Enhanced Distributed Defense Mechanism Against Volumetric DDoS Attacks

نظام دفاع موزع ومحسن ضد الهجمات الحجمية لحجب الخدمة

Student name: Emad Bani Melhem

Student number: 401220088

Supervisor: Dr. Maamoun Ahmed

A Thesis Submitted in Partial Fulfillment of the Requirements for

The Degree of Master of Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

August – 2016

Delegation

Authorization Statement

I, Emad Kamel Nahar Bani Melhem, authorize Middle East University to supply hard and electronic copies of my thesis to libraries, establishments, bodies and institutions concerned with research and scientific studies upon request, according to the university regulations.

Name: Emad Kamel Nahar Bani Melhem

Date: 6/8/2016

Signature: ……

Committee Decision

This is to certifying that the thesis entitled "Enhanced Distributed Defense Mechanism Against Volumetric DDoS Attacks" was successfully defended and approved on August 8-2016.

Examination Committee Member **Signature**

(Head of Committee)

1- Dr. Ahmad Abu Shareh .....

(Member & Supervisor)

2- Dr. Ahmad Al-Kayed on behalf of **Dr. Maamoun Ahmed**

.....

(External Committee Member)

3- Dr. Mohammad A. Shkoukani Applied Science University

.....

Acknowledgment

Prior to acknowledgments, I must glorify Allah the Almighty for His blessings who gave me courage and patience to carry out this work successfully.

Then I would like to express my deepest gratitude to my Advisor: Dr. Ahmad Abu Shareha for his persistent support and his guidance in answering all my questions about my research, I also wish to express my deepest gratitude to the members of the committee for spending their precious time on reading my thesis and giving me encouragement and constructive comments. I would like to thank all Information Technology Faculty members at Middle East University, and Thanks to my father; I could not do anything without you.

Last but not least a big thank to my loving family, my mother, my brother and my sister I love you all.

Table of Contents

Contents

List of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Appendix

List of Tables

Enhanced Distributed Defense Mechanism against Volumetric DDoS Attacks using Speak-up

By Student: Emad Bani Melhem

Student number: 401220088

Supervisor: Dr. Maamoun Ahmed

Abstract

One of the multifaceted issues in security field is Denial of Service (DoS) attack. At the beginnings of 80th, DoS abbreviation was known for the first time as a usual security issue, later on in 1999, the first incident of a Denial of Service (DoS) attack was reported, since then, the majority of DOS attacks are then distributed by default. These days' attacks are done and controlled remotely using well organized botnets, distributed widely and recruited carefully with sharp constraints, to serve a specific goal.

The major challenge that faces the establishing of a comprehensive defending mechanism against those attacks is that they done in a different shapes with different concentration points with different intensives. Due to this end, this research proposed an enhanced system for distributed defense mechanism against volumetric Distributed DOS (DDoS) attacks. This work proposed a defense mechanism based on an existed defense mechanism called, Speak Up, with the goal of enhancing the defending against volumetric DDoS attacks.

This thesis proposes lower levels in bandwidth consumption due to the proposed methodology it follows for that purpose. This research results shows that the enhanced system of Speak Up defense mechanism outperforms Speak Up mechanism in terms of defending, and bandwidth consumption.

Keywords: Enhanced Distributed Defense Mechanism against Volumetric, multifaceted issues in security field.

نظام دفاع موزع ومحسن ضد الهجمات الحجمية لحجب الخدمة

إعداد

عماد كامل بني ملحم

إشراف

د. مأمون الأحمد

الملخص

تعد هجمات حجب الخدمة (دوس) واحدة من القضـــايا متعددة الأوجه في مجال الأمن. ففي بدايات 80، حين عرف هذا الاختصـــار لأول مرة وكانت معروفة باعتبارها قضـــية أمن معتادة، في وقت لاحق في عام 1999، تم الإبلاغ عن الحادث الأول من هجمات حجب الخدمة (دوس)، منذ ذلك الحين، فإن غالبية الهجمات (دوس) تأتي موزعه بطبيعتها. تتم هجمات هذه الأيام "والتحكم فيها عن بعد باســـتخدام تشـــكيلات منظمة تنظيما جيدا، وزعت على نطاق واســـع وتم تجنيدهم بعناية مع تحديدات دقيقة، لخدمة هدف معين.

ويتمثل التحدي الرئيســـي الذي يواجه تأســـيس آلية دفاع شـــاملة ضـــد تلك الهجمات هو أنها تتم في أشـــكال مختلفة مع نقاط تركيز مختلفة مع دوافع مختلفة. ونظرا لهذه الغاية، اقترح هذا البحث نظام معزز لآلية دفاع موزعة ضد هجمات حجم الخدمة الكمية. استند هذا العمل على آلية دفاع موجودة أصلا تدعى "سبيك اب"، وذلك بهدف تعزيز الدفاع ضد هجمات حجب الخدمة الحجمية.

وتقدم هذه الأطروحة مستويات أقل في استهلاك عرض النطاق الترددي بسبب المنهجية المقترحة المعدة لهذا الغرض. وتبين نتائج البحوث أن هذا النظام المعزز للتحدث إلينا آلية الدفاع المطورة تتفوق على الالية الأصلية من حيث كفاءة الدفاع، واستهلاك عرض النطاق الترددي.

الكلمات المفتاحية : نظام دفاع موزع ومحسن، هجمات حجب الخدمة .

CHAPTER ONE
INTRODUCTION

In computer science, Denial of Service (DoS) in a network system can be defined as the system inability to serve legitimate users as they normally should. This denial of service occurred as a result of what so called DoS attack. Both computers and networks are demanding specific number of things to be operated properly, like, the bandwidth of the network, storage and available storage space, scheduling of CPU jobs, the way network resources communicate, as well as specific resources that relates to the surrounding environment, such as, electrical power, surrounding air's temperature, or water, etc. DoS attacks such resources in computers and networks.

1.1 Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Denial-of-service attacks can disable ones computer or network. Some denial-of-service attacks can be launched using limited capabilities resources targeting a relatively big and complicated site. This attack type is called "asymmetric attack." An attacker whose PC is quite old in addition to its slow modem possibly will result in disabling a machine that has higher specifications on the attacked system (Spirit, 2013). Overall, there are many forms of DoS attack, such as

1. Attempting to "flood" a network's communications channels, in that way, the legitimate traffic of a network is prevented.
2. Attempts to interrupt the connection between two or more equipment, thus, preventing any access to some service.
3. Attempts to deny the user's right to access or use some resources.
4. Attempts to disturb service to be assembled to a particular system or individual.

Distributed Denial-of-Service (DoS) attack is formed by several subverted machines, called agents, which generate a big traffic against the attacked device in order to devastating its resources and connected devices. DDoS attacks are an embodiment of offence ideally in the Internet world. Committing a DDoS attack demands little knowledge or skills. Attackers would not be frightened against punishment, since it is very difficult to trace back the attack's origin, not even agent machines, allow unaccompanied offender who ruined them. On the other hand, lacking of efficient defenses at the victim side leads to massive harm during the entire attack's period (Mirkovic et al.; 2003). DDoS characteristics hold back any successful defense, for the following reasons:

- **Large Amount of Data Flow**: Comprehensive attack generates large amount of data, which can prevent any defense mechanism. Autonomous defense is held-back since it can be done nearby the affected device. The system should alternate to processing separate packets in a reasonable sustain among the flow.
- **Apparently Legal Transmitted Packets:** Packets sent by an attacker may have the same characteristics as legal packets. This is because the intruder aims at consuming volume, regardless of the content, to cause harm. Therefore, the defending mechanism cannot attain a judgment depending on individual packets, excluding maintaining a reasonable number of statistics to compare packets and identify abnormalities.
- **Precise Recognition:** The system necessitates recognizing the entire attacks or at least most of them which impose harm among the victim.
- **Efficient Reaction:** The system must decrease the flow of attacks to convenient ranks, in spite of their volume or distribution.
- **Selective Response:** The system must distinguish among both legitimate packets and attack packets. Moreover, The system must ensure high-quality service to legitimate

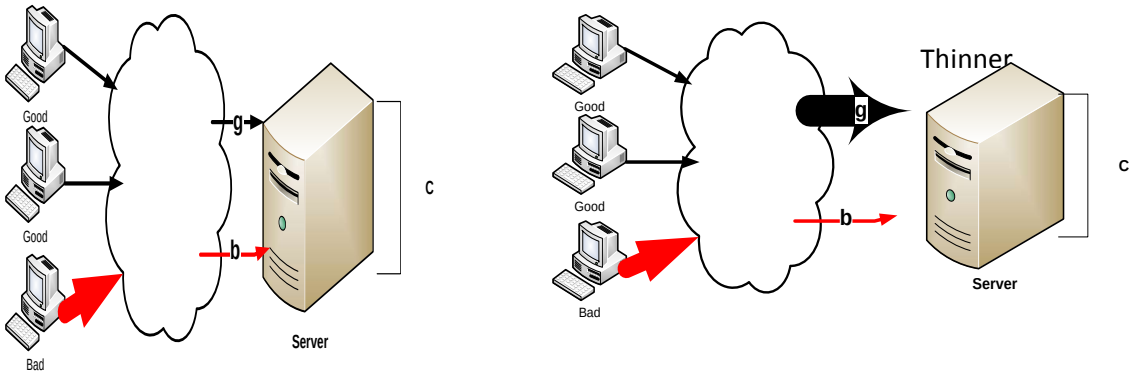
packets in network traffic throughout the attack. Harm resulted from defending the attack must be less than the harm caused by legitimate packets by clients in the nonattendance of responding (Mirkovic et al., 2003).

Given the difficulties of defending DoS and DDoS attacks and the harms causing by these attacks, there is a need for protection mechanisms to protect the network from such threat, whether it came from inside or the outside of the organization operating that network system (Agrawal et al. 2015).

1.2 Speak-Up Technique

Speak-Up technique was developed by Michael Walfish (2007). The whole idea was motivated by a simple observation that says: "attacker sends requests to a victimized server in much higher rate than legitimate users", in other words attacker attempt to overflow connection links, routers, or any waiting queues on the server side to prevent legitimate request to access.

In speak up, a server that suspects an attacks, encourages connected devices to send more request packets and uses that as a payment to gain specific service. The bad clients (attackers) are not able to respond to such encouragement since they already exhaust their available bandwidth generating the attack. Encouragement process is done by a server front-end facade called "thinner" that also protect attacked server from becoming overload. As such, the rate of legitimate request will be increased to be as equal ore more than the attacker requests and makes them more represented on server side. Figure 1.1 illustrates the speak up mechanism.



(a) without speak up **(b) with speak up**

Figure 1. 1 : An Attacked Server (Spirit, 2013).

Figure 1.1 shows that, B + g > c. The legitimate clients' traffic is in Figure 1.1 black (Walfish et al., 2010). Subsequently, the goal of speak-up is to crowed out bad request using the good request which will facilitate capturing a bigger portion of the servers resources applying the technique of defense by offense.

Dagon, et al., (2007) classify attacking pots into three types (i) based on how they transmit data: 1) those who are using DSL\cable 2) pots who are using modems, and 3) those who are using "high speed" networks. According to Dagon, et al., (2007), this grouping is reasonable, as it is being standard in industry like commodity database they are mapping connection types classified upon these categories. Besides, Dagon, et al., (2007) provide a mathematical model to represent the average available bandwidth in a "botnet" B (Gbps):

$$B = \sum_{i=1}^{3}(M_i - A_i)P_i W_i \ldots\ldots\ldots\ldots\ldots\ (1)$$

where, M_i is the average maximum bandwidth within each type (i), A_i is the average normal usage of bandwidth within each type, P_i is the probability of a pot to be belonging to type (i). P_i is calculated and set to P1 = 0.3, P2 = 0.6 and P3 = 0.1. W_i is the average hours-per-day that use each type (i) and were estimated as [0.0625, 0.1875, 0.75].

According to Walfish et al (2010) observation, B in bad client's (attack participated), is less than B in good clients. In the real-life attack scenario the intermediate-network should deal with ordinary daily loads from legitimate users and B Gbps extra loads from attackers without applying "speak up" scheme. With "speak up" scheme, the intermediate-network must be dealing with ordinary daily loads plus extra loads composed of B Gbps from attackers and B Gbps from legitimate users as a payment.

However, speak-up has some drawbacks and disadvantages, these are: high capabilities requirements and network bandwidth consumption. As for the requirements, although Speak Up mechanism is a smart defense method, it requires a server with a high capabilities and extra space and it needs to inflate intermediate network with extra legitimate request (payment requests). As for the bandwidth consumption, Speak Up consumes a huge portion of intermediate-network bandwidth.

1.3 Problem Statement

The majority of DDoS attacks in term of type are bandwidth DDOS attacks. Therefore; the current speak Up defense has a drawback as it depends on bandwidth limit as currency-based approach and it was intended to defense against application-level attacks. On February 2012, RADWARE Security Report published a security report, they concluded that application-level attacks in general and HTTP attacks in particular does not need to be huge sized to make damage and most of application-level attacks was carried out using 10 mbps of bandwidth or less as shown in Figure 1.2 (Ron Meyran, 2012). Subsequently, this size of attacks will never be noticed by speak up technique.

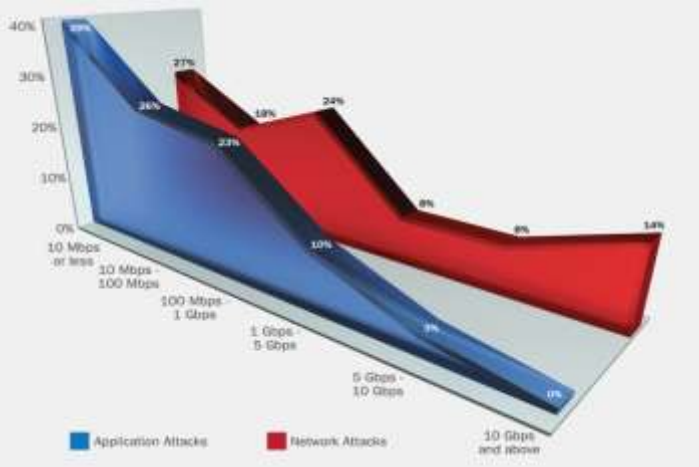


Figure1. 2: RADWARE Security Report, Network vs. Application by Bandwidth.

The second issue in speak up is the massive consumption in intermediate-network resources (Zargar et al., 2013). This problem caused by the distance between thinner and client as possible. The last problem of Speak UP is caused by the huge amount of requests as a result of good requests, bad requests, and payments requests. The served requests from good client during a specific amount of time will be affected, because these requests have to go through a lot of lines and bottlenecks crowding the other requests to reach its distention (victimized server). Subsequently, the research problem above can be further divided into the following sub-problems:

- How to decrease the intermediate-network crowds of Speak Up mechanism during attacks.
- How to quantify the effects of the number of bad clients and how.
- How to modify Speak Up to serve more good clients.

1.4 Research Goal and Objectives

The goal of this research is to propose an efficient defense approach against DDoS bandwidth attacks without depending on historical information but real time information instead, in order to

react on front of attack. This system should deal with any client according to his current attempt, without loading the intermediate-network with any extra loads. This will be achieved by following these research objectives:

1- To enhance Speak Up approach by increasing number of served requests.
2- To maintain a good serves under increasing number of bad clients.
3- To prove that applying this technique on the ISP's is more profitable than applying it at the server side as it is on the original approach.

1.5 Research Justification and Motivation

In the 3rd quarter of 2014 Akamai's "state of the Internet" published a report describing the trend of recent DDoS attacks by comparing them to 3rd quarter of 2013, and the report shows up the results which indicate the continuous increasing of bandwidth attacks, as illustrated in Table 1.1.

Table 1. 1: Trend of Recent DDoS Attacks Comparing to 3rd Quarter of 2013.

Criterion	Inc.\Dec	Percentage
Total DDoS attacks	Inc.	22%
Average attack bandwidth	Inc.	389%
Average peak packets per second	Inc.	366%
Application layer-attack	Dec	44%
Infrastructure-layer attack	Inc.	43%
Average attack duration	Inc.	5%

The Arbor Networks studies showed that attack size has doubled over the year 2010, and with the increase of bandwidth to 100 Gbps registered for the first time then.

In 2014, Arbor Security Engineering and Response Team (ASERT) monitored and observed DDoS attacks that targeting Hong-Kong in September and October (2014), and they concluded that 84%

and 88% of the attacks had been done using 10-20 Gb\sec data flow (bandwidth attacks) as shown in Figure 1.3.

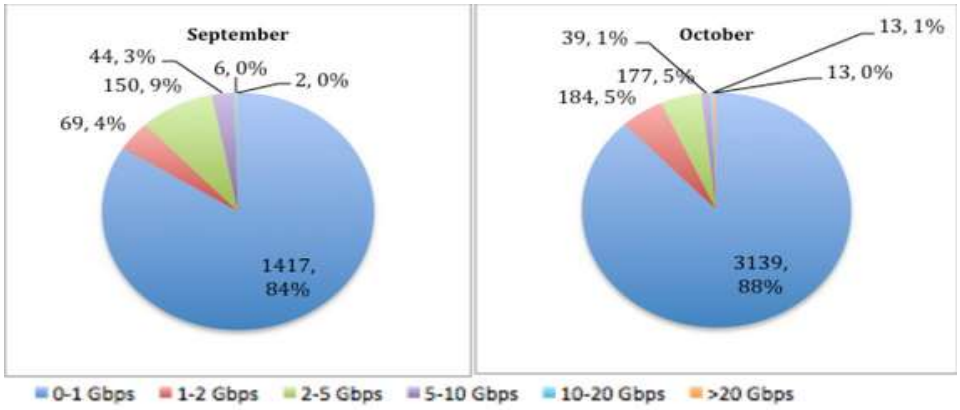


Figure1. 3: Arbor Network, Percentage of Attacks within a Given Size Range

Such traffic can confuse not only a certain destination point but all surrounding network infrastructure and even any defense system too, so these results (Akamai, state of the Internet report 2014, arbor network, and 2014) were a major motivation factor to orient the research's effort to build a defense system specialized in bandwidth attacks.

Speak up is efficient in dealing with unequal request or misleading or smart bots, if the server receives request loads from machines that wasn't symmetric under the currency-based approach, clients are loaded more with requests even if the server has no knowledge of those requests ahead, if attacker attempt to spoof his related IP addresses, speak up still able to identify them, unlike other identifying and blocking techniques, similarly, some smarter bots might have the ability to mimic legitimate requests and pass by the defense profiling mechanism.

This research proposes modern enhanced DDoS defense system that distribute the original approach into sub-sequent units called sub thinners and place them on the ISP's which makes the

response much more effective and customized to deal with the attack side only without disturbing the whole network with extra data.

1.6 Scope and Limitations

This research is targeting (volumetric) attack only that is the major causative of DDoS attack according to (Akamai, state of the Internet report 2014).

1.7 Research Contribution and Significance

The contribution of this research can be summarized as follows:

- Review the forms of DoS and DDoS attacks and the state-of-the-art defending approaches.
- Adopt an enhancing mechanism based on Speak Up defense mechanism.
- Reduce the bandwidth consumption during DDoS attack that it is decreased in noticeable manner.

The significance of this research emerges from the needs to develop a defense approach that is more capable of defending DDoS attach, reduce the number of bytes exchanged, and filtering bad bytes (sent from attackers) from good bytes (sent by legitimate clients), by making them much more represented at the server side. This research could open the gate to encouraging other researchers to think of more enhancements on Speak Up characteristics, which may lead to higher levels of Network Security.

1.8 Thesis Outline

This thesis is organized in five chapters. **Chapter One** introduced the research topic, formulated the problems, addressed the research questions and objectives, stated the research significance and research contribution in the literature. **Chapter Two** will discuss the related works and compare them based on their technical approach. **Chapter Three** gives the research methods, techniques,

approaches and processes. **Chapter Four** presents the proposed design, implementation and testing of the proposed work, side by side with the evaluation measures and the findings of the evaluation. Finally, in **Chapter Five**, the future works and recommendations are inducted.

CHAPTER TWO

LITERATURE REVIEW

Distributed denial of service (DDOS) attack can cause huge harms as it has ability to render a network inoperable or cut down service delivery. The aim of a DDOS attacker is to flood the servers, networks, and computers with endless requests to the extent that they are unable to execute the desired services. Fortunately, there are continuous developments of defensive techniques that prevent DDOS attacks.

The available DDoS defensive techniques vary depends on the mode of operation, the medium used and the resources required. This chapter provides a detailed review and analysis of various literature dedicated for DDOS attack defense.

2.1 Introduction

In the current era, there is a wide trend for businesses to host websites that allows the customers to access their account information, track financials and etc. Moreover, some businesses is depend precisely on their online availability, and without this ability productivity and profitability plummets. With the presence of DDoS attack, such type of modern business is subject to huge harms and loss. DDoS attack aim to exploit many recruited resources to generate huge traffic that can overwhelm the bandwidth, resources, access links of a victimized server., DDoS prevents legitimate users to access their demanding resources and cause a severe damage with little warning and much to recover. Subsequently, many researches had been held to design, apply, and evaluate defense mechanisms against this type of cyber-attacks.

2.2 Background

In this section, a background on the attacks type, intensions and process are given. The purpose of declaring the attacks related issues is to develop an efficient defending mechanism based on the characteristics of these attacks. DDoS attack is illustrated in Figure 2.1.

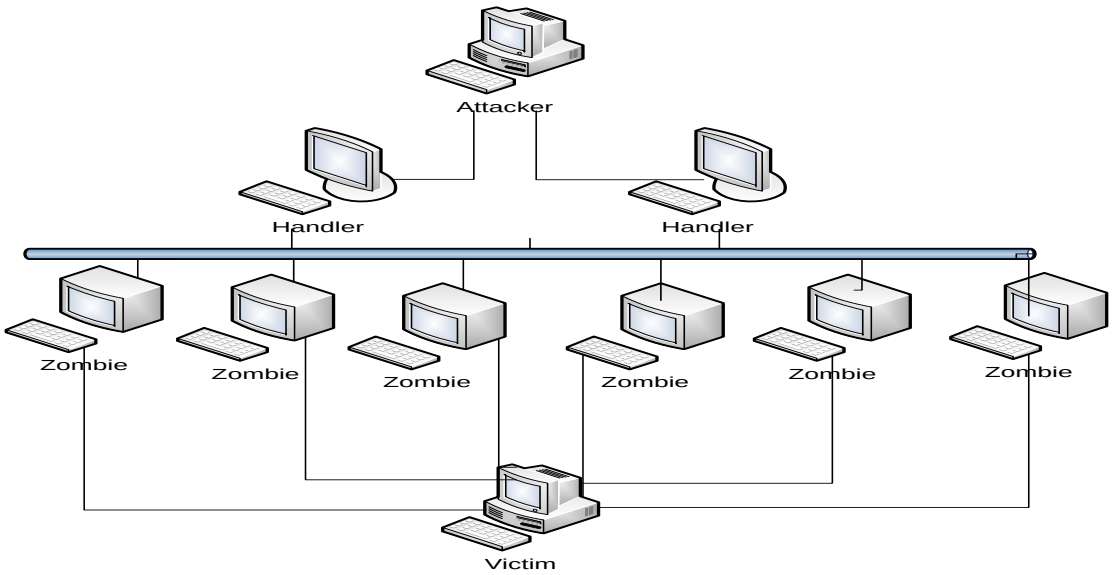


Figure 2. 1: DDoS Attack (Spirit, 2013)

2.2.1 Attacks Targets

Since DoS attacks can be in many different forms, the targets of the attacks are as follows:

Network Connectivity

Network connectivity is the most vulnerable area in a system targeted by DoS attackers. The main aim is to prevent proper communication between network components. In such attack's type, the attacker starts the procedures by creating a connection to the victim machine, though he makes sure to prevent the final connection completion. Meanwhile, the victim machine has held in reserve one of an incomplete numerous data, which are necessary to complete the awaiting connection. This resulted in denying the legitimate connections, though, the infected resource keeps waiting

for a connection that is fake and keeps a connection open waiting for it to end. Noticeably, this type of attack is not based on the attacker ability in consuming the victim's network bandwidth. Because in this case, the attacker only uses the core data for the creation of a network connection. As a conclusion to the aforementioned; any attacker is capable of carrying out this type of attack using a slow, dial-up connection against a machine that operated in a high speed network. For that end specially, this attack is considered as an optimal illustration of an 'asymmetric attack'.

Using a victims resources as the attack's source

The attacker can use the victim's own network resources to work against him. In such a case, the attacker sends un-real UDP packets and repeats an "echo" command to keep two devices busy. This results in reserving big amounts (if not all) of the network bandwidth between the two ends. This means that the entire network has been affected by the attack as well as the connected devices that initiated the connection

Consuming the network's bandwidth

An attacker to the system creates various, many packets, and transmits them through a network, which will consume the bandwidth but in vain. These packets are mostly ICMP ECHO packets, but in theory they might be anything else. Furthermore, the intruder requires the non-operating of a single machine, which means that he might be able to synchronize quite a lot of machines within altered networks for attaining the identical consequence purposes.

Other Resources' Consumption:

Intruders is able to consum other resources that forms the core of any system. However, in several systems, only a few data structures are used to hold process information, such as; process

identifiers, process entries, process slots and etc. The attacker might consider consuming these data structures using a targeting program or a program that simply makes multiple copies of itself continually. Various operating systems currently have a quota of facilities to defend itself against such attacks. Moreover, if the table of process is not overflowing yet, the CPU can consume time and process scheduling in switching amongst processes.

Changing or destroying configuration settings

Configuring a computer's components improperly could make that computer run as required or might not even run at all. The attacker can make devastating changes to a computer's configuration settings intentionally. However, if the intruder is able to change the configuration of the router, the connected network could be disabled. If an intruder can manipulate registry entries on a Windows NT operating server for example, then specific tasks might become unavailable.

Destroying or changing physical network components

This is more into physical protection. The attacker must not have to computers peripherals, routers, network wires, storage closets, and energy and cooling facilities, as well as whichever significant network components.

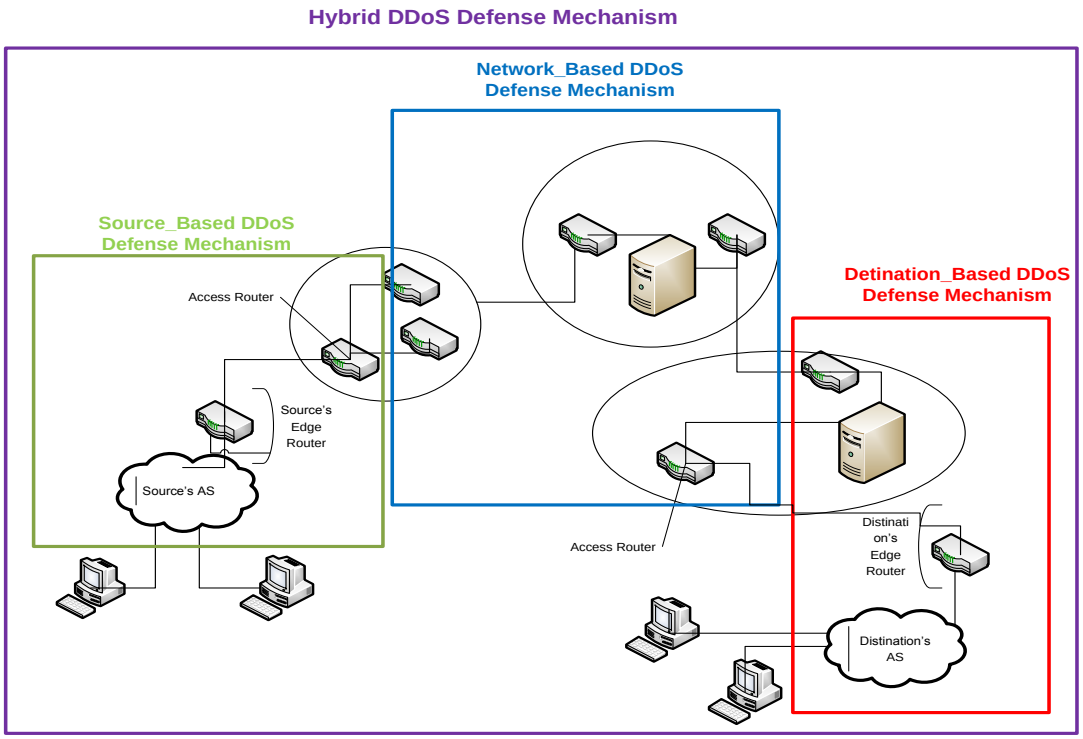


Figure 2. 2: Locations of Performing DDoS Detection & Response (Zargar, et al., 2013).

2.2.2 Attacker Intension

Each attacker is being driven by some reason, whatever was his purpose, the attack will leads to a single result at the end. However, there is a relation between the attackers intension and the defending mechanism. Understanding the attacker intension leads to decision-making models to stop and respond to such attacks. Overall, attackers' incentives can be:

1. **Financial Gains**: For example, the advertising sites are charging Google for each click on their Google-related advertisement. In order to make more money, botnets can be directed to click on such advertisement. This type is the most technical and hard to prevent.
2. **Revenge**: Attackers may launch an attack as a reaction of perceived injustice. Attackers of such intension, mostly, have less technical skills than the others.

3. **Ideological Belief**: Attackers may launch an attack because they belong to a specific group sharing the same thoughts and principles. Currently, such intension this a major incentives. For instance, political incentives led for sabotage attack on wikileaks, in 2010 (Pras, et al, 2012).
4. **Intellectual Challenge**: The attackers may launch an attack because they want to learn more or show their cyber muscles to their peers. Usually, such attackers do not make huge harm as they are less technical skilled.
5. **Cyper warfare**: The attackers may launch an attack as terrorist activities targeting economic, health, transportation systems or any infrastructure that depends on e-networks of a country. For instance, the attackes on nine USA banks on September, 2012 (Lozada, 2014).

2.2.3 Attack Launching Process

There are common steps that any attacker should follow to carry out an attack; these are (Bhuyan, et al, 2011):

- Collect information about the target network and gather vulnerabilities information that might help.
- Assessing the vulnerabilities from the previous step and recruit some network's node.
- Launch attack using recruited nodes and exploiting their resources.
- Cleaning up by deleting all registry or log history at the victim side to erase any sign of a crime.

Attacker use gathering information tools like Nmap to scan the network for loopholes then he uses malicious code to recruit participating nodes (zombies, slaves, or bots) then he elects some of them

act as passengers between attacker and nodes called (masters, handlers, or controller) and then uses them to launch and control attack by sending the orders.

There are many ways to launch an attack some attackers use Trojans or worms to disrupt a system or network, others might use attack launching tools such as IRPAS & ETTERCAP (Hoque, et al, 2014).

2.2.4 Internet-based DDoS Attacks

Two main techniques are currently widely employed on the internet to perform DDoS attacks (Zargar, et al, 2013). First: targeting a specific protocol or application that resides and runs on the victim side by sending malformed packets to confuse it's work like vulnerabilities attack that depend on the ordinary behavior of a protocol such as TCP & HTTP and use it to the advantage of attacker by handcuffing computational resources. Second: The other one which is the most accruing is that attacker tries to do one or both of:

- Prevent access of legitimate users by exhaust victim's bandwidth.
- Prevent rightful user from reaching a resource's service by over-using resources at the attacked computer's side.

2.2.5 Bandwidth Attack

Bandwidth attack is a type of denial of service attacks which based on sending a huge volume of traffic to a specific destination(e.g. server , site, ISP etc), doing so leads to consume destination system's connection links or waiting queues, making the access for legitimate user denied since the server (for example) is overloaded by a volumetric traffic and it can't handle any extra work load, attacks that target the bandwidth cause more harm than the ones that target consuming a

networks resource (Alomari, et al, 2012), these attacks usually involve a large number of participating systems called "potnets" or zombies with spoofed IP addresses leaded by one system called the "pot master" remotely via C&C command and control channel like Internet Relay Chat (IRC) commonly as a communication protocol (Zhuge, 2007).

Attackers usually make a use of two features to make their attack more powerful (Zargar, et al, 2013) reflection & amplification:

- Reflection is when an intruder transmits a SYN request to a specific server but from a not real IP address which is the victim address so the server directs response to victim system instead of attackers.
- Amplification is when attacker use a specific feature in a protocol like broadcast IP to generate number of message by sending only one.

Attackers attempt to make use of these two features combined together like in DNS amplification attack, since DNS response is usually has larger size than DNS request it considered as amplification and then reflect the attack to the victim system.

2.3 Related Work

Various defense mechanism were built trying to detect, mitigate, prevent those attacks as (Fu, 2012) classified them according to their activity level proactive defense, reactive defense, and DDoS detection. There are three basic steps to stop any DDoS attack:

- **Detection**: it is the most important part, when a technique is able to differentiate between attack and ordinary high traffic load after, during, or even after an attack.
- **Filtering**: In this step, technique tries to distinguish between participating requests and legitimate requests.

- **Response**: Most of methods do some kind of reaction to make sure it will not happening again from the same source. Like blocking or profiling a participating IP addresses.

The most comprehensive classification criteria were provided by Zargar, et al., (2013), which deployed the location of setting the defense mechanism, this could be at the source, the network, the destination or a hybrid of location.

Source-based mechanisms are installed and activated as much near as possible to network costumers to usually on the edge router of their local network or the access router's that connect sources' to prevent them from carrying out DDoS attacks, like the famous Ingress\Egress filtering at the source edge router (Ferguson, 2000).

Defense mechanisms on the destination's side is the opposite of source-based it resides and is applied at the destination side (victim) more specifically at the router on the edge of autonomous system (AS) or the access router of the destination, the good part of it is since it near to the victim it can touch the normal behavior of the victim and observe any anomalies. Hop-count filtering represents a good example (Wang, et al., 2007).

Network-based mechanism, this type is meant to deploy at the autonomous systems "AS s " routers, the main purpose is to detect attacks and react in the intermediate networks between source and destination of an attack, (Wang, et al., 2007), represent good scheme for doing so. All of previous methods are committed to a specific location, in other words these techniques are centralized (source, network, and destination), and this measured as a main drawback. Figure 1.3 illustrates that detection accuracy increases when the employment is near to the victim. Prevention and response is more efficient if the employment was near to the source.

Hybrid defense mechanisms is the defense mechanisms witch have distributed components and employed on any side of the network (source side, distention side, or intermediate network), those components are usually cooperating with each other to give better results. Zargar, et al., (2013), classified defense by offense technique “speak up”, Walfish, et al., (2007) as a hybrid defense mechanism.

2.3.1 Speak Up and DEFCOM Defense Mechanism

Mirkovic, et al. (2003) propose DEFCOM as a method to exchange information through a distributed defense mechanism. The proposed solution usesnodes structured in such a way that each node has a specialized defense ability. It is more efficient to locate detecting nodes near to the source but in the other hand, it is more efficient to employ a responding node near to the victimized system. All nodes must be able to communicate with each other to ensure successful defensive processes. Each node in DEFCOM structure should be able to do the following:

1. Alert the rest of network of an impending attack.
2. Rate limiting request oriented to upstream nearby nodes.
3. Resource requests that passed downstream nodes (legitimate) are sent to their downstream nearby nodes.
4. Classifying network traffic is applied to the downstream neighbors to ensure the bulk of legitimate traffic will reach its destination unharmed.

It is evident that there is no benefit of doing other traffic classification to the traffic coming from the node that issues the alert. This is becausethe system limits the rate of traffic that is coming from upstream nodes.

Walfish, et al. (2010) evaluated a method for defense for application-level DDoS attacks, named Speak Up. Speak Up works in such a way that a server that is attacked calls for network resources to send large amounts of data over the network traffic. Assuming that attacker consume most of their available bandwidth, the attackers are not able to respond to these requests. Non-attacker nodes, however, has the ability to upload traffic requests since they still have enough upload bandwidth and will deal with the encouragement within significantly large data traffic over the network. The proposed result of this traffic indication is that the legitimate users' crowd-out the bad users with their exhausted bandwidth, thus capturing the insignificant data sent over the traffic, which represents the attack and utilizes resources as a correspondence. Walfish et al have found that Speak Up results in spend resources by the servers over a collection of consumers in uneven proportion to their accelerated upload bandwidth. This result makes the defense viable and effective for a class of real attacks. Nevertheless, this type of defense consumes lots of bandwidths, which motivates more research work to investigate modalities of circumventing the bandwidth utilization problem.

Mehta, et al (2008) describe a technique that uses two defenses mechanisms against distributed denial-of-service (DDoS) attacks; DeFCOM and Speak-Up.Theresults from the combined methods show significant improvement. DefCOM defense utilizes a source-end, victim-end, and core defenses into a combined cover to distinguish between good and bad DDoS traffic. Source networks that do not contribute in DefCOM often suffer from slow service and limited network traffic rate. This isbecause of core nodes in DefCOM that filters packets are deficient in cheap algorithms validation aimed to separate legal transmit from non-legal (attack) transmits on the network's speed. They have to presume privately that traffic with higher rates is more likely to originate from an attack. Therefore, while trying to accelerate DDoS, DefCOM denied service

throughout attacks to rightful network users. Meanwhile, Speak Up has become a hot topic of research recently as the new promising defense technique, which encourages all clients of an attacked system to send extra payment traffic, presuming that the attackers are already consuming all their bandwidth capacity. Clients that send much payment traffics are considered rightful users and consequently added to a 'whitelist'.

Mehta et al goes on to add that Speak Up does not cost much to be set up on client's machines, who are most likely to be DDoS victims, yet, the payment traffic is required to be sent constantly. This increases the traffic cost at the attacked machine contrary to the expectation of the network. The combination of Speak Up and DefCOM into a uniform defense mechanism targets the deficiency of the separate defenses and assures the success of a collective defense against DDoS attacks. Speak Up is integrated with the main defense techniques in DefCOM and classifies users according to their traffic weight. Furthermore, since Speak-up is performed in the core, payment and attack traffic will not reach the victim, and any heavy network traffic effects are restricted to the neighborhood in a legacy networking.

2.3.2 Filtering Mechanisms

Chen, et al. (2006) proposed solution named TRACK, which is a composed technique that marks router port module and packet filtering module.The router port module was designed to mark packets by writing a port number on the router interface probabilistically.This identifier consists of a local 6-digit and it will be added to any packet that the router wants to transmit. When these packets reach the victimized system through the attacking path, the system can use the data contained in it to trace back the attacker. Consequently, the packet filtering technique will use the same data attached to packets to mitigate malicious packets. Chen et al go on to add that the TRACK's resource consumption is low since it has low communication overhead. However, the

main problem is that the attacker can modify the identification fields of packets so he cannot be located.

Argyraki and Cheriton (2009) proposed solution known as AITF, which is a hybrid DDoS defense mechanism that allows the victimized system to warn attack source and ask them to stop sending packets. Failure to do so triggers the sender's ISP to start monitoring to ensure it obedience.Both ISPs should support AITF otherwise; it will lose all access to victimized system. Argyraki andCheriton(2009) believes that this provides a strong motivation for all ISP's to support AITF especially if the victimized system is a popular point of access. The study showed how two networks that support AITF could remain connected to each other and prevent DDOS attacks. AITF uses three-way handshake to verify if packets are malicious or not. Argyraki and Cheriton(2009) goes on to add that if an attack is going on and there were a flooded link out of AITF borders, the three-way handshake may not complete causing the filter not to be installed.

Wang and Sun (2014) proposes a defense mechanism that filters DDoS attacks. The filtering is considered significant because of its defending capability against both resource consumption at the attacked client and attacks that block links. However, there is a probability of false positive and the consumptionof router’s resources rapidly, which reduces the ability to exist filter-based approaches. As a solution to this problem, the Wang and Sun (2014) propose a new technique to minimize the effects of a DDoS attack. The solution utilizes the IP traceback results to get a graph of the attack that contains possible filtering routers. Considering different abilities of routers performances of the graph obtained, the proposed filtering scheme is able to spot out some of the filtering routers that would affect the performance of filtering and minimizing false positive. Results obtained from simulating real life network topologies showed that the proposed technique

couldideally reduce the damage by a DDoS attack, yet conserve the traffic to network resources to somehow normal levels.

Ferguson and Senie (2000)proposes a DDOS straightforward defensive method, which utilizes the concept of traffic filtering to block DoS attacks. The methodology works on the premise of filtering any false IP addresses that might be transmitted from the back-end of an ISP point of aggregation. The methodology proposed by Ferguson and Senie (2000) does not, however,prevent network flooding from valid IP addresses. The ISP are required to maintain a list of advertised IP prefixes with the aim of ascertaining the validity of IP addresses. Ingress traffic filtering allowsISPs to track the origin of a forged IP address that is trying to assume the identity of a legitimate of IP address. Liu, Yang, & Lu (2008) proposed a method known as StopIt, which is a hybrid filter-based DDoS defense mechanism. The mechanism uses authentication system like apassport to ensure that there is no source ID spoofing. Liu et al (2008)describe a closed- control and open-service structure that guarantee filter installation during an attack.StopIt is used by a receiver to block any traffic that is deemed to be undesirable. The design of StopIthas structured in such a way that it is capable of vending of numerous attacks from internet bots. This ability can be achieved in a very limited time and is normally executed within the router memory. A strength of StopIt over other filtering mechanisms is that it is capable of preventing DoS attacks without interfering with normal service delivery. StopIt servers should be in constant communication with other surrounding Stop it servers to ascertain any incoming authentication requests.The StopIt mechanism has a low capability-based performance whereby an attacker can flood the router and fails to reach the victim.

2.3.3 Botnet based DDoS Attacks

Alomari, et al. (2012) is of the opinion that DDoS attacks that employ Botnets on the application layer are the newest and most confusing threats towards to network security. The study by Alomari et al (2012) provides a detailed examination of the dangers presented by Botnets attacks within the application layer. Botnets attacks are particularly worse in a Web server environment. Some of the most popular Botnet tools used in web server environment include Black energy, Low-Orbit Ion Cannon, and Aldi Botnet. The most serious category of Botnet attacks takes the form of HTTP and SYN flooding.Botnets attack culminates in the limitation of resources, restriction on revenues, and huge financial losses.

An attacker normally performs aport scan to have a clear picture on where to execute an attack. Bhuyan et al (2011) argue that port scanning can be quite complex because it is difficult to distinguish between a scan by an attacker or by the network. With over 65, 536 ports on a typical computer, an attacker is capable of capitalizing on open TCP or UDP ports to launch an attack. Bhuyan et al (2011) describe various port scanning techniques notably stealth, SOCKS port, bounce, TCP, and UDP scanning. Port scan either can be single-sourced or distributed whereby in the former the attacker utilizes a single entry point while in the former the attacker uses multiple hosts to initiate the scan. The methodologies used to detect port scanning attempts vary depending on the mode of operation and the resources used. Port scanning detection can be performed based on the flow, packet, and the alert level. Bhuyan et al (2011) go on to add that the detection techniques can use algorithmic, clustered, visual, rule-based, threshold, and softcomputing paradigms. Each of these scan detection techniques is designed in such a way that it can operate in real or non-real time environment.

Zhugeet al (2007) describe a study aimed at measuring and assessing various Botnets phenomenon.The study is aimed at discovering botnet size, lifetime, commands, distribution channels, and control mechanisms. The study comprises an examination of 3290 IRC-based botnets in China and commissioned over a period of twelve months. The measurement techniques are based on three stages that start with malware collection, malware analysis, and ends with botnet tracking. Botnets use command and control channel and servers for distribution purposes. The study found that the average lifetime of a botnet in the command and control channel is 54 days. An interesting discovery from the study is that the size of a botnet is not easy to determine because it changes dynamically every day.

Dagon et al (2007) propose a methodology for classifying botnet structures based on key values to measure their adequacy against various threats like spam andDDoS attack. Using these performance measures, Dagon et al (2007) consider the capacity of different techniques to deal with corrupt or breach botnets. An important revelation in this study indicates that scale-free botnets tend to respond well to targeted responses. Any effort to improve the strength of scale-free networks decreases the corresponding transitivity. Botmastersare not structured in away designed to prevent the transitivity problem in scale-free networks. It also shows that botnets in random graphs have high resistance to any kind of feedback (whether random or targeted). Evaluation of the effect of these feedbacks simulated on different topologies is unified with the novel measurements performance in P2P network. The results classified botnets based on thestructure and ranked or given priority using the proposed metrics. This may help make feedback more directed and provide a guideline to general remediation strategies that have a high possibility to succeed.

Fu (2012) provides a description of efficient methods that can detect and lighten the effect of DDoS attacks whilst minimize the performance degradation of the network to the lowest values possible. Managing aDDoS attacks is complex activity considering their versatile properties that include thedynamic rate of attack, varying targets types, and large botnet scalability. The complexity of managing DDoS attacks thus calls for the implementation of theefficient defensive mechanism.Fu (2012) proposes an alternative known as aport-hopping technique that addresses the DDoS problem at the application level. The method described works by allowing multiple applications to initiate communication process through periodical switching of ports.This makes difficult for the attack to target the communication ports. Fu (2012) propose a detection method known as SIEVE designed to handle clock swings among the communicating entities especially when the time server does not have enough acknowledgment information. A lightweight filtering technique that is distributed along the network channel is proposed to address the problem of DDoS attacks through flooding the bandwidth. SIEVE is dependent upon the resources available to the attacker and therefore has the capability of providing an independent filter for moderate attacker techniques. An additional complimentary filter is provided in SIEV and can manage to circumvent strong attacks from equally complex attacker techniques.

According to Fu (2012), SIEVE utilizes an overlay network to construct a distributed filtering sieve that employs a simple meddler to help in the authentication of filtered network packets. SIEVE is also structured in a way that it has a self-protecting feature aimed at protecting the connection between authentic clients and protected servers. This model is essential because it helps to address the issue of Denial of Capability (DoC). The problem of DoC is addressed through an enhancement of the network capability. It is a challenging endeavor for both the networks and the associated hosts when recovering from a DDoS attack. Consequently, Fu (2012) advocates for the

adoption of a technique named CluB aimed at mitigating the problems associated with DDoS attacks. CluB provides a good balance between the effectiveness and trade-off by adequately dealing with the granularity of control issue within the network. CluB works in collaboration with various network routing methods.The solution proposed by Fu (2012) provides an analysis of an IP-prefix based technique aimed at detecting a DDoS attack during the early formation phases of a network communication session. An additional defensive solution that is based on the network data stream is advised to be implemented in a distributed environment.

Rescorla and Modadugu (2012) focuses majorly on the description of version 1.2 of the protocol used for the Datagram Transport Layer Security (DTLS). The DTLS protocol facilitates private communications for datagram protocols. The protocol allows client/server applications to interact without the interference of an eavesdropper, denying them the ability of tampering, or forging messages exchanged. The DTLS protocol uses the Transport Layer Security (TLS) protocol and provides guarantees to equal security amongst participating parties. Datagram semantics in the transport are preserved by the DTLS protocol. This study updates DTLS 1.0 to *work with TLS version* 1.2.

2.3.4 Defense Mechanisms against DDoS Flooding Attacks in IP Spoofing Network

Zargar, et al. (2013) describes a complete defense mechanism against known and predictable DDoS flooding attacks. DDoS attack can be implemented at various protocol levels but the most common one include the network, transport, and application levels. The common element in these categories of attack is that they serve to flood the communication channel. The flooding techniques can exploit the protocol such as HTTP, TCP, and UDP. Zargar et al (2013) goes on to add that Botnet forms a particularly worse group of DDoS attack and can be categorized into either of the

three subgroups notably IRC-based, web-based, and P2P-based. There are various defensive mechanisms aimed at counteracting the effect of a DDoS attack. They are classified based on the source, application, network, destination, and through a hybrid or distributed mechanism. Some of the notable techniques described by Zargar et al (2013) include TRACK, DEFCOM, COSSACK, and TVA. The defense mechanisms are measured using various performance metrics that include the strength of the defense, scalability, compromise ability, usability, implementation complexity, delay parameters, and system performance.

Kolahi, et al (2015) describes a detailed study on how a UDP attack can affect the throughput of a TCP channel. The study also analyzes the effect of a UDP flooding on processor utilization and cycle time in web server. The performance and the effect of UDP flooding are measured in Linux Ubuntu 13 platform.Kolahi et al (2015) go to analyze the impact of defense techniques on the performance of the web server. The defensive mechanism described include ACLs(Access Control Lists), Reverse Path Forwarding, Network Load Balancing, and Threshold Limit. The study concludes that Threshold Limit is the most efficient defensive mechanism against DDoS attack in a web server environment.

Patel and Patel (2014) propose a technique aimed at distinguishing bad and legitimate traffic as well as implementing a mechanism aimed at circumventing the underlying DDoS attacks. The research study is focused on a trivial attack whereby large volumes of therequest are propagated to a web server. Consequently, the web server is unable to handle these requests, which will cause it to crash or the entire website to go offline. Patel and Patel (2014) provide an analysis of the defense mechanisms that are implemented at both the application and network layers. Some of the notable defense mechanisms described include CAPTCHA, Speak up, defense and offense wall (DOW), concealed Markov wall, DDoS shield, and DAT among others. According to the survey

done by Patel and Patel (2014) approximately 80% of all the DDoS attacks emanates from HTTP flooding followed closely by UDP, SYN, and ICMP flooding in that order. The major component of the proposed system is that of differentiating between normal and attack traffic. The proposed system uses the Human Interaction Page (HIP) to make the necessary differentiation. The system maintains a white list of normal traffic to build a database of users who are allowed to pass through the HIP. The proposed mechanism provides a hybrid solution that measures the server load, identify the attack traffic, and eventually deny server access to the abnormal traffic.

Wang, et al. (2007) proposes and describes a filtering technique aimed at preventing DDoS attacks. The technique known as Hop-Count Filtering (HFC) is built on the premise of establishing the IP to Hp count values that are recorded in a mapping table. The IP to Hop count is used to aid in the detection and discarding of IP packets that are deemed to have been spoofed. The focus on the identification of spoofed packets is particularly important because the technique is used to hide the source of the flood traffic and to force legitimate traffic to assume and amplify the identity of flooding traffic. Wang et al (2007) therefore see the importance of filtering spoofed packets as an essential mechanism aimed at preventing DDoS attacks. The HFC technique described in the study is shown to demonstrate a 90% ability to correctly identify any spoofed packets within the network. Additionally, the HCF is able to discard the spoofed packets without affecting the performance and efficiency of the network.

Chouman et al (2005) proposed a simple mechanism for defense against DDoS attacks on edge routers and focused on un-real IP addresses.In this context,edge routers maintain a matching table of the outgoing SYNs and incoming SYN-ACKs to validate SYN-ACK segments and apply the ARP protocol. When SYN-ACK pairs donot match, it is considered a threat and the router is reset at the victim's end, enabling it to accept other legitimate connection requests only. The

proposed mechanism introduced a model to encourage different networks to cooperate in protecting each other. Testing this mechanism showed promising results.

Praset al (2010) analyzed two variants of a tool named LOIC (Low Orbit Ion Cannon), which is used by the attackers. The LOIC tool works by transmitting numerous HTTP, UDP, and TCP requests to the target server. The more advanced variant allows the attacker to include an Internet Relay Chat (IRC) that will assist in controlling the LOCI tool from a remote location. The LOIC tool can be used remotely and controlled automatically such that is capable of assuming the characteristics of a botnet.The analysis concluded that the attacks initiated using the tools were relatively simple and can reveal the identity of the attacker. This indicates that the name of the commonly known hacktivist group, "Anonymous Operation", is not so accurate because the attackers' original IP address can be found out easily. If a hacker uses this tool without an anonymization networks such as Tor, the real IP address of the attacker is known clearly, which helps in tracing back the attack. Moreover, since these tools do not use mature techniques, like IP-spoofing or reflected attack it becomes easy in detecting and preventing the attack. In addition, if the attacker has no knowledge that by international data retention laws, internet service providers (ISP) must provide storage of internet usage for at least 6 months, then it becomes easy to trace back the attacker even when the attack is outdated.

Meyran (2012) serves to provide insightful information aimed at debunking the myth that the effect of a DDoS attack is synonymous with the size of the flooding traffic or packet size. The reality is that size does not necessary matter and that majority of DDoS attacks are less that 10 Mbps. The type of the attack has a bigger ramification rather than the size of the attack. The Radware report described by Meyran (2012) indicates that HTTP and HTTPS flooding attacks have the most impact compared to large UDP attacks that spans in the range of 10 Gbps.Meyran (2012) goes on

to suggest that a firewall or an IPS alone is not enough to prevent a DDoS attack. The same report by Radware Group indicates that 32% of DDoS attacks were implemented due to weak links in firewall and IPS configurations. There is a need to perform a detailed risk analysis aimed at assessing the manner in which the business can withstand a DDoS attack. Additionally, it is vital to collect as much information as possible concerning the bandwidth, size, frequency, and type of potential DDoS attacks. The internet service provider (ISP) can easily supply this information. Further action calls for the deployment of anti-DoS software that are implemented above the firewall and IPS.

2.3.5 General Defense Mechanisms against DDoS Attacks

Chou, et al (2009) describes a proactive surge protection (PSP) technique that aims to form a kind of thefirst line defense against DDoS. The proposed system also has the ability to lessen the damage caused by the attack by isolating traffic flows in the bandwidth. The PSP technique can find application when upgrading an already existing router-based defense. A unique element of this technique is that it works independently without the need to understand the header information in an unauthenticated packet. Chou et al (2009) performed an evaluation work for the PSP technique in large commercial settings utilizing both distributed and targeted attacks. The results show that about 95.5% of the network might be severely destroyed, but applying the PSP mechanism reduced the amount of damage significantly. The number of packets lost dropped by 90.36%. The evaluation also showed that PSP can maintain lower levels of lost packets even with increased number of attacks.

Mishra, et al. (2011) aims to provide a detailed classification of the defensive mechanisms used to prevent DDoS attacks. Mishra et al (2011) go ahead to note that preventing a DDoS attacking is a

tough challenge and thus it is important to establish a mechanism that would assist in maximizing fault tolerance and the level of service delivery within the affected network. The defensive mechanisms are grouped into two major categories; fault tolerance and quality of service. Fault tolerance according to Mishra et al (2011) is applied at three different levels notably hardware, software, and system. Fault tolerance mechanisms ensure that the network is capable of offering the required services within the boundaries of the available resources. The quality of service mechanisms, on the other hand,ensure that the network is capable of delivering the desired output even after an attack. Some of the techniques used for quality of service includeIntServ, DiffServ, class-based queuing, throttling, pushback, proactive roaming of server, and accounting of resources.

Ranekarand BhagatPatil (2015) provide a detailed survey of the different mechanisms for defending DoS attacks. Traffic sampling is a technique that involves the analysis of traffic parameters such as IP header, size, protocol, request type, and transmission and access time. This helps to identify and separate legitimate and attack traffic. Another technique incorporates the use of client puzzles to assist in the authentication process. Ranekar and BhagatPatil (2015) go on to describe another mitigation technique that is based on packet filtering and implemented through probabilistic functions and hop counts. Another technique described in the survey incorporates a mechanism whereby the network processing ability is used to segregate various types of traffic and to enforce quality of service within the network. Other techniques include IP traceback, use of attack graphs in a virtual environment, swing defense technique, and router throttle among others.

Luo, et al. (2015) provides a survey of current DDoSattacks and the available defense techniques. The study finds that a defense mechanism is mostly needed for successful defense against DDoS. Luo et al (2015) stress the importance of understanding the principles of Software-Defined

Networking (SDN) and how it used to manage modern network architectures. The survey points out that SDN has powerful capabilities that can be utilized to counter DDoS attacks. SDN has the added advantage in that it creates room to separate the control function from the application switch. It is possible to have various functions aggregated into the SDN interface. Functions such as routing, virtualization, and access control can be configured separately. This makes it easy for SDN to manage security operations in real-time and in a cloud-based environment.

Das et al. (2015) stated that a secure network is one that can protect itself from complex attacks. Attacks such as IP spoofing and DDoS can be quite complex to manage and thus they require an equally efficient mechanism to counteract their effects.Das et al (2015) identify MAC flooding as the most serious type of DDoS attack that is targeted to the OSI reference model. The best countermeasure to this type of attack is to institute switch counters. Additionally, it is important to implement port security to ensure that the attacker is unable to access the MAC table of the target network.

Shang-Fuand Jian-Lei (2012) aim to provide an overview and analysis of the security issues in peer-to-peer networks. It is noteworthy that trust and anonymity is a sensitive issue in p2p networks and thus it is paramount to have a mechanism for enforcing the necessary security parameters.DDoS attacks in P2P networks area common thing and thus efficient security mechanisms must be put in place. Tariq et al (2011) note that majority of DDoS attacks in P2P networks takes the form of packet flooding. The proposed defensive mechanism is implemented at the router whereby it has the ability to detect an attack and consequently notifies the neighboring peers about the impending attack. The proactive approach is able to not only counter the attack but also improve thequality of service within the P2P network.

Beitollahiand Deconinck (2011) proposed a mechanism, for dealing with DDoS attacks based ona collaborative effort between the victim's server and the ISP routers on the customer's end. The routers in this context must be in a state of forwarding traffic to the victim's server. The mechanism described by Beitollahi and Deconinck (2011) works in three interconnected phases. The first phase is the control phase whereby traffic measurement parameters are set and lower and upper boundaries determined with the aim of identifying any bandwidth flooding. The second phase is the stabilization stage whereby the victim's server is able to make configurations and installation of a leaky bucket on all edge routers and maintain a feedback loop for resizing the contents of the leaky bucket. The final stage involves the implementation of a fingerprinting operation aimed at identifying and separating the good and bad traffic in the leaky bucket. The size of the leaky bucket is dynamically allocated based on the identity of the router traffic. Simulation results show that their technique has effective defenses on the victim server against various DDoS attacks.

Hoque et al (2014) provide a classification of tools used in an attack to help theresearcher in the network security field. The study also presents a wide and organized survey of currently used tools and systems that can support both attackers and network security representatives. Information gathering in a network is accomplished suing various packet-sniffing tools such as Net2pcap, Tcpdump, ethereal, snoop, angst, and Dsniff among others. Furter category of network attacking tools includes Trojans, packet forging, DDoS, fingerprinting, and application layer attacks. DDoS attack tools can further be categorized based on automation degree, vulnerability level, impact, agent used, therate of attack, type of victim, and the network used. Notable DDoS attack tools include Burbonic, Torga, Jolt, LOIC, Nemsey, panther, UDPFlood, and Crazy Pinger among others.Hoque et al (2014)provide a comprehensive list of attack detection tools used to thwart an attack. Notable tools include FIRE, Nsom, Payl, Antid, Alert-ID, Nfids, Snort, and NetStat among

others. The detection tools use various approaches including rule-based, fuzzy logic, anoutlier, statistical, and mobile based.

2.4 Summary and Conclusion

The most common issue found in all the related to research works is the layer at which they perform the defense mechanism; the network layer. However, some studies (Alomari, et al., 2012; Patel, & Patel, 2014) were conducted in detecting the DDOS attacks on web servers.Other studies (Argyraki&Cheriton, 2009; Zargar, et al., 2013) discussed the defense of an attack occurring amongst network layer but against flooding attacks, while the rest of studies discusses the DDOS attacks in general. Moreover, (Alomari, et al., 2012; Dagon, et al., 2007; Liu, et al., 2008; Zhuge, 2007) studies directed their attention to botnet-based DDOS in terms of structures and classifications.

Since this study is concerned with proposing the adoption of Speak Up defense mechanism, the research has provided alternative defenses such as the approach presented in (Chen, 2006). Other approaches include the multifaceted defense proposed in (Fu, 2012), as well as, (Liu, et al., 2008; Singh, et al., 2015) which proposes defense mechanism against DOS attacks. (Ferguson&Senie, 2000; Wang, & Sun, 2014; Wang, et al., 2007) are studies which focus on defense against spoofed IP traffic using filtering.

It is obviousthat there are not enough studies, which are concerned withthe enhancement of Speak Up defense mechanism. This paper (Walfish, et al., 2010) presents the design, implementation, analysis, and experimental tests results of applying Speak Up defense technique to sort out application level Distributed denial-of-service (DDoS), (see Table 2.1) .Furthermore, (Argyraki,

&Cheriton, 2009) proposes a system where a network-layer defense mechanism is implemented to protect against bandwidth flooding in an active internet traffic.

Table 2.1 provides a comparison of the parameters used to quantify the effectiveness of the proposed filtering, which can be useful for comparing purposes of the research results between the Speak Up defense mechanism and the enhancement of the Speak Up mechanism.

Table 2. 1: Summary of Features of Defense Mechanisms against Network and Transport Layer Level DDoS Flooding Attacks based on their deployment location (Zargar, et al., 2013)

		properties	challenges	benefits
Centralized	Source-based	Detection and response are deployed at the source hosts	Sources are found in different domains, thus, it is difficult for each of the sources and filter attacks flows accurately. hard to differentiate legitimate and DDoS attack at the sources, due to thehigh volume of the traffic Low motivation for application, due to having not so clear who would have to afford the expenses associated with these services	Targets detecting and responding (i.e. filter) to the attack traffic at the source and before lots of resources are consumed.
	Destination-	Detection and response are released at the destination nodes (i.e., attacked resource)	No accurate detection and action to the attack before arriving the victims and lots of wasted resources.	Effective in detecting DDoS attacks since it has direct access to the aggregate traffic close to the destination nodes

	Network-based	Detection and response are done at the intermediate networks (i.e., routers)	Routers are demanded to provide high storage and processing capabilities. Attack detection is not easy since it lacks the availability of sufficient aggregated traffic aimed at the victims' end.	detects and acts (i.e. filter) on the attacked traffic at the intermediate networks and nearby the source
distributed	Hybrid (distributed)	Detection and response are carried out on different locations: detection takes place at the destinations & intermediate networks, while the response is performed mainly at the sources & upstream routers close to the sources There is a cooperation among various defense components	Complexity and overhead due to the cooperating and communicating distributed nodes and resources all over the internet Poor incentives from the service providers to cooperate/collaborate with each other.	More resistant to DDoS attacks. More components at the different levels (e.g., destination, sources, and network) are available to handle and respond to DDoS attacks.

Table 2. 2: Parameters used to assess AITF effectiveness (Argyraki, &Cheriton, 2009).

Metric	Description	Units
Tail-circuit capacity (C_{tc})	The capacity of the bottleneck links between the receiver and its gateway	Bps
Tail-circuit RIT (RTT_{tc})	The round-trip time between the receiver and its gateway	Seconds
Aggregate undesired-traffic rate (R_{ut})	The maximum rate at which at which undesired flow arrives at the receiver's tail circuit	bps
Average undesired-flow rate ($\hat{r}_i$)	The average rate at which at which each undesired flow arrives at the receiver's tail circuit	Bps
Aggregate identification overhead(B_{id})	The total number of unidentified bits that the receiver must get before identifying all undesired flows	bits
Identification time (T_{id})	Tid = B_{id}/R_{ut} A measure of the amount of time it takes to identify an undesired flow. It corresponds to the average identification overhead divided by the average undesired flow rate	seconds
Number of undesired flows (N_{uf})	The total number of different undesired flows sent to the receiver during the attack. Each undesired flow corresponds to a single source	
Request time (T_{req})	$T_{req} = N_{uf}/REQ_{fit}$the amount of time it takes to send filtering requests against all undesired flows	seconds

CHAPTER THREE

PROPOSED WORK

This chapter proposed a speak up mechanism with separate sub-thinners on the ISP's, in order to prevent bad network requests from over-flooding the network's bandwidth, and allowing good clients to make best use of network, even when it's under attack.

3.1 Introduction

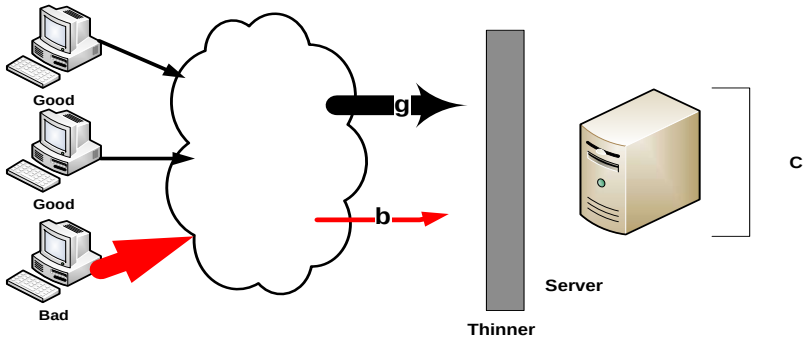
The proposed approach defen/protect server against Distributed Denial of Service (DDOS). This is achieved by enhancing the Speak Up approach proposed by (Welfish, et al, 2010). As mentioned in chapter 2, the Speak up approach tends to urge all the clients to send high volumes of data to the traffic, instead of being idle, while bad request exhaust the server, for that, the bad request by attackers has already exploited their bandwidth and cannot respond to the encouragement request, hence, the good request/clients will crowd out the bad clients. The encouragement requests in the current Speak Up done by the thinner; thinner (front-end server) that deals with the incoming requests, and send notification requests in a case of an overloaded server. The methodology used in this research altered the scheme of the Speak Up by using multiple sub thinners instead of main thinner, and locate it on client side, e.g. (located in Internet Service Provider ISP Side).

3.2 Proposed Work

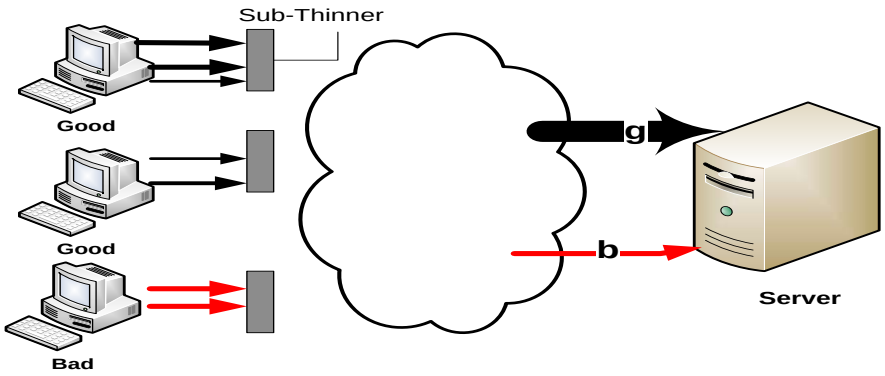
The proposed enhancement of the Speak Up approach for defend of offense DDOS operates by placing multiple sub-thinners near toclients side (e.g. sub-thinner allocated at Internet Service Provider ISP), each can deal with their own requests. By this approach all sub-thinners can hold the load of their sub network without affecting the main server. In this approach, if one of the sub-

thinner has an overloaded request, then this sub-thinner send an encouragement request for his clients without affecting other sub-thinners.

Figure 3.1(a), and (b) show the original scheme of the Speak Up, and the proposed scheme of Speak Up respectively.



(a)



(b)

Figure 3. 1: Speak Up original and proposed scheme

There are three main advantages of the proposed approach of Speak Up:

- First, the server will never notice if there is an attack or not, since the sub-thinner managed the requests instead of the server.
- Second, if there is an attack for the server, the sub-thinner will manage this, without affecting other sub-thinners jobs. So there is no denial of service for the major clients, only clients that share the same sub-net will be affected.
- Third, the bandwidth of the server will not be altered, because the Speak Up data, and headers are managed by sub-thinners and will not reach the server.

Sub-thinner Processing Scenarios

Initially, suppose that the sub-thinners are HTTP servers. Whenever one of the sub-thinner or more have a high load of requests (enter overloaded mode), only the sub-thinner that is overloaded will do the following:

1 The requests with the highest bandwidth have more chance passing to the server.

2 The sub-thinner will alter the response from the server by adding speak up header, and then pass it to the clients.

3 As the assumption that bad clients has already extended their bandwidth and can't react to this request, then they cannot maximize their request bandwidth, while the good clients have not extended their bandwidth yet, and can respond to sub-thinner request, giving them a better chance reaching the server. Figure 3.2 shows the process of the enhancement speak-up.

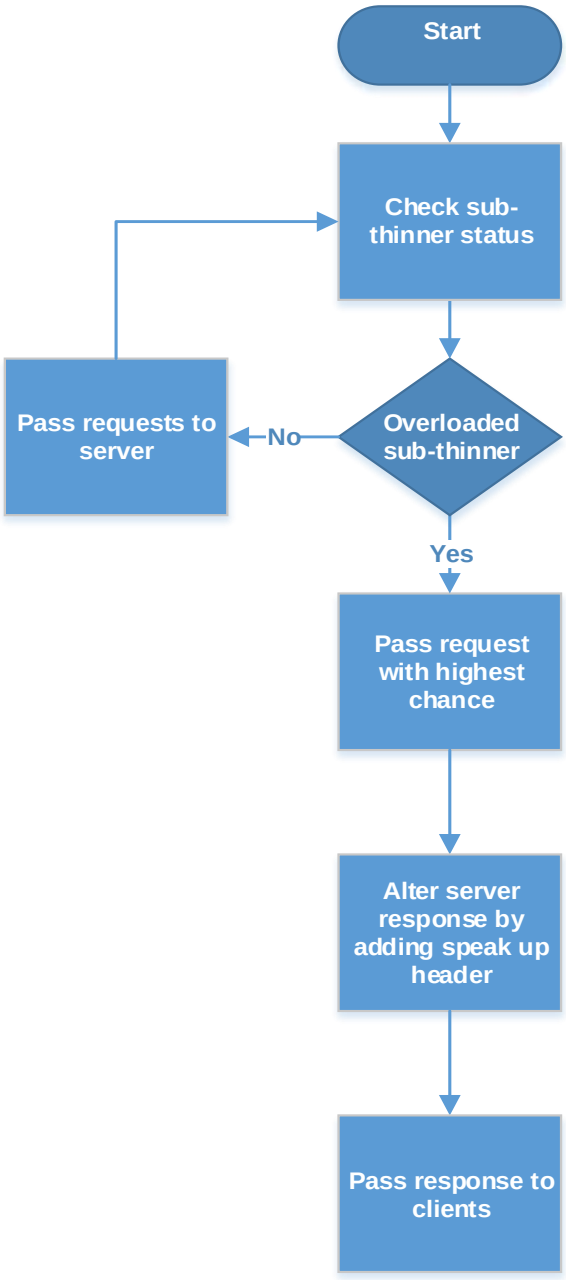


Figure 3. 2: Flowchart for Sub-thinner Process.

The two main tasks of the sub-thinner are summarized by the following:

- **Check Sub-thinner Status**: Initially, the sub-thinner will act normally by passing client's requests to the server, if an overloaded happen to the sub-thinner, and then the sub-thinner

will select some of the requests and pass them to the server (high bandwidth requests have a better chance to be selected by the sub-thinner).

- **Altering the Response from the Server to Clients**: In case there is an overload on the sub-thinner, the sub-thinner will alter the response from the server by adding a Speak Up header to the response include the Speak Up data size the clients should fill, then pass it to clients. This header encourages the clients to distend his next requests by filling the Speak Up header with dummy data that regarding the Speak Up header size, thus make them get a better chance of response. After the selection process of the clients requests the sub-thinner remove the speak Up data then pass the request to the server.

CHAPTER FOUR

RESULTS AND DISCUSSION

In this chapter, the performance of the modified Speak Up defense mechanism evaluated, as mentioned in chapter 3, the evaluation metrics will used to judge the performance of the enhanced Speak Up are bandwidth consumption, impact on other traffic, and finally the amount of good and bad requests passing the sub-thinner. To investigate the effectiveness and the performance of allocated sub-thinner, we compare the amount of bad requests passing the sub-thinner, with the amount or load of the bad requests on the original thinner using in original Speak Up. Also, a comparison for the amount of good clients requests served in two situation; when the server have overload (has been attack), and in the ordinary situation. We compared the performance of the server with original Speak Up, without Speak Up, and with the enhancement Speak Up.

4.1 Environment Setup

The simulation environment implemented using Java programming. We assume the bandwidth for all clients is 100KB/S, and the bandwidth for both the server and the sub-thinner is 120MB/S. The server can serve up to 700 request/second. We use HTTP server for testing purpose, and the simulation time is one hour. There are two types of clients; good and bad clients. First assumption that all connections are stable, and there is only one type of request (normal HTTP GET request), and the clients served equally.

We have the following assumption regarding client requests:

- The probabilities of bad clients are 10%, 20%, and 30% of total clients.
- The probability of good clients request is six requests per minute.

4.2 Simulation Tools

The proposed approach has been simulated using Java Code from scratch. The approach used in this research was evaluated according to the same criteria that the original approach was evaluated (Walfish, et al, 2010), for the sake of a mature comparison between the two approaches, these criteria's are:

1) Validating the sub-thinner's task of pass requests to the server:

   At a specific moment when the server is overloaded during an attack and thinner blocks all incoming requests, there are a plenty of malicious requests using the server resources, the mechanism of passing requests from thinner to the server should ensure that is the portion of resources used by malicious requests is decreasing, we will evaluate to what degree this approach will meet this goal.

2) Impact on other traffic:

   This research will show how it can reduce the impact on other traffic compared to the original approach.

3) Good and bad requests sharing bottleneck:

   This will be tested by experience what would happen if an attacker attempt to carry out his attack using 40% of each single bot's bandwidth.

4.3 Experimental Results

The primary question for this study is to prevent bad clients (attackers) from overloading the server, and to give the good clients a good chance to be served. An assumption that there are sub-thinners located at Internet Server Provider (ISP), the sub-thinner should handle the load instead of the server, by passing only a fixed amount of requests.

To evaluate the Speak Up with sub-thinners, we test the network performance by varying number of Good client (G), and Bad clients (B), and then we calculate the number of served requests for Good client, and the ratio of total served requests.

Table 4. 1: Good client information

Number of Good Clients	# of refused connections from Good Clients- with (sub-thinner)	# of refused connections from Good Clients- normal network	# of served connections from Good Clients- with (sub-thinner)	Total # of requests- with (sub-thinner)	# of served connections from Good Clients- normal network	Total # of requests- normal network	Served Ratio() % with (sub-thinner)	Served Ratio()% with normal network
350	0	0	126146	126146	126176	126176	100%	100%
630	0	0	226588	226588	226683	226683	100%	100%
700	0	0	251587	251587	251696	251696	100%	100%
1050	41903	13	335077	376980	377069	377082	89%	100%

In the first scenario, assumed that there is no attack on network (number of bad client = 0), Figure 4.1 shows the served ratio of good clients requests in a case of un-attacked network, we compared the results for both; normal networks (without using any thinner), and network with sub-thinners. Where the served ratio calculated by the following formula:

$$\text{Served ratio} = \frac{\text{served(requests of good clients)}}{\text{served(requests of G clients)} + \text{refused(requests of G clients)}}$$

Where served is the requests served by the server, and refused is the requests didn't served by the server.

As noticed from figure 4.1 that the presence of sub-thinners does not affect the performance of the network in the regular case, also the served ratio for the enhanced approach (sub-thinner) having the best results during an attack, that's enhanced the overall performance of the network, while the served ratio for the network with speak-up approach during an attack is much better than a network without any defense system, the enhanced approach overweight the performance of the speak-up approach, since the enhanced approach have the ability of handling the problem (attack) in the clients side, or ISP side, thus relieves the load on the server side, and give the good clients a better chance to be served.

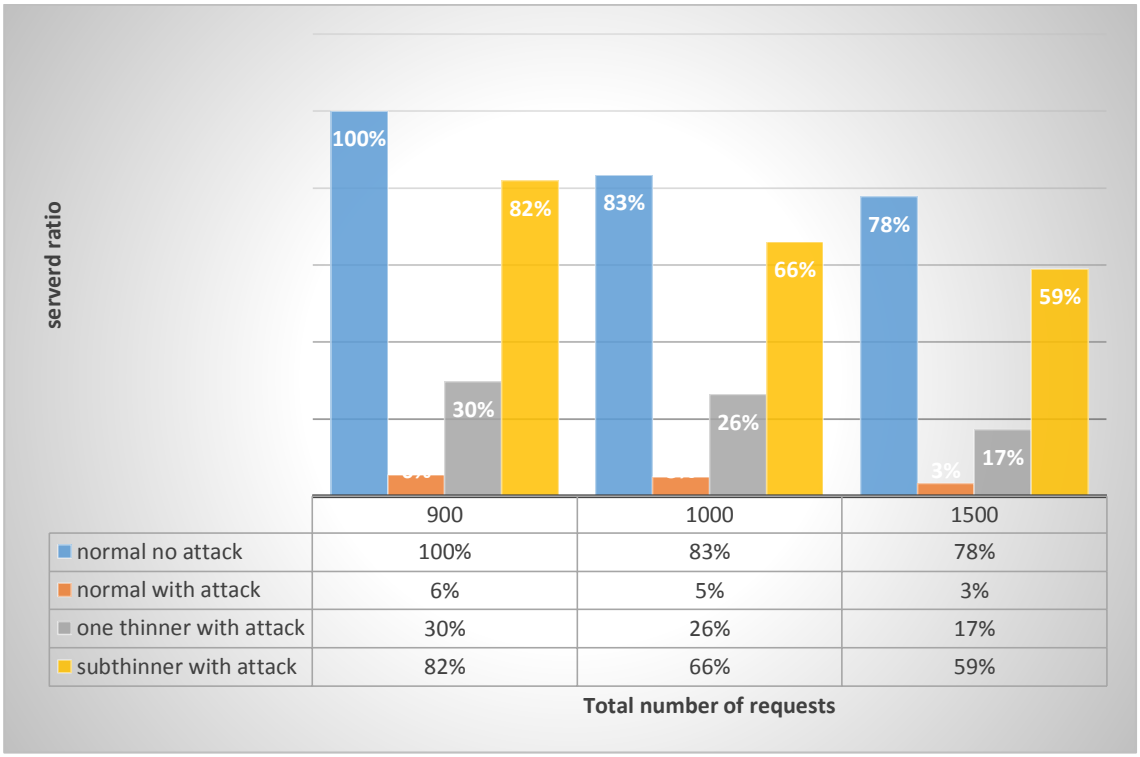


Figure 4. 1: Served ratio for several network cases with 20% bad clients of total clients.

There are four cases for evaluation purposes; checking the server performance of un-attacked without using speak up, the second case is for an attacked server with speak up, the third case is

for attacked server without speak up, and finally an attacked server with enhancement speak up. Table 4.2 shows the information records for a normal network in regular case (without an attack), to evaluate the performance of the network, we demonstrate the status using several number of requests (700, 1050, 1400, and 1500). As we noticed that the served ratio decreases by increasing the number of request even if there is no attack on the server, this due to the server capacity.

Table 4. 2: Normal network performance with no attack.

Good Clients	Bad Clients	Total Clients	**# of refused connections from Good Clients**	**# of served connections from Good Clients**	**Total Request**	**Served ratio**
700	0	700	0	251696	251696	100%
1050	0	1050	13	377069	377082	100%
1400	0	140	83534	419355	502889	83%
1500	0	1500	1199482	419146	538898	78%

Table 4.2, Table 4.3, Table 4.4 and Table 4.5 show the information records for a normal network during attack, network with speak-up approach during attack, and a network with enhanced speak-up (sub-thinner) approach respectively. All of these tables shows the number of good clients, number of bad clients, the number of refused requests from good clients, and the number of served requests form good clients.

Table 4. 3: Normal network performance during attack with 20% bad clients.

Good Clients	Bad Clients	Total Clients	**# of refused connections from Good Clients**	**# of served connections from Good Clients**	**Total Request**	**Served ratio**
728	172	900	247469	14467	261936	6%
814	186	1000	278225	14577	292802	5%
1208	292	1500	419897	14443	434340	5%

Table 4. 4: Network performance during attack with speak-up with 20% bad clients.

Good Clients	Bad Clients	Total Clients	**# of refused connections from Good Clients**	**# of served connections from Good Clients**	**Total Request**	**Served ratio**
728	172	900	170515	72011	242526	30%
814	186	1000	201495	72189	273684	26%
1208	292	1500	343217	71850	415067	17%

Table 4. 5: Network performance during attack with enhanced speak-up approach with 20% bad clients.

Good Clients	Bad Clients	Total Clients	**# of refused connections from Good Clients**	**# of served connections from Good Clients**	**Total Request**	**Served ratio**
724	176	900	46707	212776	259483	82%
804	196	1000	98114	190458	288572	66%
1195	305	1500	175629	252735	428364	59%

To demonstrate the results, the subsequent figures display the results in a better way, Figure 4.2 shows the results for served requests of the good clients for a normal network without any attack. As the number of requests increased, the amount of refused requests increased, due to the server capacity.

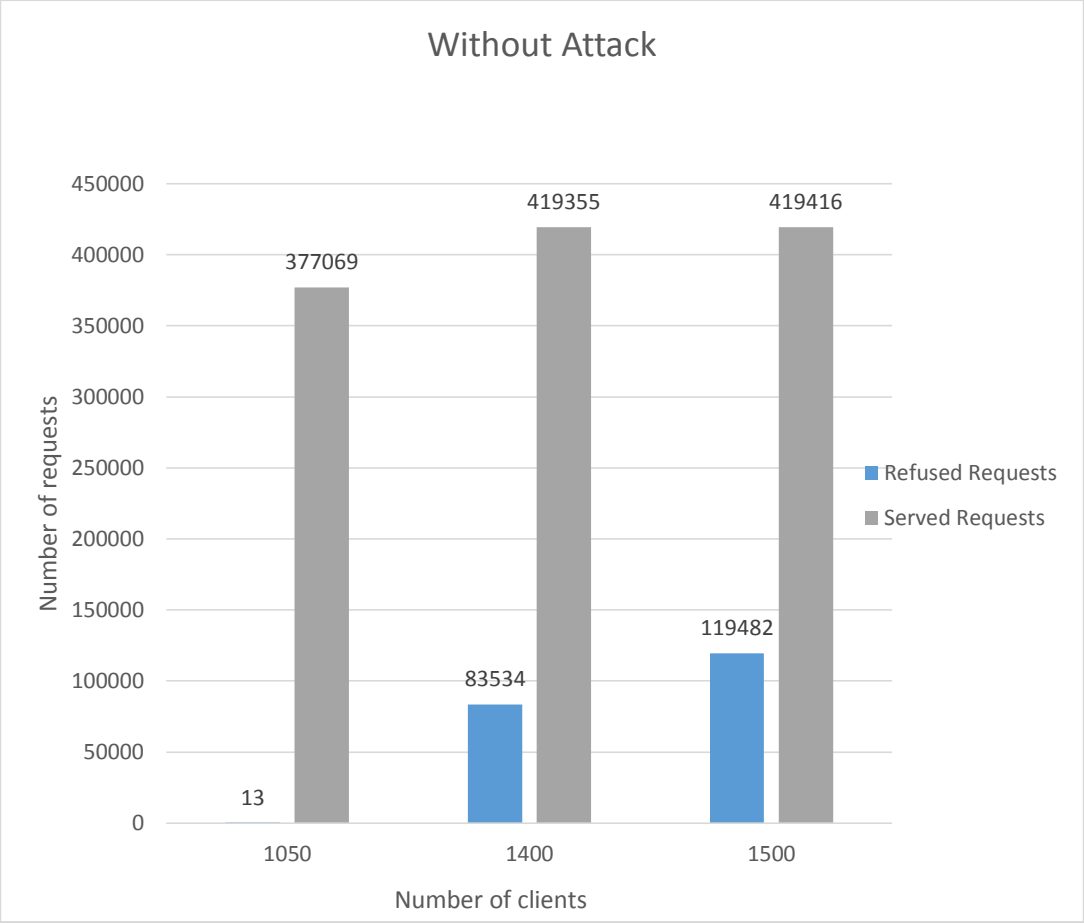


Figure 4. 2: Server status without attack.

To evaluate the performance of speak-up approach and the enhanced speak-up, there are three assumptions for the amount of bad clients; 10%, 20%, and 30% of total clients. Figure 4.3 shows the results for an attacked server using speak up mechanism, the amount of bad clients is about 10% of total clients, as the figure shows that the amount of refused requests is increased as the number of clients increased. It is obvious from the figure that the refused requests are more than the served request.

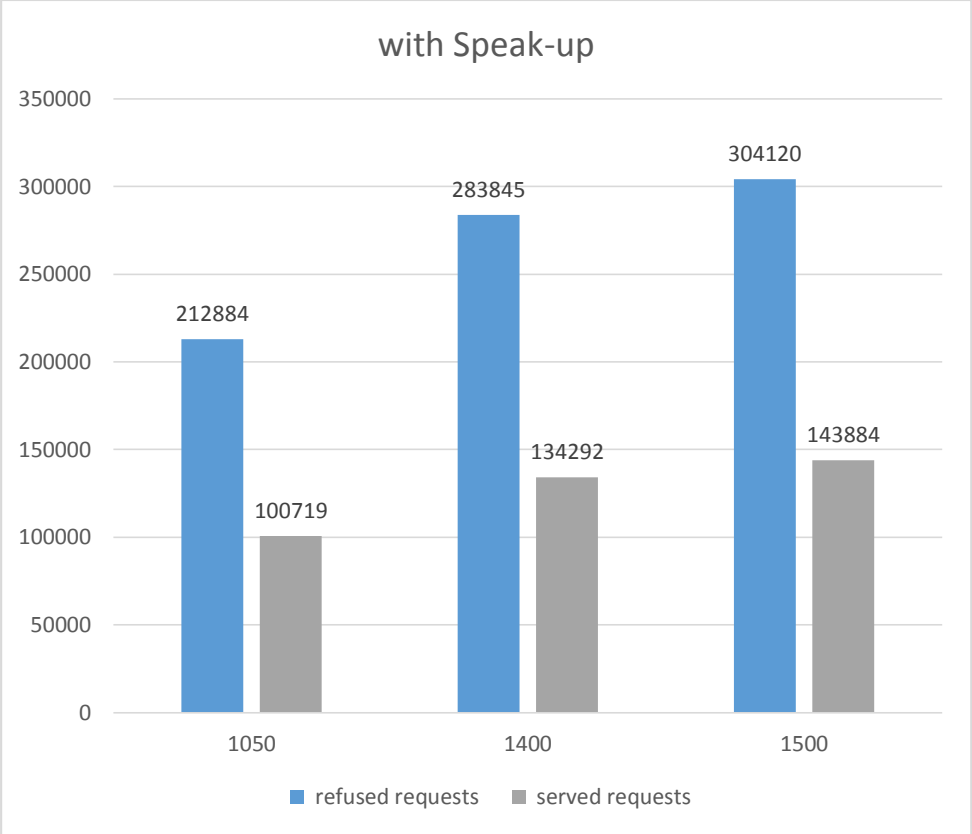


Figure 4. 3: Server during attack with speak up with 10% bad clients.

Figure 4.4 shows the results of the same number of clients or an attacked server using speak-up approach, but with 20% bad clients, it's clear that the number of served requested for good clients decreases when the amount of bad clients increased. Also figure 4.5 shows the results of an attacked server with 30% bad clients of the total number of clients, with speak-up approach the number of served request from good clients decreased as the number of bad clients increased.

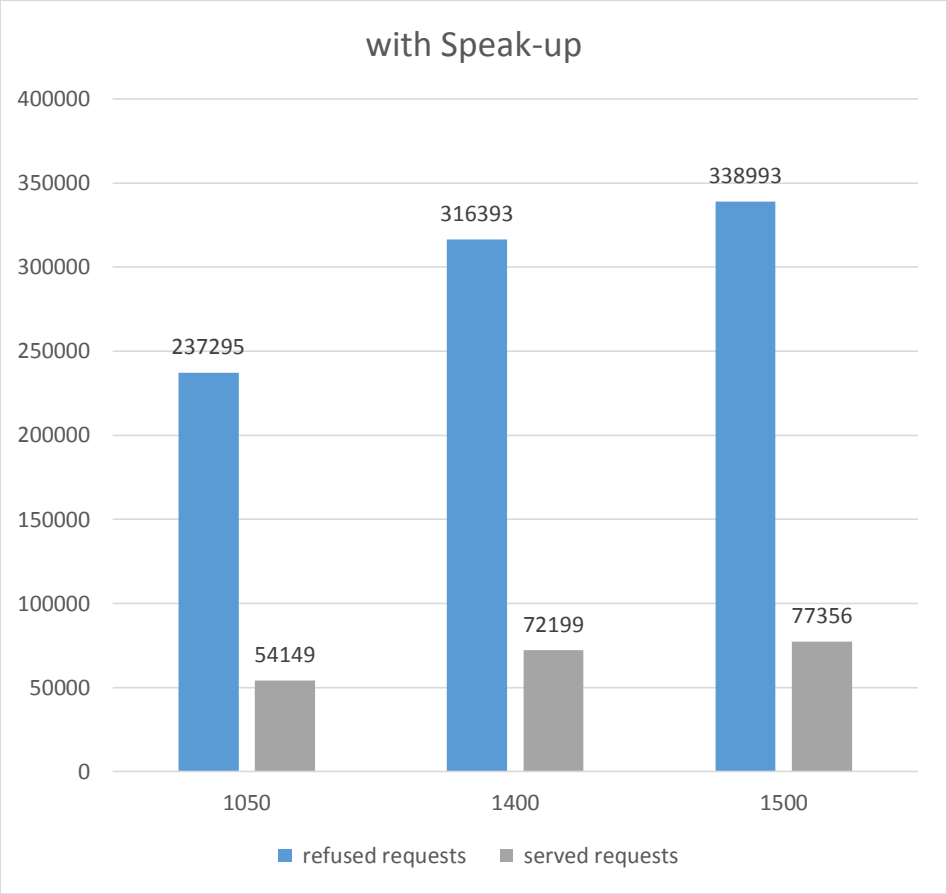


Figure 4. 4: Server during attack with speak up with 20% bad clients.

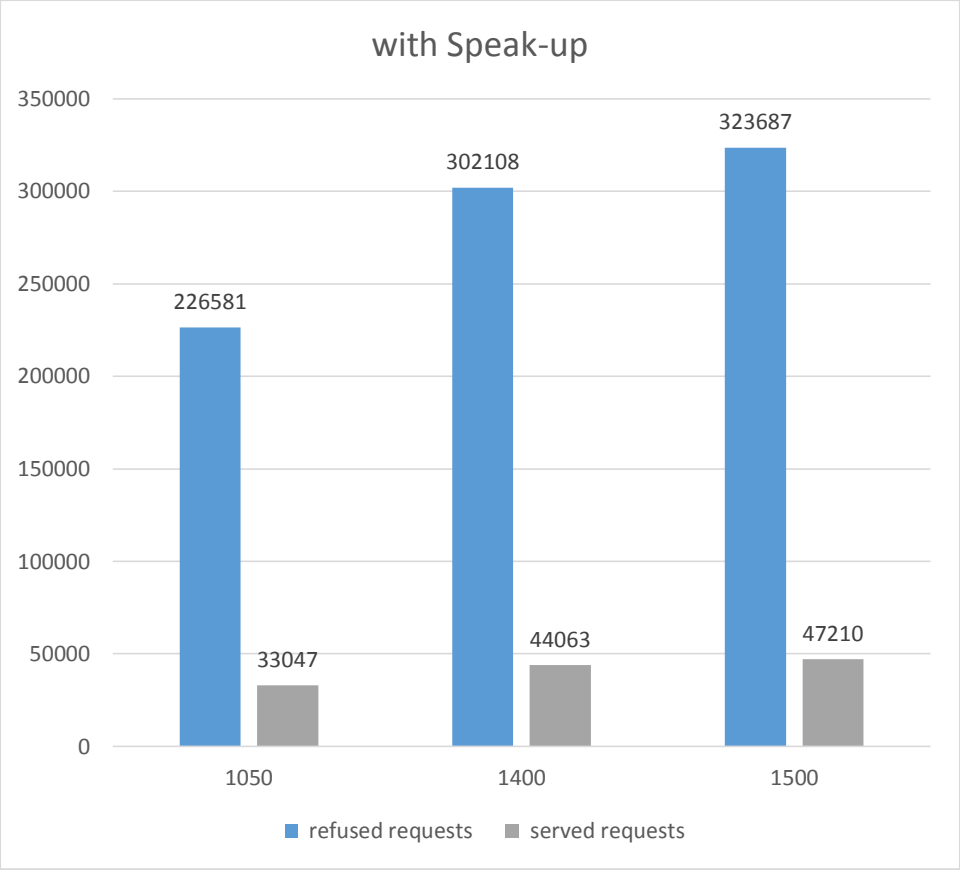


Figure 4. 5: Server during attack with speak up with 30% bad clients.

Figure 4.6 shows the results of refused and served request of an attacked server without using speak up mechanism and with 10% bad clients of total clients. The results shows that the number of served requests when using speak up is much better than the results of server without using speak up.

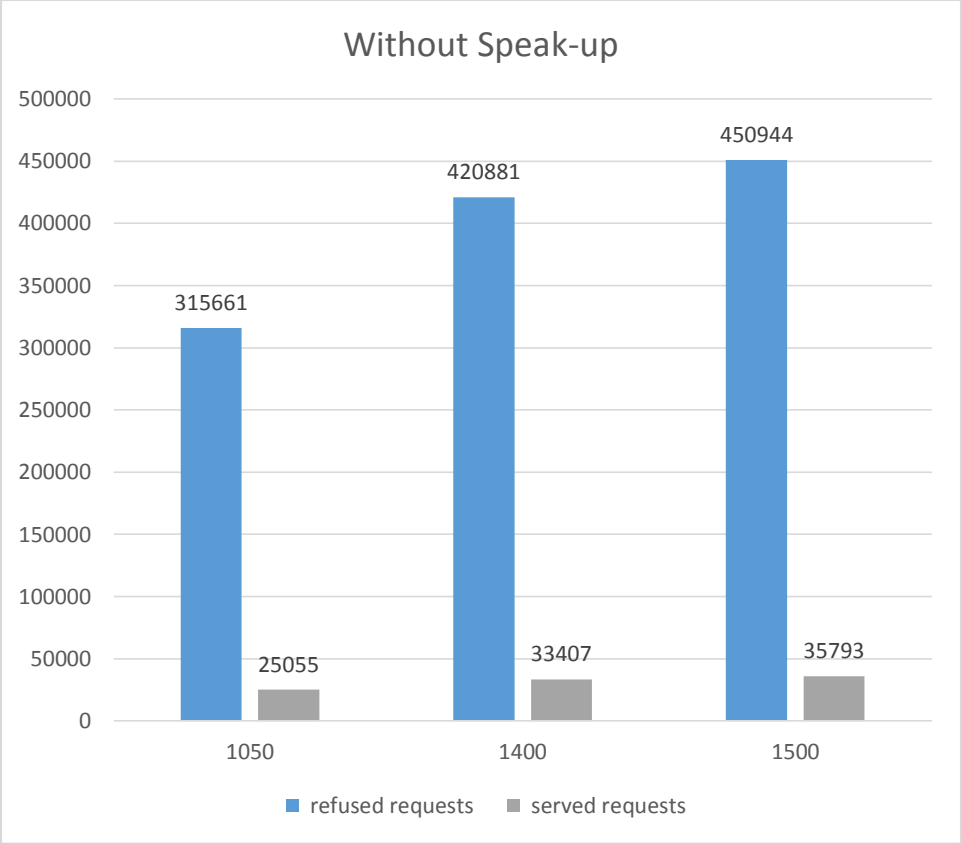


Figure 4. 6: Server during attack without using Speak up with 10% bad clients.

Figure 4.7 and figure 4.8 shows the results of an attacked server without using speak-up defense with 20%, and 30% bad clients of total clients respectively. The results shows the amount of served requests from good clients are too bad, the performance of the network Impacted significantly, as the number of bad clients increased, the amount of served requests of good clients decreased significantly.

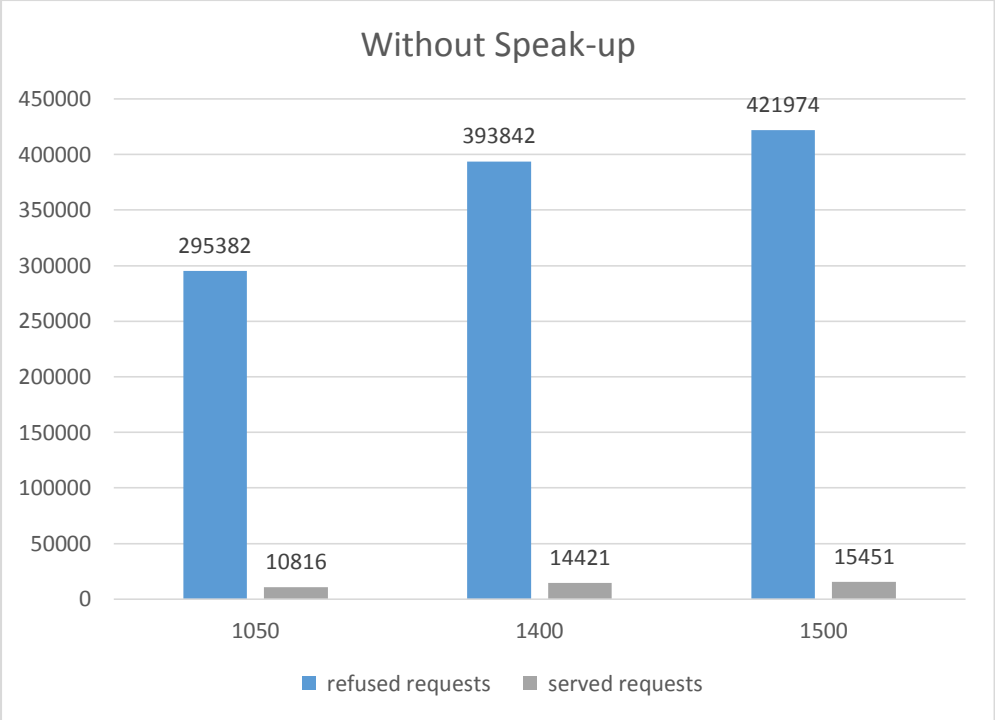


Figure 4. 7: Server during attack without using Speak up with 20% bad clients.

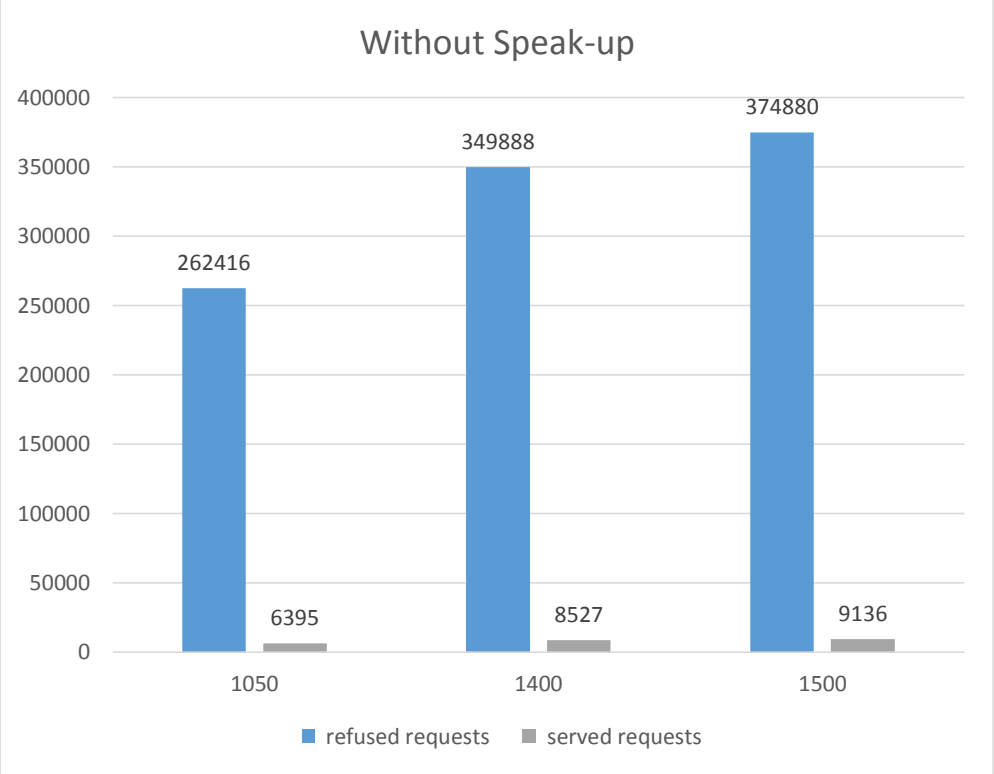


Figure 4. 8: Server during attack without using Speak up with 30% bad clients.

Finally, figure 4.9, figure 4.10, and figure 4.11 shows the results of an attacked server with an enhanced speak up approach, with the amount of bad clients 10%, 20%, and 30% respectively. The results show that using the enhanced speak up affect the performance of the network significantly. The amount of served requests from good clients has the best results in comparison with speak-up approach, and a network without any defense. Increased the number of bad clients impacted the number of the served requests slightly.

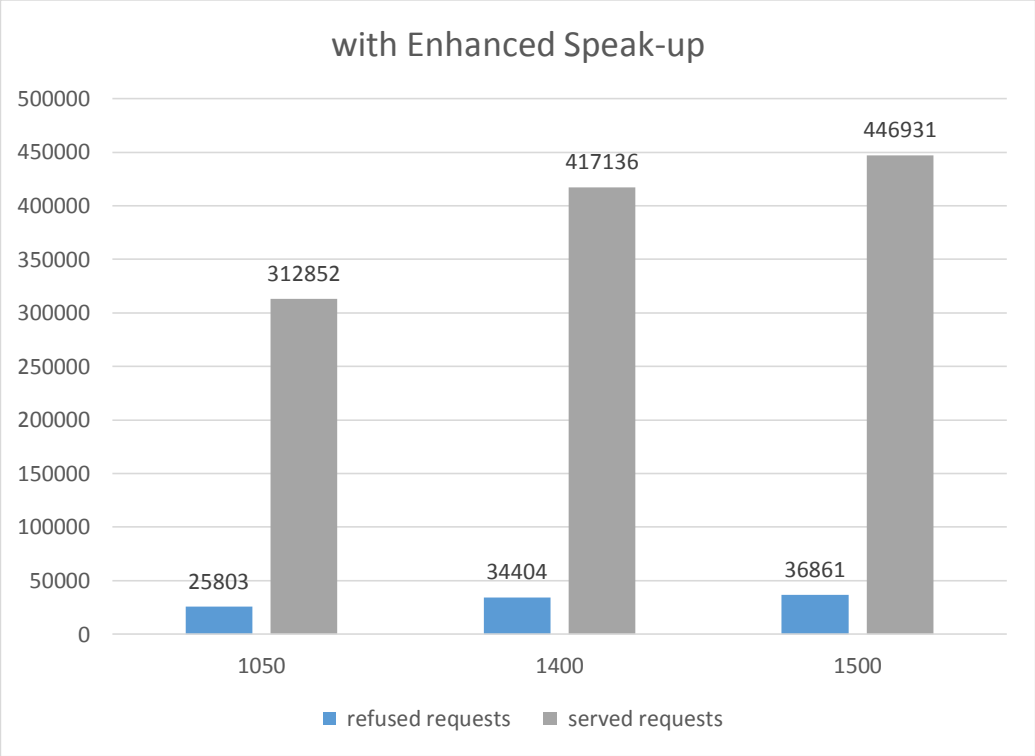


Figure 4. 9: Server during attack using enhanced speak up approach with 10% bad clients.

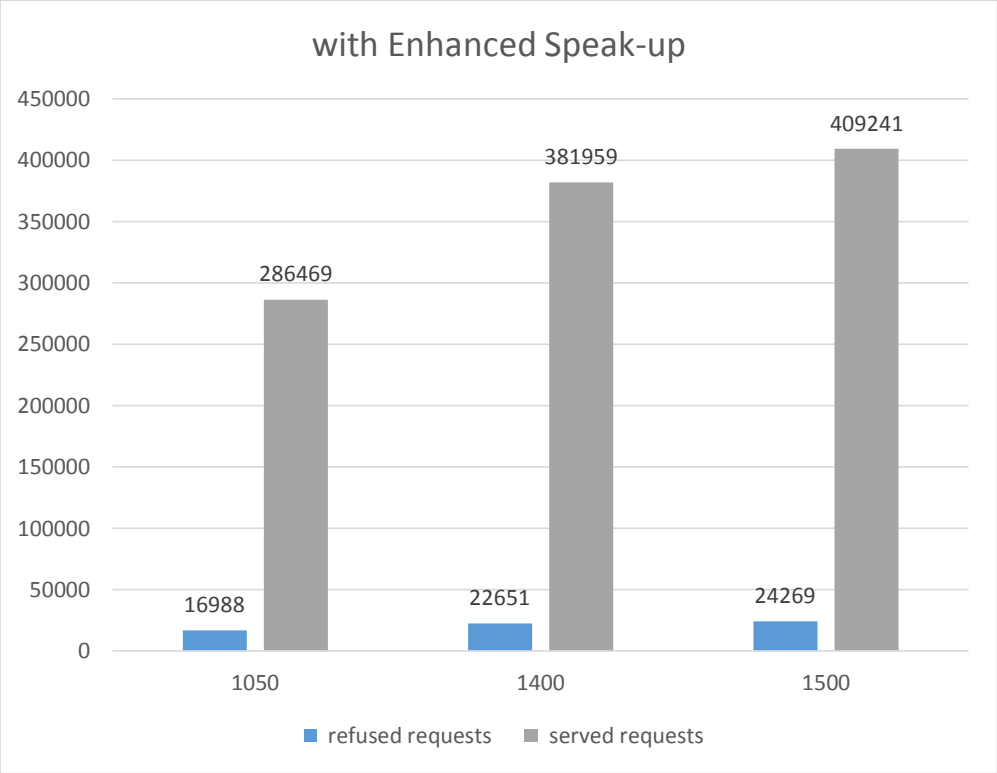


Figure 4. 10: Server during attack using enhanced speak up approach with 20% bad clients.

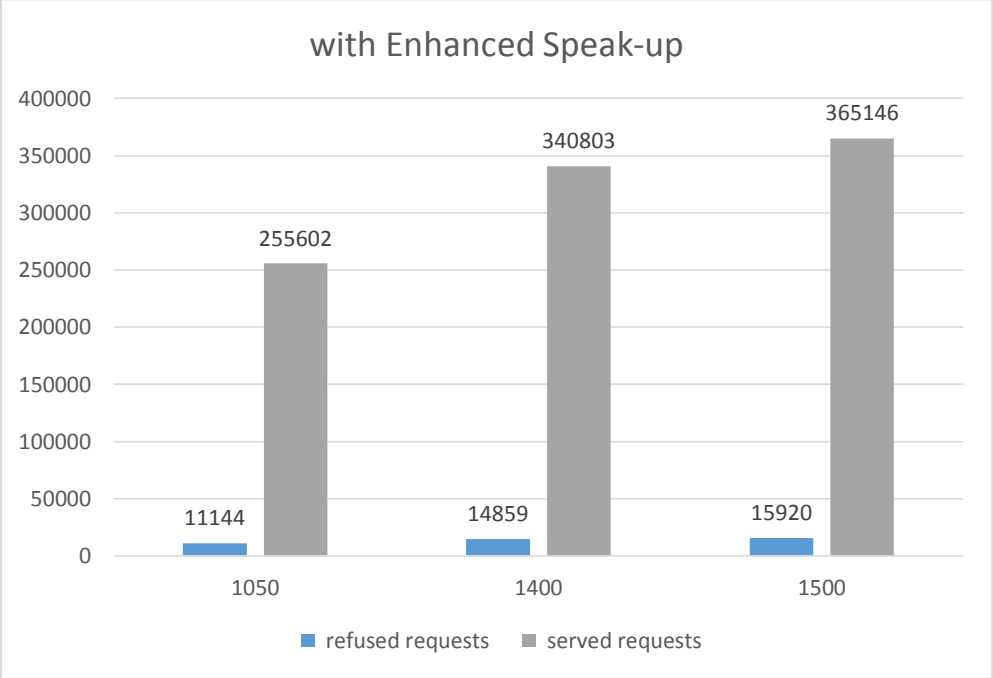
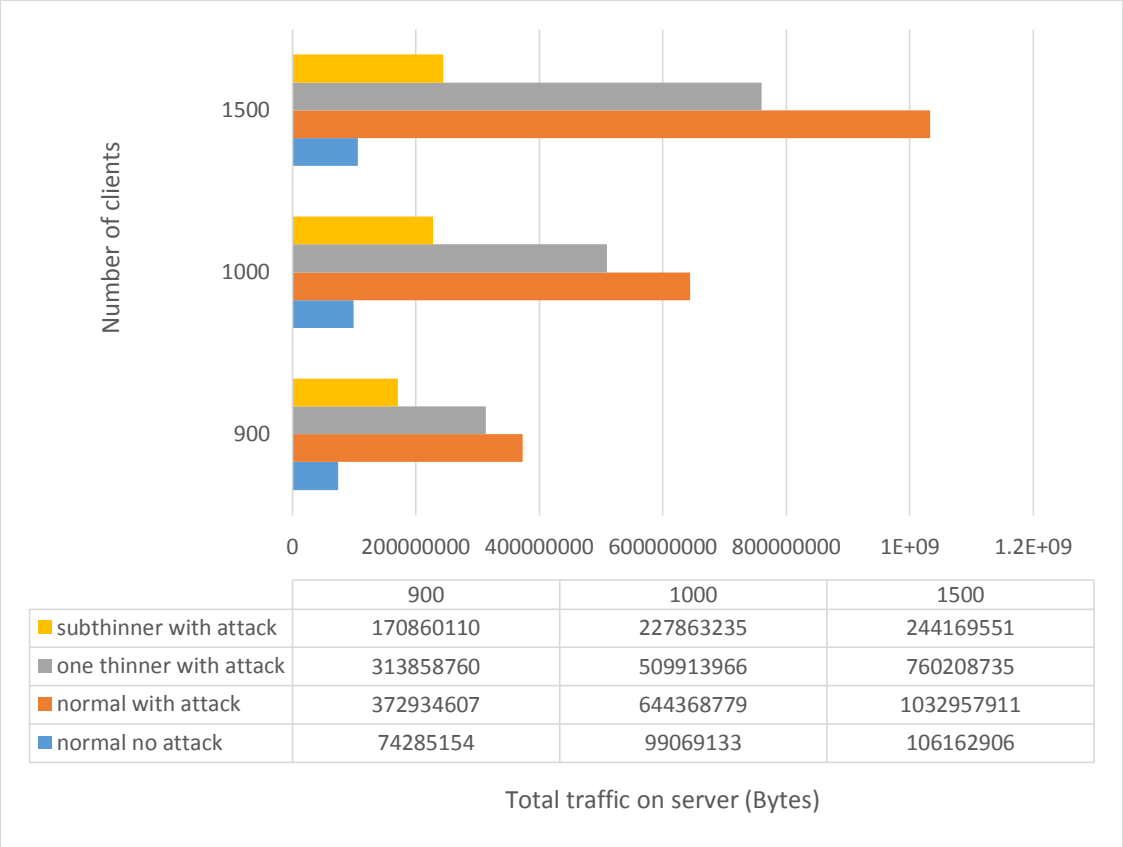


Figure 4. 11: Server during attack using enhanced speak up approach with 30% bad clients.

As we noticed from the results above that whenever the ratio of bad clients increased, the total number of requests increased, since the bad clients request many dummy request to overload the server.

Figure 4.12 shows the results of traffic on the server side, it's clear that the normal network without any attack has the least traffic on the server. The important idea is how the server can hold the traffic during attack, figure 4.12 shows three cases of attack; normal network without any defense system, network with speak-up approach, and network with enhanced speak-up approach (subthinner). It's clear that normal network without any defense system has the heaviest load on the server, while the speak-up approach the server still has a huge load but the most of this load from good clients, since the speak-up requests the good clients to enlarge their requests. Finally the results of the enhanced speak-up shows that the server has the least load among all the networks cases during an attack, this due to the defense of attack handled at the clients side (ISP sides), that allows only limited amount of requests to pass the thinner to server.



	900	1000	1500
subthinner with attack	170860110	227863235	244169551
one thinner with attack	313858760	509913966	760208735
normal with attack	372934607	644368779	1032957911
normal no attack	74285154	99069133	106162906

Figure 4. 12: Traffic on server side with 20% bad clients.

4.4 Conclusion

From the results of this chapter, we conclude that the speak-up defense approach hold the problem of an attacked server at the server side, this mechanism give the good clients a better chance to be served, but the server still overloaded. An enhancement of the speak-up approach is proposed by using subthinner on the clients side (ISPs side) instead of one thinner at the server side, this enhancement relieve the server from the load, since the sub-thinner pass only a limited amount of requests. At the evaluation and results for the proposed approach, the enhancement approach of the speak-up overweight the performance of the speak-up approach in terms of the number of good clients served, and the traffic on the server, this enhancement affects the overall network performance.

CHAPTER FIVE
Conclusions and Future Work

5.1 Conclusions

It's very important task to secure the services over the networks especially in the recent years since we face a huge technology revaluation in online services (online banking, PAYPAL, and many others).

This research was implemented a lower level in bandwidth consumption. Although, the experiment extracted results shows that the enhanced system of Speak Up defense mechanism outperforms Speak Up mechanism in terms of defending, and bandwidth consumption. On the other hand provide this methodology in order to introduce more level in security consider as important aspect.

- Proposed technique is capable to serve more request from good requesters.
- The more number of client the less served ratio from good client but still way better than the original approach.
- Proposed technique proved significant enhancement in intermediate bandwidth consumption.
- The comparison of intermediate bandwidth consumption between Speak Up and the enhanced approach showed that the more number of clients the more efficient bandwidth consumption of intermediate network.

The experiment results were structured in the way to make it more understandable as graphs and numeric numbers; by this more knowledge about the methodology results could be extracted by other researches.

Though, the methodology faced some of limitations in its working behavior that's due to the lack of multiple services resources (deep multi-layer services), were these kind of services structure as a more than one level of accumulative levels that interact with each other with a high speed and more security over levels in order to provide more level of data transmission security. In addition to following limitations:

- This research defines a strategy that can only react to bandwidth attacks.
- The proposed technique can deal only with predefined ISP's.
- The attack can't be prevented if it initialized somewhere between the ISP and client.

5.2 Future works

There are number of enhancements that could be made upon this methodology in the aim to provide more effective results in security defense as will be listed as future work. Among the most commonly used meta-heuristics for security studies that includes optimization based on ant colony and swarm intelligence. Optimization has attracted attention and has been successfully applied in various situations, as it allows the efficient finding of optimal solutions in a large search space. Under swarm intelligence agents generate individual models and organize themselves through interactions with its neighbors, it is an intelligence of social insects and collective forms of existence and organization. In social species colonies teamwork is largely self-organized and coordinated through the different interactions between individuals. Self-organization is an attribute

of social species; it refers to the ability, in the absence of external-control to generate improvements in order or to produce new forms of organization against environmental changes.

Since no single species can be intelligent, but also at other levels of life as communities and ecosystems are likely to develop self-organization as fundamental attribute of collective intelligence. Hence, as a smart network security the using of ant colony or swarm intelligence as a hybrid implementation with this study methodology would provide more optimization level upon security issues.

Appendix A

A .1 Implementation and code segments

As mentioned earlier, the simulator was developed with Java under the Eclipse environment, the simulator is designed to simulate the traffic and requests from good and bad clients to a server. Simple network layers are implemented to satisfy the network requirements and parameters, such as bandwidth, number of allowed connections, speed of clients, capacity of the server, and number of requests per second. The following screen shots are taken from running the simulator.

Figure A.1 shows the main screen of the simulator with the packages for each segment of the simulator: part A shows the package that runs without the developed sub-thinner, while part B shows the package that applies the sub-thinner to test data.

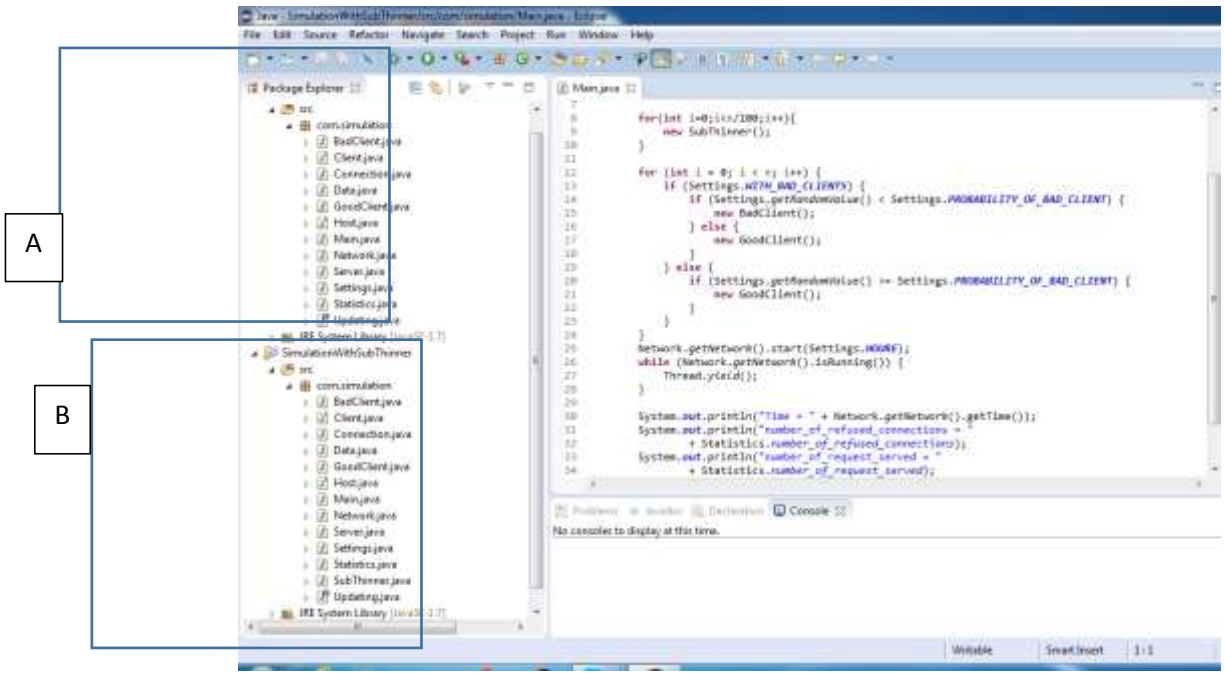


Figure A. 1: Main window with simulator packages: A: no sub-thinner and B: with sub-thinner.

The simulator runs twice: one with the sub-thinner not effective, and another activating the sub-thinner to filter good from bad requests over the network in order to compare the results.

Before running the simulation, a set of settings need to be defined in order to determine whether the simulator is running with speak-up or without it. The frequency at which network requests are submitted is also defined along with activating the bad client detection (or deactivating for the purpose of testing and results comparison). Figure A.2 below shows the settings class that is used in this research work.

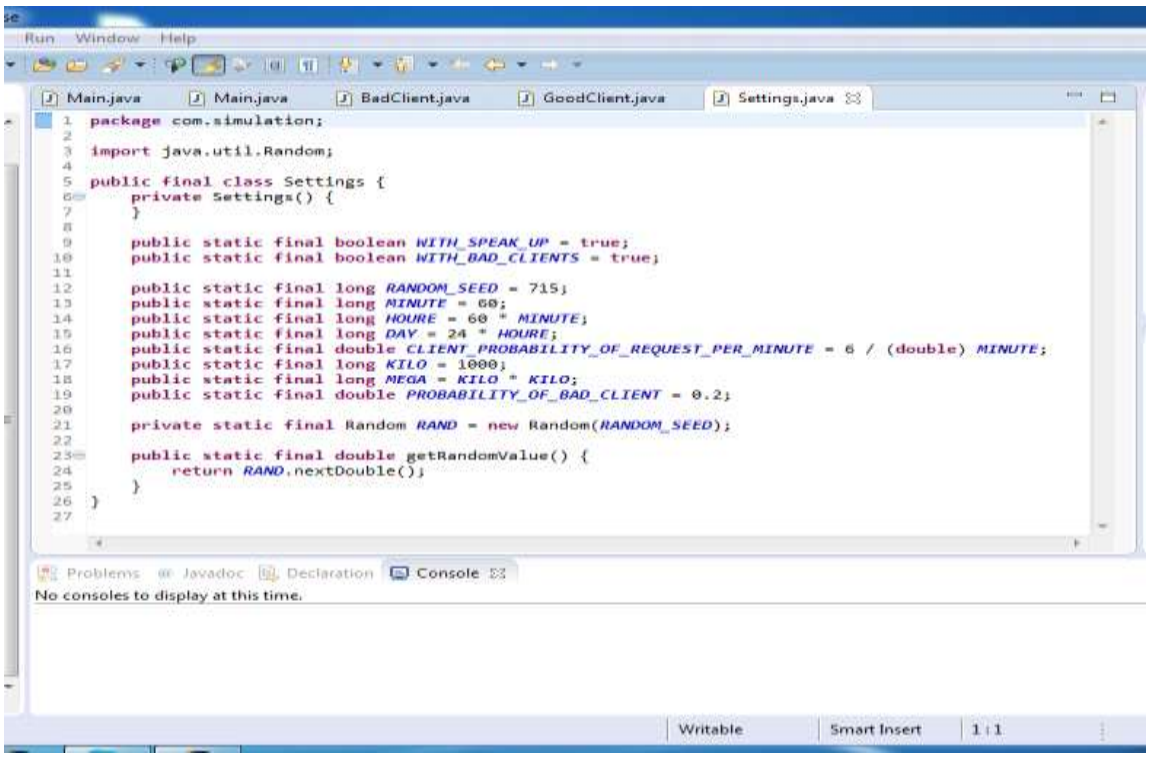


Figure A. 2: the settings tab in the simulator.

When running the simulator, the flow of good clients' requests is tested by calling a dedicated class. In this class the probability of having good network requests is calculated depending on the random values generated in the settings class, according to which these requests are classified as "good" clients' requests and not filtered by the sub-thinner. Figure A.3 below shows the implementation of the good client's class.

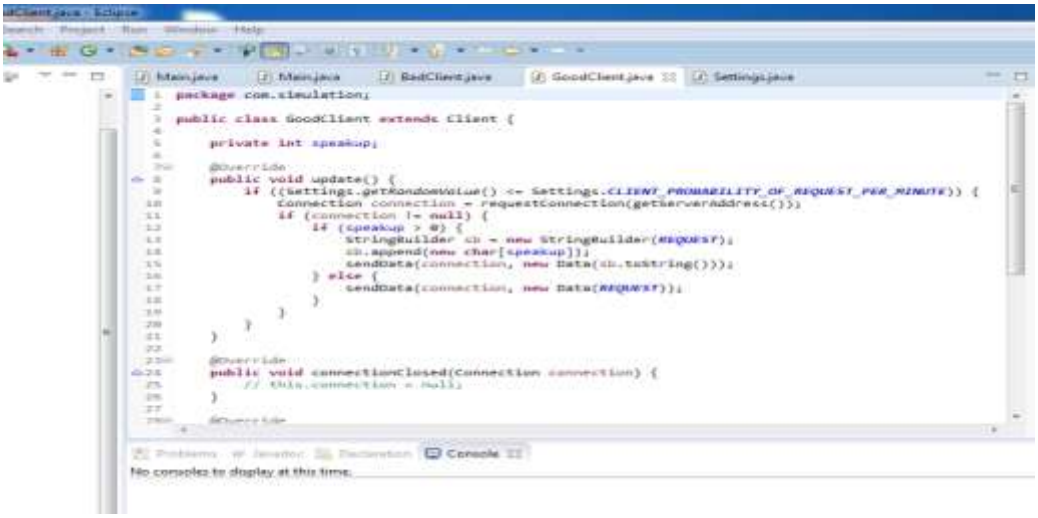


Figure A. 3: good client testing class.

The bad clients' testing class examines the maximum number of connections of the client and determines how much more bandwidth is remaining to stop it from overflowing the network. The sub-thinner closes the connection of the client if it was classified as "bad" client by this class. Figure A.4 shows the code segment of the bas client class.

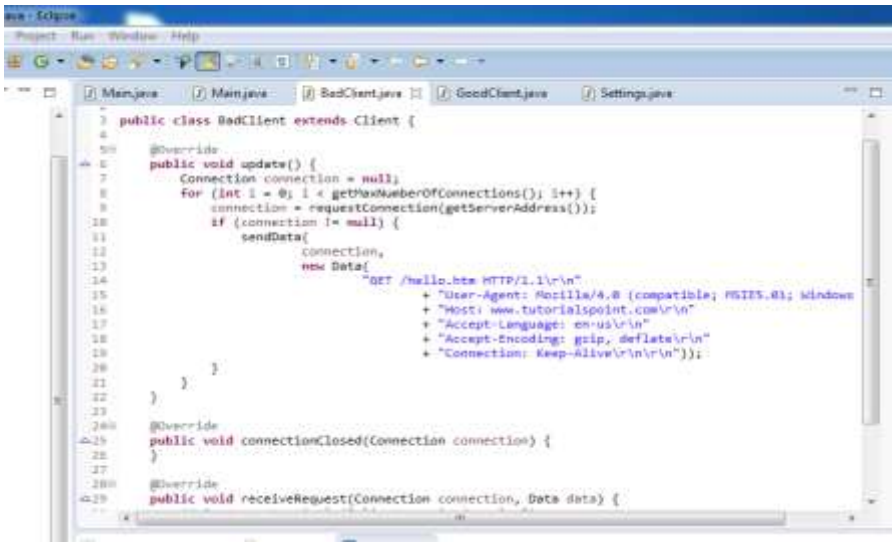


Figure A. 4: bad clients testing class.

References

Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., &Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. *International Journal of Computer Application*,49(7), 0975 – 8887

Argyraki, K., &Cheriton, D. R. (2009).Scalable network-layer defense against internet bandwidth-flooding attacks. *IEEE/ACM Transactions on Networking (TON)*, 17(4), 1284-1297.

Beitollahi, H., &Deconinck, G. (2011).A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks. *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 1*(1), 11-20. doi:10.1109/TrustCom.2011.6

Bhuyan, M. H., Bhattacharyya, D. K., &Kalita, J. K. (2011). Surveying port scans and their detection methodologies. *The Computer Journal, bxr035*.

Chen, R., Park, J. M., &Marchany, R. (2006). TRACK: A novel approach for defending against distributed denial-of-service attacks. *Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Virginia Tech.*

Chou, J., Bill, L., Sen, S., &Spatscheck, O. (2009).Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks**.***IEEE/ACM Transactions on Networking, 17*(6), 1711-1723. doi:10.1109/TNET.2009.2017199

Chouman, M., Safa, H., &Artail, H. (2005).Novel defense mechanism against SYN flooding attacks in IP networks. *Canadian Conference on Electrical and Computer Engineering, 1*(1), 2151-2154.doi:10.1109/CCECE.

Dagon, D., Gu, G., Lee, C. P., & Lee, W. (2007). A taxonomy of botnet structures. In Computer Security Applications Conference, 2007.ACSAC 2007.*Twenty-Third Annual (pp. 325-339). IEEE.*

Das, R., Karabade, A., & Tuna, G. (2015).Common network attack types and defense mechanisms**.** *2015 23th Signal Processing and Communications Applications Conference (SIU), 1*(1), 2658-2661. doi:10.1109/SIU.2015.7130435

Ferguson, P., &Senie, D. (2000). Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing.*ACM*.

Fu, Z. (2012). Multifaceted Defense Against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation**.***Chalmers University of Technology*.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., &Kalita, J. K. (2014**).**Network attacks: Taxonomy, tools and systems**.** *Journal of Network and Computer Applications, 40, 307-324.*

Kolahi, S., Treseangrat, K., &Sarrafpour, B. (2015).Analysis of UDP DDoS flood cyber-attack and defense mechanisms on Web Server with Linux Ubuntu 13. *2015 International Conference on Communications, Signal Processing, and Their Applications (ICCSPA), 1*(1), 1-5. doi:10.1109/ICCSPA.2015.7081286

Liu, X., Yang, X., & Lu, Y. (2008, August).To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. *In ACM SIGCOMM Computer Communication Review (Vol. 38, No. 4, pp. 195-206).ACM.*

Luo, S., Wu, J., Li, J., & Pie, B. (2015).A Defense Mechanism for Distributed Denial of Service Attack in Software-Defined Networks**.** *2015 Ninth International Conference on Frontier of Computer Science and Technology (FCST), 1*(1), 325-329. doi:10.1109/FCST.2015.11

Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V., &Shenker, S. (2002).Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review, 32(3), 62-73.*

Mehta, M., Thapar, K., Oikonomou, G., &Mirkovic, J. (2008).Combining Speak-Up with DefCOM for Improved DDoS Defense. *IEEE International Conference on Communications, 1*(1), 1708-1714. doi:10.1109/ICC.2008.329

Meyran, R. (2012).DDoS attack myths: Does size really matter? (online), available:http://blog.radware.com/security/2012/02/ddos-attacks-myths/

Mirkovic, J., Robinson, M., &Reiher, P. (2003, August).Alliance formation for DDoS defense. In Proceedings of the 2003 workshop on New security paradigms (pp. 11-18). *ACM.*

Mishra, A., Gupta, B., & Joshi, R. (2011).A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques. *2011 European IN Intelligence and Security Informatics Conference (EISIC), 1*(1), 286-289. doi:10.1109/EISIC.2011.15

Patel, D. A., & Patel, H. (2014, June).Detection and Mitigation of DDOS Attack against Web Server. In *International Journal of Engineering Development and Research* (Vol. 2, No. 2 (June 2014)). IJEDR.

Pras, A., Sperotto, A., Moura, G., Drago, I., Barbosa, R., Sadre, R., ...&Hofstede, R. (2010). Attacks by "Anonymous" WikiLeaks proponents not anonymous.

Ranekar, A., &BhagatPatil, A. (2015).Survey of DOS defense mechanisms. *2015 International Conference OnInnovations in Information, Embedded and Communication Systems (ICIIECS), 1*(1), 1-5

Rescorla, E., &Modadugu, N. (2012), "Datagram Transport Layer Security Version 1.2", (online), Available: https://tools.ietf.org/pdf/rfc6347.pdf Published October 23.

Shang-Fu, G., &Jian-Lei, Z. (2012).A Survey of Reputation and Trust Mechanism in Peer-to-Peer Network**.** *2012 International Conference on Industrial Control and Electronics Engineering (ICICEE), 1*(1), 116-119.

Singh, S.; Khan, R.A.; Agrawal, A., (2015) "Prevention mechanism for infrastructure based Denial-of-Service attack over software Defined Network," in Computing, Communication & Automation (ICCCA), 2015 International Conference on , vol., no., pp.348-353, 15-16 May

Tariq,U.,Malik, Y., Abdulrazak, B., &Hong, M (2011) Collaborative Peer to Peer Defense Mechanism for DDoS Attacks, Procedia Computer Science, 5(6), 157-164.

Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D., &Shenker, S. (2010). DDoS defense by offense. ACM Transactions on Computer Systems (TOCS),28(1), 3.

Wang, H., Jin, C., & Shin, K. G. (2007). Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Transactions on Networking (TON), 15(1), 40-53.

Wang, Y., & Sun, R. (2014).An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks**.** Journal of Networks, 9(4), 874-881.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. Communications Surveys & Tutorials, IEEE, 15(4), 2046-2069.

Zhuge, J. (2007). Characterizing the IRC-based botnet phenomenon. Universität Mannheim/InstitutfürInformatik.