ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON DISTRIBUTED DENIAL OF SERVICE ATTACK AND DEFENCE

Divya Bhavasar
Master of computer engineering, ParulInstituteof EngineeringandTechnology, India

Abstract

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS)attack is an attempt to make a machine or network resource unavailable to its intended users.DOS attack reduces the efficiency of the server, inorder to increase the efficiency of the server itis necessary to detect the dos attacks. the reliability and security of the Internet not only advantages on-line businesses, but is also an issue for national security. In today's fast growing of internet usage the security of the data, resources and other confidential files are more important aspects. There are so many types of DDoS attacks occurred by attacker on network.DoS causes serious damages to the services running on the victim. Therefore, effective detection of DoS attacks is essential to the protection of online services. Work on DoS attack detection mainly focuses on the development of network-based detection mechanisms. To meet the increasing threats, more advanced defenses are necessary.

Keywords: Network Security, Distributed Denial of Service , Denial of Service .

INTRODUCTION

Importance of network security[10]

- To secure the confidential data
- To prevent computer against unauthorized access by attacker
- To maintain the stability of network bandwidth
- To maintain communication between legitimate computers

Layer wise Attacks on Networks[1]

Table 1 : Layer wise Attacks on Networks[1]

Layer	Example of Attack
Application Layer	Repudiation, Viruses ,Malicious URLs
Transport Layer	Session Hijacking
Network Layer	Distributed Denial DoS (Denial of Service), Information Disclosure Spoofing Attack of Service , Packet Replication
Physical Layer	Cable Cut, Jamming
Data Link Layer	Flooding Attacks
Multiple Layers	Denial of Service Attacks

A Distributed Denial of Service (DDoS) attack uses many computers to launch a large scale coordinated DoS attack against one or more targets. DDoS attack has the capability to exhaust victim's computing and communication resources within a short period of time[8].

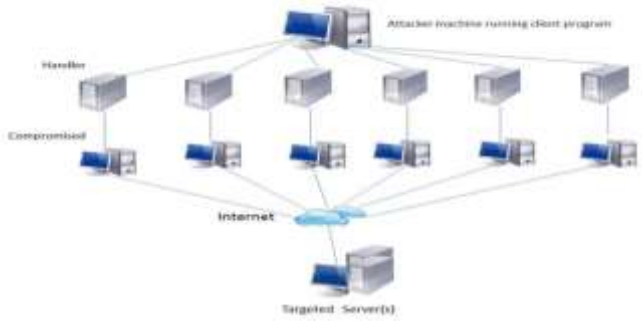

Figure 1: DDoS Attack Scenario[8]

The Distributed Denial of Service (DDoS) attack is a bandwidth attack, where attack traffic is directed from multiple distributed sources. The attack power of a DDoS attack is based on the huge number of sources. Hence, the DDoS attack can consist of all types of traffic. There are two common scenarios for DDoS attacks, typical DDoS attack and the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

distributed reflector denial of service (DRDoS) attack.

Typical DDoS attack contains two levels. The first is to compromise weak systems available in the Internet and install attack tools in these compromised systems. This is known as turning the computers into zombies. Second, the attacker sends an attack command to the zombies through a channel to launch a attack against the victim. The attack traffic is sent from the zombies to the innocent third-parties. The attack traffic could use genuine or spoofed source IP addresses.

There are two major motivations for the attacker to use randomly spoofed IP addresses:
(1) to hide the identity of the zombies and reduce the risk of being traced back;
(2) to make it hard to filter this type of traffic without disturbing the legitimate traffic.
In this Paper , we propose several novel defense mechanisms against this type of attack.

Attackers Motivations for doing the DDoS attacks:
DDoS attackers are usually motivated by various incentives. We can categorize DDoS attacks based on the motivation of the attackers into five main categories[8]:

• Financial/economical gain: These attacks are problematic for corporations. Because of the nature of their malicious thoughts, attackers are generally the technical and the experienced attackers. Attacks that are done for financial gain are mostly the most harmful and hard-to-stop attacks.

• Revenge: Attackers of this category are generally frustrated individuals, possibly with lower technical skills, who usually carry out attacks as a response to a perceived injustice.

• Ideological belief : Attackers who belong to this category are motivated by their ideological beliefs to attack their targets. This category is currently one of the major incentives for the attackers to launch DDoS attacks.

• Intellectual Challenge: Attackers of this category attack the targeted systems to experiment and learn how to launch various attacks. They are usually young hacking enthusiasts who want to show off their capabilities. Nowadays, there exist various easy to use attack tools and botnets to rent that even a computer amateur can avail of in order to launch a successful DDoS attack.

• Cyberwarfare: Attackers of this category usually belong to the military or terrorist organizations of a country and they are politically motivated to attack a wide range of critical sections of another country. Executive civilian departments and agencies, private/public financial organizations energy/water infrastructures and telecommunications and mobile service providers.

Network level DDoS flooding attacks:
These attacks are launched using UDP, TCP,ICMP protocol packets. The types of attacks in this category are as follows[10]:

Flooding attacks: Attackers focus on disturbing genuine user's connectivity by exhausting victim network's bandwidth.

• Protocol take advantage ofation flooding attacks: Attackers takes advantage of specific features or implementation bugs of some of the victim's protocols in order to consume the victim's resources (e.g., TCP SYN flood, TCP SYN-ACK flood, ACK & PUSH ACK flood and etc).

• Reflection-based flooding attacks: Attackers generally send forged requests (e.g., ICMP echo request) instead of direct requests to the reflectors; so, those reflectors send their replies to the victim and consumes victim's resources (e.g., Smurf and Fraggle attacks).

• Amplification-based flooding attacks: Attackers take advantage of services to produce multiple messages for each message they receive to increase the traffic towards the victim. Botnets have been frequently used for reflection and amplification purposes. Reflection and amplification techniques are generally used as Smurf attack where the attackers send requests with spoofed source IP addresses (Reflection) to a large number of reflectors by take advantage of spoofing IP broadcast feature of the packets (Amplification).

- Distributed Denial of Service (DDoS) Attack on Network:

A distributed denial of service attack (DDoS) involves sending forged requests of some type to a more number of computers that will reply to the requests. Using Internet Protocol address spoofing,

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

the source address is set to that of the targeted victim, which means all the replies will go to the target.[8]

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby seducer hosts to send Echo Reply packets to the victim.[8]

Types of Distributed Denial of Service (DDoS) Attacks

DDoS types[8]:

ICMP is the language used by computers on the Internet to talk to each other about errors and other status related issues. Whilst they are generally considered to be low priority messages, some ICMP messages perform an important role. Others are less important and can be easily filtered. Generally ICMP messages used in a DDoS attack can be easily filtered although it is easy to blast out large volumes of packets using this protocol as there is no built in flow control mechanism.

TCP is the language that computers use to order their data that needs to be in defined, ordered streams – when you have to make sure you get it all completely right, all the time such as with web browsing or email. It is slightly harder to use TCP for DDoS attacks as you have to prevent the management of the connection to speed up the flow of attacking packets.

UDP is another way for computers to transfer data but it is one that is used for data that does not need to be in a reliable stream; it does not matter if some of it gets lost en route or delivered out of sequence as . the stream moving along fast and you cope with a few lost packets.

Again, as with ICMP packets, it is relatively easy to use UDP for blasts of DDoS packets as there is no built in mechanism to control the rate that packets are sent at. UDP is often used for streaming videos, VoIP phones and Domain Name System (DNS) queries[8].

- ICMP ping flood
- UDP food
- Smurf attack
- SYN Flood
- GET Request
- Frag Flood
- DNS Amplification Attack

LITERATURE SURVEY

1 A System For Denial-of-Service Attack detection based on Multivariate Correlation Analysis[1]

Multivariate correlation analysis algorithm for detection of denial of service,
Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers.

A DoS attack detection system is proposed that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features.

MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition.
This makes the proposed solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.

A triangle-area-based technique is proposed to enhance and to speed up the process of MCA.
System Architecture :

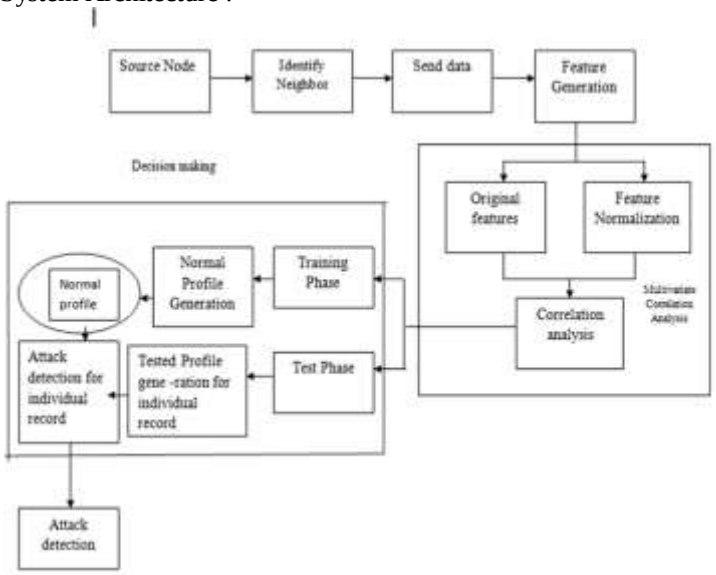

Figure 2: System Architecture of Existing System[1]

2.Network-based detection systems

Network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. Network-based detection systems can be classified into two main categories

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Misuse-based detection systems :
It detects attacks by monitoring network activities and looking for matches with the existing attack signatures. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks.

Anomaly based detection :
It monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly-based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities.

Feature correlation analysis :
An algorithm to discriminate DDoS attacks from flash crowds by analyzing the flow correlation coefficient among suspicious flows.
A covariance matrix based approach was designed to mine the multivariate correlation for sequential samples.

Disadvantages :
Misuse based detection systems is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise.

Anomaly-based detection systems commonly suffer from high false positive rates because the correlations between features/attributes are intrinsically neglected or the techniques do not manage to fully exploit these correlations.

Feature correlation analysis can only label an entire group of observed samples as legitimate or attack traffic but not the individuals in the group.

3 Analyzing well-known countermeasures against distributed denial of service[5]
Classifies DDos defence techniques based on defence points defence methods can be classified in four categories:

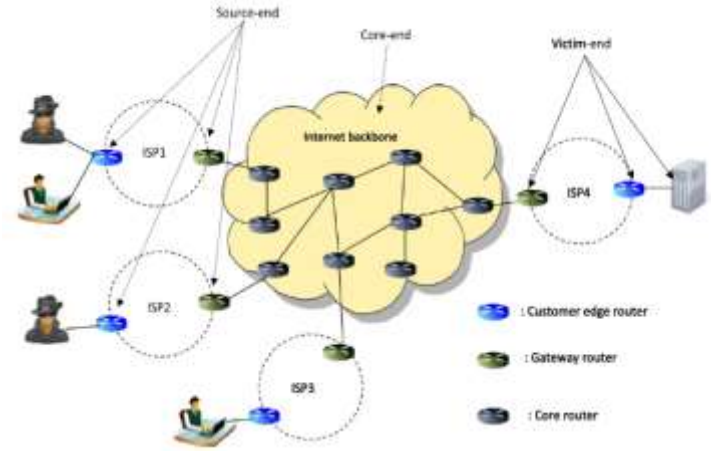

Figure 3: Defense points[5]

1. Source-end defence techniques
Source-end defence points are the best points to filter or rate-limit malicious traffic because minimum damage occurs for valid traffic.

2. Core-end defence techniques
In these techniques any core route independently tries to detect malicious traffic and then filter or rate-limit the traffic.

3. Victim-end defence techniques
Victim-end defence points can easily separate DoS traffic from valid traffic. The major problem with victim-end defence techniques is that victim-end defence points are not good points for rate-limiting or filtering attack traffic because the bandwidth might be saturated.

4. Distributed defence techniques
Source-end points are promising points to rate-limit or filter malicious traffic; core-end points are promising points to only rate-limit traffic regardless of type of traffic and finally victim-end points are promising points to detect and discriminate DoS traffic from valid traffic. So, a cooperative mechanism between source-end and victim-end, or between core-end and victim-end, or between source-end, core-end and victim-end can be favourite defence techniques against DDoS attacks.

4 Packet track and trace back mechanism against denial of service attacks[9]
packet track and traceback mechanism to detect ddos attack which features rapid response and high accuracy. The denial of service attack is a main type of threat on the Internet today.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

On the basis of path identification (Pi) and Internet control message protocol (ICMP) traceback (iTrace) methods, a packet track and traceback mechanism is proposed. routers apply packet marking scheme and send traceback messages, which enables the victim to design the path tree in peace time. During attack times the victim can trace attackers back within the path tree and perform rapid packet filtering using the marking in each packet.

5 Detection on Application Layer DDoS using Random Walk Model[2]

Application layer asymmetric DDoS attack has the characteristics of low-rate, genuine IP address and real request, which is very different from previous DDoS attacks.

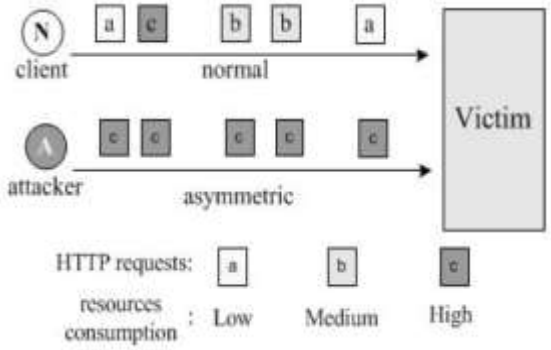

Figure 4: Aysmmetric HTTP-request attack model[2]

The attackers its use page request sequence to describe the user browsing behaviour, and then detect the attackers based on analyzing their sequences similarity.

Then model the user browsing behaviour as a page request sequence, and construct the random walk graph based on the page request sequence. After training the random walk model, we get the page transition probability, and predict the user's subsequent page request sequence.

Then calculate the similarity between the predicted page request sequence and observed sequence in the subsequent observation period and use it to judge whether the user is an attacker or a legitimate one.

6 A Multi-Queue Algorithm for DDoS Attacks[3]

Algorithm for gateway and router to prevent DDoS attacks. The algorithm combines two simple congestion control methods. Simulation results show that our algorithm efficiently increases the throughput of normal flows under DDoS attacks comparing to common Drop Tail algorithm.

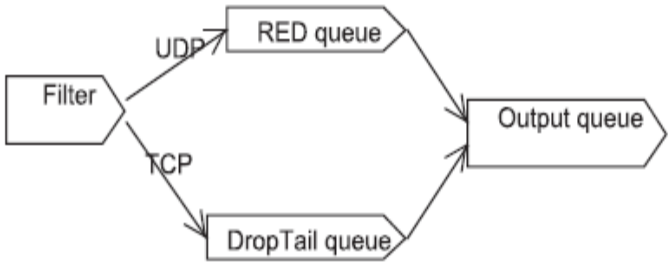

Figure 5: Structure of the algorithm[3]

1.Drop Tail algorithm

Drop Tail algorithm implement in the link with responsive flow for detect the TCP packet flow. Drop Tail became a failure since unresponsive UDP packets will occupy most of the queue there by causing responsive flows packets to be drop.

2.Random Early Detection (RED)

Random Early Detection is implemented on the unresponsive flow link. For detect the UDP packet Flow . The objective of this mechanism is to minimize packet loss and queuing delay, maintain high link utilization and remove biases against burst sources. It is implemented on a router or gateway to control congestion caused by DDoS.

7 Bro: A System for Detecting Network Intruders in Real-Time[11]

Bro, a stand-alone system for detecting network intruders in real-time by passively monitor a network link on which the intruder's traffic transits.

An overview of the system's design, which emphasizes high-speed (FDDI-rate) monitoring, real-time notification, clear difference between mechanism and policy, and extensibility. To achieve these ends.

Bro is divided into an "event engine" that reduces a kernel filtered network traffic stream into a series of higher level events, and a "policy script interpreter" that interprets event handlers written in a specialized language used to express a site security policy. Event handlers can update state information, synthesize new events, record information to disk, and generate real-time notifications via syslog. We also discuss a number of attacks that attempt to subvert passive monitoring systems and defenses against these, and give particulars of how Bro analyzes the four

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

applications integrated into it : Finger, FTP, Portmapper and Telnet. The system is publicly available in source code form.

8 Parametric Methods for Anomaly Detection in Aggregate Traffic[6]
Parametric methods to detect network anomalies using only aggregate traffic statistics, in contrast to other works requiring flow separation, even when the anomaly is a small fraction of the total traffic.

By adopting simple statistical models for anomalous and background traffic in the time-domain, one can estimate model parameters in realtime, thus obviating the need for the long training phase or manual parameter tuning. The proposed bivariate Parametric Detection Mechanism (bPDM) uses a sequential probability ratio test, allowing for control over the false positive rate while examining the trade-off between detection time and the strength of an anomaly. Additionally, it uses both traffic-rate and packet-size statistics, yielding a bivariate the model that eliminates most false positives. The method is analyzed using the bivariate SNR metric, which is shown to an effective metric for anomaly Based detection. The performance of the bPDM is evaluated in three ways: first, synthetically-generated traffic provides for a controlled comparison of detection time as a function of the anomaly level of traffic. Second, the approach is shown to be able to detect controlled artificial attacks over the USC campus network in varying real traffic mixes. Third, the proposed algorithm achieves rapid detection of real denial-of-service attacks determined by the replay of previously captured network traces. The method developed in this paper is able to detect all attacks in these scenarios in a few seconds or less.

9 Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns[7]
Current DDoS attacks are carried out by attack tools, worms and botnets using different packet-transmission strategies and various forms of attack packets to beat defense systems. These problems lead to defense systems requiring various detection methods in order to identify attacks.

Moreover, DDoS attacks can mix their traffics during flash crowds. By doing this, the complex defense system cannot detect the attack traffic in time. In this paper, we propose a behavior based detection that can discriminate DDoS attack traffic from traffic generated by real users. By using Pearson's correlation coefficient, our comparable detection methods can extract the repeatable features of the packet arrivals. The extensive simulations were tested for the accuracy of detection.

We then performed experiments with several datasets and our results affirm that the proposed method can differentiate traffic of an attack source from legitimate traffic with a quick response. We also discuss approaches to improve our proposed methods at the conclusion of this paper.

10 Collaborative Detection of DDoS Attacks over Multiple Network Domains[13]
Presents a new distributed approach to detecting DDoS (distributed denial of services) flooding attacks at the traffic flow level. The new defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP).

At the early stage of a DDoS attack, some traffic fluctuations are detectable at Internet routers or at gateways of edge networks. We develop a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider. The system is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alerts reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflicts at different ISP domains, a new secure infrastructure protocol (SIP) is developed to establish the mutual trust or consensus. We simulated the DCD system up to 16 network domains on the DETER testbed, a 220-node PC cluster for Internet emulation experiments at USC Information Science Institute. Experimental results show that 4 network domains are sufficient to yield a 98% detection accuracy with only 1% false-postive alarms. Based on a 2006 Internet report on AS (autonomous system) domain distribution, we prove that this DDoS defense systrem can scale well to cover 84 AS domains. This security coverage is wide enough to safeguard most ISP core networks from real-life DDoS flooding attacks.

Limitations of the Existing System

- Node trust level is not considered
- Vulnerable to DOS attackers

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Conclusion and future enhancement

The introduced techniques can filter the network traffic of legitimate and attack But in the existing technique, When packet is send from source to destination, packet will route from various nodes .This existing technique doesn't identify that the node is attacker or legitimate. So Node Trust level is assigned and while taking the routing path, the node, which is having high trust value is considered for routing for the packets.

References

1 Zhiyuan Tan, Aruna Jamdagni, Xiangjian He‡, Senior Member, IEEE,Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE, " A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. , NO. , 2014 , IEEE

2 Chuan Xu ,Guofeng Zhao, China Zhaogf, Shui Yu "Detection on Application Layer DDoS using Random Walk Model", ,IEEE ICC 2014.

3 Fabian Nkemneme and Ruizhong Wei† Department of Computer Science, Lakehead University Thunder Bay, ON, Canada "A Multi-Queue Algorithm for DDoS Attacks" , P7B 5E1, 2014 , IIEE.

4 Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE,"A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS,2013.

5 Hakem BeitollahI ,Geert Deconinck "Analyzing well-known countermeasures against distributed denial of service attacks"ELSEVIER-2012.

6 G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

7 Thapngam, ShuiYu; Wanlei ,Zhou; Beliakov, G. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns" ,2011, IEEE.

8 Team Cymru " DDOS Basics"2010 Team Cymru, Inc.

9 LI Li, SHEN Su-bin"Packet track and traceback mechanism against denial of service attacks"ELSEVIER-2008.

10 Michae Howard, James A. Whittaker "Network Security Basics, " Nov-Dec 2005 IEEE SECURITY & PRIVACY.

11 V.Paxson, "Bro: A System for Detecting Network Intruders in Realtime," Computer Networks, vol. 31, pp. 2435-2463, 1999,IEEE. .

12 Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998,IEEE.

13 Yu Chen, Member IEEE, Kai Hwang, Fellow IEEE, and Wei-Shinn Ku, Member, IEEE , "Collaborative Detection of DDoS Attacks over Multiple Network Domains",IEEE.