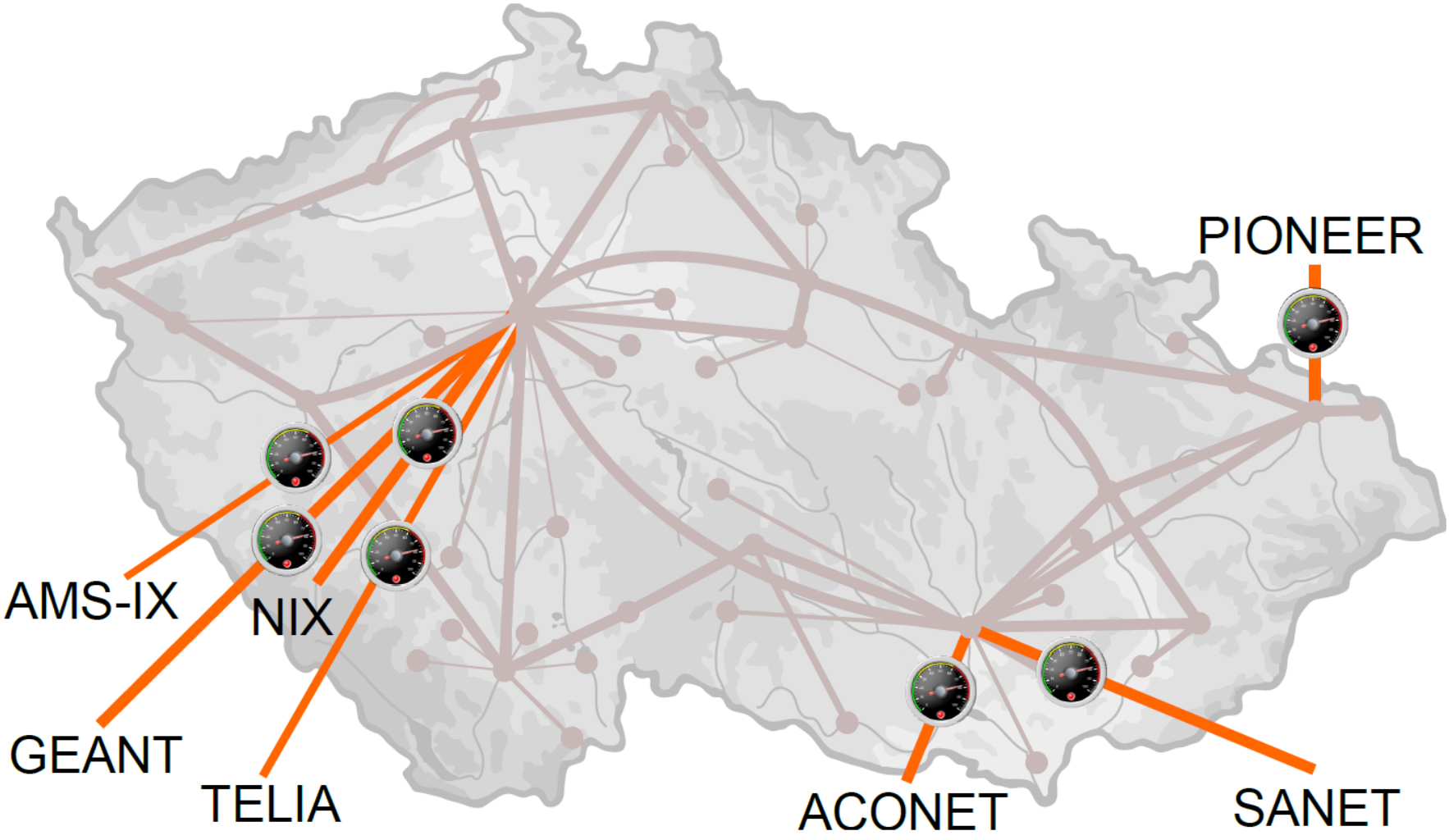
Hardware acceleration of IDS for high-speed networks

Lukáš Kekely (kekely@cesnet.cz)

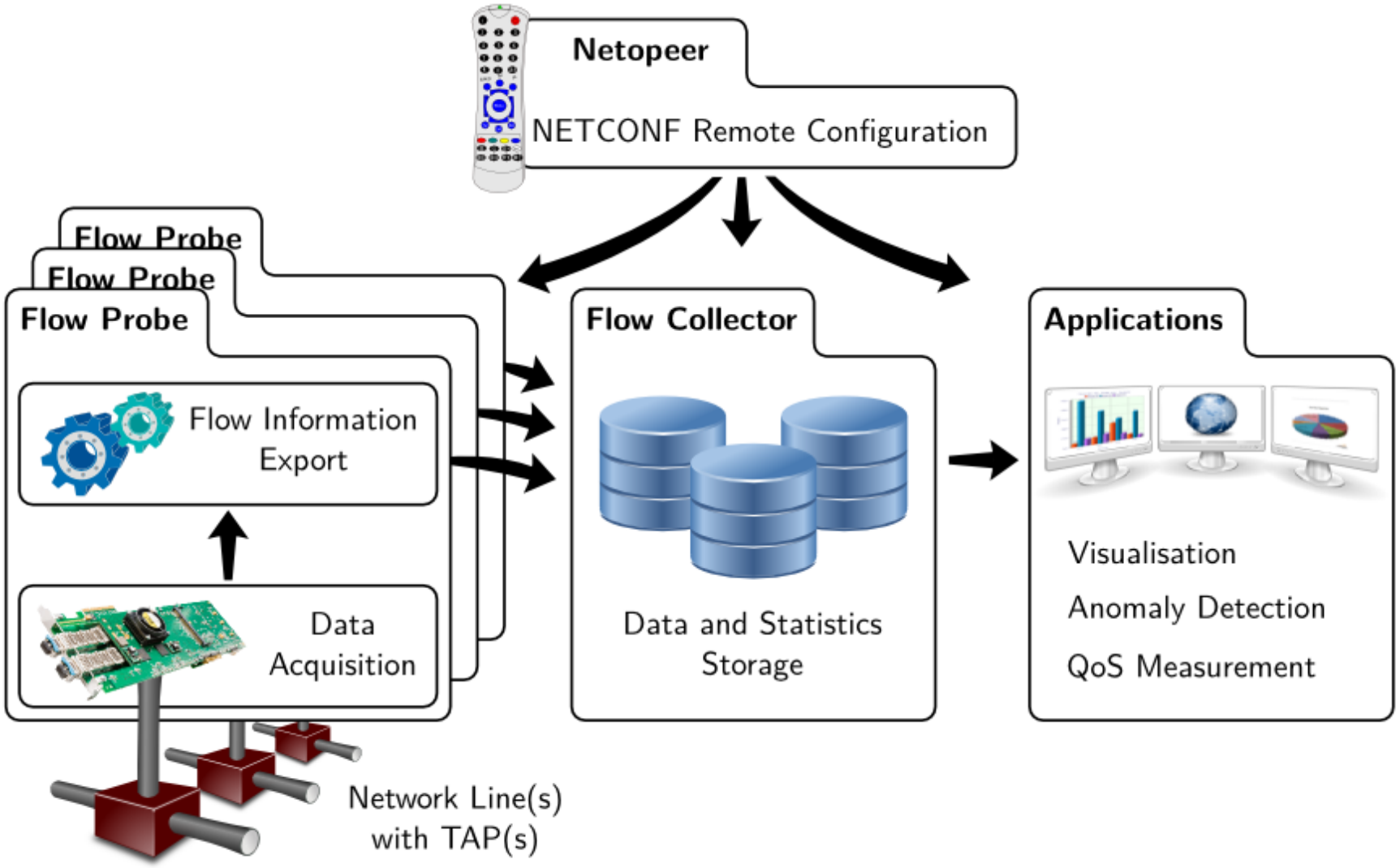
17th July 2017, 43rd NMRG meeting

Liberouter group

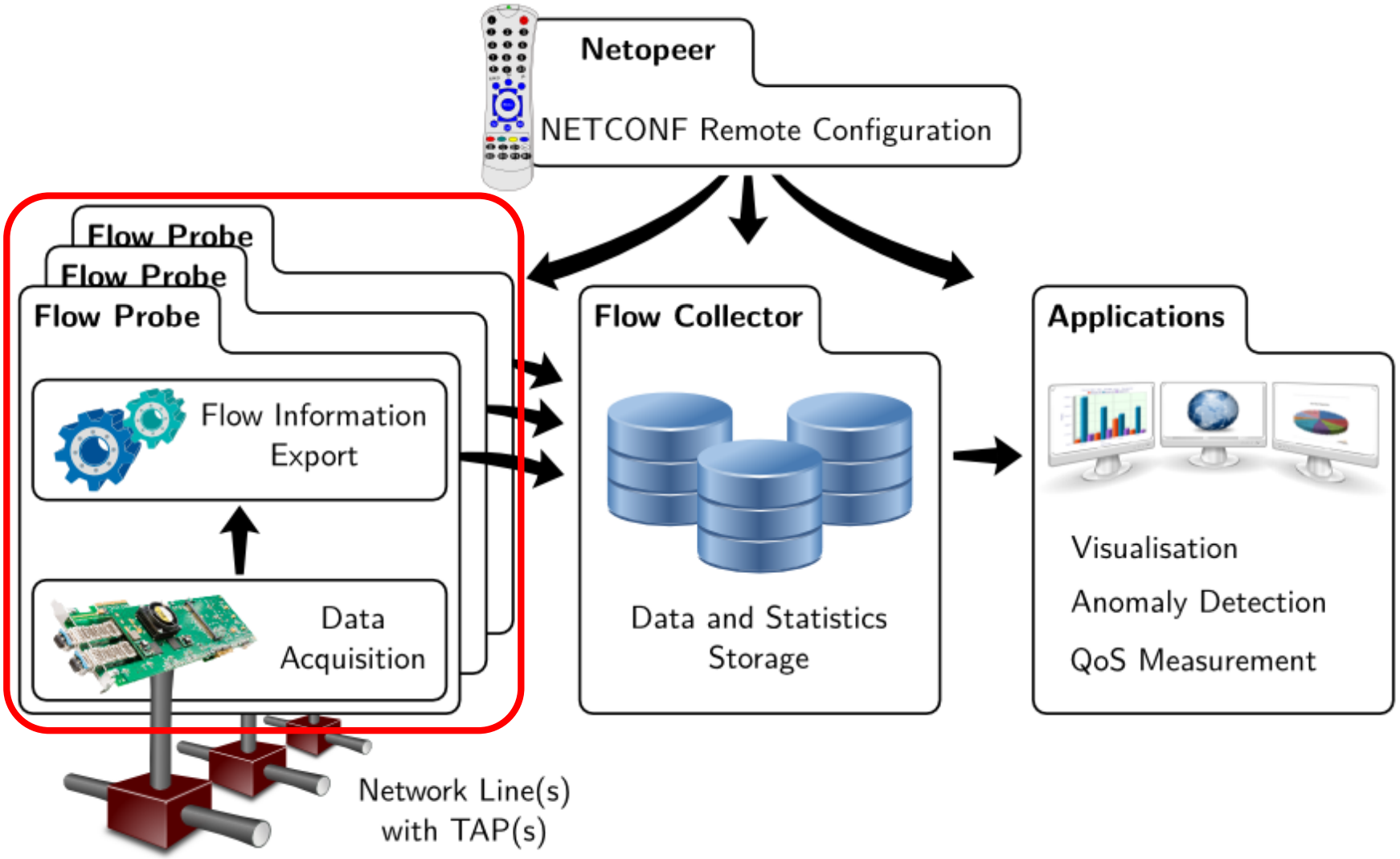


- guarding the perimeter of CESNET

Toolset


Netopeer
NETCONF Remote Configuration
Flow Probe
Flow Probe
Flow Probe
Flow Information Export
Data Acquisition
Network Line(s) with TAP(s)
Flow Collector
Data and Statistics Storage
Applications
Visualisation
Anomaly Detection
QoS Measurement

Presentation scope



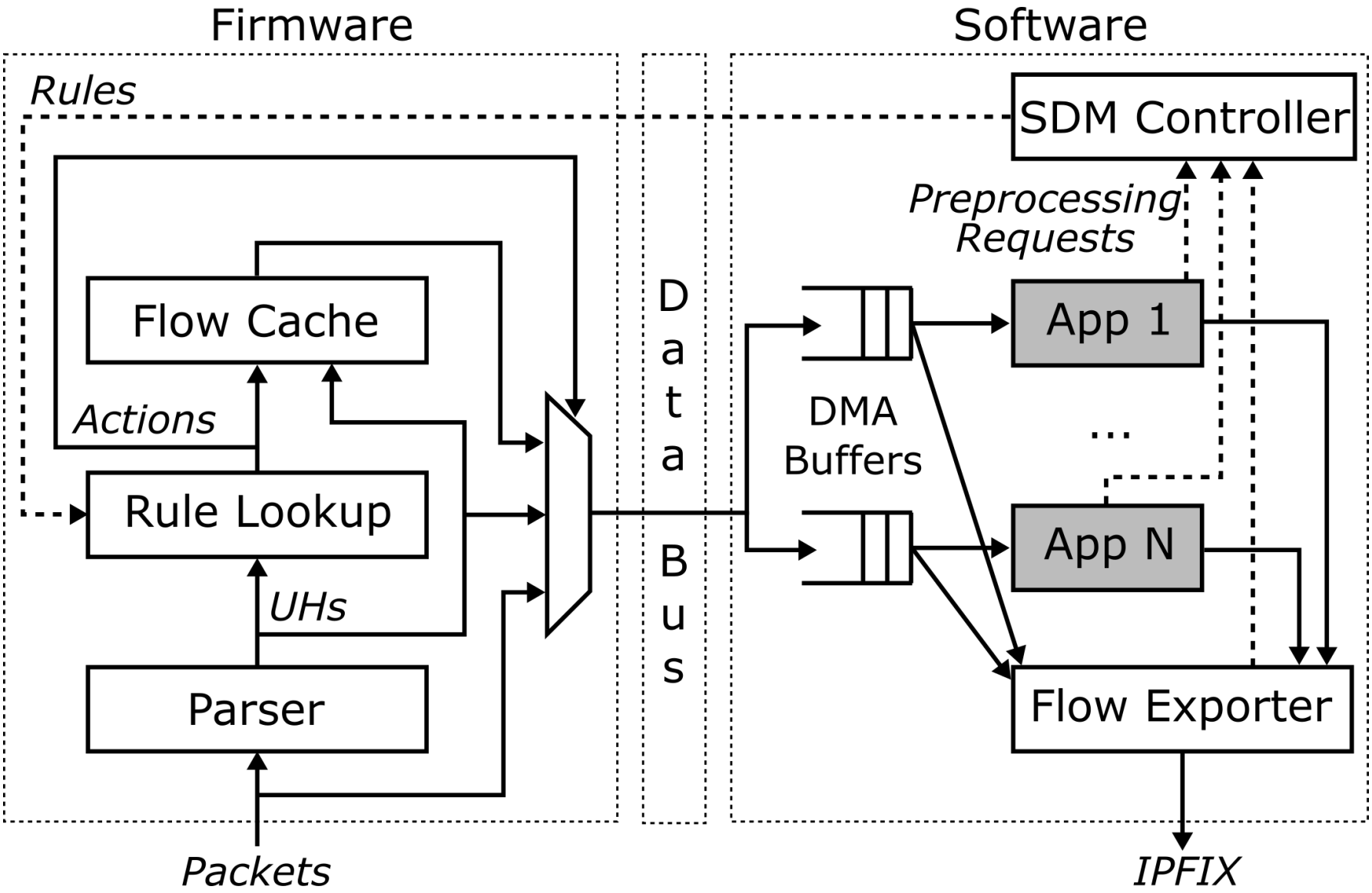
Monitoring probe

- Standard approach:
  - operation as standard NIC (capturing packets)
  - software processing of the whole traffic

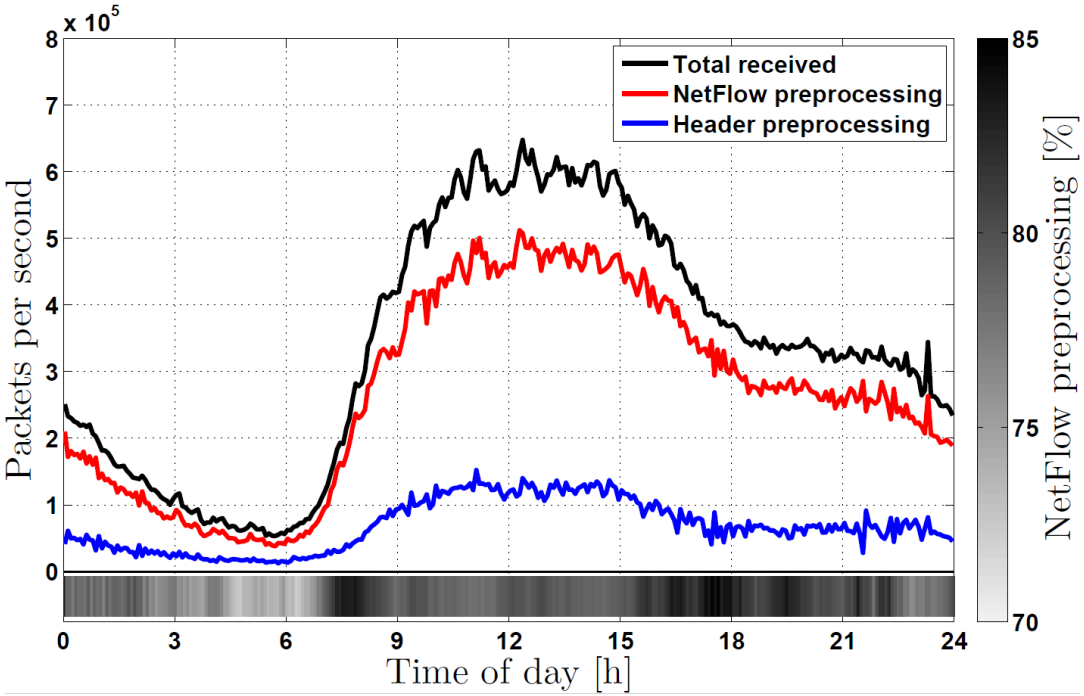
- Accelerated approach:
  - accelerated traffic preprocessing in card
  - SW performs advanced/specific processing
  - our unique concept of:

Software Defined Monitoring

SDM concept


Firmware
Software
Rules
SDM Controller
Preprocessing Requests
Flow Cache
Actions
Rule Lookup
UHs
Parser
Packets
Data Bus
DMA Buffers
App 1
...
App N
Flow Exporter
IPFIX

SDM results



Use case	Preprocessing method [% of packets] None	Header	NetFlow	Drop
NetFlow	–	20.55	79.45	–
Port scan	–	17.54	–	82.46
Heartbleed	4.91	–	–	95.09
HTTP	22.82	–	–	77.18
HTTP+NetFlow	23.34	10.56	66.10	–

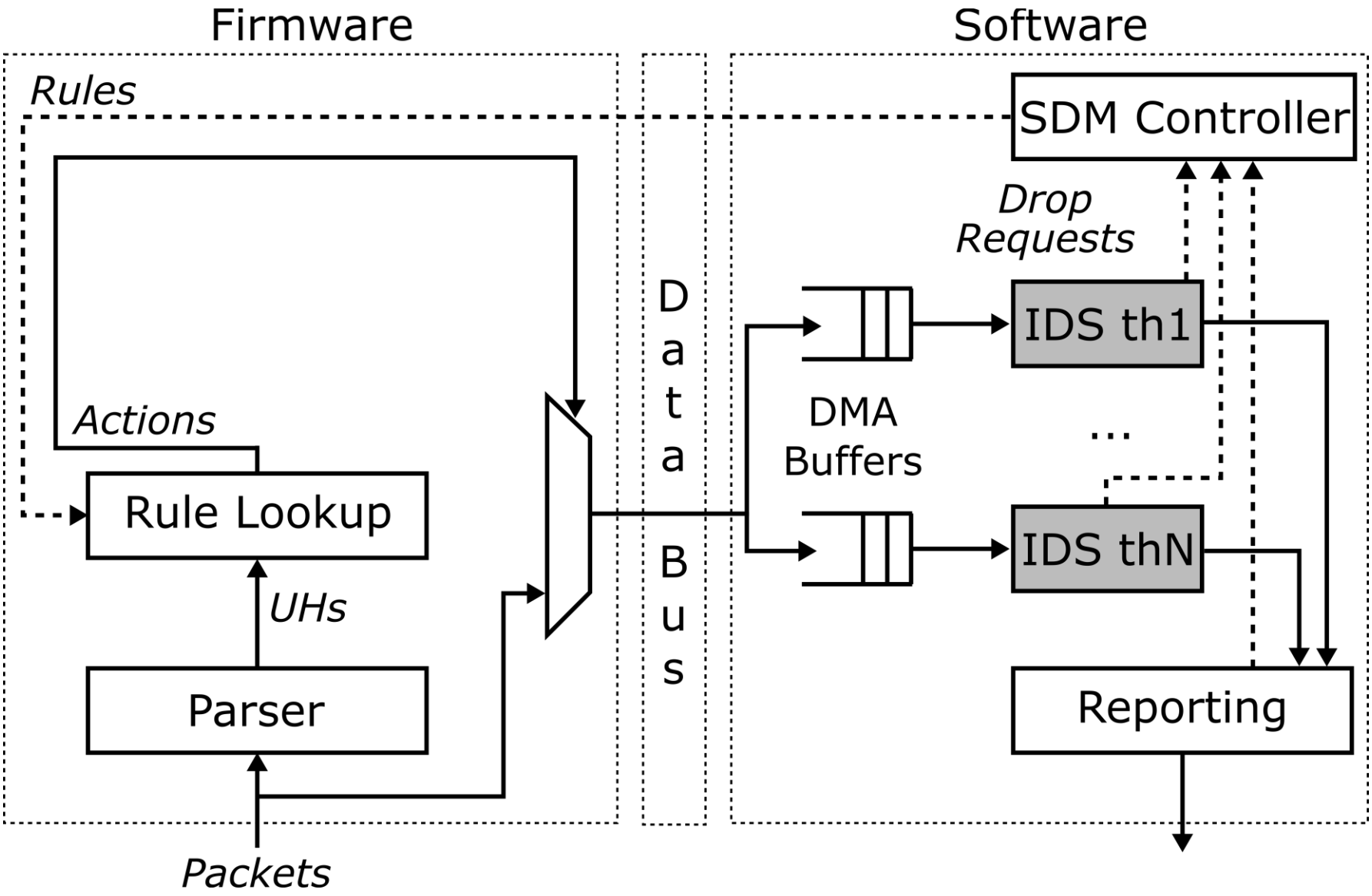
Use case	SW load [%] None	Bytes	Flows covered by rules [%]
NetFlow	20.66	0.98	6.37
Port scan	17.54	0.86	6.53
Heartbleed	4.91	3.77	0.95
HTTP	22.82	27.82	1.98
HTTP+NetFlow	34.02	29.00	6.04

- monitoring tasks can be accelerated
  - INFOCOM paper, IEEE ToC article
- can SDM be used to accelerate IDS?

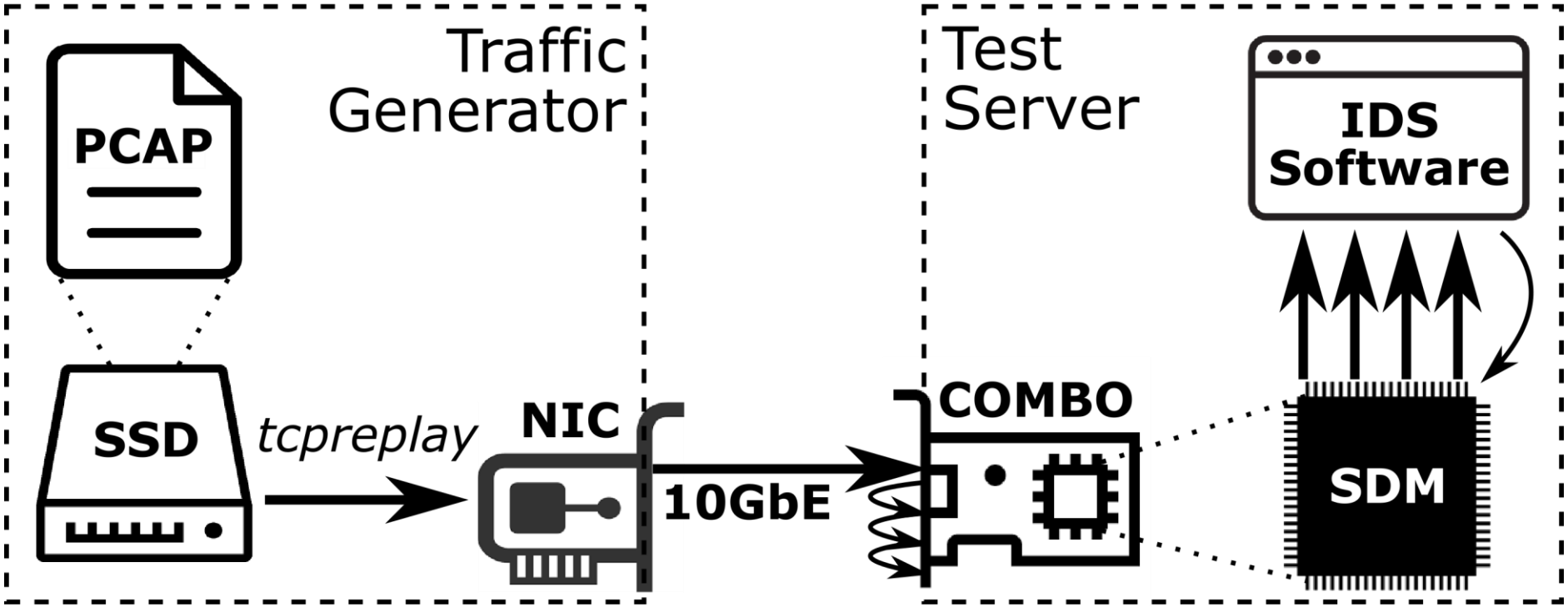
IDS assumptions

1. performance of software IDS is limited
   - insufficient for current multi Gbps networks
2. default discarding method is blind
   - input buffer overflow if IDS is not fast enough
3. informed drops enable better results
   - IDS packet processing rate is the same
   - more interesting data are processed
4. the most relevant are initial packets
5. majority of traffic belongs to few flows
   - only drop trailing packets of a few heavy flows

IDS over SDM


Firmware
Software
Rules
SDM Controller
Drop
Requests
Data
Bus
IDS th1
DMA
Buffers
...
IDS thN
Actions
Rule Lookup
UHs
Parser
Reporting
Packets

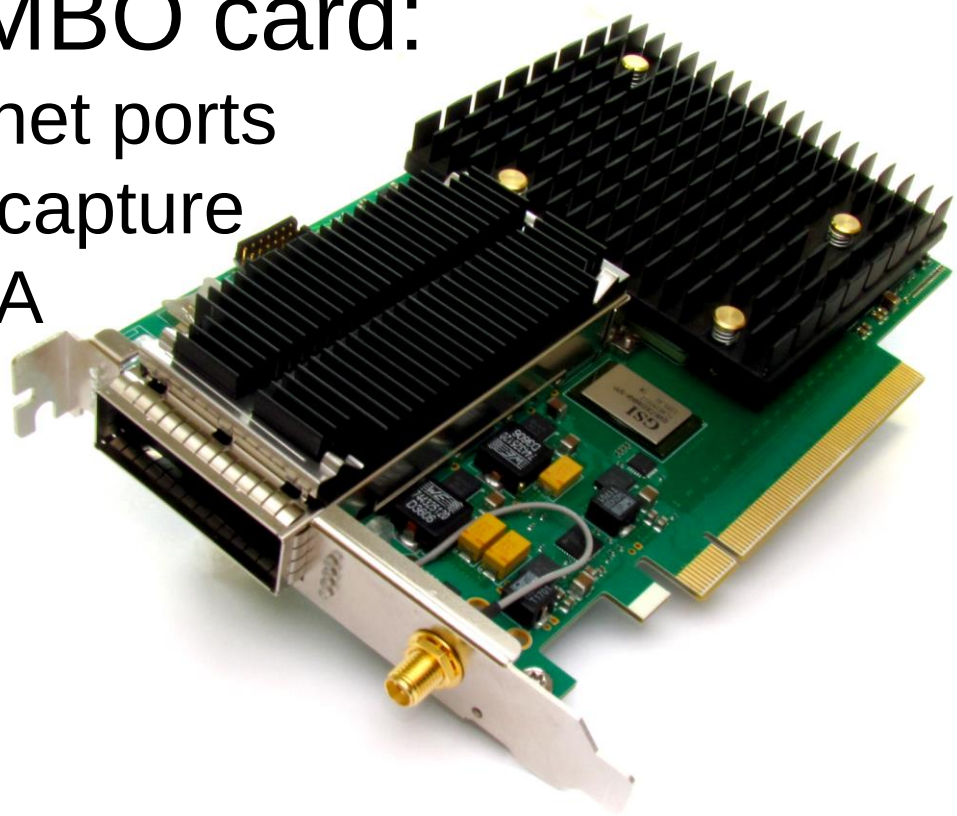
Test setup



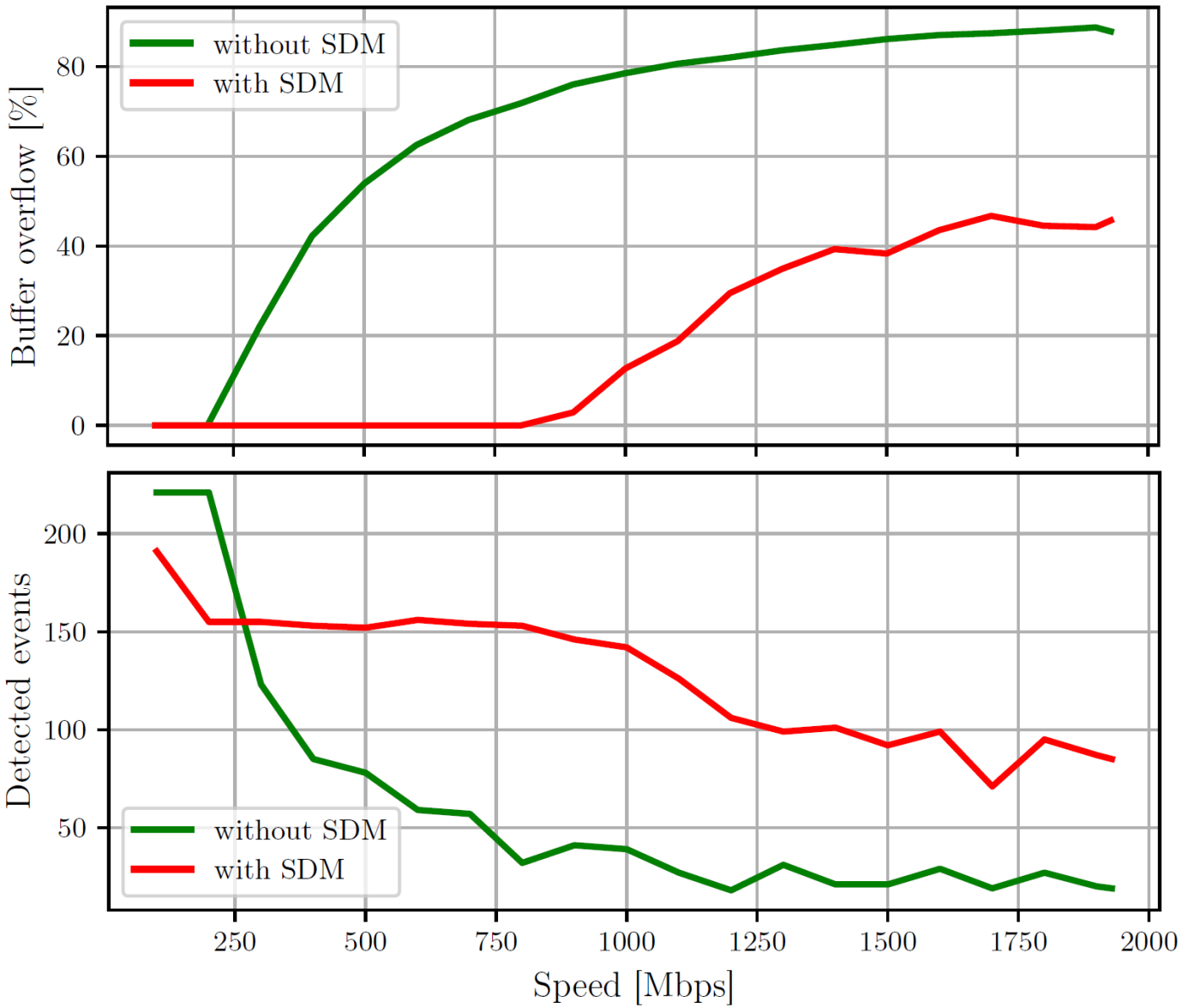
- Tested IDS:

Test server

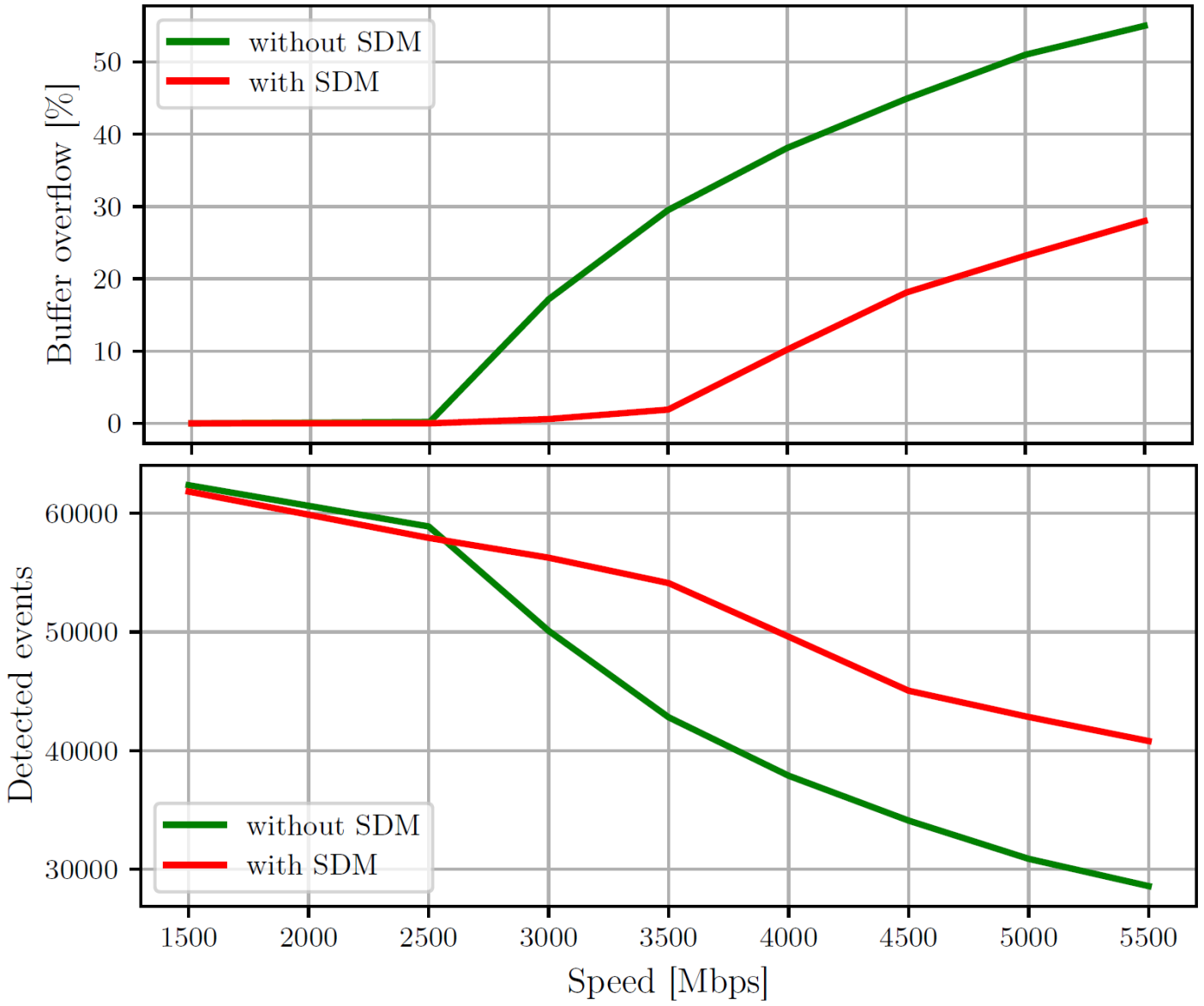
- Supermicro X9DRG-QF server
- 2x Intel Xeon E5-2650 (8x 2.6GHz)
- 64GB DDR3 RAM
- acceleration COMBO card:
  - 10x 10 Gbps Ethernet ports
  - line rate 100 Gbps capture
  - Xilinx Virtex-7 FPGA
  - SDM firmware



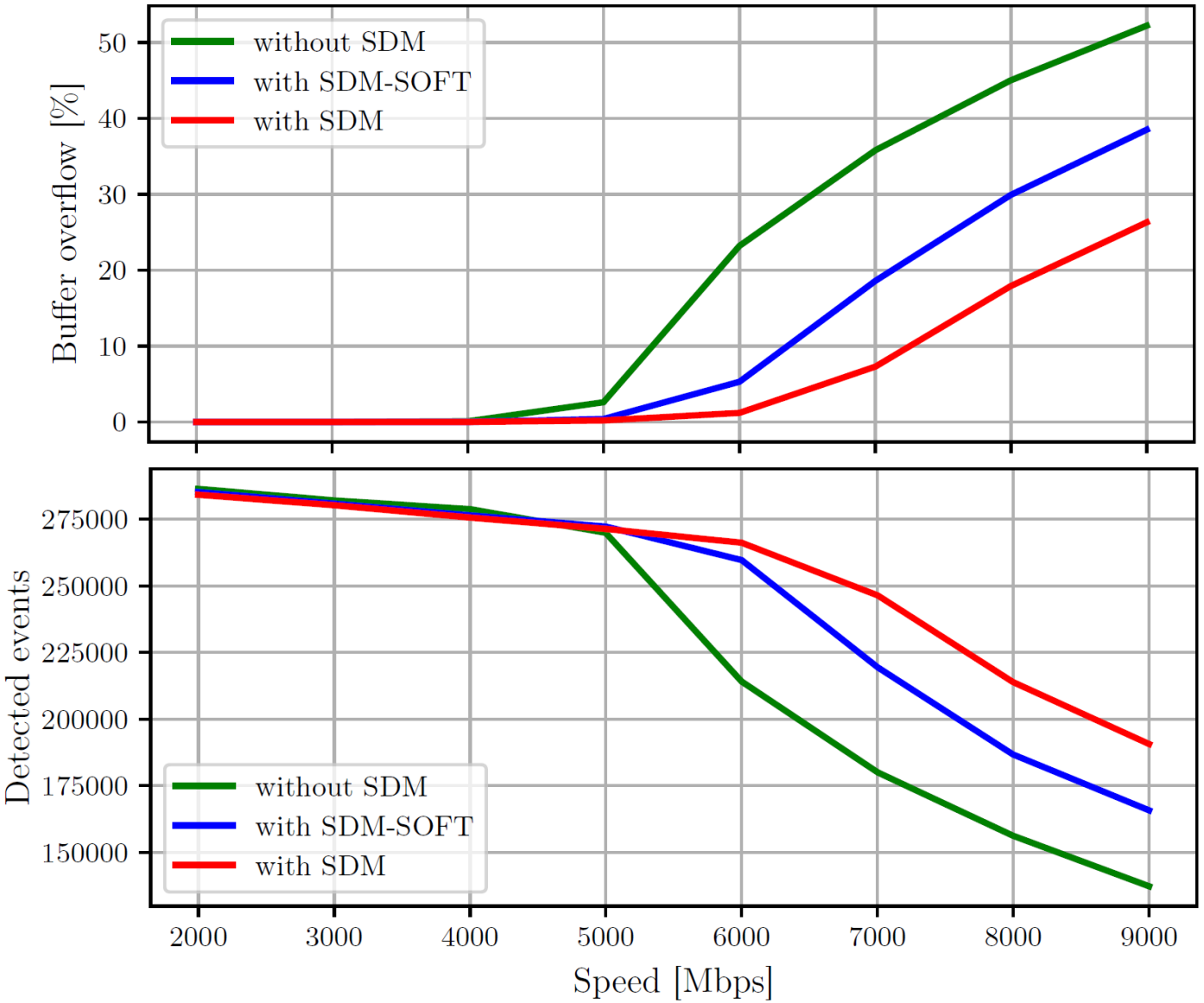
Snort @ libpcap



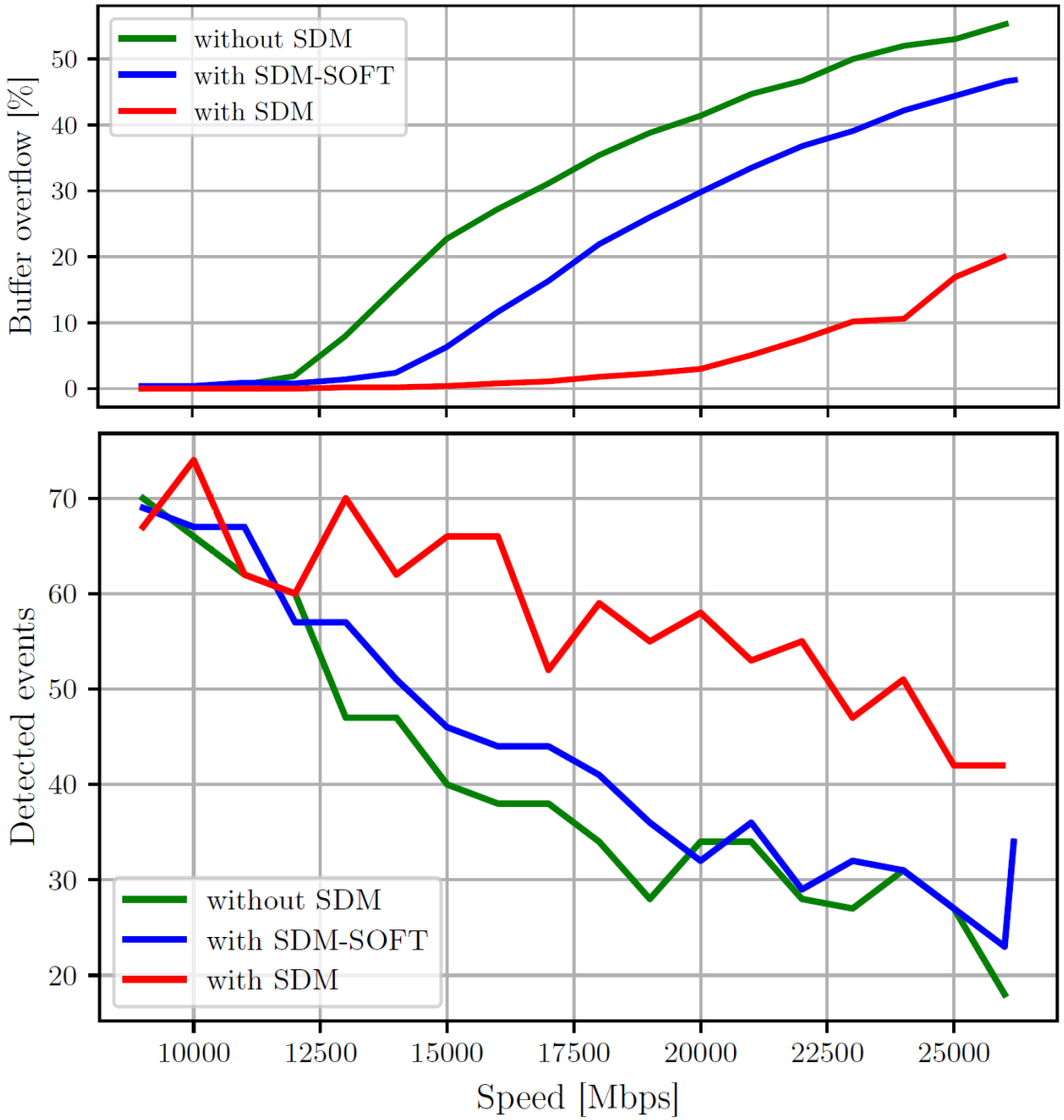
Suricata @ libpcap



Suricata @ SZE2



Suricata (small) @ SZE2



Summary

- IDS can be accelerated by SDM
  - significantly reduced packet loss
  - higher achievable processing throughput
  - better detection accuracy at faster lines
- SDM is applicable in yet another area
  - designed primarily for monitoring
  - can accelerate security applications as well
- INFOCOM paper in preparation

Thank you for your attention!

More info:

- *https://www.liberouter.org/*
- *kekely@cesnet.cz*