Building Optimized Packet Filters with COFFi

Sven Hager Frank Winkler Björn Scheuermann Klaus Reinhardt

Computer Engineering Group
Humboldt University of Berlin, Germany
Email: {hagersve, fwinkler, scheuermann, reinhakl}@informatik.hu-berlin.de

I. Introduction

Many companies and institutions employ packet filter firewalls in order to effectively regulate network traffic. Unfortunately, the constant growth of network bandwidth makes the task of matching packet headers against potentially large rulesets more difficult, and prohibits the sole use of entirely software-based firewalls which cannot cope with such huge amounts of traffic. Instead, high-speed firewalls are often implemented in ASICs which offer a high degree of parallelism, many opportunities for operation pipelining, and low-latency access to network data. However, due to their static nature, ASICs must provide generic filtering circuitry that is hardly able to take full advantage of firewall ruleset properties, thus leading to a waste of hardware resources.

Therefore, we propose a methodology to automatically compile stateless firewall rulesets to efficient circuit descriptions in synthesizable VHDL format which can be deployed in FPGA devices. The generated filtering circuitry matches incoming packet header fields against each firewall rule in parallel and leverages a pipelined design which allows for a TCAM-like deterministic classification throughput of one packet header per clock cycle. The employed matching logic is tailored to the checks specified by the translated rules and thus compact. Furthermore, the structure of the generated circuits allows for inter-rule optimizations that are performed during logic minimization. During this process, redundant hardware representations of checks that are shared between multiple rules are removed.

As opposed to previous works in this domain [1], [2], we exploit the structure of the given ruleset in order to aggregate the independent match results in a priority encoder of logarithmic depth, thereby achieving short processing latencies and low hardware resource consumption. We call this approach *COFFi: Custom Optimized FPGA Firewalls*.

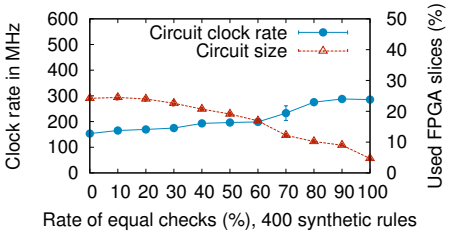

Figure 1: Measuring the influence of ruleset check overlap.

II. Evaluation

We evaluated our approach by compiling various synthetic rulesets to corresponding filtering circuit descriptions that were subsequently synthesized, placed, and routed by the Xilinx ISE 14.4 CAD tool, targeting a Virtex 5 FPGA[1]. First, we measured the impact of rule check overlap on the characteristics of the generated circuits. The amount of check overlap is the number of header field tests that are used in multiple rules and can thus be shared by circuit representations of such rules. Thus, a check overlap should result in smaller and faster circuits. This is confirmed by the results in Figure 1. Next, we compared the pipeline depths of the COFFi circuit structure and the structure proposed by Lee et. al. in [2] by generating rulesets with an increasing number of rules. Figure 2 shows that the pipeline depth of the COFFi circuits is orders of magnitude smaller than of the circuits proposed in [2] (note the logarithmic y-axis), therefore leading to much shorter processing latencies.

References

[1] R. Sinnapan and S. Hazelhurst, "A reconfigurable approach to packet filtering," in *FPL '01*, Aug. 2001, pp. 638–642.

[2] T. Lee, S. Yusuf, M. Sloman, E. Lupu, and N. Dulay, "Compiling policy descriptions into reconfigurable firewall processors," in *FCCM '03*, Apr. 2003, pp. 39–48.

[1] device XC5VSX50T, package FF1136, speed grade -1

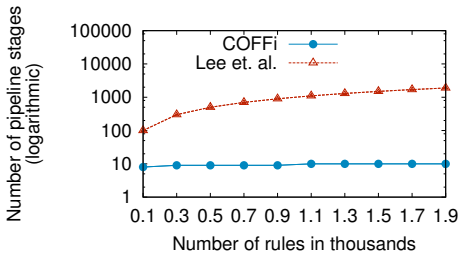

Figure 2: Comparison of pipeline depths.