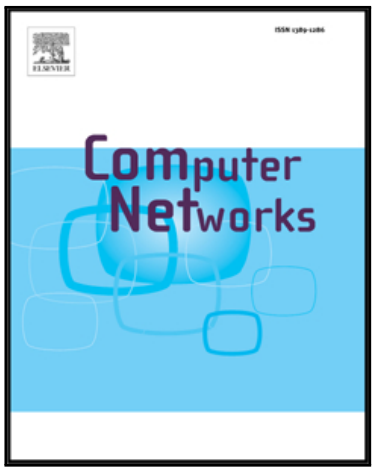

RuleBender: Tree-based Policy Transformations for Practical Packet Classification Systems

Sven Hager, Patrik John, Stefan Dietzel, Björn Scheuermann

PII: S1389-1286(18)30086-0
DOI: 10.1016/j.comnet.2018.02.019
Reference: COMPNW 6417

To appear in: *Computer Networks*

Received date: 18 July 2017
Revised date: 23 December 2017
Accepted date: 14 February 2018

Please cite this article as: Sven Hager, Patrik John, Stefan Dietzel, Björn Scheuermann, RuleBender: Tree-based Policy Transformations for Practical Packet Classification Systems, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.02.019

RuleBender: Tree-based Policy Transformations for Practical Packet Classification Systems

Sven Hager[a], Patrik John[b], Stefan Dietzel[a], Björn Scheuermann[a]

[a] *Humboldt University of Berlin, Rudower Chaussee 25, 12489 Berlin, Germany*
[b] *mm1 Technology GmbH, Schiffbauerdamm 19, 10117 Berlin, Germany*

Abstract

Many existing packet filter implementations use rule set guided packet classification to discriminate incoming network traffic. However, these implementations often rely on slow linear search through the rule set, which diminishes the achievable throughput. Therefore, we propose RuleBender, a rule set transformation technique that encodes decision tree search structures into the transformed rule set, which in turn can be traversed significantly faster. To this end, RuleBender uses the widely supported jump action feature, that enables the redirection of the matching flow to another rule in the otherwise linearly traversed rule set. That way, incoming packets are directed to small sub rule sets that can be searched quickly. In contrast to related work, RuleBender is not restricted to rules that exclusively define geometric matching criteria such as range or subnet tests, but instead inherently supports complex tasks such as payload inspection. RuleBender-generated rule sets can lead to throughput increases up to 13x when compared to the unmodified rule sets, and up to 4x when compared to related work.

Keywords: Packet classification, Rule set transformation, Decision tree

1. Introduction

Packet classification is a core building block of a vast variety of networking devices, such as routers, firewalls, and SDN switches. These systems process incoming network packets based on their header fields and determine the action that must be applied to the packets by consulting a pre-

Email addresses: hagersve@informatik.hu-berlin.de (Sven Hager), p.john@mm1-technology.de (Patrik John), stefan.dietzel@hu-berlin.de (Stefan Dietzel), scheuermann@informatik.hu-berlin.de (Björn Scheuermann)