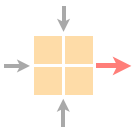

Networked Systems
ETH Zürich — seit 2015

Thesis Title

Semester/Master Thesis

Author: Firstname Lastname

Tutor: Name of the tutor(s)

Supervisor: Prof. Dr. Laurent Vanbever

December 2019 to July 2020

Abstract

An abstract is a short summary placed prior to the introduction used to help readers determine the purpose of the thesis. While the length of the abstract varies by field of study, it is typically a paragraph in length (3-5 sentences), and never more than a page.

Contents

Chapter 1

Introduction

Motivate the problem, introduce your work and give an overview of the report.

1.1 Motivation

The motivation to write this thesis was ...

1.2 Task and Goals

Describe your task and the goals you achieved.

1.3 Overview

Section 2 describes ..., Section 3 presents ...

Chapter 2

Background and Related Work

In this chapter, we give the reader the required background knowledge in order to understand our work. In addition, we also discuss related work.

A chapter can be further divided in sections and subsections. We can also refer to such a section 2.1.

2.1 Background

- A simple bullet list
  - Which can be used for several levels

1. The same applies to enumerated lists.

We can also add a figure 2.1.

Figure 2.1: This is a figure caption

Tables can also be useful.[1]

Column 1	Column 2 (additional line)		Column 3
C1,R2	C2,R2		C2,R3
C1,R3		C2&C3,R3	
C1,R4	C2,R4		C3,R4

Table 2.1: Table 1

2.2 Related Work

If we refer to another paper, book, website, ... we add a citation [**?**].

[1] Tips for beautiful tables: `https://texdoc.net/texmf-dist/doc/latex/booktabs/booktabs.pdf`

2.2.1 ACC-Turbo

ACC-Turbo, as proposed in [**?**], is a in-network DDoS defense, designed to mitigate pulse-wave DDoS attacks, but applicable to any volumetric attacks. The novelty of ACC-Turbo is its capability to run at line rate, mitigating attacks in real time ($\leq$1s reaction time). To achieve this, ACC-Turbo uses online clustering and programmable scheduling. Online clustering is based on the idea, that one can observe traffic aggregates. Each incoming packet is assigned to one of a predefined number of clusters, based on its features which can be arbitrary packet header fields. Both the number of clusters, as well as the choice of features are parametrized, although limited by hardware capabilities. The authors of ACC-Turbo provide an implementation in P4 for the Tofino 1 programmable switch, which works with 4 clusters and 4 features. Distances between packets and clusters are determined using a fast, linear version of the manhattan distance. For nominal features, a distance of 1 is assumed if the feature does not match, while for ordnial features, the numeric difference is taken. Programmable scheduling is done offline. The control plane continuously polls information about the clusters from the data plane and determines if there are clusters which are probably part of an attack. This is determined by looking at the throughput, packet rate and size of each cluster. Then, the clusters are mapped to a priority queue which deprioritizes clusters which are probably part of an attack. ACC-Turbo was evaluated using both, a hardware-based and a simulation-based approach. In the hardware-based evaluation, ACC-Turbo was compared to Jaqen [**?**] and stood out especially by its fast reaction time and a more generic approach. On the other hand, ACC-Turbo suffered from slightly higher benign packet drops, once an attack was mitigated. The simulation-based evaluation showed ACC-Turbos's capabilities beyond the current limitations of commodity hardware. The result was, that using a higher number of clusters and features, the results can be further improved, which will become possible with new generations of commodity hardware soon. Also, a better distance function might be used, if hardware permits. The limitations of ACC-Turbo lie in two main points. The first is, that ACC-Turbo can only prevent volumetric attacks. Secondly, ACC-Turbo assumes, that attacks are detectable by similarity of packets, i.e. they form traffic aggregates. An attacker could break similarity at packet level or at aggregate level.

Discussion ACC-Turbo's most convincing advantages, are the capability to work at line-rate and the genericity of the approach. One design consideration was to define a distance of 1 for non-matching nominal features. However, this value is chosen arbitrary and has no relation to the range calculations of ordinal features. Thus, although it seems to work well in practice, more research would be required to find out whether the influence of nominal parameters gets marginal because of this decision or not. As ACC-Turbo does only work for volumetric attacks and traffic aggregates, it is a good idea to use it together with other DDoS defenses, which are designed for low traffic and spread attacks.

Chapter 3

Design

This chapter describes your work in detail and is normally the longest chapter. You can also create multiple chapters describing your work.

It is often useful to format your text with **bold** or *italic words*. In addition, it can be helpful to format text as verbatim:

```
Verbatim representation
    of     my
text.
```

Finally, you can also add a mathematical formula inline $a^2 + b^2 = c^2$ or in its own block:

$$\cos(2\theta) = \cos^2\theta - \sin^2\theta \tag{3.1}$$

Chapter 4

Evaluation

Another important chapter is the evaluation which should clearly describe the experiments you performed (setup, number of measurements, ...), show the results you achieved in figures and/or tables and discuss and compare the results.

Chapter 5

Outlook

What are consequences of your work? Do you see possibilities for future work?

Chapter 6

Summary

Give a final, short summary of your work.

Appendix A

My Appendix

If you want to add material which is not absolutely necessary to understand and follow your work, put it in the appendix. Here you could also show important code snippets or additional plots.