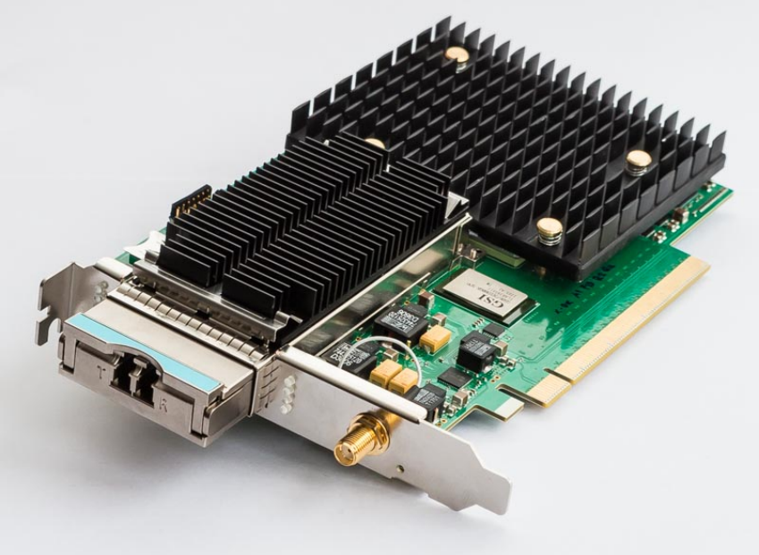
CTU in Prague

Change-Point Detection Method on 100Gb/s Ethernet Interface

Adaptive Hardware Acceleration of Intrusion Detection



Pavel Benáček • Rudolf B. Blažek • Tomáš Čejka • Hana Kubátová

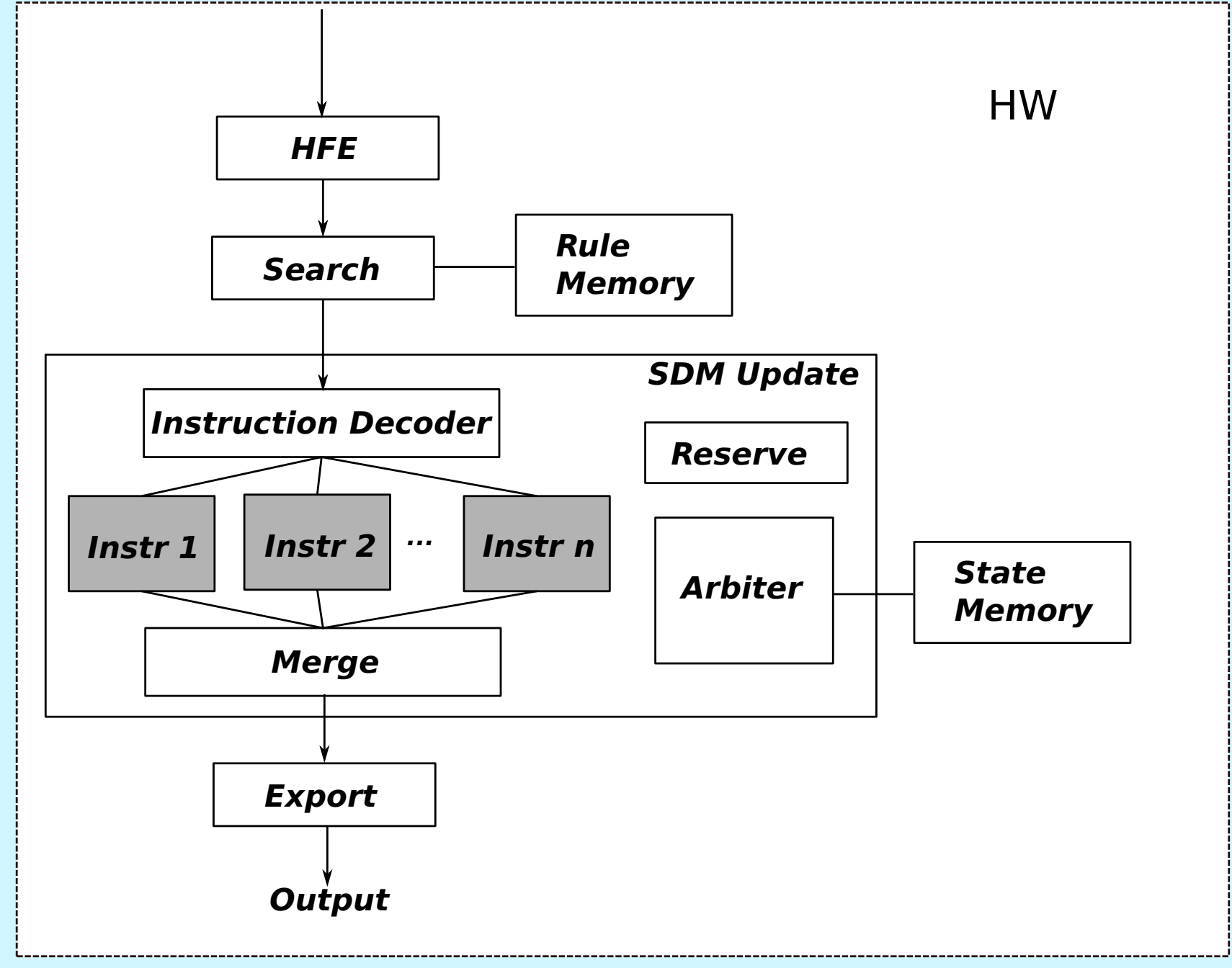
The Context and Problem

- Current monitoring systems usually consist of monitoring probes and one or more collector servers:
  - Probes capture and quickly process huge amounts of data at network link speed.
  - Collectors gather information on network traffic from probes and store it for later analysis.
- In high-speed networks it is difficult and often impossible to use commodity hardware to process all network data in software:
  - Processing at link-speeds leads to information loss.
  - Cause: Insufficient bandwidth of communication paths between hardware and software components.
- We propose hardware-accelerated network data processing and anomaly detection in a monitoring probe.
  - The aim is to enable real-time detection in networks with speeds up to 100 Gb/s on one Ethernet port.

Software Defined Monitoring

- Rapid development of hardware-accelerated methods enabled by:
  - High-level synthesis from C/C++
  - Using software defined monitoring approach
- Software defined monitoring system components:
  - Firmware for a hardware module (SDM plug-in)
  - Computer-based software
    - Monitoring applications: Advanced monitoring tasks, such as analysis of application protocols
    - Controller unit: Dynamically removes and inserts processing rules (packet actions) into hardware module
- Components are connected via a PCI-Express bus
- SDM concept introduced in: L. Kekely, V. Pus, and J. Korenek, "Software defined monitoring of application protocols," *INFOCOM 2014 Proceedings IEEE*, pp. 1725–1733.

SDM Plug-in Implementation



- Packet protocol headers are extracted in the Header Field Extractor (HFE)
- Matching update requests are found in Rule Memory
- Synchronization tags are assigned to requests
- SDM Update Block:
  - This block processes packets, manages network flow records, updates aggregated data records
  - Instruction Decoder sends requests to "Instr X" blocks using a routing table
  - Reserve block controls access to shared State Memory for synchronization for concurrent processing of update requests (via synchronization tags).

The Detection Method

- Feasibility demonstrated by implementing a sequential non-parametric cumulative sum (NP-CUSUM) procedure:

$$S_n = \max\{0, S_{n-1} + X_n - \hat{\mu} - \varepsilon\hat{\theta}\}, \quad S_0 = 0$$

X_n . . . here ratio of SYN and FIN TCP packets in a time window
$\hat{\mu}$ . . . an estimate of the mean of X_n before the attack (here 1)
$\hat{\theta}$ . . . an estimate of the mean after the attack started
ε . . . a tuning parameter for optimization

  - For a fixed average false alert rate (FAR) nearly minimizes average detection delay ... asymptotically as FAR decreases.
  - Change-Point Detection is suitable since network intrusions appear at unknown points in time and lead to a change of some statistical properties of the network traffic.
- NP-CUSUM is implemented as one of the gray "Instr X" blocks in the plug-in architecture diagram.
- NP-CUSUM introduced in: A.G. Tartakovsky, B.L. Rozovskii, R.B. Blazek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *IEEE Transactions on Signal Processing*, vol. 54, no. 9, pp. 3372–3382, 2006.

The Hardware Platform

- The implemented NP-CUSUM algorithm was tested on Virtex-7 H580T FPGA platform in an existing 100 Gb/s monitoring probe.
- The probe is being developed by CESNET as the COMBO-100G card (https://www.liberouter.org)
- Specifications:
  - 1 × CFP2 transceiver cage
  - PCI-Express generation 3, 16 lanes
  - FPGA Virtex-7 H580T
  - 3 × QDR-IIIe SRAM 500 MHz 72 Mib each
  - 8 × DDR3 DRAM, 800 MHz, 4 Gib each
  - Precise timestamp input

Results

Table 1: FPGA resources for the hardware plug-in.

Name	BRAM 18K	DSP48E	FF	LUT
Expression	-	-	0	458
FIFO	-	-	-	-
Instance	-	-	280	252
Memory	-	-	-	-
Multiplexer	-	-	-	1842
Register	-	-	2253	-
ShiftMemory	-	-	0	806
Total	0	0	2533	3358

Table 2: Performance of the CPD hardware plug-in.

Parameter	Fixed-point	Floating-point	Required
Clock period	4.08 ns	16.48 ns	5 ns
Frequency	245 MHz	60.679 MHz	200 MHz
Latency	12	11	-

Table 3: FPGA resources – SDM system & 1 plug-in.

Resource Name	Used Resources [-]	Utilization Percentage
LUTs	47731	13%
Registers	21089	2%
BRAMS	107	11%

The translated source code of the new hardware plug-in is wrapped in a VHDL envelope that adapts the behavior of all predefined interface signals.

The envelope can be reused, hence the SDM system acts as a framework for rapid creation of new advanced hardware modules for network monitoring and anomaly detection.

- None of the Block RAMs (BRAM 18K) and DSP48E blocks were used.
- Look-up tables (LUT) and Flip-Flops (FF) take less than 1% of FPGA resources.
- Fixed-point implementation satisfies one-cycle Initiation Interval requirement for processing 100 Gb/s network traffic.
- With synthesis optimization, e.g. register duplication, all other requirements for 100 Gb/s processing have been met.
- Table 3 – about 87% of resources are available after implementing the whole synthesized SDM system with one CPD hardware plug-in.
- It is thus feasible to include several similar hardware plug-ins for parallel detection of various anomalies without significant latency increase.

Czech Technical University in Prague, Faculty of Information Technology

CESNET, a.l.e., Prague, Czech Republic