TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

A
THESIS REPORT
ON

DEFENSE AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACK USING COLLABORATION BETWEEN ROUTERS

SUBMITTED BY
SANTOSH BARAL
069/MSCS/665

SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING AS A PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE MASTERS DEGREE IN COMPUTER SYSTEM AND KNOWLEDGE ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
LALITPUR, NEPAL

October 2016

Acknowledgements

I am grateful to my Thesis supervisor **Prof. Dr. Subarna Shakya** for his cooperative support, guidance and suggestion at various stages of the Thesis, especially at times of dire straits. I deeply value his work as my mentor by providing me with constant counseling and precious feedbacks on Thesis progress. I am also very grateful to our Program Coordinator **Dr. Sanjeeb Prasad Pandey** for providing valuable guidance and feedback. I would also like to express my sincere thanks to **Prof. Dr. Sashidhar Ram Joshi** and **Dr. Basanta Joshi** for providing precious suggestions about thesis concept and its inception.
I would also like to thank **Dr. Arun Timilsena** and **Dr. Aman Shakya** for their constant support and encouragement on research activity during masters program. I would like to express sincere gratitude to **Dr. Diwakar Raj pant**, HOD Department of Electronics and Computer Engineering and Deputy HOD **Dr. Nanda Bikram Adhikari** and **Dinesh Baniya** for providing sound academic environment.

Lastly, I would like to thank all who were directly/indirectly involved in this thesis.

Abstract

Denial of Service (DoS) attacks constitute one of the major threats and among the hardest security problems in todays Internet. Of particular concern are Distributed Denial of Service (DDoS) attacks, whose impact can be proportionally severe. With little or no advance warning, a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time. Because of the seriousness of the problem many defense mechanisms have been proposed to combat these attacks. This thesis work has been carried out to prevent flood based DDoS attack in collaborative manner. Detection of anomaly traffic is being carried out with exponential moving average and t-digest model which will calculate the extreme quantile very accurately. In each flowing packet, identification field has been modified so as to have router identification which will then used to detect and drop the packet after identification of attack.After detection of attack traffic at node near victim, the attack information is being shared with other router and each router will act upon the attack traffic so as to drop these packets at the node near the attack source.

Keywords *DDoS attack,Defense against DDoS, Router to Router Model*

Contents

List of Figures

List of Tables

Abbreviations

IDS	**I**ntrusion **D**etection **S**ystem
DDoS	**D**istributed **D**enial of **S**ervice **A**ttack
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
BGP	**B**order **G**ateway **P**rotocol
NS3	**N**etwork **S**imulator 3
PPM	**P**robabilistic **P**acket **M**arking
EMA	**E**xponential **M**oving **A**verage
SMA	**S**imple **M**oving **A**verage
MSE	**M**ean **S**quared **E**rror

Chapter 1

Introduction

The denial of service attack refers to disruption of service at target machine. This can be done either by exploiting the software vulnerabilities of target machine/system or sending massive volumes of legitimate traffic so as to occupy and overwhelm all the resources that could being handled by target machine. According to WWW Security FAQ [1], Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests can not get through. Most of DDoS attacks take advantage of the large number of hosts on the Internet that have poor or no security. In order to compromise the victims key resources (such as bandwidth and CPU time), the attacker have to aggregate a big volume of malicious traffic. Most of the time, the attacker collects many of zombie machines or bots to flood packets simultaneously, which forms a Distributed Denial of Service(DDoS) attack.

A denial-of-service (DoS) attack occurs when the victim receives a malicious stream of packets that exhausts some key resource; this results in denial-of-service to the victims legitimate clients.The attack may exhaust a key resource by misusing some vulnerability in the software running at the victim (vulnerability attacks) or by simply sending a higher volume of traffic than the victim is provisioned to handle (flooding attacks). Vulnerability attacks usually contain packets of a special type or content to perform the exploit. As vulnerabilities can frequently be exploited by a few packets, vulnerability attacks are of a low-volume. Both of these features (special type packets and low volume) simplify handling of vulnerability attacks.

The victim can either patch its vulnerability or detect the special type packets and handle them separately. Flooding attacks overwhelm the victims resource by sheer volume. This strategy is more difficult to counter, as malicious packets can be of any type or content and the high volume hinders detailed traffic analysis. As DoS attacks involve only one attacking machine, a common approach to defending against flooding attacks is to equip the victim with abundant resources. The attacker then needs to find and subvert a better-provisioned machine to perform a successful attack. The difficulty of the attackers task to find the adequate agent machine increases with the amount resources allocated to the victim. The Figure 1.1 below shows the increase in DDoS attack in terms of bandwidth usage at the victim. It can be see how serious is the problem by looking at this figure as the victim gets overwhelmed by 500Gbps of traffic in 2015.

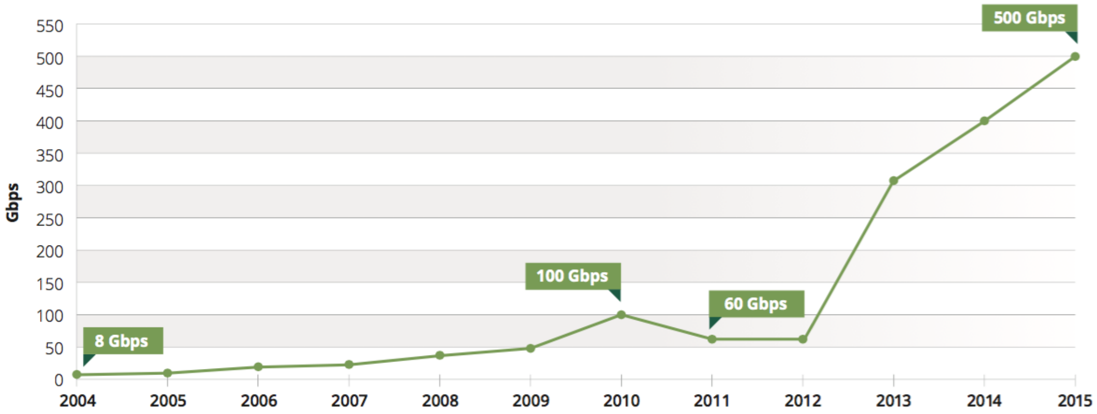

FIGURE 1.1: Survey peak attack size year over year
Source: Arbor Networks

1.1 Type of Attack

Preventing or mitigating DDoS attacks is not an easy job. First we have to understand how the attacks work. To achieve the goal of DDoS, the adversary can adopt various means: It can study the flaws of communication protocols (or their implementations) and insert malformed or bogus packets to subvert the legitimate communications. This kind of attacks can be called semantic attacks. In semantic attacks, a single machine can complete the attack goal, since one malformed packet is enough to imped the service. Semantic attacks can be prevented by fixing the corresponding bugs in the protocols or applications. While usually the adversary does not need to inspect the implementation of protocols, it may just flood seemingly legitimate traffic to congest the victims network or keep the victim busy processing the packets, so that the legitimate clients cannot get served. This kind of attacks can be called brute force attacks. To successfully flood packets to overwhelm the victims network, usually the adversary needs to recruit many compromised machines or zombies to flood packets simultaneously. Brute force attacks are the most common forms of the distributed denial of service attacks. The focus of this thesis is to defend against brute force attacks.

1.1.1 Semantic attack

Some typical examples of semantic attacks are:

Teardrop

The adversary sends incorrect IP fragments to the target. The target machine may crash if it does not implement TCP/IP fragmentation reassembly code properly. This kind of attack can be prevented by fixing the IP implementation bugs in operating systems.

Ping of Death

A ping of death is an attack that the adversary sends the victim a ping packet which has more than 65535 bytes. Since many systems can not handle ping packets larger than 65535 bytes, handling packets of this size may cause a buffer overflow which may cause a system crash.

BGP Poisoning

The BGP protocol is used to establish routing paths between networks in Autonomous system level. The routing information is updated by exchanging the BGP advertisement between routers. Usually, the routers update their routing tables without verification of the BGP advertisements. The adversary can subvert the network communication by announcing a better route to some destinations, then all the packets to the destinations are routed to the adversary. Also the adversary can disturb the BGP routing by announcing fake BGP advertisements with addresses of other routers. Then the corresponding traffic will be routed to those routers which do not have optimal routes to the destination.

1.1.2 Brute Force attack

Brute force attacks aim at exhausting the victims network bandwidth or computing resources by means of flooding massive malicious packets. To deplete the victims computation resources, the adversary usually uses the packets of Internet protocols which have request-reply scheme, such as TCP, HTTP. During the attacks, massive spurious requests are flooded to keep the target busy serving them, thus impeding the legitimate usage. To deplete the bandwidth, the adversary can basically flood any types of packets to congest the target network link. Examples can be UDP flooding and ICMP flooding.

SYN Flood

In a SYN flood attack, the adversary takes the advantage of the three-way hand- shake for a TCP connection. In normal execution, when a TCP server receives a SYN packet, it opens a session for this new connection and sends back a SYN/ACK packet to the initiator. When it reaches a timeout and there is no ACK packet received from the corresponding initiator, the session will be closed and the corresponding resources for the session are released. During the attack, the adversary continues sending SYN packets without sending back the final ACK packets for the TCP handshakes, the servers resource (e.g. memory) can be quickly depleted by maintaining many half open sessions, thus legitimate connection requests cannot be served.

HTTP Flood

In HTTP flood attacks, the adversary floods massive spurious HTTP requests for downloading a web file from the target server. This file is usually a large file that the server may need to load from the hard disc and spend considerable CPU time to transfer it via packets. However, continuously requesting big files can be suspicious. To avoid being detected, the adversary can instruct zombie machines to get a specific web page as the start and then follow the links on that page recursively, which can mimic the normal web browsing behaviors.

ICMP Flood (Smurf Attack)

In an ICMP flood attack, the adversary floods ICMP Echo packets to some network which broadcasts these messages to all the hosts in the network. These ICMP Echo packets have the victims IP address. All the hosts who receive the echo packet will send Echo reply packets to the victim, which exhaust the victims bandwidth. Actually, this kind of attack is a mixture of a semantic attack with brute force. The way the attack works is based on response mechanism in ICMP. However, from the perspective of the victim, it is brute force, as the type of the attack is just flooding packets from many machines. Similar to ICMP flooding attack, the adversary can take advantages of any reply-based protocol to launch reflected attack, by spoofing requests from the victim to a large set of Internet servers, resulting in a big volume of reply messages towards the victim network.

UDP Flood

During a UDP flood attack, the victims network is overwhelmed by a large volume of UDP packets. The attack packets are usually with random port numbers. When the victim receives a packet, if there is no application listening at the corresponding port, then the victim may generate an ICMP packet of ”destination unreachable” to the sender. Thus massive UDP packets to the victim's inactive ports may exhaust both incoming and outgoing capacities of the victim.

1.2 Chalanges of DDoS

DDoS attacks are powerful, since the adversary can get very big aggregated bandwidth from many compromised machine, it is very easy to overwhelm the victims network due the asymmetry of the bandwidth resources. Defending against DDoS is a difficult task, not only because of its big attack scale, but also because of the various strategies that the attacker can adopt. In particular, challenges for DDoS defense include:

The attacking sources are distributed In DDoS attacks, the attacking traffic consists of many malicious flows originating from hosts which are usually scattered among the Internet. If the malicious traffic is composed of a huge number of small malicious flows, it is difficult to distinguish the good and malicious traffic. Besides, the Internet infrastructure seldom provides services to the end hosts for controlling traffic sent to them. Instead, based on the end-to-end paradigm or simple core and complex edge, when packets are forwarded in the Internet, the intermediate networks (especially the core routers) will do the best-effort to deliver the packets to their destinations. So when DDoS attacks happen the victim usually does not have the ability to prevent the traffic of others from reaching its network. It is frequently necessary to have a distributed, possibly coordinated response system. It is also desirable that the defense mechanism can be deployed in a distributed manner at many points of the Internet, thus filtering the malicious traffic as much as possible before it reaches the target. However, global deployment is always hard to achieve due to the distributed administration of the Internet.

IP spoofing is quite common in DDoS attacks IP spoofing refers to assigning an IP packet with a source address which is not the address of the sender. The attacker can use spoofed IP addresses in the malicious packets to cover the real identities of the attacking sources. IP spoofing may affect the accuracy of the counter measures of DDoS attacks. Since some of the attack detection mechanisms identify the abnormal traffic by source addresses, if the source addresses are spoofed, traffic from innocent hosts may be blocked but the malicious traffic may still reach the victim if the attacker changes addresses in the malicious packets.

The attack rate can be dynamic During a DDoS attack, all zombie machines may flood the victim simultaneously with all their sending capacities. The aggregated attack traffic can suddenly grow far beyond the target link capacity. However, big abrupt changes of the traffic can be easily detected, so the adversary may gradually increase the attack traffic rate to consume the link bandwidth slowly to avoid being discovered. The adversary can also attack the target link with periodic short traffic bursts (which refers to pulsing attack) that keep protocols who have congestion-control mechanisms, such as TCP, sending packets with low rates.

The attacker may have various attack abilities It would be even worse, if the adversary can combine other malicious behaviors with DDoS attacks. For example, the adversary may eavesdrop some network links and it can analyze packets sent by legitimate hosts (which is referred as sniffing); the attacker may also pretend to be other network hosts (which is referred as man-in-the-middle) so that it may subvert the corresponding communications of other hosts; several malicious hosts may even collude to confuse or deceive legitimate hosts or network administrative entities. So the problem is even more complicated and difficult, if we want to deal with such powerful attackers.

The legitimate traffic should be affected as little as possible Mitigating is always a two-fold project: On one hand, the illegitimate traffic should be filtered as much as possible, while on the other hand, the network performance for the legitimate traffic should be degraded as little as possible. Actually, there is a trade-off between the two aspects of the project: to effectively and accurately filter out malicious traffic, fine-grained traffic inspection or classification algorithms are needed. However, the time complexity of such inspection or classification procedures is not trivial. Continuously operating such algorithms will definitely harm the throughput of the legitimate traffic, since packets may be queued in the checking entities and need more time to be forwarded. Due to the big scale of the DDoS attacks (e.g. the attack rate can reach more than 10Gbps), the network checking entities which execute packet inspections and filtering may run out of resources and become potential targets of the DDoS attacks.

1.3 Defense Approach

The defense mechanisms for the DOS can be categorized into three basic models: (1) the Victim Model (VM), (2) the Victim-Router Model (VRM), (3) the Router-Router Model (RRM). Each model is classified according to where the defense mechanism is employed, and how the network components, such as the victim and router, cooperate together.

1.3.1 Victim Model (VM)

The VM is a traditional defense model that identifies and filters attack traffic at a single location, namely, the victim. The key issue of the VM is to be able to identify the attack traffic pattern accurately and efficiently.

1.3.2 Victim-Router Model (VRM)

The VRM is a cooperative model that identifies and filters the attack traffic at multiple locations. The defense process is triggered by the signal from a victim and accomplished with the cooperation from participating routers. There are two key points for this model. The first is that the victim identifies the attack source using information inserted by the upstream routers. The second is that the victim directs the routers close to the attack sources to filter attack traffic. To implement this model, routers need to run a lightweight packet marking process to include path information into the packets. In addition, the victim needs to analyze the incoming packets to locate the attack sources. Once the victim identifies the attack sources, control messages will be sent to the routers that are adjacent to the attack sources. The routers will then start to filter attack traffic according to the received control messages.

1.3.3 Router-Router Model (RRM)

The RRM is a distributed defense model that detects the attack traffic by sharing information among participating routers. The ultimate goal of DDoS defense is to filter attack traffic close to the attack sources so that both network and server resources will be saved. Therefore, routers close to attack sources should be able to identify attack traffic quickly and accurately.In the RRM model, each router reports any suspicious network behavior to other routers. At the same time, each router combines the reports from other routers with network statistics observed locally to decide whether an attack has happened.This thesis aim techniques for defending against DDoS attacks using Router-Router Model.

1.4 Problem Statement

There are different ways to defend against the Denial of Service. The detection and prevention of DDoS attack is challenging day by day. Most DDoS attack includes large volume of traffic which will then compromise the victim . Due to this unnecessary traffic will float in the different network operator.The challenge is to develop a scalable mechanism so that the DoS traffic will be stopped at the source end without misclassifying any legitimate traffic.

1.5 Objectives

The objective of this thesis work is

1. Detect the anomaly for time series network packet flood attack
2. Share the attack information among router as as to minimize the effect of DDoS attack.

1.6 Scope of the work

Most of DDoS attack happen in two way. One is due to vulnerable in application software and other is with sending flood of valid traffic until target networ/system's die due to run out of cpu/memory. As attack for vulnerable software machine may be fixed by fixing the application package, this study is only limited to attack due to network flood attack which might be any flood(udp flood, icmp flood and other).Also this study will be limited to the simulation case in network simulator (NS3).So there might be difference in regards to real world router in terms of memory/disk and processing capacity.

Chapter 2

Literature Review

A numerous approach has been proposed to combat the denial of service attack so far. Due to very versatile nature of architecture, device and protocol being used in internet, it is very difficult to have a single system which would responsible to defend against DoS attack. Some of privious work are described below which are related to proposed work.

Talpade [2] designed a scalable network monitoring system called NOMAD which is able to detect network anomalies by making statistical analysis of IP packet header information. It is useful for detecting anomaly of local network traffic but does not support for high bandwidth traffic which are aggregated from distributed sources.

Another detection method uses the Management Information Base (MIB) data from routers. The router has different packet and routing statistics which is provided by MIB data. Different statistical patterns of MIB data were identified by Cabrera [3] which helps to identify early detection of DDoS attack. But this approach is found to be effective for controlled traffic loads only, it further requires to be evaluated in real network environment.

Huang and Pullen [4] proposed a method based on statistical analysis of subset of dropped packets due to congestion. If anamolous traffic is indicated by statistical results, a signal is sent to the router to filter the malicious packets.

Lee and Stolfo [5] use data mining techniques to discover patterns of system features and describe program and user behaviour and compute a classifier that can recognize anamalies and intrusions. This approach focuses on the host based intrusion detection.

Mirkovic [6] proposed a system which is based on source based attack prevention. The system can be installed at the edge routers of network and monitors the traffic flowing through it. If there is packet which are found to be assymetrical to normal, then the system will limit the flow of packet. If there is assymetry in the packet rate for short duration, then there might be false positive result.

ICMP traceback has been proposed by Bellovin [7]. According to this mechanism, every router samples the forwarding the packets with a low probability (1 out of 20,000) and sends an ICMP traceback message to the destination. If enough traceback messages are gathered at the victim, the source of traffic can be found by constructing a chain of traceback messages. A mojor issue of this approach is the validation of the traceback packets. It can be gurentee that every router will implement a certificate-based scheme to prevent false ICMP message from attacker. An alternative to this method is proposed called Intention-Driven ICMP Traceback [8].

Probabilistic packet marking (PPM) was originally introduced by Savage [9], who described efficient ways to encode partial route path information and include the traceback data in IP packets. It is an approach that can be applied during or after an attack, and it does not require any additional network traffic, router storage, or packet size increase. Even though it is not impossible to reconstruct an ordered network path using an unordered collection of router samples, it requires the victim to receive a large amount of packets. The advantage of this approach is that no extra traffic is generated, since the extra information is bound to the packets. Furthermore, there is no interaction with ISPs and this mechanism can be used to trace attacks after an attack has completed.

Song and Perrig [10] improved the performance of PPM and suggested the use of hash chains for authenticating routers. They use a 5-bit distance field, but they do not fragment router messages. This marking scheme is efficient and accurate in the presence of a large number of DDoS and a clever encoding scheme is used to reduce the storage space requirements. On the other hand, this mechanism assumes that the victim has a map of upstream routers to all attackers and its incremental deployment is not supported.

Adler [11] and Park and Lee [12] study tradeoffs for various parameters in PPM. Park and Lee propose to put the distributed filters on the routers and filter the packets according to the network topology. This scheme can stop the spoofed traffic at an early stage. However, in order to be effective, there is a need to know the topology of the

Internet and the routing policy between Autonomous Systems, which is hard to achieve in the expanding Internet.

A new packet marking technique and agent design has been proposed by Tupakula [13] to identify the approximate source (nearest router) of the attack with a single packet, even in case of attacks with spoofed source addresses. The scheme is a controlleragent model invoked only during attack times which not only is able to process the victims traffic separately without disturbing other traffic but, also to establish different attack signatures for different attacking sources.

Snoeren [14] proposed a hash based IP traceback technique that uses a source path isolation engine. It generates audit trails of traffic and can trace the origin of single IP packet delivered by a network in recent past. It uses a very efficient method to store the information that a packet traversed through a particular router. The main advantage of it over ICMP traceback messages and PPM is that it can traceback the attack path even for low volume packets received at the victim.

Traffic Pattern Analysis [15] is another method in order to response to DDoS attacks. During a DDoS attack, traffic pattern data can be stored and then analyzed after the attack in order to find specific characteristics and features that may indicate an attack. The results from this analysis of data can be used in order to update load balancing and throttling techniques as well as in developing new filtering mechanisms in order to achieve the prevention from DDoS attacks.

Chapter 3

Research Methodology

Due to distributed nature of Internet, sophistication and strength of attacks also becomes distributed and hence numerous defense mechanism have been proposed to defense against such distributed attacks. Every network connected to Internet is working as per the policy defined by its network operator. Attack will be generated and propagated through different network operator and reach the target machine. Based on following assumption, the defense against such attacks has been carried our in this thesis.

- If a traffic at some node is found to be increased suddenly, then this could lead for probable attack. [16]
- For effective prevention, each node along the traffic should be aware of present network condition so that is deploy better prevention.
- The communication channel is secure for sharing the information between routers.
- After detection of anomaly, the privileged and unprivileged traffic will be distinguished by XOR packet marking scheme [17].

3.1 Architecture Overview

The architecture of the current work includes three phase

- Anomaly Detection

- Packet Marking
- Sharing the attak

These are further discussed below.

3.1.1 Anomaly Detection

The anomaly detection has been carried our by calculating Exponential Moving Agerage (EMA). Firstly, the time series data has been fed to the model which calculate the difference between actual value and predicated value.

Choosing Exponential Moving Average over Simple Moving Average(SMA) is that the EMA gives more weight to recent data than the SMA does. Because of this difference, the EMA responds more quickly in regard to the latest traffic changes. According to Wikipedia[18], An exponential moving average (EMA), also known as an exponentially weighted moving average (EWMA), is a type of infinite impulse response filter that applies weighting factors which decrease exponentially. The weighting for each older datum decreases exponentially, never reaching zero. The graph at below shows an example of the weight decrease

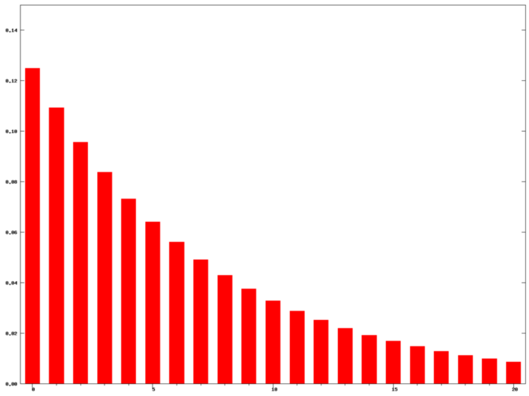

Figure 3.1: Weighting factor for EMA
Source: Wikipedia

The EMA for a series Y is calculated recursively:

$S_1 = Y_1$

for $t > 1, S_t = \alpha \cdot Y_t + (1 - \alpha) \cdot S_{t-1}$

Where:

- The coefficient α represents the degree of weighting decrease, a constant smoothing factor between 0 and 1. A higher α discounts older observations faster.
- Y_t is the value at a time period t.
- S_t is the value of the EMA at any time period t.

The following diagram describes the model

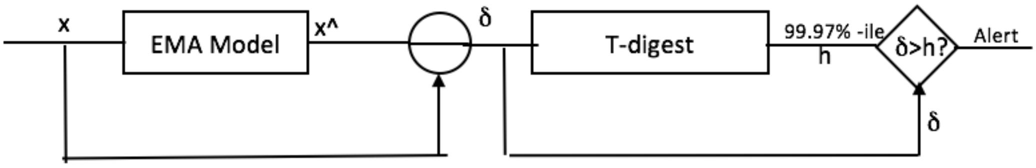

Figure 3.2: Anamoly Detection Model

The time series network traffic are fed into the input of model first. Those traffic are then categorized according to services to which they are destined for. According to destination traffic, next value is being predicated by Exponential Moving Average. Both input value and predicated value are being fed into difference engine which then calculate difference. The difference becomes the input for TDigest Model proposed by Ted [19]. TDigest calculates the percentile value for each difference input. If the percentile is more than 99.97, then it can be said that current traffic is anomalous.

3.1.2 Packet Marking

Each packet flowing into the router gets marked. The marking consists of two files of 17 bits. This 17 bit is taken out of 16-bit identification field and 1 bit from reserved flag field. The first field is called path field, which is 12 bit digest of the path that the packet has traversed. The router signature will get injected into the path field. The router signature is taken from router own ip address. Router signature is bits of 0-2,9-11,17-19,25-27 are taken from routers 32 bit IP address. The selection of bit is carried out to avoid same signature for different router because of similar network address if consecutive 12 bits are taken. The marking will be done in such a way that, if the packet first arrives at edge router, then the path field equals to the router signature. For the other router, it will be XOR of existing path field and the current router signature.The second is called distance field which is 5 bit long. It is set to 0 when the packet first arrives at the edge router and increments for successive traverse of packet.

Algorithm 1: Marking Algorithm

```
if Edge Router then
    pkt.path = router signature;
    pkt.distance = 0;
else
    pkt.path = pkt.path $\oplus$ router signature;
    pkt.distance++;
end
```

3.1.3 Sharing the Attack

Because of marking procedure, all the packet that traversed through router gets marked and arrive at the victim. And victim gets distinctive IP header marking for each packet. Once the alarm for attack is fired, victim knows about the attack and it is assumed that victim has knowledge of ongoing DDoS attack. So when the attack is detected, detection system at victim use the marking of the incoming packet and share it with the other router. The attack information is only shared to the router from which the attack is being generated. This can be done simply by xoring the router signature of upstream router with the current signature of router. The router then use the signature to detect the source of attack traffic and share with the source router.

Algorithm 2: Sharing attack information

```
For each upstream router if pkt.path = router signature(current router) then
    return upstream router
else
    new path = pkt.path $\oplus$ router signature(upstream router);
    pkt.distance–;
end
```

3.1.4 Data Collection

For this thesis, the traffic is being generated by ns3 itself. The attack and normal traffic are both generated by ns3 application. The node generating normal traffic will generate at speed of 256kbps and the attack node will generate the traffic at higher speed.The attack traffic is generated at the speed of 2Mbps and is being generated at the time of 3rd, 5th, 8th, 12th, 17th, 23thhour for 15 minutes. The traffic generator follows an On/Off pattern as provided by ns3, called On and Off states. The duration of each of these states is determined with the onTime and the offTime variables. During the Off state, no traffic is generated. During the On state, traffic is generated. This traffic is characterized by the specified data rate.

Chapter 4

Result and Analysis

4.1 Calculation of value of α

As mentioned in section 3.1.1, the EMA for a series Y is calculated recursively:
$S_1 = Y_1$
for $t > 1, S_t = \alpha \cdot Y_t + (1 - \alpha) \cdot S_{t-1}$

The value of α has to be calculated so that it will detect anomaly traffic and also keep record of past entries. The average of network traffic is being stored every minute and exponential moving average is calculated. The value of α is incrementally increased from 0 to 1. For each α, the difference between Y_t and S_t is calculated. The difference is then squared and averaged to get Mean Squared Error. α is to be chosen for which it has least Mean Squared Error and it is calculated as 0.032.

4.2 NS3 Simulation Environment

The experiment has been carried out in NS3. It is a discrete-event network simulator, targeted primarily for research and educational use. NS-3 is free software, licensed under the GNU GPLv2 license. The table below describes Simulation Environment for NS-3 that has been considered while doing this thesis work.

Total Nodes	12
Attack Nodes	2(3 node send normal traffic other intermediate)
Simulation Time	24 hour
Attack rate	2Mbps
Normal rate	256kbps

Table 4.1: Simulation Environment

Following network topology as shown in 4.1 is being used to carry out this thesis work. In which 2 of host connected to two nodes acts as attack source and one server node is treated as victim.

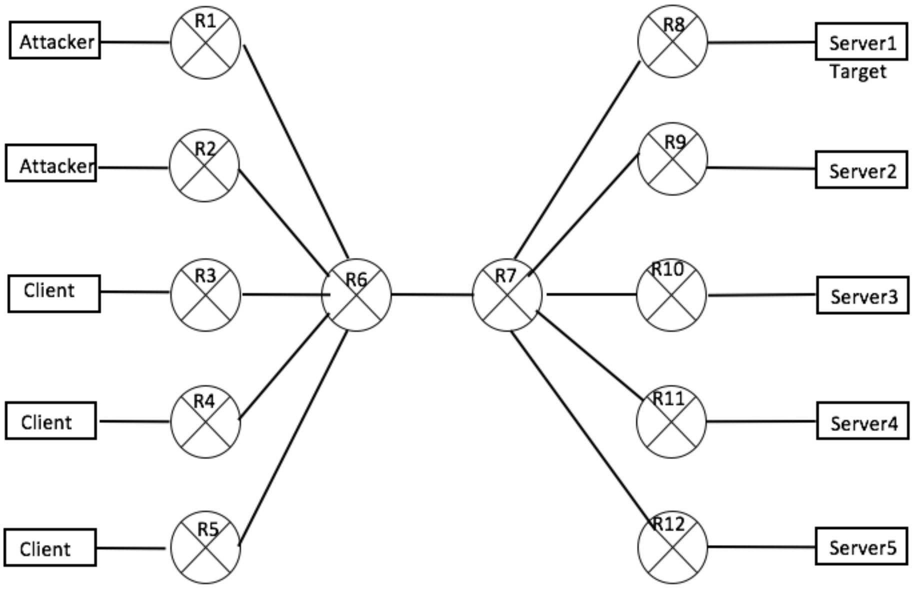

Figure 4.1: Network diagram used for experiment

4.3 Anomaly Detection and Sharing among router

Anomaly is being detected with the t-digest model which will take input as difference between traffic flowing into the router and corresponding exponential moving average.The traffic flowing through a node connected to victim is depicted in Figure 4.2.The figure also has information for anomaly level which is found to be equal to 1 for the traffic where there is increase in network traffic to high level. For the other part it is found to be 0. When the attack is being detected, the anomaly level is found to be 1 and the corresponding router get attack alert.

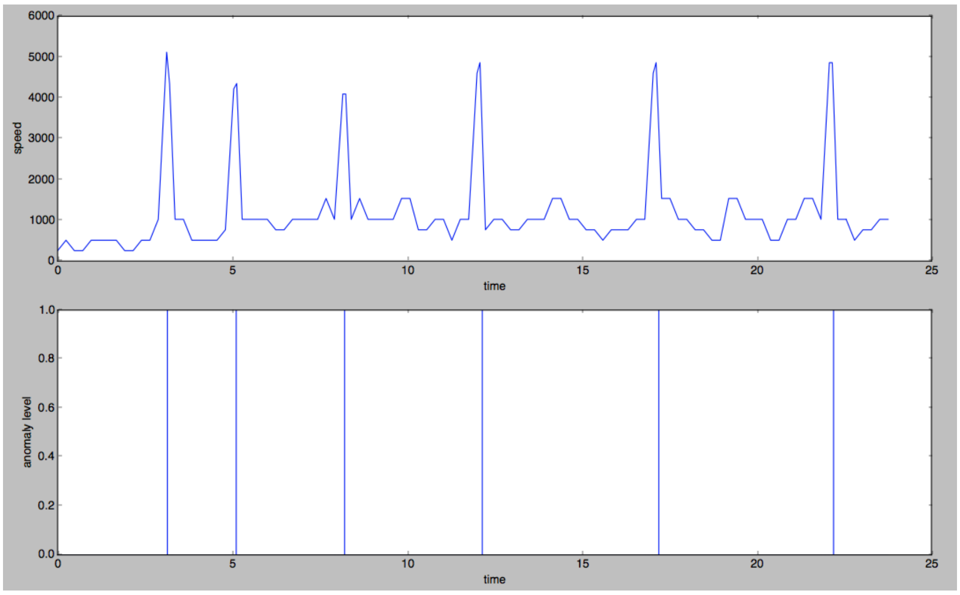

FIGURE 4.2: Anomaly Detection Model and T-Digest outcome

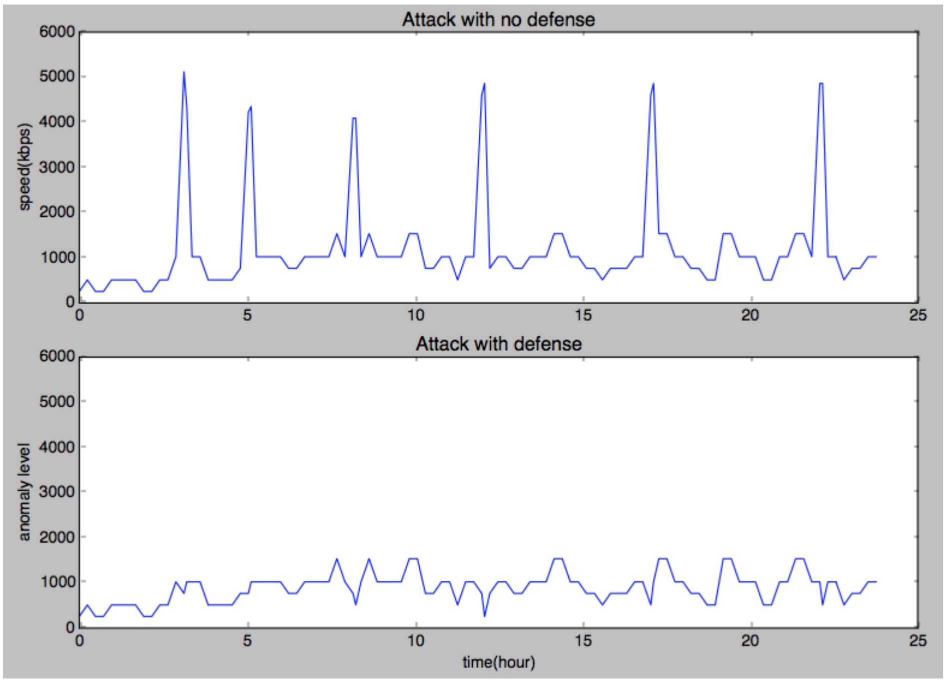

FIGURE 4.3: Attack traffic with and without defense

Then victim will analyse look for attack signature and select the attack traffic to share it with the router from where the attack originates. The attack source router has been identified by algorithm 2. After the source router near the attak has been identified, the source end will analyse it and drop the attack traffic.The Figure 4.3 shows the traffic without defense mechanism being applied at top and with the application of defense approach at the buttom.

Chapter 5

Conclusion and Limitation

It is crucial to detect the DoS flooding attacks at their early launching stage before widespread damages done to legitimate applications on the many victim system. This thesis work is based on detecting the flood based anomaly that is flowing into the router and alert corresponding router having attack traffic detected. With the help of victim, the attack information is being shared to corresponding router which the packet traverses. The attack source is been identified with the help of marking algorithm instead ot t-digest because there might be the case that there is no or very slight change in traffic at node near attack source but the rate is higher at the node near victim. After successful identification of node near source, The router will then block those attack traffic at the early stage.

Detecting the anomaly traffic is key point of any DoS attack which is carried out in this thesis work successfully. However the source address service identification has not been carried out automatically in this thesis work which can be considered as limitation of the work. Since this is done manually, no false positive and false negative alarm analysis has been carried out.

Though there are numerous approach proposed and analysed for combating dos attack and all have different approaches for solving different area field of dos attack. There are different method and approaches to extend for finding anomaly traffic. One can use p-value and z-score further to have more accurate anomaly score. One could also add a method for victim to automatically calculate the attack source. Also more parameters could be used so as to defend against more number of attackers.

References and Bibliography

[1] Lincoln D Stein and JN Stewart. The world wide web security faq, version 3.1. 2. *World Wide Web Consortium (W3C)*, 2002.

[2] Rajesh Talpade, Gitae Kim, and Sumit Khurana. Nomad: Traffic-based network monitoring framework for anomaly detection. In *Computers and Communications, 1999. Proceedings. IEEE International Symposium on*, pages 442–451. IEEE, 1999.

[3] Joao BD Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravil K Prasanth, B Ravichandran, and Raman K Mehra. Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study. In *Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on*, pages 609–622. IEEE, 2001.

[4] Yih Huang and J Mark Pullen. Countering denial-of-service attacks using congestion triggered packet sampling and filtering. In *Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on*, pages 490–494. IEEE, 2001.

[5] Wenke Lee, Salvatore J Stolfo, et al. Data mining approaches for intrusion detection. In *Usenix security*, 1998.

[6] Jelena Mirkovic, Gregory Prier, and Peter Reiher. Attacking ddos at the source. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, pages 312–321. IEEE, 2002.

[7] SM Bellovin. Icmp traceback messagesinternet draft. *Network Working Group*, 2000.

[8] Allison Mankin, Daniel Massey, Chien-Lung Wu, Shyhtsun Felix Wu, and Lixia Zhang. On design and evaluation of" intention-driven" icmp traceback. In *Computer*

Communications and Networks, 2001. Proceedings. Tenth International Conference on, pages 159–165. IEEE, 2001.

[9] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Network support for ip traceback. *IEEE/ACM Transactions on Networking (TON)*, 9(3):226–237, 2001.

[10] Dawn Xiaodong Song and Adrian Perrig. Advanced and authenticated marking schemes for ip traceback. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 878–886. IEEE, 2001.

[11] Micah Adler. Tradeoffs in probabilistic packet marking for ip traceback. In *In Proceedings of 34th ACM Symposium on Theory of Computing (STOC*. Citeseer, 2001.

[12] Kihong Park and Heejo Lee. On the effectiveness of probabilistic packet marking for ip traceback under denial of service attack. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 1, pages 338–347. IEEE, 2001.

[13] Udaya Kiran Tupakula and Vijay Varadharajan. A practical method to counteract denial of service attacks. In *Proceedings of the 26th Australasian computer science conference-Volume 16*, pages 275–284. Australian Computer Society, Inc., 2003.

[14] Alex C Snoeren, Craig Partridge, Luis A Sanchez, Christine E Jones, Fabrice Tchakountio, Stephen T Kent, and W Timothy Strayer. Hash-based ip traceback. In *ACM SIGCOMM Computer Communication Review*, pages 3–14. ACM, 2001.

[15] Ruby B Lee. Taxonomies of distributed denial of service networks, attacks, tools, and countermeasures. *Princeton University*, 2004.

[16] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[17] K Stefanidis and DN Serpanos. Packet-marking scheme for ddos attack prevention. *Published by*, page 97, 2005.

[18] Wikipedia. Exponential moving average, 2013. URL https://en.wikipedia.org/wiki/Moving_average.

[19] TED DUNNING and OTMAR ERTL. Computing extremely accurate quantiles using t-digests. 2013.