Aalto University
School of Science
Degree Programme in Computer Science and Engineering

Alvaro Garcia

Distributed Denial of Service Attack and Software Defined Networking:

Improving mechanism defense of DDoS with SDN

Master's Thesis
Espoo, March 15, 2014

DRAFT! — February 4, 2014 — DRAFT!

Supervisors: Assoc. Prof. Aapo Kalliola
Advisor: Assoc. Prof. Aapo Kalliola

Aalto University
School of Science
Degree Programme in Computer Science and Engineering

ABSTRACT OF
MASTER'S THESIS

Author:	Alvaro Garcia		
Title:	Distributed Denial of Service Attack and Software Defined Networking: Improving mechanism defense of DDoS with SDN		
Date:	March 15, 2014	**Pages:**	13
Major:	Computer Science and Engineering	**Code:**	T
Supervisors:	Assoc. Prof. Aapo Kalliola		
Advisor:	Assoc. Prof. Aapo Kalliola		

The original aim of the Internet was to provide an open and scalable network among research and educational communities, where billions of users are served through a global system of interconnected computer networks.

Since DoS attacks are becoming more commons and emerging new technologies to separate the control plane and the data plane from the network devices (SDN), throughout this survey we will investigate how Software Defined Networks can help to prevent and locate these kinds of attacks. We will study the different DoS attacks and the current mitigation techniques. We will discuss as well, which of these techniques could be improved with SDN and how develop them. In the end, we will implement and test some identified mitigation techniques and we will study their behavior.

Keywords:	DoS, DDoS, SDN, OpenFlow
Language:	English

Acknowledgements

This work would not have been completed without help and support of many individuals. I would like to thank to my supervisor Keijo Heljanko for providing me an opportunity to conduct my Thesis under his invaluable guidance and support over the course of it. I am grateful to Aalto University for giving me the chance of finishing my studies in Finland and for the opportunity of using Triton cluster for this Thesis. I would like also to thank to my roommates at Aalto: Bailo, Canellas and Guillermo for all the unforgettable moments we shared.

This Thesis is dedicated to the three pillars of my life: my mother and her indefatigable support, my father and his efforts of making me happy no matter what happens and to my brother Jorge because without him I would be lost. To my family, to whom I owe my life. Thanks.

Espoo, March 15, 2014

Alvaro Garcia

Abbreviations and Acronyms

2k/4k/8k mode	COFDM operation modes
3GPP	3rd Generation Partnership Project
ESP	Encapsulating Security Payload; An IPsec security protocol
FLUTE	The File Delivery over Unidirectional Transport protocol
e.g.	for example (do not list here this kind of common acronymbs or abbreviations, but only those that are essential for understanding the content of your thesis.
note	Note also, that this list is not compulsory, and should be omitted if you have only few abbreviations

Contents

List of Figures

Chapter 1

Introduction

The original aim of the Internet was to provide an open and scalable network among research and educational communities, where billions of users are served through a global system of interconnected computer networks.

Unfortunately, with the rapid growth of the Internet over the last two decades, the number of attacks on the Internet has also increased rapidly. One of this attacks, consist in disrupt the service provided by a network or server, either crashing the system sending some packets that exploit a software vulnerability or sending a large number of useless traffic to collapse the resources of the service. This kind of attack is known as Denial of Service (DoS) attack.

There are some design principles of the Internet that facility these kinds of attacks:

Resource sharing: in IP networks, doubt to packet-switched service, users shares all the resources, and one user's service can be disturbed by other user's behaviour, so bandwidth attacks can disrupt service for legitimate users.

Simple Core and Complex Edge: One of the principles of Internet is that the core network should be simple and push all the complexity into the end hosts. That means that the core of the networks is not able to integrate complex application, as authentication, security. Due to this simplification, when an attacker sends packets into the network and the victim receive them, it is almost impossible recognize the real owner of the packets.

Fast Core Networks and Slow Edge Networks: The Core Networks needs to have a high capacity due to the heavy traffic that has to support from many sources to many destinations. In contrast, an edge network needs less

capacity because it only needs to support its end users. A disadvantage is that traffic from high-capacity core can crush the slow-capacity edge.

Taking advantage of these principles and their vulnerabilities, have been arising a large number of different DoS and DDoS attacks. The two main impacts of DoS and DDoS attacks are the consumption of the host's resources and the consumption of the network bandwidth. Jelena Mirkovik presents a taxonomy for classifying both attacks. This classification depends on the degree of automation (the attacks might be manual, automatic, semiautomatic), depends also which weakness of the victims want to be exploit, which is the rate of the attacks and the amount of traffic send it, how the attacker try to hide its identification.

On the other hand, the rapid growth of the attacks has led to a parallel development to counteract them. In a general view of the defense techniques, there are four categories of defense against DoS attacks:

Attack Prevention: The aim of this technique is try to stop the attacks before it cause damage on the victim. One of the attacker's techniques to hide its identity is spoof the source address of the attack traffic. This approach tries to make sure that only valid traffic can pass through.

Attack Detection: When an attack skips the attack prevention phase, the victim has to try to detect the attacks when they occur, which is important to direct any further action.

Attack Source Identification: Once an attack has been detected, it should try to identify the source that the attacks want to exploit and take the necessary steps to resolve the problem (as block the traffic at its source).

Attack reaction: If the attack skips the steps below and it is already attacking the resource, there should be a reaction to minimize the damage of the attackers and try to get the end of the attack.

In the current network architecture, the network devices (particular routers) are bundle with a specialized control plane and various features. This vertical integration essentially binds you to whatever software and features are shipped with those particular devices. Software Defined Networking effectively breaks these pieces apart.

SDN is a type of network architecture that separates the network data plane (network devices that forwarding traffic) from the control plane (software logic that controls ultimately how traffic is flowing through the network).

One of the reasons to separate the control plane and the data plane is that the software control of the network can evolve independently of the

hardware. A second reason is that it allows the network to be controlled from a single high-level software program.

1.1 Motivation

In order to make a good observation and analysis of the rock mass during the preliminary stages of a project, a rock mass classification method is needed. There are several methods to perform this job but not all of them can cover all the situations. In Finland, a Q-System Course was carried out in Aalto University in order to teach the method and have a better knowledge about it.

Referring to the rock mass quality of the zone already explained, and thus for the exceptionality favorable bedrock conditions are well suited for any kind of rock construction in Finland, one of the most appropriate rock mass classification method is the Q-System method and that is reason enough for make a detailed investigation like this project.

1.2 Objectives

The aim of this project is analyze all the data that the participants recollected from the Test Tunnel in order to know the degree of subjectivity of Q-System and how to improve the teaching method. The study is also useful because of the different way to make the exercises in the Tunnel, logging of the core boxes and mapping of the wall of the tunnel, and compare the several observations made by different kind of backgrounds between the participants.

Inquire to others kinds of rock mass classification methods will be rewarding as well, in order to go in depth in the investigation of the project.

1.3 Structure of the Thesis

You should use transition in your text, meaning that you should help the reader follow the thesis outline. Here, you tell what will be in each chapter of your thesis.

Chapter 2

Background

2.1 DDoS attack and defense mechanisms

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent the legitimate users of a service from using that service [1] provided by a network or server. There are two manner to launch this kind of attack. The first approach is overwhelm the network and occupy all the resources of a service sending massive volumes of useless traffic

2.2 OpenFlow

2.3 NOX

Bibliography

[1] CC., C. Denial of service attack. http://www.cert.org/tech_tips/denial_of_service.html.

Appendix A

First appendix

This is the first appendix. You could put some test images or verbose data in an appendix, if there is too much data to fit in the actual text nicely.

For now, the Aalto logo variants are shown in Figure A.1.

(a) In English

(b) Suomeksi

(c) På svenska

Figure A.1: Aalto logo variants