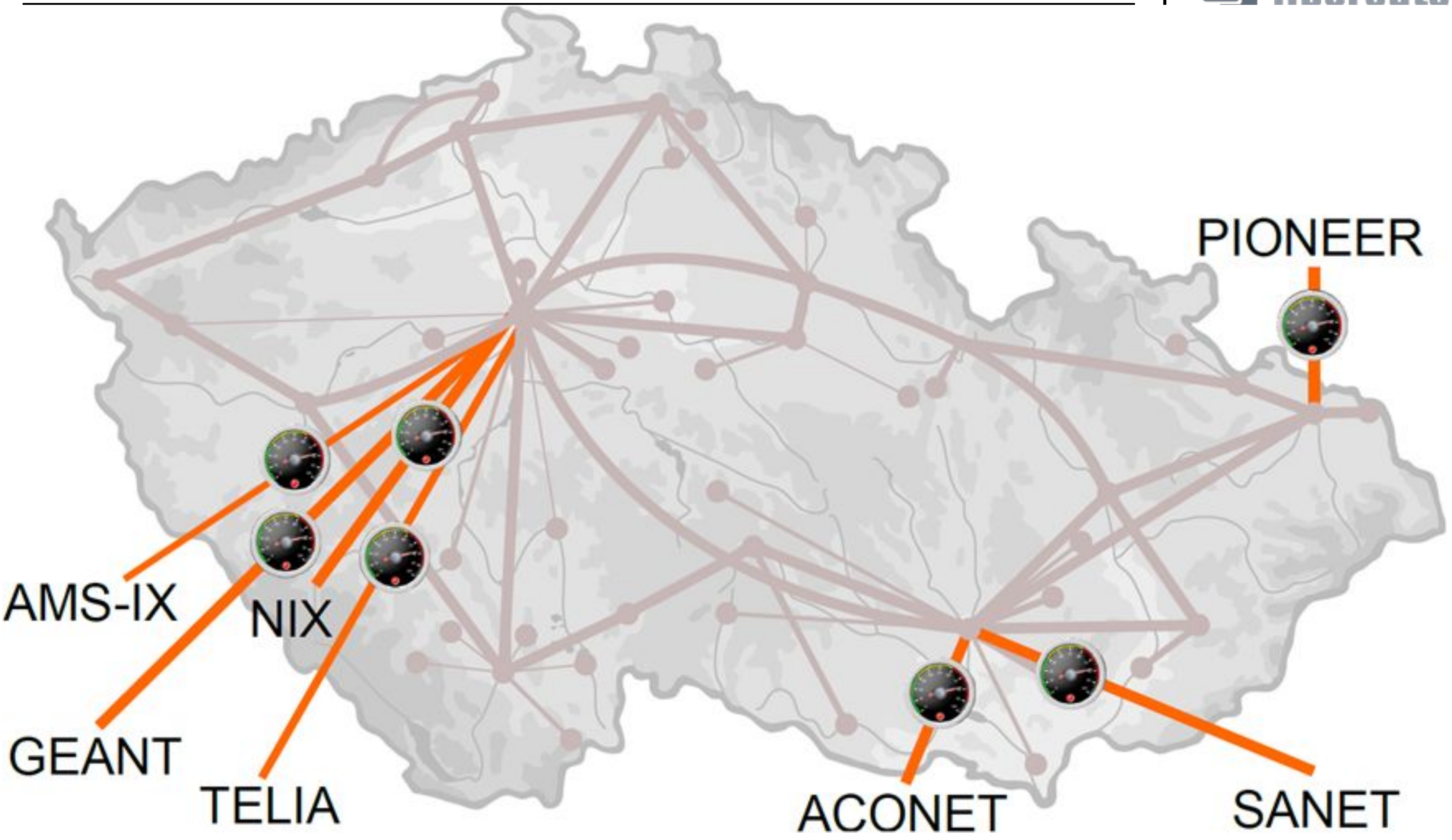
# Performance Measurements and Acceleration Potential of Suricata IDS

Lukáš Kekely (kekely@cesnet.cz)

28. 11. 2017, Copenhagen

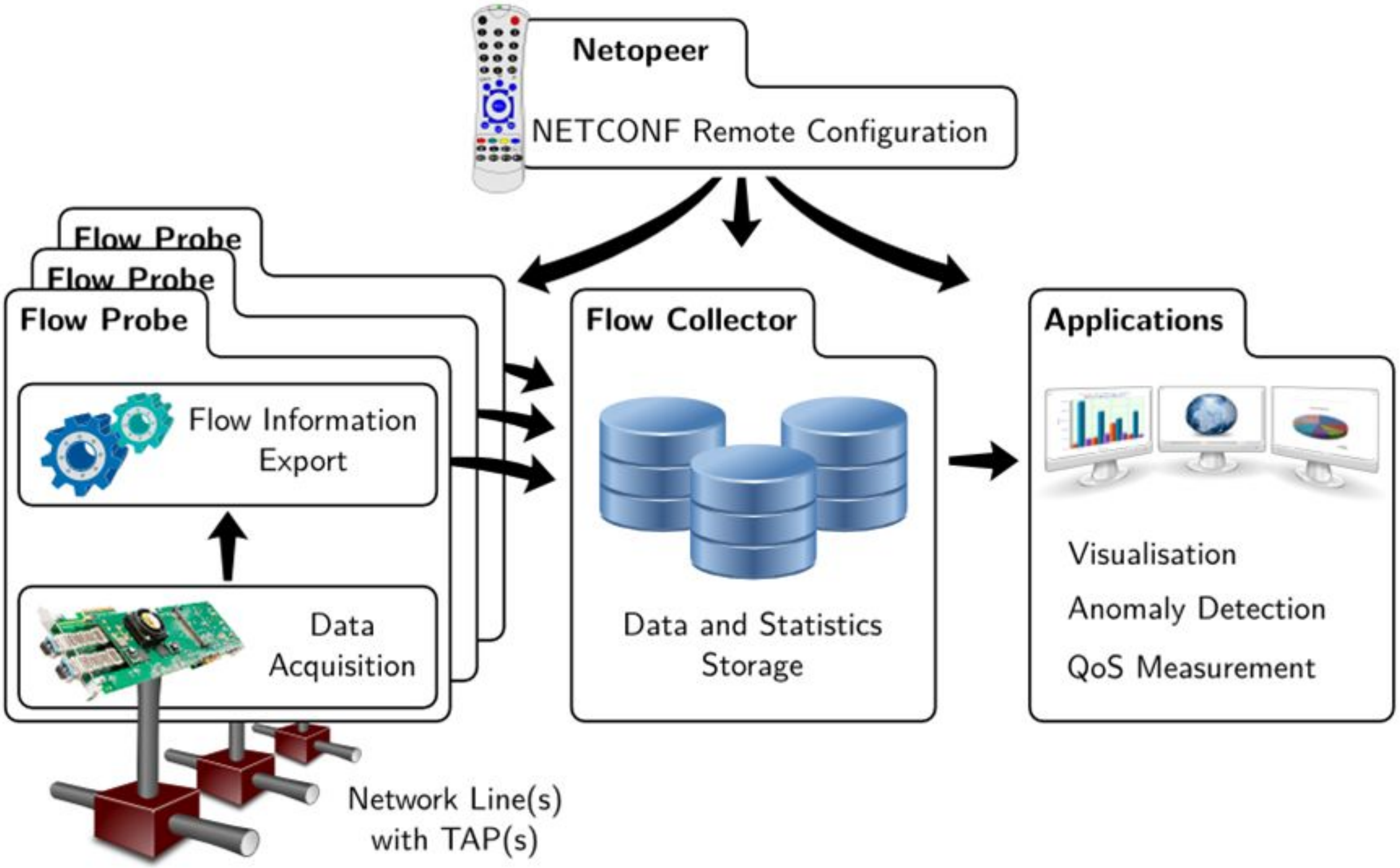
3rd SIG-PMV Meeting

# Liberouter group



- guarding the perimeter of CESNET network

# Toolset



Netopeer

NETCONF Remote Configuration

Flow Probe

Flow Probe

Flow Probe

Flow Information Export

Data Acquisition

Flow Collector

Data and Statistics Storage

Applications

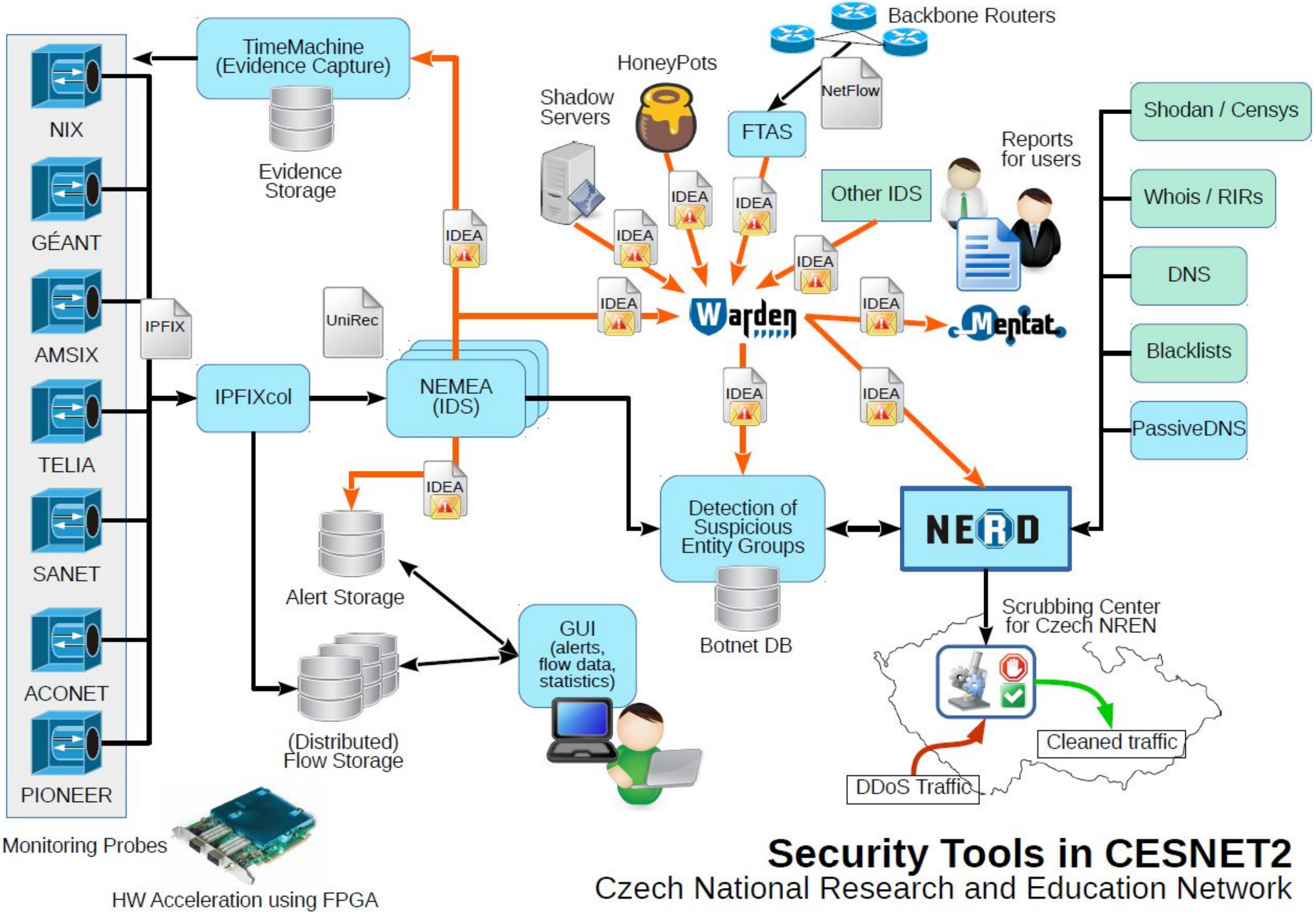
Visualisation

Anomaly Detection

QoS Measurement

Network Line(s) with TAP(s)

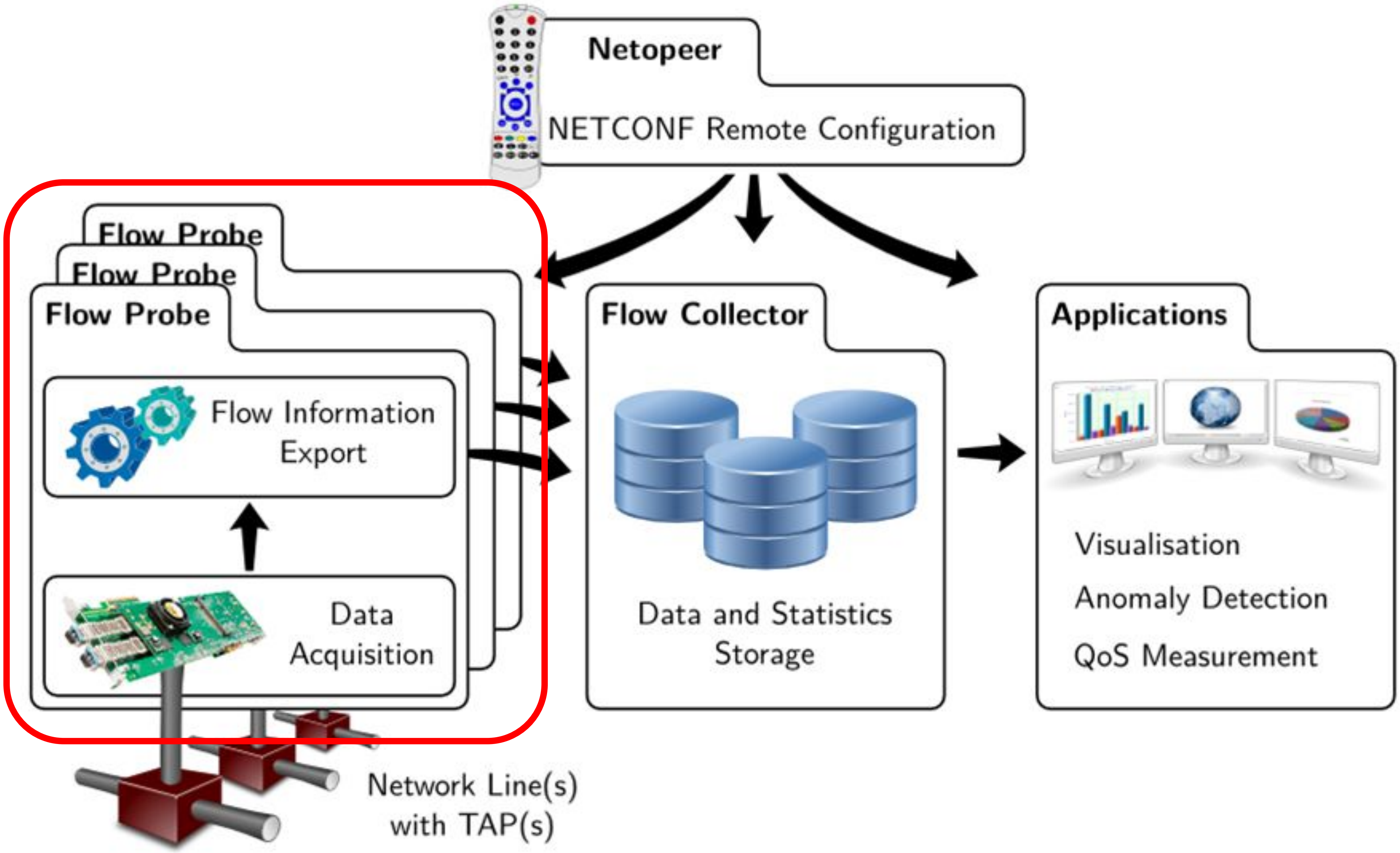
# Toolset (detailed)



**Security Tools in CESNET2**

Czech National Research and Education Network

# Presentation scope



# Monitoring probe

- Standard approach:
  - HW operates as standard NIC (only capturing packets)
  - software processing of the whole network traffic

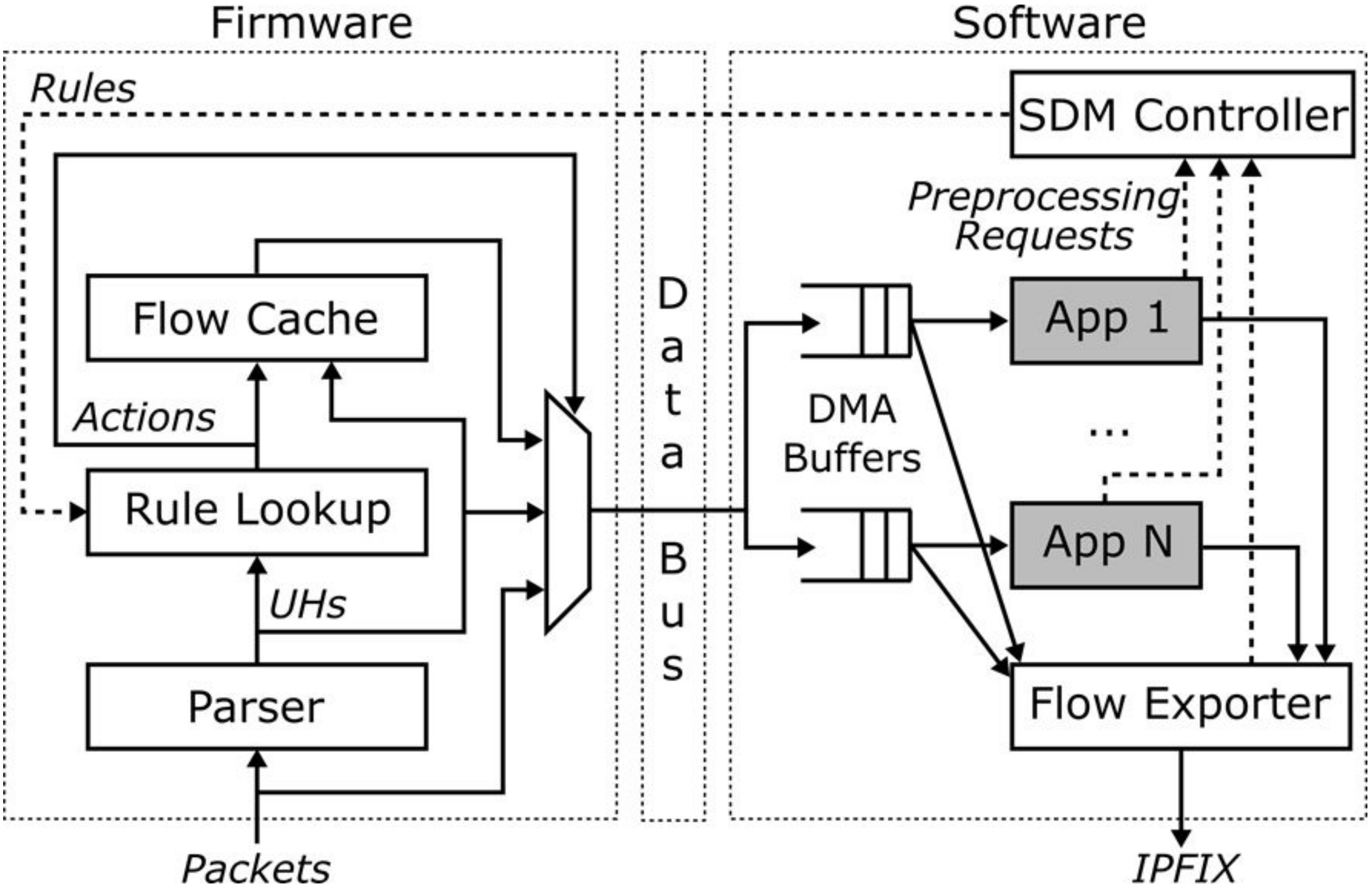
- Accelerated approach:
  - accelerated traffic preprocessing directly in card
  - SW performs only advanced/specific processing

# Monitoring probe

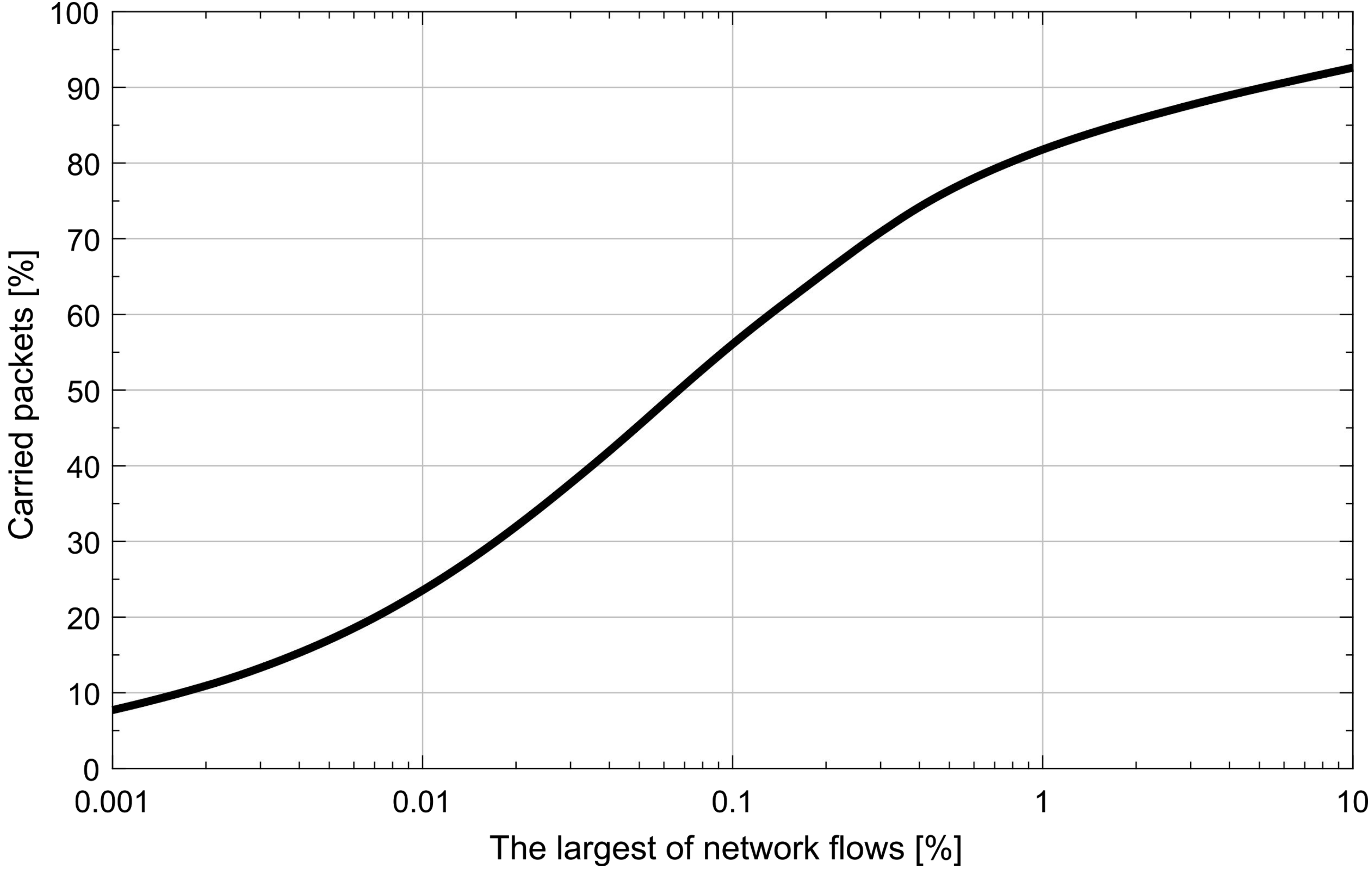
- Standard approach:
  - HW operates as standard NIC (only capturing packets)
  - software processing of the whole network traffic
- Accelerated approach:
  - accelerated traffic preprocessing directly in card
  - SW performs only advanced/specific processing
  - our unique acceleration concept of:

***Software Defined Monitoring***

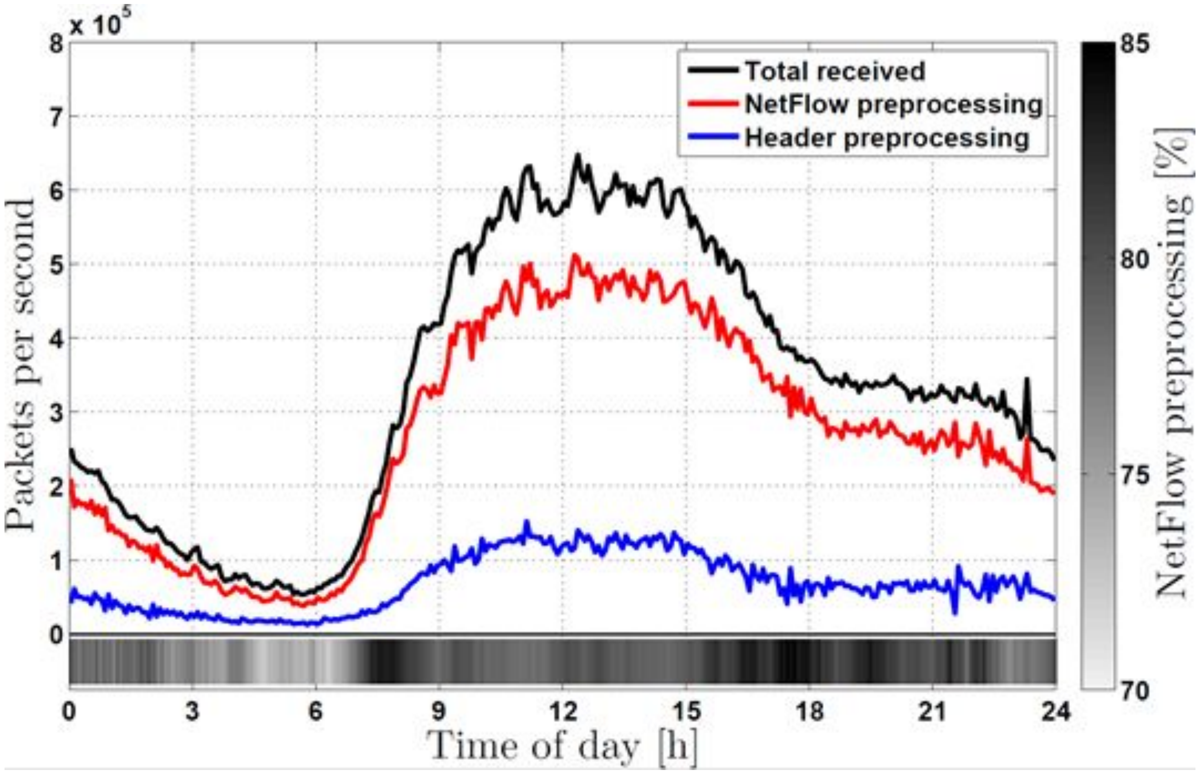
# SDM concept

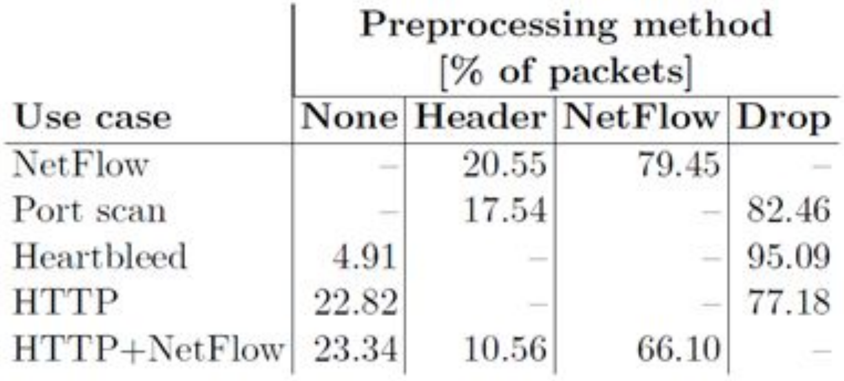

Firmware
Software
Rules
SDM Controller
Preprocessing Requests
Flow Cache
Actions
Rule Lookup
UHs
Parser
Packets
Data Bus
DMA Buffers
App 1
...
App N
Flow Exporter
IPFIX

# Heavy-tailed character

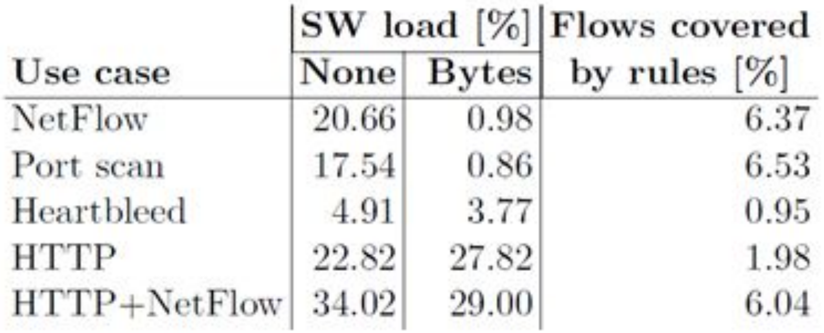


# SDM results





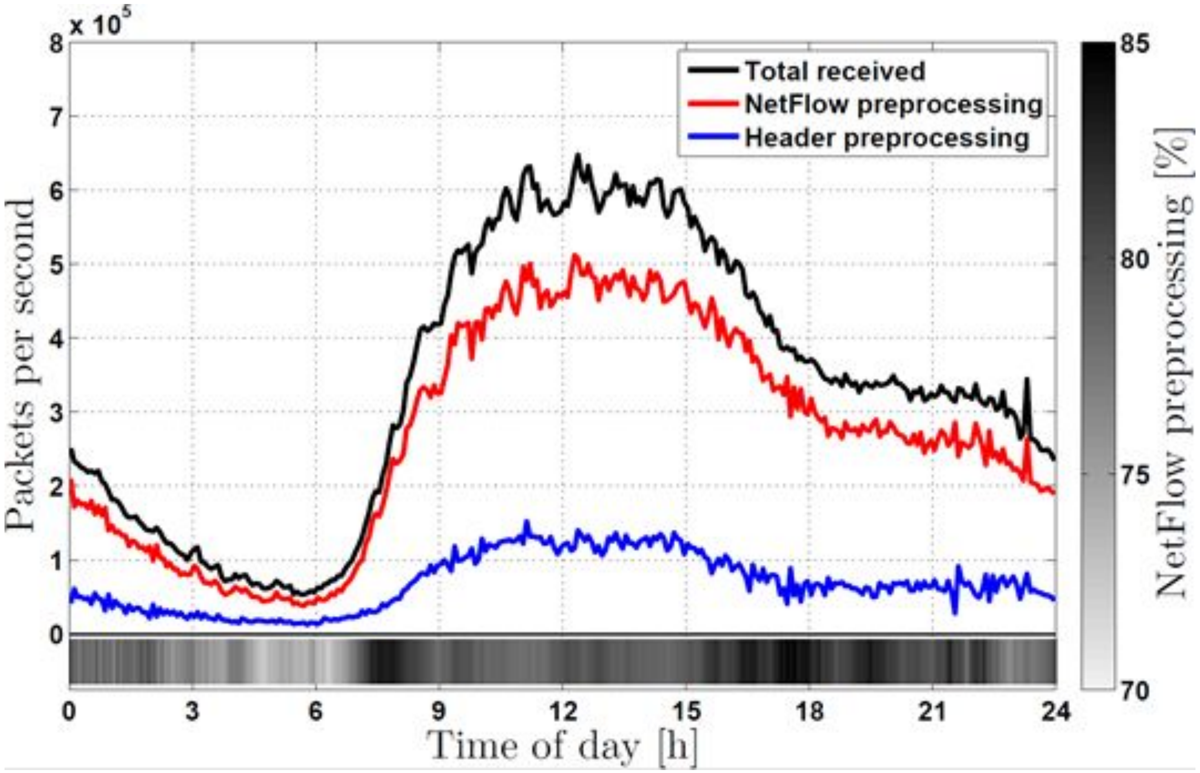
|  | Preprocessing method [% of packets] |  |  |  |
|---|---|---|---|---|
| Use case | None | Header | NetFlow | Drop |
| NetFlow | – | 20.55 | 79.45 | – |
| Port scan | – | 17.54 | – | 82.46 |
| Heartbleed | 4.91 | – | – | 95.09 |
| HTTP | 22.82 | – | – | 77.18 |
| HTTP+NetFlow | 23.34 | 10.56 | 66.10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

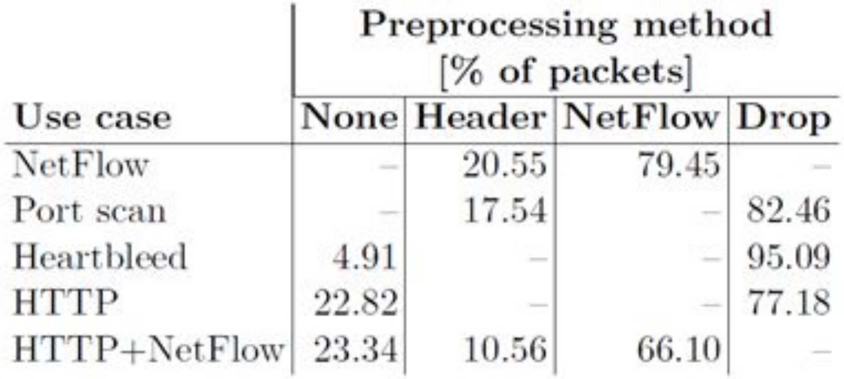


|  | SW load [%] |  | Flows covered |
|---|---|---|---|
| Use case | None | Bytes | by rules [%] |
| NetFlow | 20.66 | 0.98 | 6.37 |
| Port scan | 17.54 | 0.86 | 6.53 |
| Heartbleed | 4.91 | 3.77 | 0.95 |
| HTTP | 22.82 | 27.82 | 1.98 |
| HTTP+NetFlow | 34.02 | 29.00 | 6.04 |

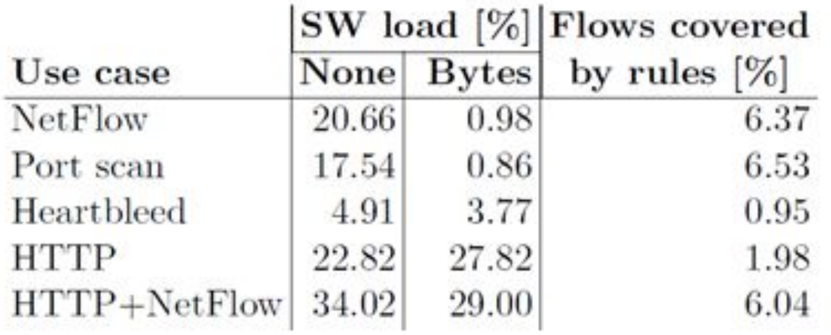
- various monitoring tasks can be accelerated
  - INFOCOM paper, IEEE ToC article

# 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 [%] | | Flows covered by rules [%] |
|---|---|---|---|
| | None | Bytes | |
| 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 |

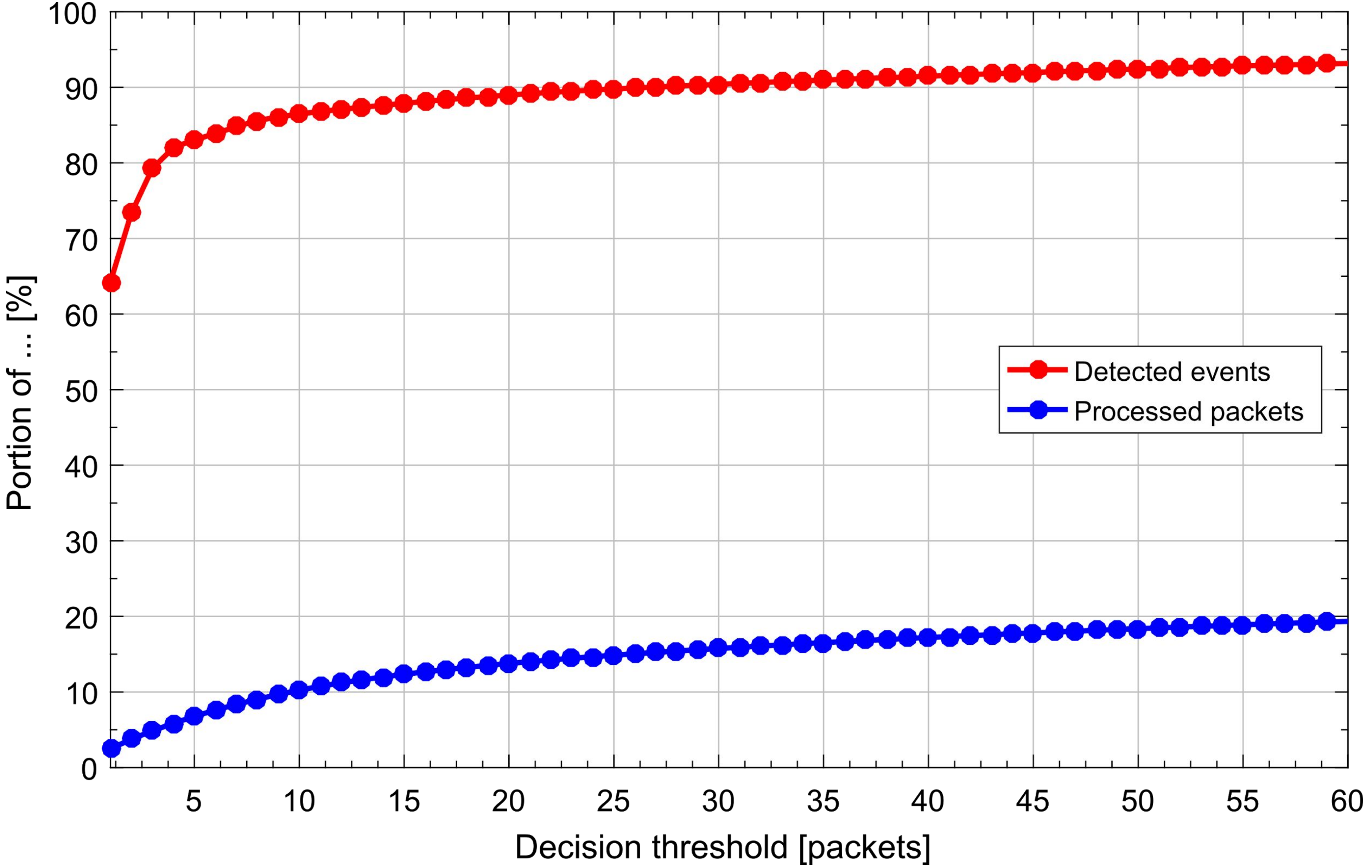
- various monitoring tasks can be accelerated
  - INFOCOM paper, IEEE ToC article

- **can SDM be used to accelerate IDS as well?**

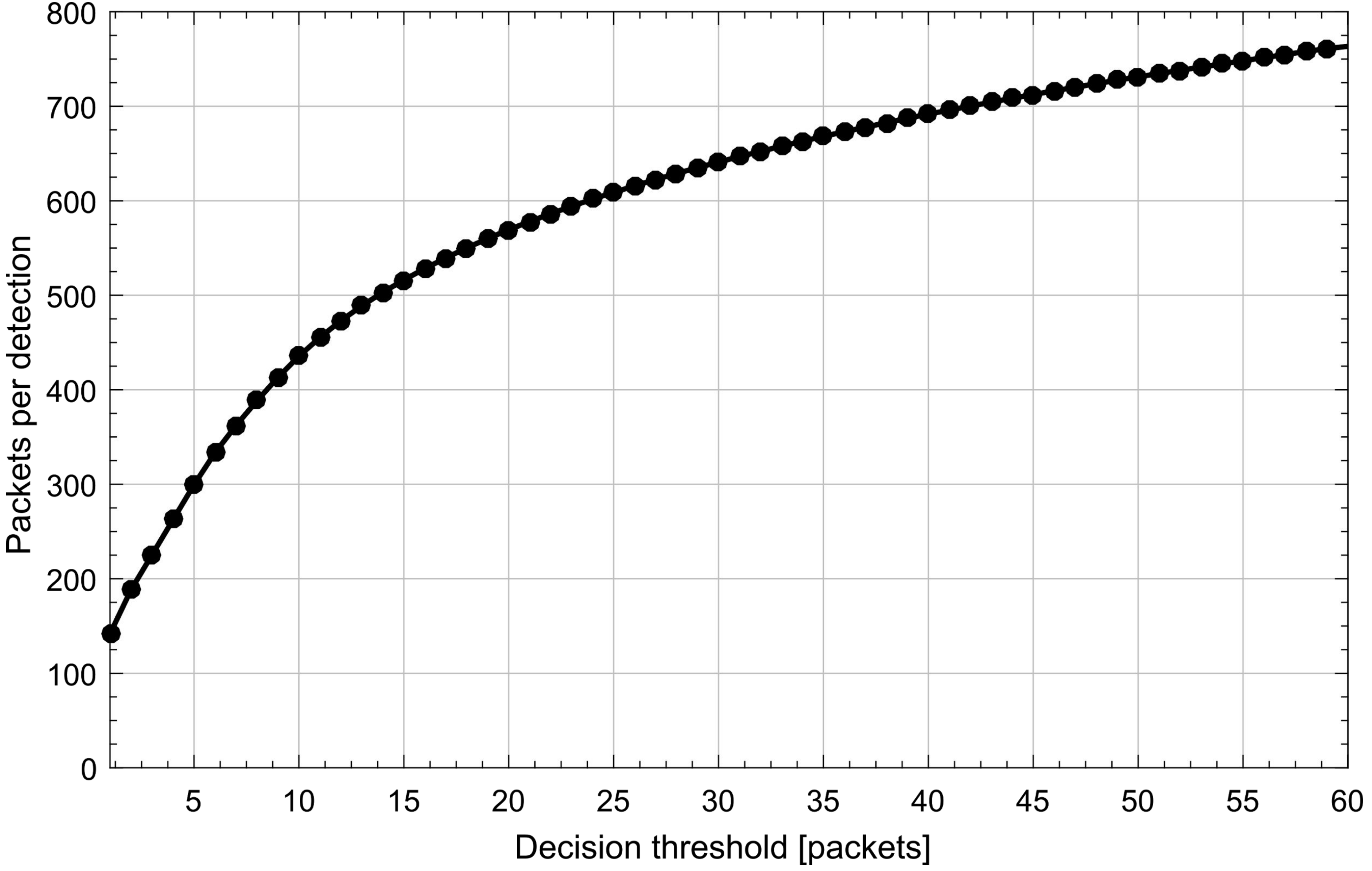
# Key assumptions

1. IDS is not fast enough to process 100 Gbps
2. blind packet discarding reduce detection rate
   - missing packets lead to overlooked threats
3. the most relevant are the initial packets of flows
   - these packets should be preferred in overloaded IDS
4. informed packet discarding is better than blind
   - packet rate is constant, processing more relevant data
5. several large flows carry the most of the traffic
   - acceleration of only the largest yields good speedup

# Effect of initial packets

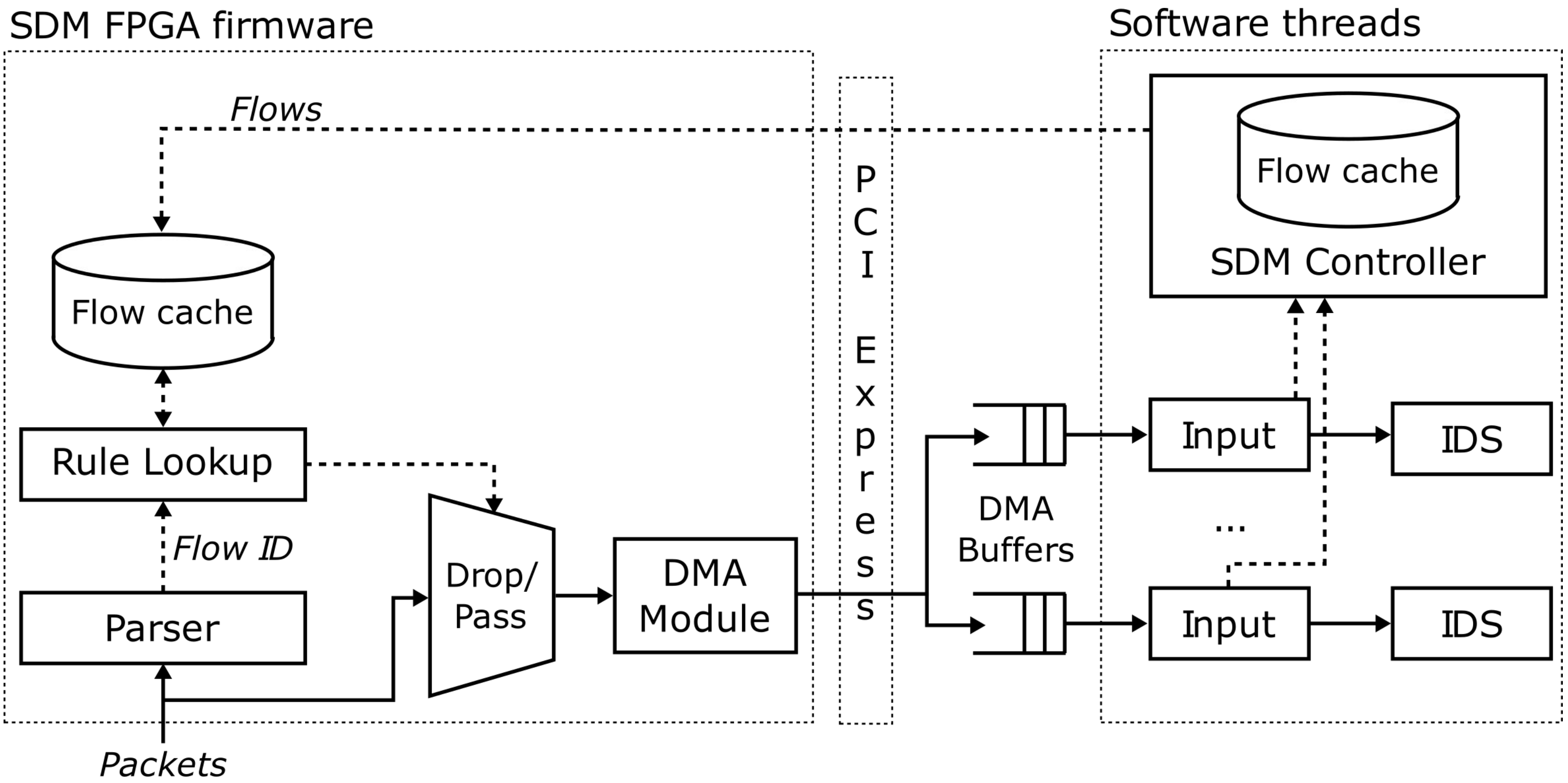


# Effect of initial packets

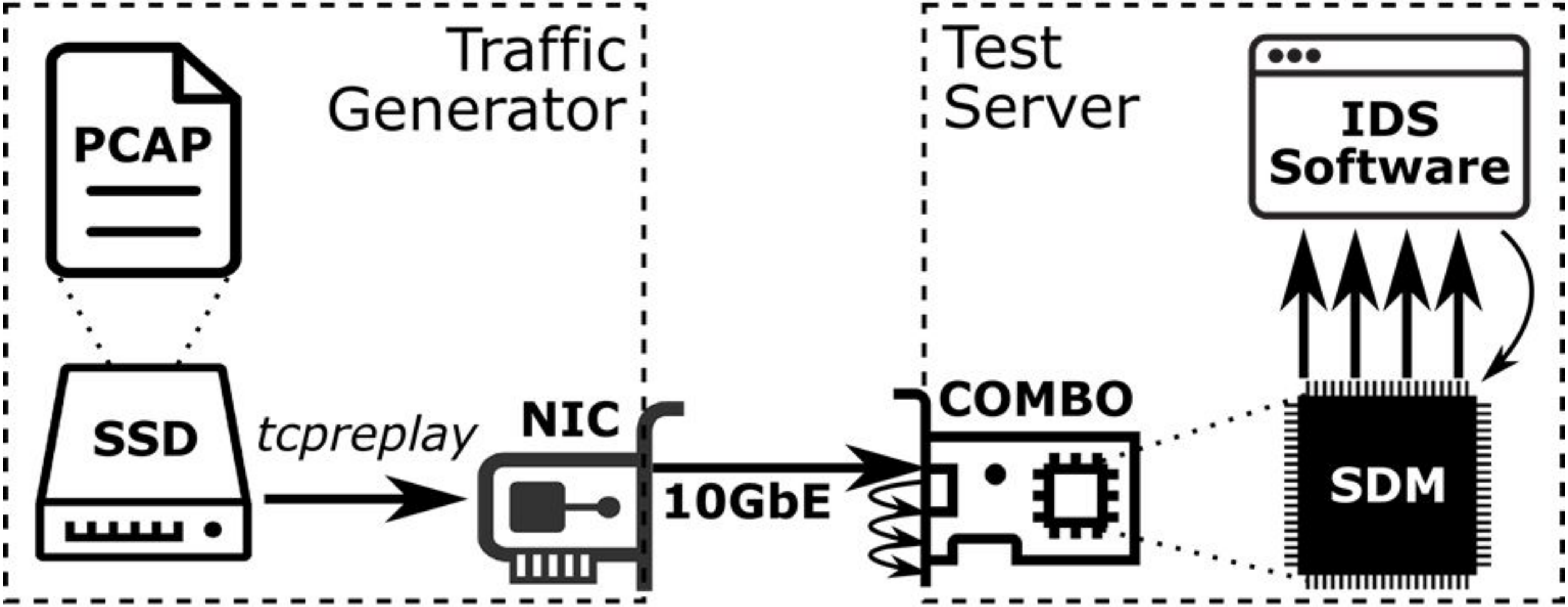


# Acceleration

- **without** - Suricata over standard NIC
- **SW accelerated** - SW discard over NIC
- **HW accelerated** - accelerated discard in NIC

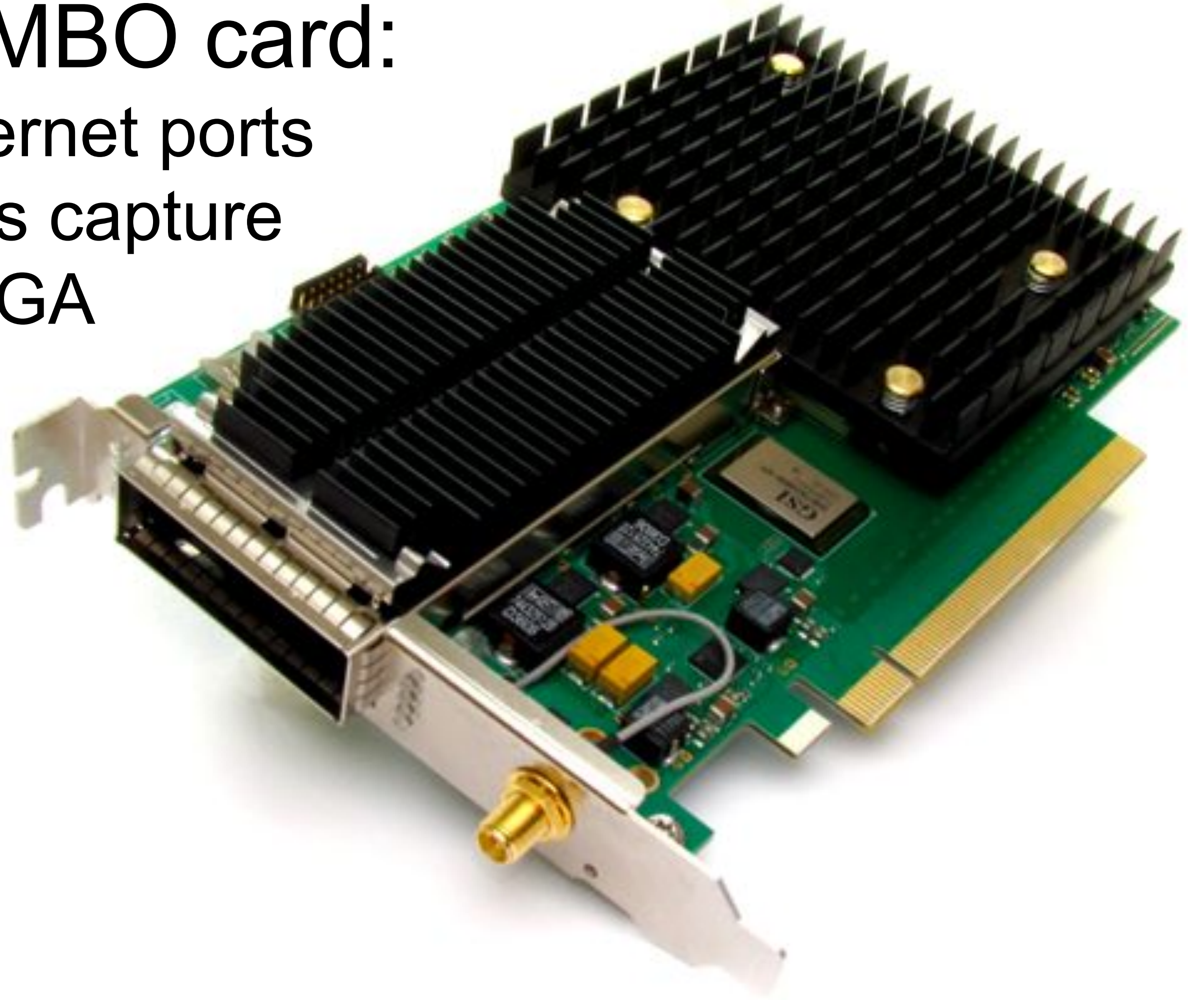


# Test setup


Traffic Generator
PCAP
SSD
tcpreplay
NIC
10GbE
Test Server
COMBO
IDS Software
SDM

# Test server

- Supermicro X9DRG-QF commodity server
- 2x Intel Xeon E5-2670 (8x 2.6GHz) CPU
- 64GB DDR3 operating memory
- acceleration COMBO card:
  - 10x 10 Gbps Ethernet ports
  - line rate 100 Gbps capture
  - Xilinx Virtex-7 FPGA
  - SDM firmware

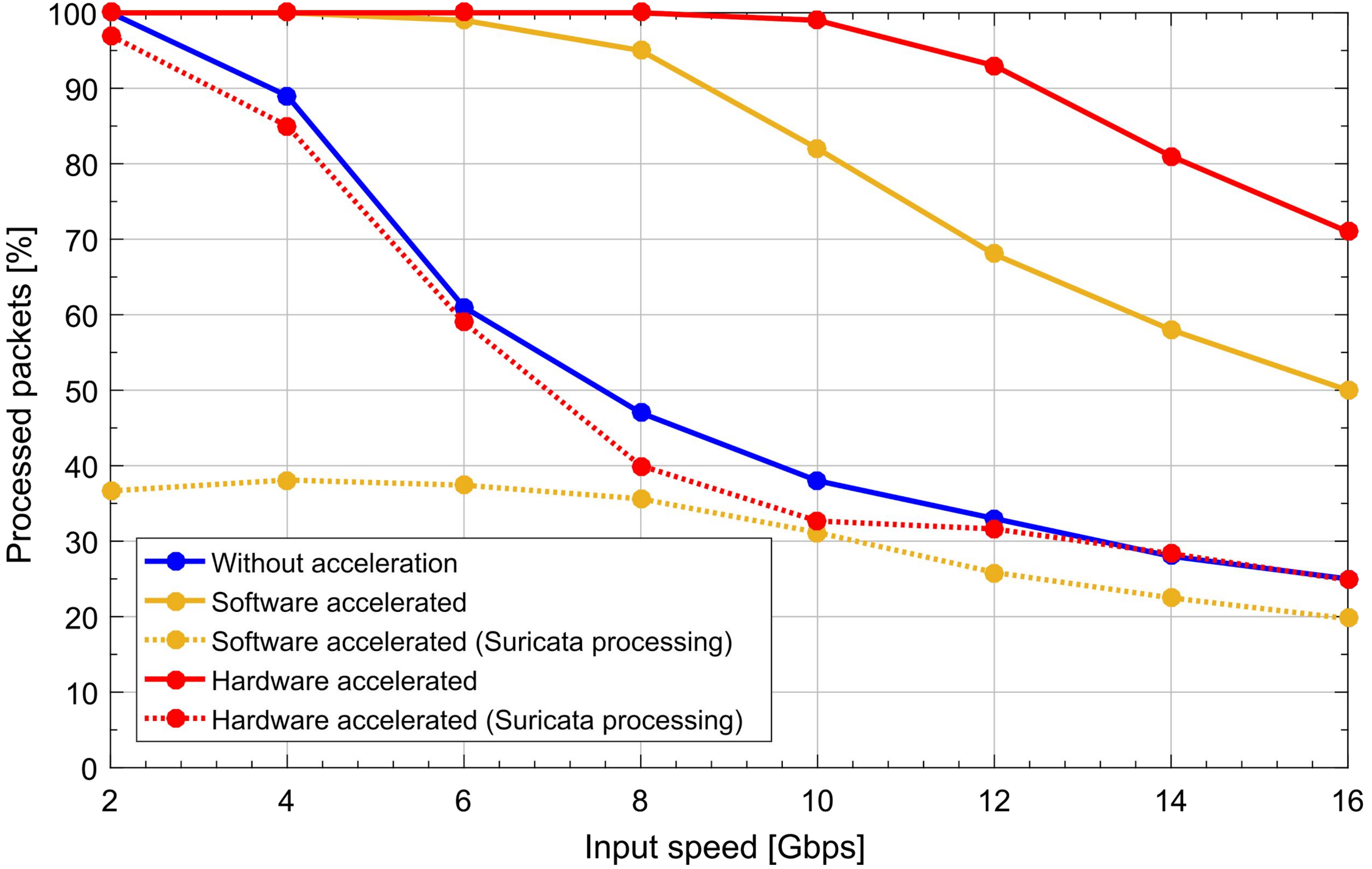


# Suricata IDS

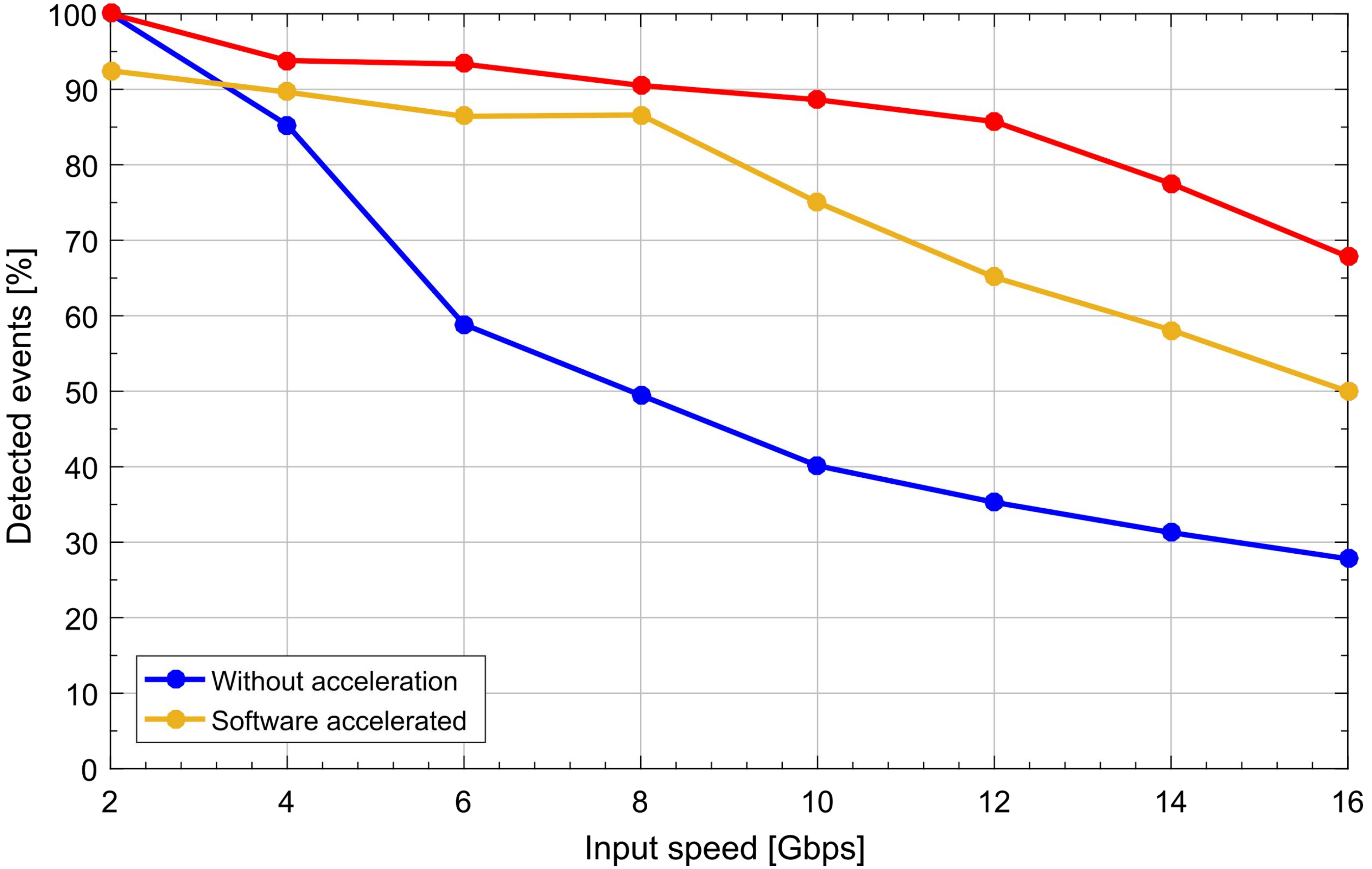
- high-performance intrusion detection system
- support of multi-threaded processing
- support of plugins to extend functionality
  - implementation of connection to SW/HW acceleration

- two tested rulesets:
  - **Full** - 13 642 rules from EmergingThreats database
  - **Malware** - selected subset of 967 rules

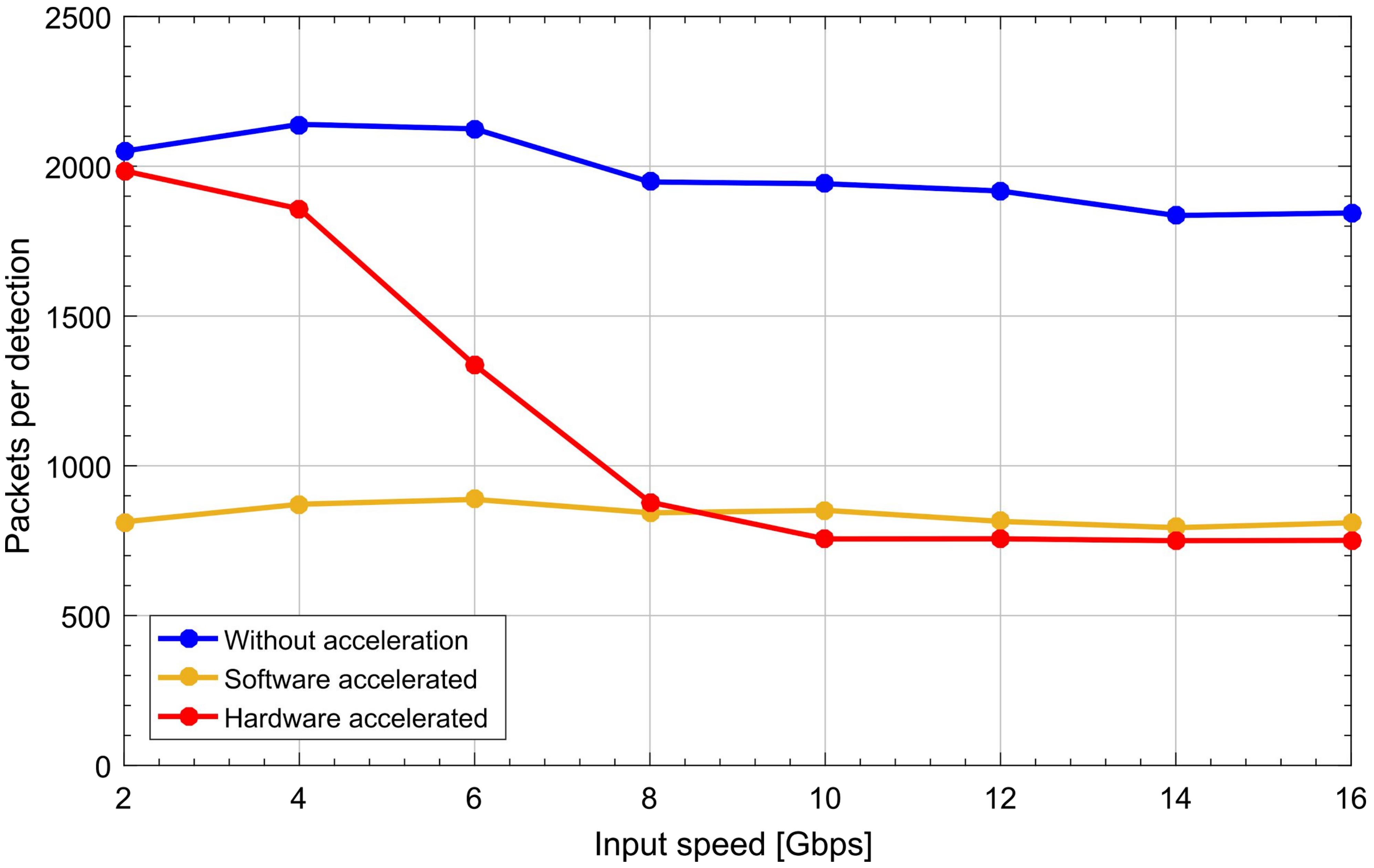
# Full (processing)



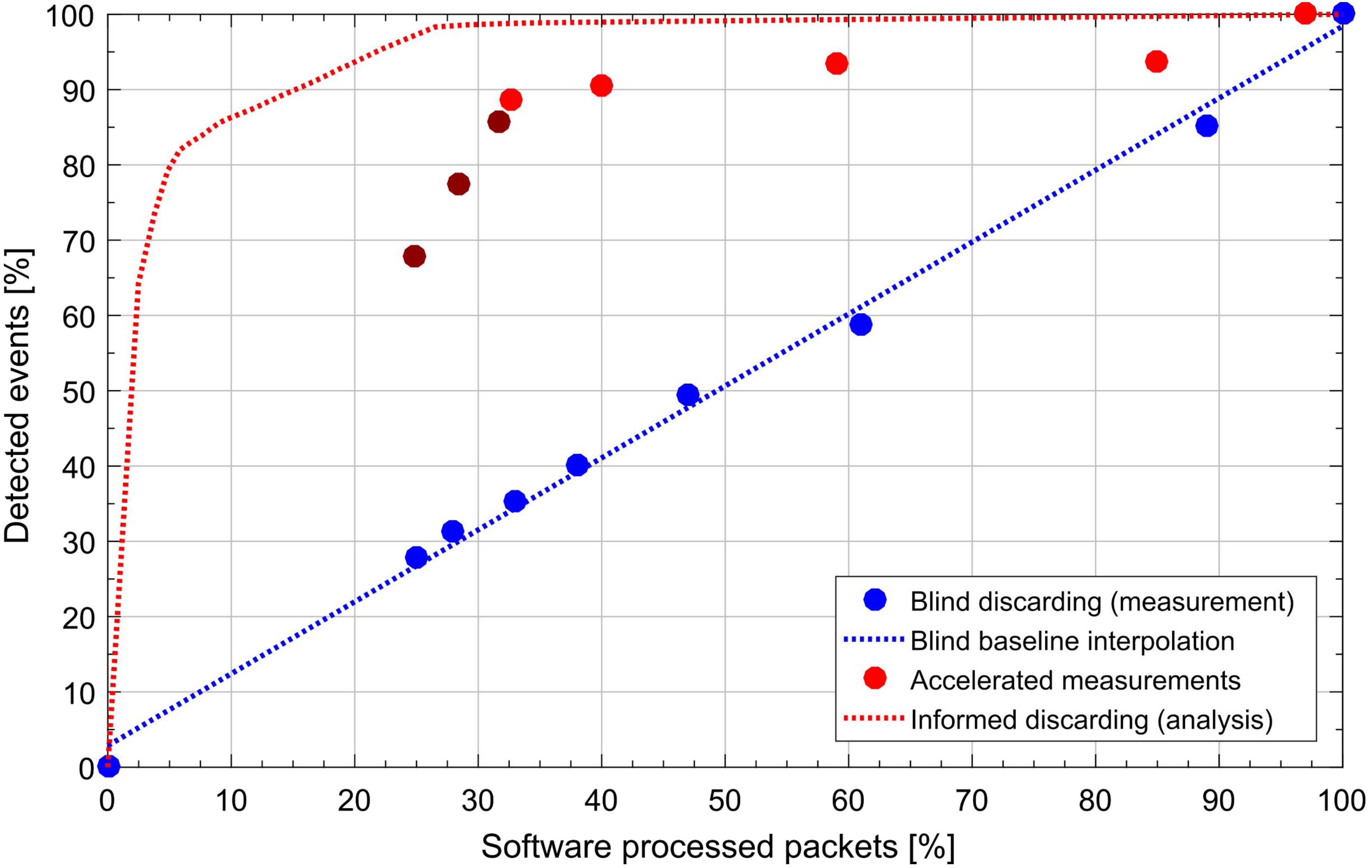
# Full (detections)



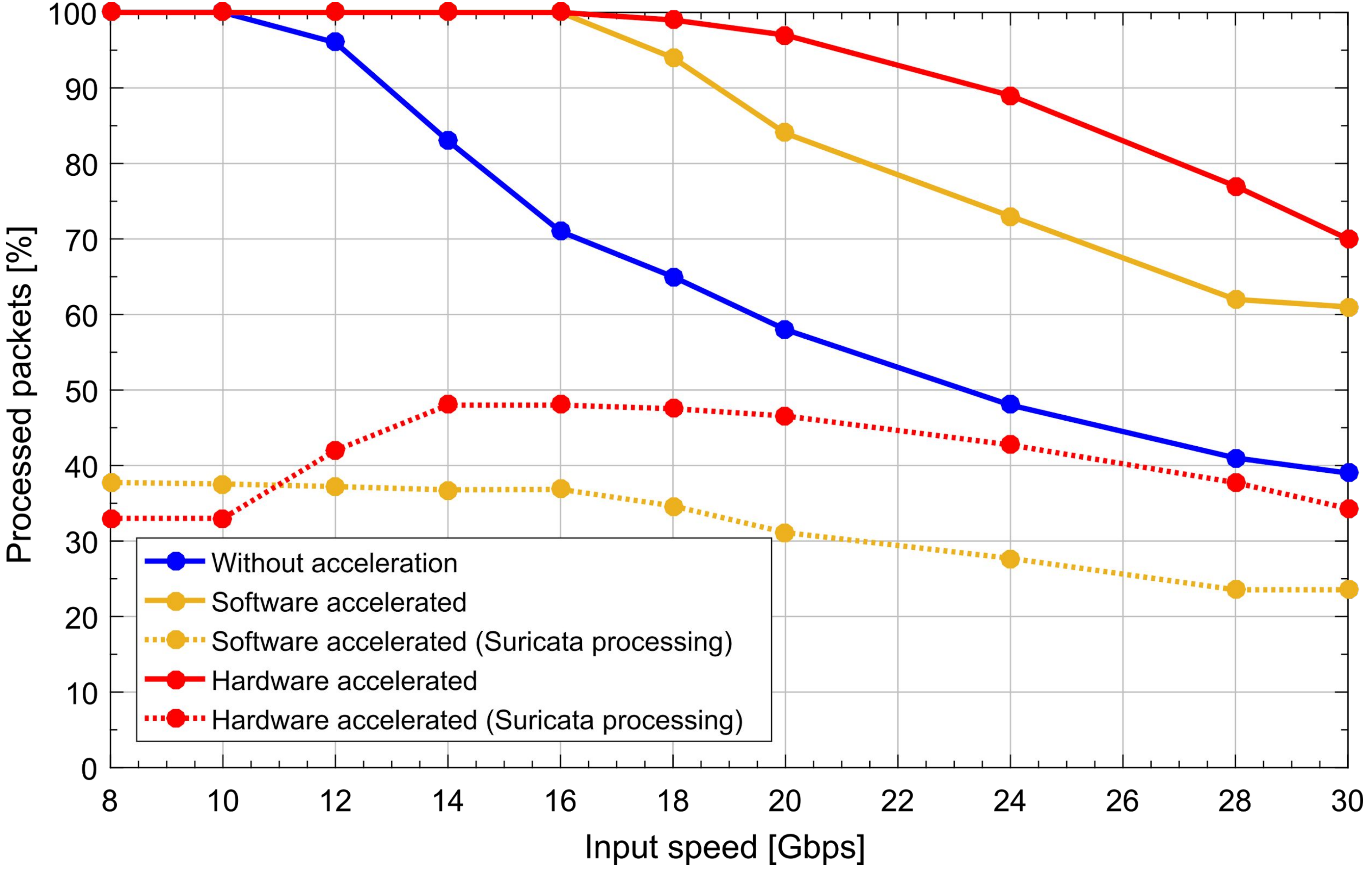
# Full (effectiveness)



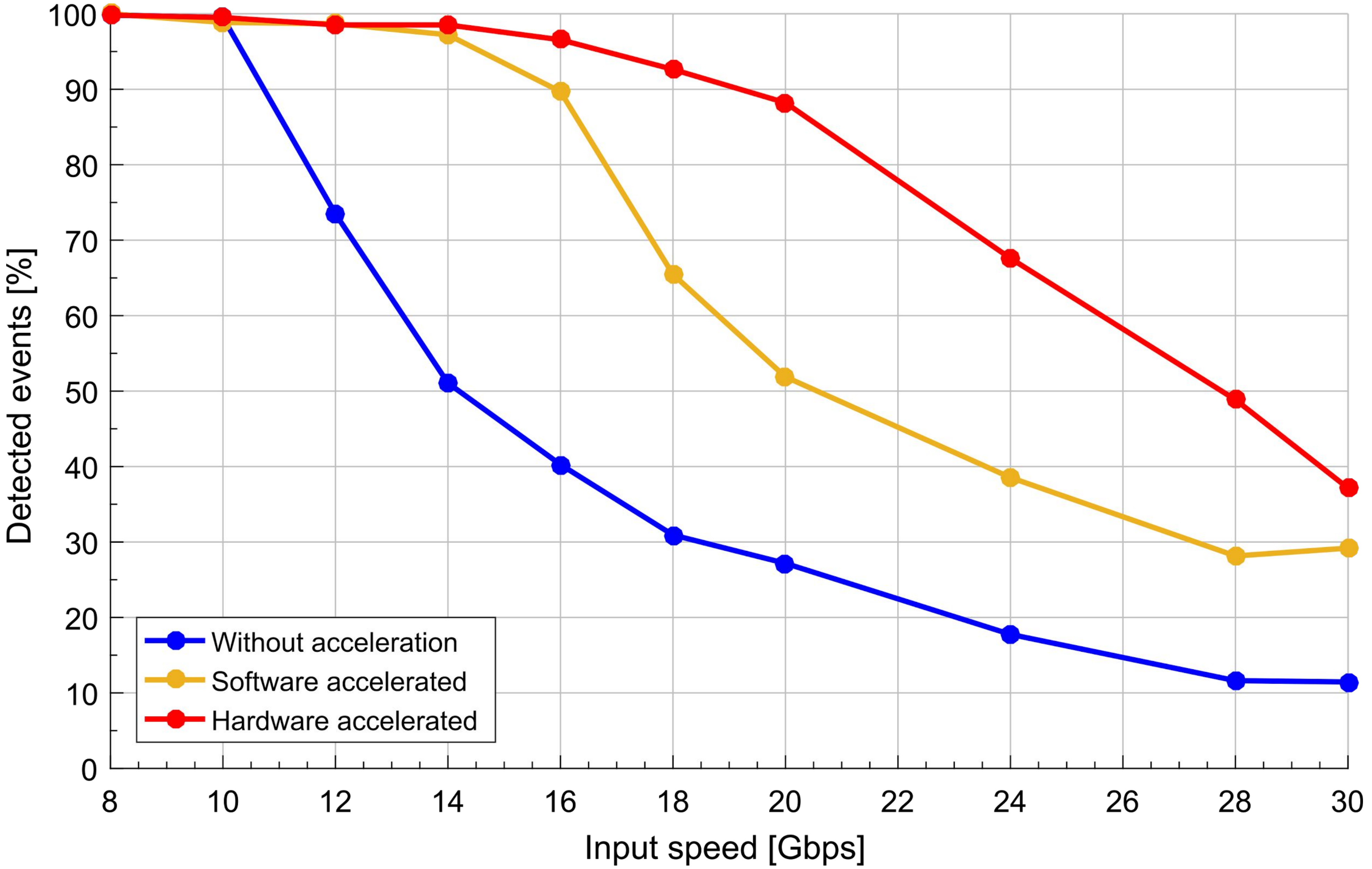
# Full (conclusion)



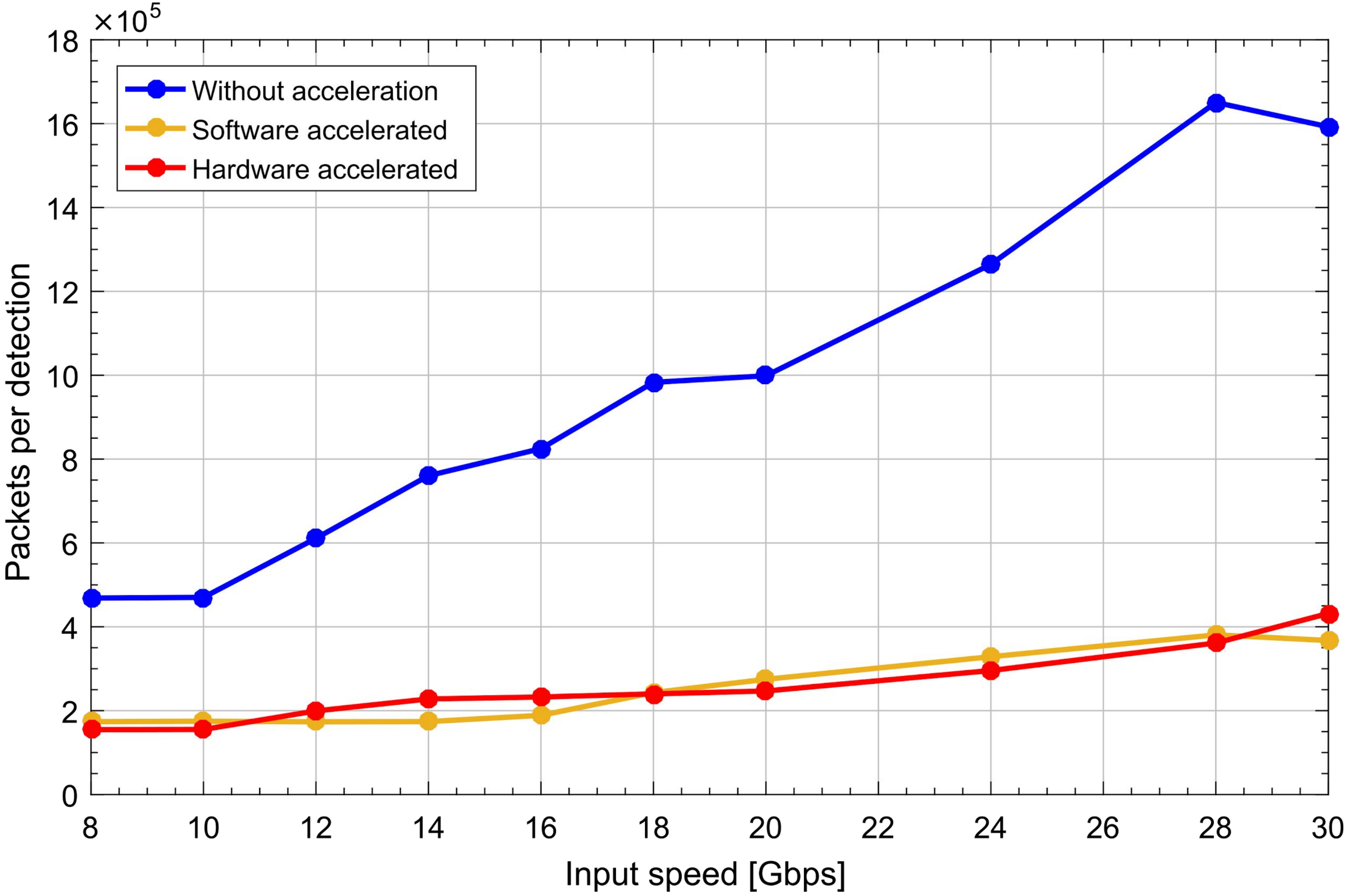
# Malware (processing)



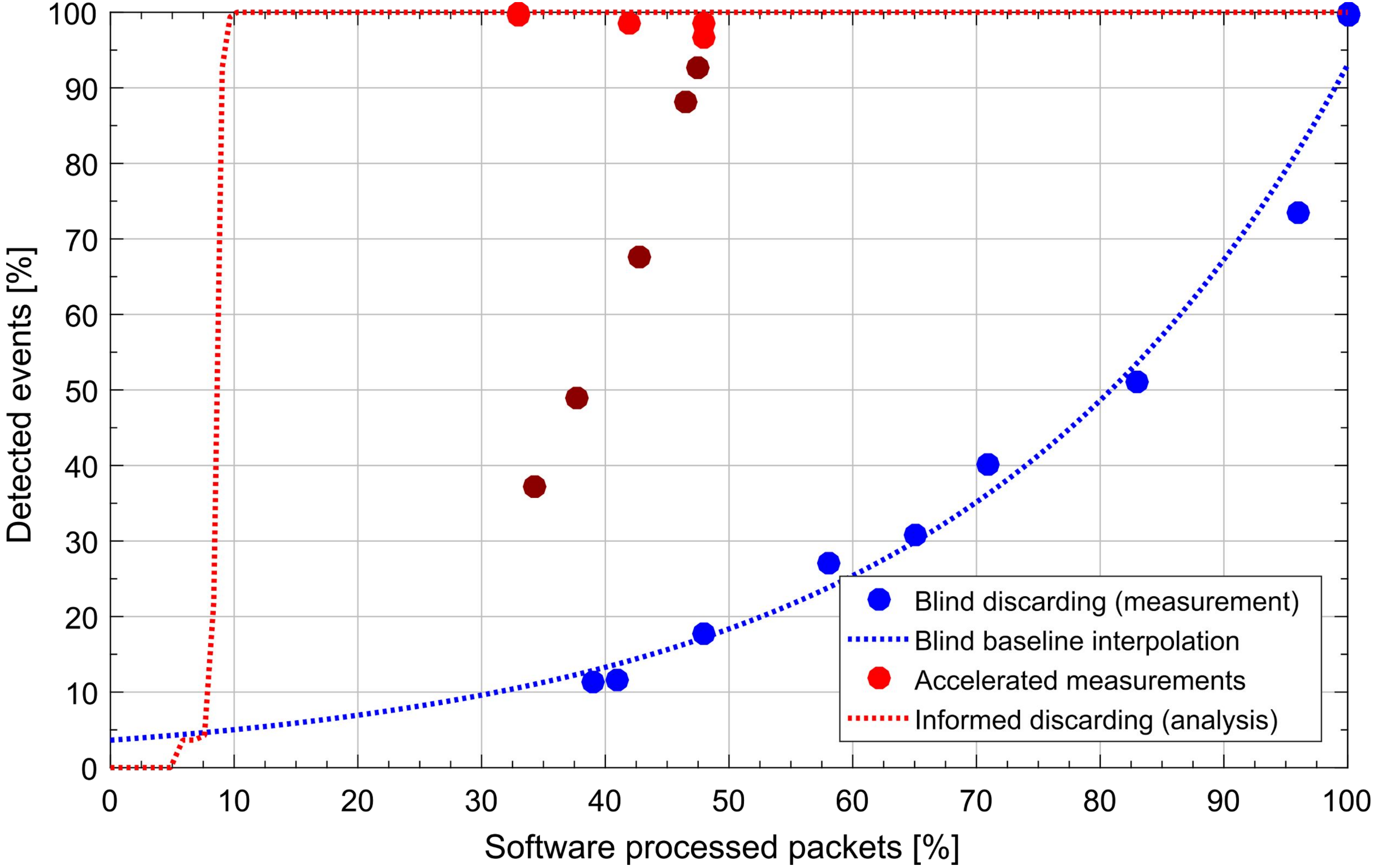
# Malware (detections)



# Malware (effectiveness)



# Malware (conclusion)



# Summary

- flow offload can notably accelerate IDS
- informed packet discarding is better than blind

- achieved **2x or 3x higher throughput** of IDS
- detecting **3x more events** when overloaded

# Thank you for your attention!

**More info:**

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