TDDA: Traceback-based Defence against DDoS Attack

Akash B. Naykude
Department Of Computer Engineering
S.B.Patil College Of Engineering
Indapur PuneMaharashtra India
e-mail: akashnaykude143@gmail.com

Krushna D. Kudale
Department Of Computer Engineering
S.B.Patil College Of Engineering
Indapur PuneMaharashtra India
e-mail: krushna.kudale@gmail.com

Sagar S. Jadhav
Department Of Computer Engineering
S.B.Patil College Of Engineering
Indapur PuneMaharashtra India
e-mail: jadhav.153@rediffmail.com

Sumaiya sheikh
Department Of Computer Engineering
S.B.Patil College Of Engineering
Indapur PuneMaharashtra India
e-mail: zoyashaikh1786@gmail.com

Yogendra Patil
Department Of Computer Engineering
S.B.Patil College Of Engineering
Indapur PuneMaharashtra India
e-mail: patyogendra@gmail.com

Abstract— Look In today's fast growing of internet use, security of the data and information, resources and other useful files are more important viewpoints. Distributed Denial-of-Service (DDoS) attacks are responsible for making a machine or network resource unavailable to its appropriate users. Also a DDoS attack reduces the efficiency or capability of the server to doing its job. That's why they are very challenging issues for us. The problem is rises when spoofed IP addresses are present in the attack packets. In order to solve this critical situation of problem, that's why we proposed a new mechanism to efficiently reduce the impact or outcome caused by DDoS attacks. In some cases, even if the attacking traffic can be filtered by the victim side, here also the attacker may blocks the access of the victim by consuming the computing resources or by consuming a large amount portion of the bandwidth of the victim. This paper is proposes a Traceback-based Defense against DDoS Attacks (TDDA) approach to resolve this problem very goodly. In this paper, we present and design one technique that can be impressively filter out the majority of DDoS attack traffic. Our primary objective or intention for this work is to improving the overall throughput and performance of the appropriate traffic and also reduce the attack traffic to maintain the quality of service for that user.

Keywords- DDoS Attack, IP Spoofing, IP Traceback, Packet Filtering, Traffic Control.

*****

I. INTRODUCTION

DDoS is nothing but Distributed Denial of Service, which is one type of attack, utilizes multiple distributed attack sources. Normally, the attacker uses a large number of controlled agents or slaves (also referred to as zombies) distributed in different locations to launch a large number of DoS attacks against a single target or multiple targets. Simply consider one example related to DoS attack. Suppose we want to make a call or telephone call, but sometimes we can't do this. It will happen on major special holydays. The reason behind it is that telephone system is designed to handle a limited number of calls at a time. Imagine that an attacker wanted to make the telephone system unusable by customers or users. Making this repeatedly (call after call) is an attempt to make all circuits busy. This type of attack is called a *denial of service* attack.

In February of 2000, one of the first major DDoS attacks was done against Yahoo.com. In this attack what happened is that the Internet was getting off for about 2 hours [10]. Simple strategy of Distributed Denial of Service (DDoS) attack is that it uses many computers to launch a large scale coordinated DoS attack against one or more targets. DDoS attack has the capability to slow down victim's computing and communication resources within a short period of time. The Distributed Denial of Service (DDoS) attack is also a bandwidth attack, where attack traffic is directed from multiple distributed sources, that's why the attacking power of a DDoS attack is based on the huge number of multiple sources. Hence, the DDoS attack is more powerful and it can be consist of all types of traffic to the victim or that particular user's network connection and communication [15].

In this study, we propose a distributed scheme to detect and respond to a large subset of DDoS attacks. Actually the most common DDoS attacks target is the computer networks bandwidth or connectivity and our goal is to recover or avoid these types of situations or conditions. In Section II we described related work, in which we describes what type of work and solution is implemented in this paper. In Section III we present DDoS attacks overview. In Section IV we present DDoS Attack Taxonomy which is nothing but classification of DDoS. In Section V we described Proposed System. In Section VI we described DDoS Attack Detection and Defense Schemes.

II. Related Work

There have been lots of proposals and solutions against the DDoS attacks problem. In this paper we try to present some structure and solutions to avoid the DDoS attacks and analyze and classify the solutions to the DDoS attacks. By considering the total concept of each solution, we can know about the effectiveness of the solutions and our main purpose is to clearly describe the existing problems. So that why, a better way for understanding of DDoS attacks can be achieved or obtained from more efficient defense mechanisms.

The DDoS defense mechanisms can be divided into three parts [14]. These three categories are as follows: Survival Mechanisms from DDoS, Proactive techniques against DDoS and Reactive Mechanisms against DDoS**.** The distributed behaviour and working of DDoS attacks makes them extremely difficult to detect or traceback and defend. Attackers normally use spoofed (fake) IP addresses in order to hide their own true identical information, which makes the traceback or detection of DDoS attacks even more and more difficult.

There are lots of attacks had been launched in different-different organizations since summer of 1999 [1]. See, in February 2000, most famous site Yahoo.com is in under attack of DDoS for near about 2 hours. Also in [1]-[9] stated that in October 2002, several root servers are get shut downed for an hour. The region behind is that DDoS Attacks [1]-[10]. Another big DDoS flooding attack was happened in February 2004, on SCO group website [1]-[11].

The goal of attack detection is to detect every attempt of DDoS attack as early as possible and compulsory get result in positives condition. Mechanisms of event patterns are also called signatures; pattern detection is sometimes called "*signature-based detection*". But it can only detect known attacks, and it is usually helpless against new attacks or even slight variations of old attacks that cannot be matched to the stored signature. Now On the other hand, known attacks are easily and reliably detected, and no false positives are encountered.

In this work, we extend or improved the idea of various attacks of DDoS and express that Concept in suitable manner. The current state of the system is periodically compared with the models to detect anomalies and frauds.

So that's why is important to defence against this type of attacks. When an attack is detected and recorded, the next thing is that to find out who is the originator behind this. This turns out to be a really hard problem in the Internet. But no need to worry about that because the solution is given in this research and also it is helpful for us.

III. Proposed System

In this section we described the flow of proposed system. The primary difficulty of dealing with DDoS attacks is *IP Spoofing* [3], which is a normally very simple technique common in DDoS attacks and also other network related frauds. At the time of launching an attack, the attacker can include spoof IP addresses in the attack packets to hide their own identity for being traced and blocked from anyone, so as to continue its attack one victim. The source address being distributed along the large amount of different spoofed addresses and it uses some detection tools to identify the traffic problems [12].

But in currently running flooding attack, if some action is not taken to avoid the attack traffic, lots of the legitimate traffic would be placed by the upstream routers before completing its destination. In other words, we can say that the legitimate traffic would suffer from *collateral damage.* The traffic is sometimes either harmed by the congestion of network, or it is filtered by the present defense mechanism.

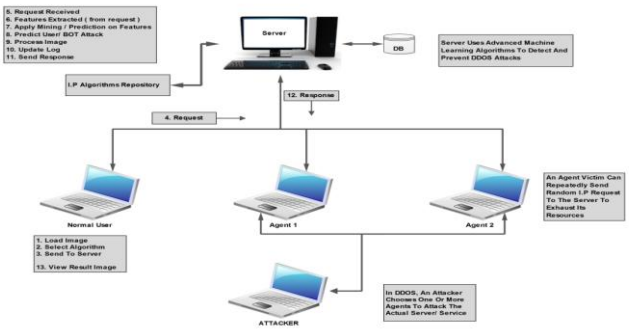

Fig.1. Proposed System

We also focused on the flooding-based DDoS attacks, because this could potentially stops or disables the essential Internet services in few minutes. Look, In order to design a strong and effective DDoS defense mechanism, we done an intensive survey has been proposed on the DDoS attack as well as its existing solutions. Throughout the study, we discover that there are different proposals available for IP traceback, which aim at locating the potential attack sources. Nevertheless, they cannot be employed to defend against DDoS attacks [15].

See, the attacker communicates with many numbers of masters to recognise which agents are running on that time, when to schedule attacks for completing the target, and when to upgrade particular agents. Usually, attackers will try to place the master software agent on a specific router or network server which can be able to handles large amount of traffic. That's why they make it more complicated to identify messages between the master and agents. These users of the agent systems are typically have no knowledge that their system has been compromised and considering that they are now part of DDoS attack. When involving in a DDoS attack, each and every agent program uses only a small amount of resources like both memory and bandwidth also [2].

IV. DDoS Attack Overview

These DDoS attacks do not creates damage on data directly, or permanently, but they are able to reduce the availability of the resources.

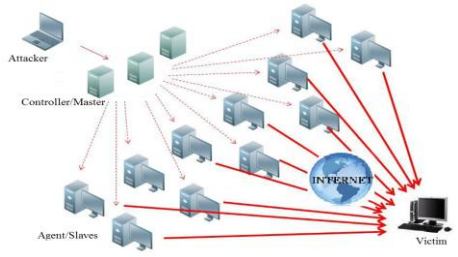

Fig.2. DDoS Attack

See the figure 2, it shows that the DDoS attack concept and actually what will be the way or process is happened in DDoS attack. It also shows the simple view of DDoS attack. The target under attack is defined as *primary victim (Masters)*, while the compromised hosts used to launch the attack are often called *secondary victims (Agents)*. The use of secondary victims in performing a DDoS attack provides the attacker with the ability to create and perform a much larger and more disruptive attack, while making it more difficult to track down the original attack source. The *masters* are software packages located on computing systems throughout the Internet that the attacker uses to communicate indirectly with the *agents* [9]. The agent software exists in compromised systems that will eventually carry out the attack on the victim system.

For more clarify concept of DoS attack, see the basic and very simple example of DoS attack on TCP protocol. A client sends a request to a server for announcing its intention to start a conversation in between them. After client request the server responds with an acknowledgement to client, accepting the establishment of a connection or fix to its connection queue. Now it is the client's turn to acknowledge the start of the communication by sending its packet. But a malicious client may never do that, as a result the server ends up with its connection queue entry tied up (and unused) for a significant amount of time (at least as long as the timeout), before it can be released. If this above scenario repeating over multiple times (almost) simultaneous, using this bogus communication [5]. Then obviously the result is very bad and harmful.

Fig.3. DoS Attack

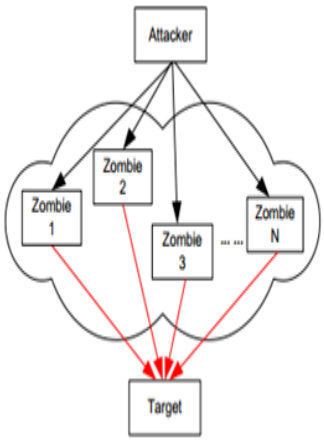

Fig.4. DDoS Attack

See these both figures, it shows that more clear difference between DoS and DDoS attacks. In figure 3 attacker can directly attacks on victim by using internet medium. In this mechanism of DoS, large number of malicious packets is sent by single machine only. But in next figure which is figure 4 shows that attacker cannot directly attack on victim, instead it uses malicious zombies or agent for this.

V. DDoS Attack Taxonomy

In this DDoS attack taxonomy section we described classification of DDoS attack. There are a lots of DDoS attack techniques types [6][10]. We present taxonomy (classification) of the DDoS attack in figure 5. There are two main classes of DDoS attacks: Those are nothing but *Bandwidth Depletion* and *Resource Depletion.*

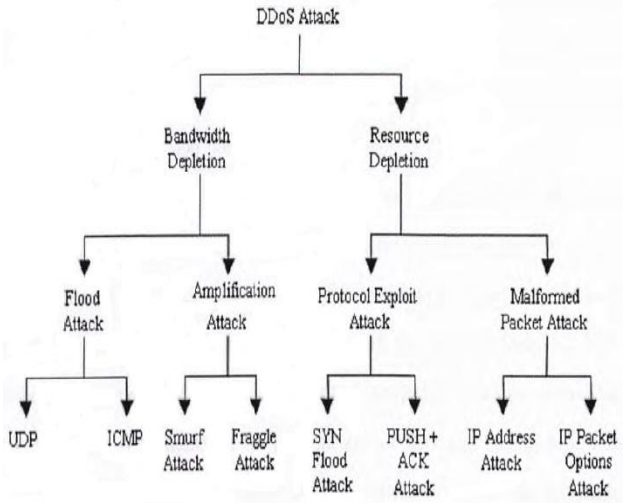

Figure 5 shows the taxonomy of DDoS attack in suitable manner.

A. *Bandwidth Depletion Attacks:* This mechanism is designed to mix unwanted traffic into the victim network. It includes two main classes of DDoS bandwidth depletion attacks. One of them is flood attack. In this flood attack, it involves the agents or zombies for sending large amount of traffic into a victim system, for purpose of accessing the victim system's bandwidth. Another attack is amplification attack. In this attack, attacker or the agents (zombies) sending messages to a broadcast IP address, reason behind it is that to amplifies malicious traffic that reduces the victim system's bandwidth [4]. The DDoS uses these both attack for access the connected network of user.

B. *Resource Depletion Attacks:* A DDoS resource depletion attacks having capability to access network resources of appropriate user or victim [14]. Usually the attacker sending packets for purpose of get misuse of network protocol communications or sending bad packets that access well network resources so that none options are remains in front of that particular users.

After words the other sub types of attacks are comes in the classification. Which are nothing but UDP and ICMP. As we know about User Datagram Protocol (UDP) is a connection-less protocol. In this protocol if packets are sent via UDP protocol, then here is no handshaking required in between sender and receiver, and unfortunately the receiving system will just receive packets for another process [6][8][10]. A large number of UDP packets sent to a victim system can reaches in whole the network. In Internet Control Message Protocol (ICMP) it allows the user to send a request to a destination system for its working strategy and receive a response with the round trip time for more processing.

In a DDoS Smurf attack, this type of attack amplifies the original packet tens or hundreds of times. Actually its purpose is to copying various packets and spread over the networks. A

DDoS Fraggle attack is similar to a Smurf attack. In this attack the attacker sends packets to a network amplifier. But Fraggle attack is uses UDP ECHO packets and Smurf attack uses ICMP ECHO packets.

SYN Flood Attack is a TCP-based attack. Working of this attack is, sending a large number of spoofed TCP connection requests to the server. Thus, other legitimate connection requests are denied or rejected. In a DDoS SYN Flood attack, the attacker instructs the zombies to send such bogus TCP SYN requests to a victim server. For access the server's processor resources, and hence prevent the server from responding to legitimate requests [11].

Result come from this is that, volume of TCP SYN attack requests is larger and they continue over time, the victim system will run out of resources, which is very bad and be unable to respond to any legitimate users. *PUSH + ACK Attack* is the TCP protocol attack, packets that are sent to a destination are buffered or stored within the TCP stack and at the time of full stack, the packets are get sent on to the receiving system. However, the sender can request the receiving system to unload the contents of the buffer before the buffer becomes full by sending a packet with the PUSH bit set to one. PUSH is a one-bit flag within the TCP header [4].

Another type of TCP-based attack is to congest a victim's incoming link. In these attacks, the victim normally responds with RST packets, and at that time attack packets are also the RTS form packets. *Malformed Packet Attack* is an attack where the attacker informs to the agents (zombies) to send wrong or bad IP packets to the victim system and the purpose is to crash or break down the victim system. Here also two types of malformed packet attacks [7]. In this first IP address attack, the packet having same IP addresses of source and destination. This can be saturates and confuses the operating system of that victim system and also result comes into crash of that system. In an IP packet options attack, If this attack packet is multiplied using present agents, it can break down the processing capability of that victim machine.

VI. DDoS Detection And Defense Schemes

In this DDoS Detection and Defense section, we have described useful information related to the attacks of a DDoS and also the techniques which are useful to resolve this type of problems. Detection and defense schemes are very useful for the knowing attack tracing and avoiding techniques.

- DDoS Detection Phase:
  - A. *Traffic monitoring:* Attack detection work is mainly performed by the special agents because that agent has an ability to read and write or modify each and every packet going through that router. In traffic monitoring, observation mechanism is done by using some calculations of obtained result the detection is done. When Specific agent detects a suspected victim, it will send an alert message to the nearest connected agent to start the response phase.
  - B. *Anomaly Detection:* The important event of surprisingly big TCP packet rates and from an IP address is employed to detect TCP-based attacks. The guaranteed-delivery nature of the TCP rules of conduct needs the exchange of responses (ACK) between senders and receivers. Therefore, for usually TCP communications, the number of packets sent to and received from a host should be balanced. A zombie that floods a victim will hardly receive any proper ACK packet.
  - C. *Response Phase:* This response phase is working when a DDoS attack is detected. After detection of DDoS Attack this get activates.

- *DDoS Defense Phase:* DDoS defense schemes can be divided into three classes: victim side, source-side, and intermediate router defense mechanisms. All of these approaches have their own advantages and disadvantages. Here we discuss them one by one.

A. *Victim-side defense mechanism*: Here the detection system is used for detection of intrusion either online or offline technique, using misuse based intrusion detection approach or anomaly based intrusion detection approach. But one disadvantage of this approach is that it detects the attack only if it reaches the victim and detecting an attack when legitimate clients have already been denied.

B. *Source-side defense mechanism*: This Source-side mechanism is similar to the victim-side detection concept. The observation engine compares both incoming and outgoing traffic conditions with some already defined rules. One thing is that detecting and stopping a DDoS attack at the source side is the best possible defense technique. But also it is not easier too. Because in these types of attacks, sources are widely distributed and a single source behaves almost similarly as in normal traffic.

C. *Intermediate network defense mechanism*: In this mechanism detection and traceback of attack sources are very easy because of collaborative operation. Routers can form an overlay mesh network to share their observations and conditions. The main difficulty with this approach is deploying ability. To achieve a goal of full detection accuracy, all over routers on that Internet should have to apply this detection scheme, because of unavailability of this scheme is only a few routers may be cause failure to the detection and traceback process.

We classify DDoS defense mechanisms using two different criteria. The first classification categorizes the DDoS defense mechanisms according to the activity deployed. Thus we have the following four categories [7]:

- Intrusion Prevention,
- Intrusion Detection,
- Intrusion Response, and
- Intrusion Tolerance and Mitigation.

- *Intrusion prevention:* The best way of defense strategy against any attack is to completely prevent that upcoming attack. In this stage we try to completely stop DDoS attacks which may occur in

the first place. And for that purpose ingress filtering, egress filtering, rout based distributed packet filtering, history based IP filtering is used [7].

- *Intrusion detection*: It has been considered a very active research area of detection. By applying intrusion detection, security increases because a host computer and a network can protect itself against being a source of network attack and also being a victim of a DDoS attack. An intrusion detection system works using the database of known signatures or by recognizing anomalies of those system behaviors.
- *Intrusion response:* Whenever an attack is identified or detected, identify the attack source or from where it occurs and block that traffic permanently. The blocking can be done usually under manual control. IP traceback, ICMP traceback are approaches that useful for targeting, tracing and identifying of the real attack source.
- *Intrusion tolerance and mitigation:* Total Research on intrusion tolerance proves that it is not possible without any specific technique to prevent or stop DDoS attack completely. But by using some techniques avoidance as well as defense is possible. Intrusion tolerance can be divided in two categories those are fault tolerance and quality of service (QoS) techniques [7].

Traceback-Bases Defense Against DDoS Attack System is useful to prevent or detect the distributed denial of service attack as well as it protect or defend against that attacks. As we know about the todays insecure things of internet, we cannot take risk of our important data and also we cannot trust any security mechanism directly. For the increased security using TDDA system we can manage our internet traffic and also handle these malicious attacks from crashing our system. We have to consider some things related to prevention of these attacks. In which social networking, share marketing, and online transactions[16] etc. interfaces of network are not secure to do without any protection. Because, if we do these type things without any protection, then we faces various problems under the networking today.

The victim can also suffer from a DDoS attack with two major impacts or categories. First is, the victim has limited number of resources for processing the incoming packets from network and the victim's resources, like CPU and memory, will be exhausted, and then the victim will be unable to handle for normal traffic and result goes to break down the connection[13]. Second is, use and consumption of network bandwidth by attacker, result will get legitimate flows being blocked forcefully. In order to handle an acceptable performance of throughput, the huge number of traffic filters installed on a router protects the victims as well as secure overall network communication. Attack is detected first on the victim side monitors traffic analysing engine and can be identify that attack traffic. In today's world, many servers have installed Host-based IDS for such a purpose. Normally Defenders do work when the attack occurrence is confirmed by particular network[17]; the next work is to limit that attack rate in selective manner without breaking service of those appropriate users, so that contiguous damage of that user get minimized quickly.

VII. CONCLUSION

Distributed Denial of Service attacks can causes several problems like, breaks the stability of internet on server, loss of network resources, communication, and bandwidth, work delay, etc. DDoS attacks are not only a serious problem for the wired networks but also for the wireless infrastructures. DDoS attack affects on both victim as well as network link also. These problems are very harmful for us. We need to survive from this for better work, effective communication and cooperation between users.

In this paper, we have presented an overview of DDoS attacks, taxonomies or classification of DDoS attacks, DDoS attacks detection and defense schemes, and overall architectural view and related terms. DDoS creates various types of issues related to our network connection and now a days networking security concepts are required to secure our connection. That's why a possible solution to counter DDoS attacks and also DDoS examples are presented in this paper. The key idea behind it is that, to improve the quality of way, for network servers and help to solve the DDoS problem and to facilitate more comprehensive solutions.

This paper describes the detailed survey and information of different Distributed Denial of Service traceback mechanisms. For future work, we need to implement and evaluate the securing of the TDDA system itself.

REFERENCES

[1] 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.

[2] Ho-Yu Lam, Chi-Pan Li, Samuel T. Chanson and Dit-Yan Yeung Department of Computer Science Hong Kong University of Science and Technology Clear Water Bay, Kowloon, Hong Kong" A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks".

[3] Zhenhai Duan, *Member, IEEE,* Xin Yuan, *Member, IEEE*, and Jaideep Chandrashekar, *Member, IEEE* "Controlling IP Spoofing Through Inter-Domain Packet Filters".

[4] Yulong Wang and Rui Sun State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China "An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks".

[5] Robert Stone, UUNET Technologies, Inc. robert@uu.net, "CenterTrack: An IP Overlay Network for Tracking DoS Floods".

[6] *Christos douligeris and aikaterini mitrokotsa,* department of informatics, university of piraeus, piraeus, greece, "DDoS attacks *and* defense mechanisms: a classification".

[7] Christos Douligeris *, Aikaterini Mitrokotsa, Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece, Received 9 October 2003; accepted 13 October 2003, Responsible Editor: I.F. Akyildiz, "DDoS attacks and defense mechanisms: classification and state-of-the-art".

[8] Valentin Razmov, (valentin@cs.washington.edu), Computer Science and Engineering Department,University of Washington, May 10, 2000, "Denial of Service Attacks and How to Defend Against Them".

[9] Monowar H. Bhuyan, 1Department of Computer Science & Engineering, Tezpur University, Napaam, Tezpur-784028, Assam, India, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions".

[10] Stephen M. Specht, Ruby B. Lee, Electrical Engineering, Princeton University Princeton, NJ 08544, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures".

[11] John Ioannidis, Steven M. Bellovin, *smb@research.att.com*, AT&T Labs Research," Implementing Pushback: Router-Based Defense Against DDoS Attacks".

[12] Vahid Aghaei-Foroushani* and A Nur Zincir-Heywood," IP traceback through (authenticated) deterministic flow marking: an empirical evaluation".

[13] *Vahid Aghaei Foroushani, A. Nur Zincir-Heywood*, Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada, vahid@cs.dal.ca," *TDFA: Traceback-based Defense against DDoS Flooding Attacks*".

[14] Darshan Lal Meena, *(Ph.D Scholar) Department of Computer Science, MP, Bhoj Open University, Bhopal (MP) -462016 INDIA."*A Survey on Different Solutions to DDoS Attacks".

[15] Divya Bhavasar, Master of computer engineering, parul institute of engineering and technology, india," a survey on distributed denial of service attack and defence".

[16] A.John1, T Sivakumar.2, Department of Computer Science, Ramanujam School of Mathematics and Computer Science Pondicherry University, Puducherry, India, "DDoS: Survey of Traceback Methods".