, www.nemertes.com, 888---241---2685, DN2400, pp.1-9.
7. J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," Computer Journal of ACM IGCOMM, vol. 4, no. 2, 2004, pp. 39-53.
8. Muhammad Aamir and Mustafa Ali Zaidi, "DDoS Attack and Defense: Review of Some Traditional and Current Techniques", https://www.jstage.jst.go.jp/article, DOI: 10.4036/iis.2013.173, pp.1-19.
9. Sreeja Rajesh, "International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013, pp. 555-558.
10. Y. Xie and S. Z. Yu, "Monitoring the Application-Layer DDoS .Attacks for Popular Websites," in Proc. Networking, IEEE/ACM Transactions, Feb. 2009, pp. 15-25.