Chapter 1

Introduction

In this chapter, a brief introduction on Distributed Denial of Service(DDoS) attacks and its various types from different perspectives are reported. The motivation, objectives and contributions of my research are presented. This chapter also discusses the desired features of a DDoS defense system.

1.1 Introduction

Now a days one of the most commonly observed threat over the Internet is Distributed Denial of Service (DDoS) attack. In a distributed Denial of Service attack, a group of compromised machines called as zombies or bots, send co-ordinated traffic to the victim, in an attempt to exhaust different resources like CPU, memory or link bandwidth of the victim so that the victim becomes paralyzed or disconnected and thus prohibiting the legitimate users to reach the victim. The victim of a DDoS attack can range from a single web server to the Internet connection to an entire university or the entire city or even the entire country [1]. In most of the cases, the users of the compromised machines which participate in an attack are unaware about the fact. The bots are controlled or activated by a master, which is the actual attacker. The attacker first compromises a group of machines and installs the bot program into them. Then the master communicates and sends different commands to these zombies to perform the attack. In real situation however, an attacker might not always need to first create a botnet by compromising a set of vulnerable machines. In [106], the authors discussed how an actual DDoS attacker can get access to a ready made botnet. A detailed description on different types of DDoS attacks, along with different tools to perform such an attack can be found in [2, 3].

1.1.1 Types of DDoS Attack

Based on the Open Systems Interconnection (OSI) layers whose services are used to carry on the attack, DDoS attacks can be classified into two categories.

1. Application Layer attack: In such an attack the attacker uses layer 7 i.e., application layer protocols like HTTP and HTTPS to send traffic to the victim. Such traffic normally carries CPU intensive queries to the server and makes it busy for ever. The volume of the traffic that is needed to put a server down is comparatively less than that of the other type i.e., network layer attack. The traffic in application layer attack is indistinguishable from the legitimate traffic making it very difficult to detect. A detailed description of application layer DDoS attack can be found in [4]

2. Network/Transport layer attack: Here the attacker mainly tries to exhaust resources like the bandwidth of the links which carry traffic to the victim, or the memory of different devices for example routers, switches and firewalls. To achieve this the zombies send huge amount of layer 3/4 traffic to the victim. Such an attack is normally big in volume ranging from a few mbps to many hundreds of gbps. Different network layer protocols like Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP)and Transmission Control Protocol (TCP) are used in such an attack. The most commonly used network layer DDoS attacks are TCP SYN flooding [2, 5], ICMP echo [2], UDP flooding [2], DNS amplification attack [6], NTP amplification attack [7] etc.

Other than the above mentioned classification, DDoS attacks are classified based on other different characteristics too. Mircovic et al. in [2] classify DDoS attacks based on attack rate dynamics into four categories:

1. Constant rate attack: The attack rate reaches its maximum within a very short duration of me. All zombies after receiving command from attacker start sending attack traffic at a constant rate. This type of attack creates a sudden packet flood at the victim end.

2. Increasing rate attack: Instead of attacking the victim with full force instantly, the attacker gradually increases the traffic intensity towards the attacker. This approach is taken by the attacker to understand the victim's response towards attack traffic to evade detection mechanisms.

3. Pulsing attack: In this type of attack the attacker activates the bot periodically to send attack traffic to the victim. Such a mechanism is used to remain undetected by a detection mechanism. Shrew [8] is an example of pulsing rate DDoS attack, which sends short synchronized bursts of traffic to disrupt TCP connections on the same link, by exploiting a weakness in TCP's retransmission timeout mechanism.

4. Sub-group attack: As in the case of pulsing rate attack, here also the attacker sends pulses of attack traffic to the victim. However, the zombies are divided into groups and these groups are activated and deactivated in different combination. Such a mechanism is used by the attacker to remain disguised and carry on the attack for longer duration of time [1]. Figure 1.1 shows different types of DDoS attack based on attack rate dynamics.

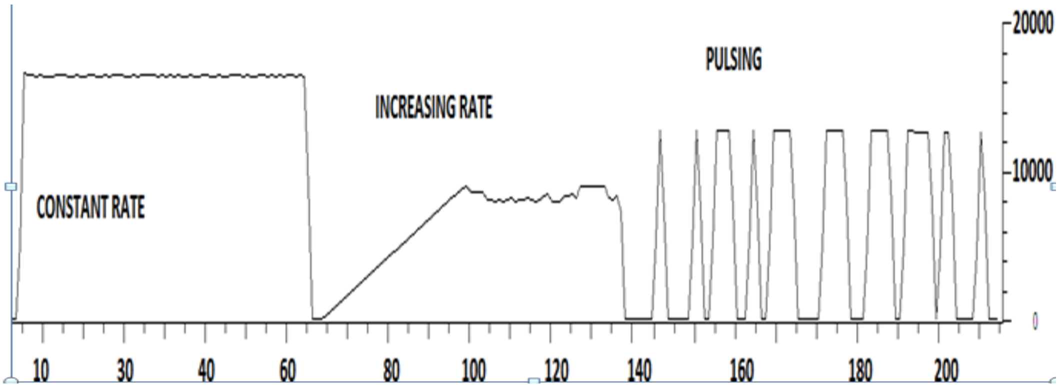


Figure 1.1: Different types of DDoS attacks based on attack rate dynamics

Based on the traffic volume, DDoS attacks are classified as

1. Low rate DDoS attack: To perform a DDoS attack it is not necessary to send huge traffic to the victim. The attacker can perform the attack by sending attack traffic at a low rate matching the legitimate traffic profile. For example, in case of an application layer attack the attacker tries to exhaust the victim's processing resources by sending CPU intensive queries. Similarly, in shrew [8],[128] attack the volume of the attack traffic is comparatively low.

2. High rate DDoS attack: In a high rate DDoS attack, the attacker sends huge volume of attack traffic towards the victim. It is the most common type of DDoS attack.

Based on whether the attack traffic is sent to the victim directly or to some other users, DDoS attacks are categorized as:

1. Direct attack: In direct-attack, the attacker sends the attack traffic directly to the victim.

2. Indirect attack: In indirect-attack, the attacker instead of attacking the victim directly, attacks the links and other services which are important for the victim to remain functional. Link flooding attacks like crossfire[1], coremelt[9] are examples of indirect DDoS attack. Figure 1.2 shows an indirect attack scenario.

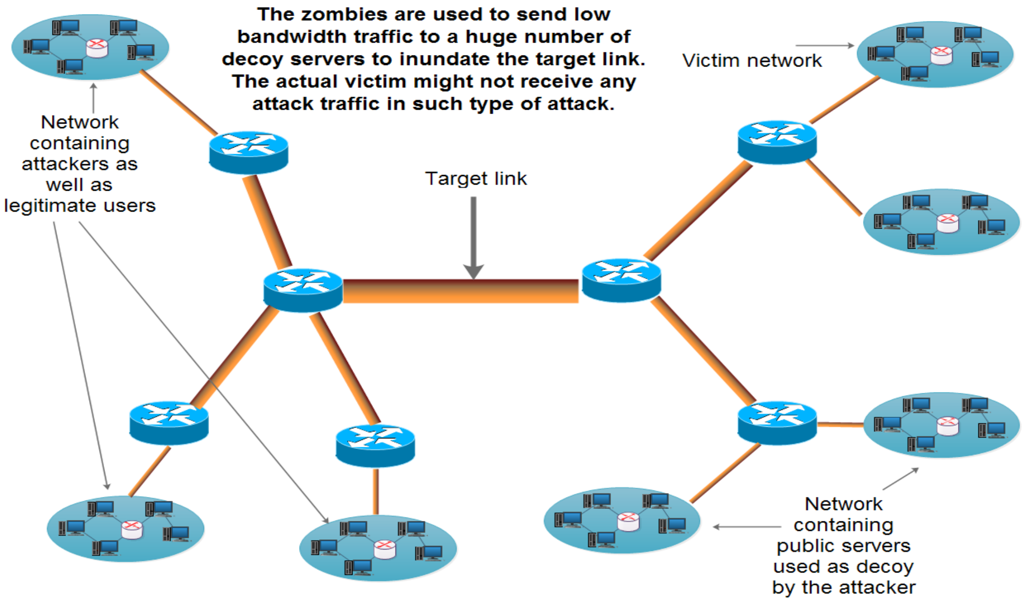

The zombies are used to send low bandwidth traffic to a huge number of decoy servers to inundate the target link. The actual victim might not receive any attack traffic in such type of attack.
Victim network
Network containing attackers as well as legitimate users
Target link
Network containing public servers used as decoy by the attacker

Figure 1.2: Indirect attack

In a DDoS attack it is not always the zombies which send attack traffic to the victim. Servers running UDP based services in many cases are used by attackers to carry on massive DDoS attacks. Such servers are used as reflectors by the attacker. Based on this characteristic DDoS attacks are classified into two categories:

1. Direct attack: In direct-attack the attacker uses the zombies to carry out the attack.

2. Reflection/amplification attack: As mentioned, in this type of DDoS attack, the attacker sends request to the reflector servers with the source spoofed as the victim's IP. As a result the server replies the victim by sending messages which is normally many times larger than the original request message size. Hence this type of DDoS attacks are also called as amplification attack. The attacker uses this technique to amplify the attack traffic upto several hundred times. DNS amplification attack and NTP attacks are examples of reflection

based DDoS attack (DRDoS). A detailed description of reflection attack along with different potential UDP services and their amplification factor which could be used to amplify the attack traffic can be found in [6].Figure 1.3 shows pictorial representation of a reflection/amplification attack.

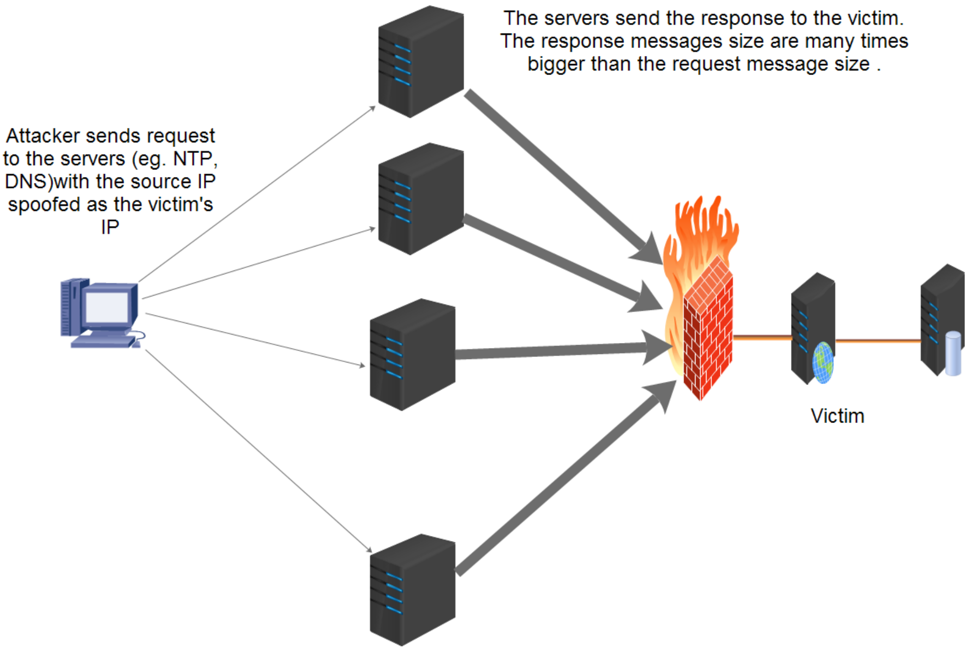

The servers send the response to the victim.
The response messages size are many times bigger than the request message size .
Attacker sends request to the servers (eg. NTP, DNS)with the source IP spoofed as the victim's IP
Victim

Figure 1.3: Reflection/Amplification attack

1.2 The Strength of DDoS Attackers

DDoS attacks have been haunting the Internet security over a decade. The current trend shows that DDoS attack frequency is increasing with time. Here, the main strengths of the DDoS attackers which make DDoS attacks difficult to eliminate from the Internet have been enumerated.

1. The attacker can spoof the source IP of the attack packets, which gives two folded advantages. First, the attacker can hide its identity and second, the attacker can use this mechanism to amplify the attack traffic by hundreds of magnitude as in the case of DRDoS attack.

2. The attacker can arbitrarily change different fields of layer 3/4/7 protocol header. For example, in a TCP SYN flooding attack the attacker can alter fields like SIP, TTL of the IP layer header as well as set/reset different TCP flags in the transport layer header.

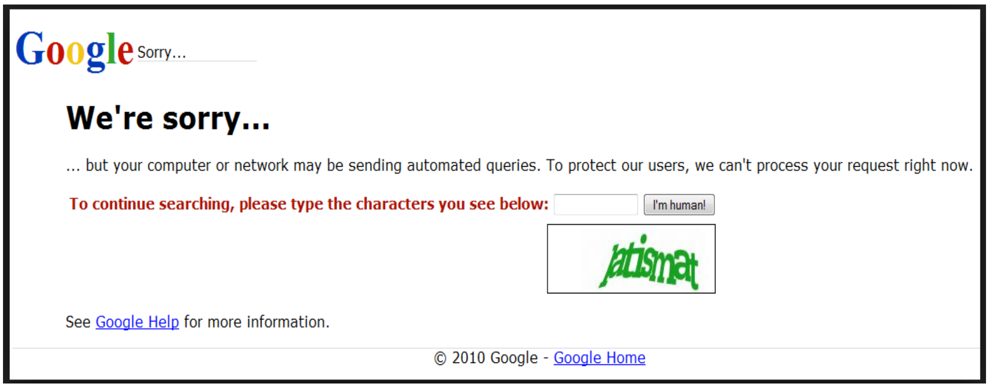
3. The attacker can change the attack rate, attacking bots even the victim dynamically. Also the attacker can mix multiple attack vectors, even across the layer, as in the case of multi-vector DDoS attack, making defense more difficult.

4. The attack traffic can be made completely indistinguishable from the legitimate traffic in terms of content. For example in a HTTP GET or POST flooding attack [10], the attacker sends a huge number of seemingly legitimate HTTP GET or POST request to the victim server. In a crossfire attack [1] the bots send completely legitimate HTTP traffic to the decoy servers in order to flood some of the selected links carrying major portion of the traffic to the intended victim to/from the Internet.

5. A DDoS like situation such as huge traffic, increase number of users, slowed down servers/networks etc can also be resulted from other types of events like flash crowds, BGP table misconfiguration, hardware failure etc. A defense system is expected to have the ability to differentiate these situations from DDoS attack.

1.3 Motivation

Although we don't see big sites like google and facebook going down, even temporarily it does not mean that DDoS attacks are not being tried against them. For example, many of us have experienced google's "Unusual traffic from your computer network" message shown in Figure1.4 while surfing the site. These network giants have very big network and other resources to mitigate the impact of the attacks at real time. However, networks like government sites, news sites, technological



Google Sorry...

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

To continue searching, please type the characters you see below:

See Google Help for more information.

© 2010 Google - Google Home

Figure 1.4: Google's unusual traffic message.

repositories, gaming servers are successfully attacked and put down recently. Some of the major DDoS attacks seen in the recent time are mentioned below

1. DDoS attack occurred against Dutch government sites [11]: This attack was performed on February 10th, 2015 against the sites of the federal government directly. As reported, the sites were down for 10 hours during the attack. Some other sites hosted on the same network were also impacted by the attack. The attack was reported to use different and dynamic attack patterns and methods which made the attack successful.

2. DDoS attack occurred against National Security Agency (NSA) of United States [12]: This attack was performed on 25th October, 2013 against the intelligence organization of the United States government. As reported the attack successfully paralyzed the site for an extended period of time. The attack was suspected to be performed by the hacktivism group Anonymous [13]. The role of a Foreign Government behind the attack was also not nullified.

3. DDoS attack against Github [14]: Github, a code repository hosting service which is widely used by software developers around the world to manage source code, was the target of a massive DDoS attack late on 24th March 2015 , allegedly launched by China. The attack was reported to continue for 24 hours with partial success. The attack used layer 7 to perform the attack.

4. DDoS attack against thousands of French websites[15]: During the second week of January 2015, more than 19,000 websites ranging from military regiments to pizza shops were under minor DDoS attacks. The huge number of victim sites targeted by this attack was reported as a peculiar thing about the attack.

5. DDoS attack against Dyn [17]: This 1.2 Tbps DDoS attack was performed against Dyn, a domain name system (DNS) service provider on 21 October, 2016. The DDoS attack which affected much of Americas Internet was conducted by making use of Mirai botnet. Mirai is a botnet of around 10,000 infected "Internet of Things"(IOT) devices such as TVs, refrigerators and cameras. As reported some of the major sites hugely affected by the attack includes Twitter, Spotify, CNN, PayPal and Fox News.

The above mentioned incidents indicate the need of research in the DDoS attack detection and mitigation field, so that such incidents and many others like them can be prevented.

1.4 Desired Features of a DDoS Attack Defense System

The primary goal of the defending side of DDoS attack is to keep the victim alive and reachable to the legitimate users even if the victim is undergoing a DDoS attack. A DDoS defense thus, has to have the following characteristics

1. Real time detection and scalability: A defense system should be able to detect an ongoing attack before the attack paralyzes the victim with its overwhelming malicious traffic. Since the attack rate of today's DDoS attacks are hundreds of Gbps, both the time and space complexity of the detection mechanism plays an important role in the scalability of the defense system.

2. Maintaining QoS to the legitimate users: One of the major obstacle in defending DDoS attack is that the attack traffic is indistinguishable from the legitimate traffic in their content. Hence, only detecting an attack is not sufficient to protect the victim, special mechanisms are needed to separate the legitimate traffic from attack traffic, so that the QoS to the legitimate users can be maintained.

3. Source Identification: A DDoS attack defense system should be robust against IP spoofing. It should have proper mechanism such as traceback or pushback to locate origin of the attack sources.

4. Extensibility: Since the DDoS attacks are evolving with time, a defense mechanism also should be flexible enough to incorporate new extensions to deal with new variants of DDoS attack.

In [16] the authors have discuss different performance measurement metrics for a DDoS attack defense system such as accuracy, holistic defense, implementation complexity and deployment location.

1.5 Objectives of the Research

The following objectives were aimed to achieve.

(a) Light weight DDoS Detection Mechanism: A desirable property of a DDoS attack defense system is to detect the attack in real time. Also, the detection

mechanism should be light in terms of computation and memory so that it can be easily deployable in high speed routers.

(b) DDoS detection and mitigation mechanism based on usual Internet traffic characteristics: DDoS attack packets are generally indistinguishable from normal packets based on its content. However, a DDoS defense should be able to pinpoint the attack packets to mitigate the attack. Hence, a DDoS defense mechanism is aimed to develop which is capable of detecting the attack traffic accurately.

(c) Defense against spoofing based DDoS attack: One of the most common characteristics of DDoS attack traffic is the use of spoofed source IP addresses. Spoofing is used by the attacker to hide itś identity. Hence, a spoofing detection mechanism is aimed to develop to mitigate spoofing based DDoS attacks.

(d) Development of a traceback mechanism: A DDoS defense mechanism should not only be able to detect an attack but also it should be able to block the attack traffic close to the attack source itself. However, spoofing makes it difficult to pin point the exact location of the attack source. Hence, a traceback mechanism is desirable to trace back the attack sources up to their LAN, even if they are spoofed.

1.6 Thesis Contribution

Based on the objectives as reported in the above section, following contributions have been made.

(a) A Light Weight DDoS Detection Mechanism: A light weight DDoS detection mechanism has been developed which monitors the number of sources communicating with the victim. Also, the packet rate of the sources are monitored. An attack alarm is generated if there is any sudden change in these two observed parameters. Non-parametric CUSUM[18] has been used to detect sudden change in these parameters. We used both test bed generated attack traces as well as publicly available attack traces to validate our method. Experimental results show that our detection mechanism is capable of detecting an ongoing DDoS attack in near real time.

(b) A DDoS attack detection and mitigation system: Based on observing the bi-directional nature of a communication, a DDoS detection and mitigation system has been developed. Our approach is not only capable of detecting an attack at near real time but also can filter the attack packets from normal packets more accurately. We have performed extensive experiments to show the behavior of our model at different attack situations such as constant rate attack, subgroup attack, randomly spoofed attack, low rate attack and high rate attack.

(c) Packet marking based anti spoofing techniques: In this work, initially a path encoding scheme called as XORID has been introduced, which enables a packet to carry a code in its 16-bit ID field. The advantages of our proposed method have been demonstrated over other existing similar methods. Further, a source end packet marking scheme called as SEM also has been reported to overcome some of the drawbacks associated with path based marking schemes. The experimental results show that SEM is superior in terms of both false positive rate as well as false negative rate than the existing schemes.

(d) A logging based IP traceback mechanism: An effective logging based traceback mechanism has been developed, which is capable of tracing back a flow up-to its originating LAN. The proposed mechanism requires comparatively less storage in an intermediate router than the existing schemes. The proposed mechanism has been validated both theoretically and experimentally, and it has a zero false negative rate and a low false positive rate in terms of attack source identification.

1.7 Thesis Organization

The layout of the chapters in the thesis is as follows

Chapter 1. Introduction
This chapter gives a brief introduction to DDoS attack along with their many different types. This chapter discusses the motive, objectives and contributions made in the dissertation.

Chapter 2. Related Work and Background
In this chapter I present a brief discussion about different approaches taken by the

researchers to defend against DDoS attacks. The existing solutions are discussed from different perspectives such as based on their activation time, deployment locations, OSI lair and computational models. This chapter also discusses some of the basic concepts used in the research.

Chapter 3. A Light Weight DDoS Detection Mechanism
The first contributory work, i.e. a light weight DDoS detection mechanism is presented in this chapter.

Chapter 4. A DDoS Attack Detection and Mitigation System Based on Bidirectional Nature of Internet Communications
The second contributory work which detects and mitigates a DDoS attack by observing the bidirectional nature of the Internet communication is presented in this chapter.

Chapter 5. Packet Marking Based Anti Spoofing techniques
The third contributory work to defend against spoofing based DDoS attacks is presented in this chapter.

Chapter 6. A Logging Based IP Traceback Mechanism
This chapter discusses a space efficient logging based IP traceback mechanism to locate the true attack source.

Chapter 7. Future Work and Conclusion
This chapter presents the summary of my contributions along with the future direction of the research.

Appendix A- TUCANNON - A DDoS Attack Generation Tool
It reports a tool developed to generate different types of DDoS attacks in a controlled test bed environment.