

Review of:
Assisting Network Intrusion Detection with Reconfigurable Hardware

- Paper by:
 - R. Franklin, D. Carver and B. L. Hutchings (Brigham Young)
- Published in:
 - FCCM
 - April 2002
- Survey by:
 - Bharath Madhusudan

The Challenge

- Perform String Matching at Wire Speeds
- Impediments
 - Need to examine entire packet payload
 - Inefficient in software since several searches have to be performed on a single packet (motivates algorithmic attacks)

Applications

- Intrusion Detection
- URL based load balancing by layer 7 switches

Style of the Paper

- Background / Existing Work
- Technical Approach
- Performance Metrics

Technical Approach

- JHDL based module generator reads the expressions from the Snort rule database and combines them into one large regular expression.
- This is then given to Xilinx's place and route software to generate a bit-stream that can be loaded into Xilinx Virtex FPGAs.

Performance Analysis

- FPGA and Software implementations were compared

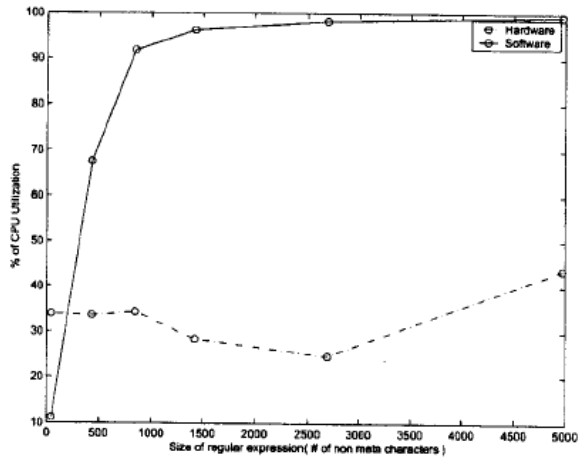
Table 2: FPGA vs. software regex performance for a 1MB data set sent in 1kB chunks

Size of Regular Expression (# of non-Meta characters)	Hardware Latency (ms)	Software Latency (ms)	Hardware Throughput kB/s	Software Throughput kB/s	Hardware CPU Utilization	Software CPU Utilization
47	< 1	< 1	390	432	33.9%	11.2%
435	< 1	3.2	340	197	33.6%	67.6%
844	< 1	37.6	381	23.5	34.3%	91.9%
1,420	< 1	104	284	8.90	28.4%	96.3%
2,689	< 1	240	291	4.63	24.7%	98.3%
4,971	1.2	970	331	0.99	43.7%	99.4%

Table 3: FPGA vs. software regex performance for a 10MB data set sent in 16kB chunks

Size of Regular Expression (# of non-Meta characters)	Hardware Latency (ms)	Software Latency (ms)	Hardware Throughput kB/s	Software Throughput kB/s	Hardware CPU Utilization	Software CPU Utilization
47	< 1	< 1	862	884	19.3%	11.8%
435	< 1	50.9	870	278	18.1%	97.3%
844	< 1	602	824	24.0	16.3%	98.3%
1,420	< 1	978	826	14.9	19.3%	99.6%
2,689	< 1	1930	838	7.58	20.1%	99.6%
4,971	7.38	8400	784	1.72	38.5%	99.8%

CPU Utilization

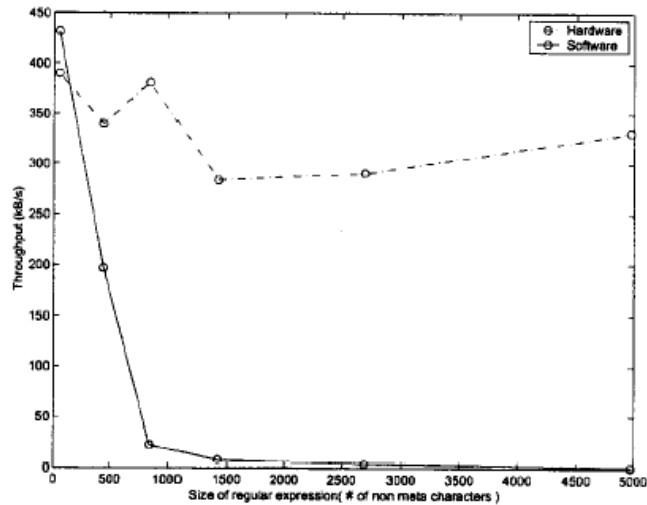


CS6812: Research Seminar on Reconfigurable Hardware



7

CPU Throughput



CS6812: Research Seminar on Reconfigurable Hardware



8

Issues

Scalability issues

- Would it be realistic to assume that in a few years' time the Snort database will expand to a point where we will require 10s of FPGAs hence making this economically infeasible?

Overhead required to reprogram

- Might make it unsuitable for applications other than ID

Design Issue

- NFA vs. DFA

Conclusion

- FPGAs appear to be good candidates to implement ID systems that perform string matching at wire speeds
- More packets can be examined as compared to conventional software based ID systems