Hardware Acceleration of Network Security and Monitoring Applications

Lukáš Kekely supervised by Jan Kořenek
(ikekely, korenek@fit.vutbr.cz)
Faculty of Information Technology, Brno University of Technology

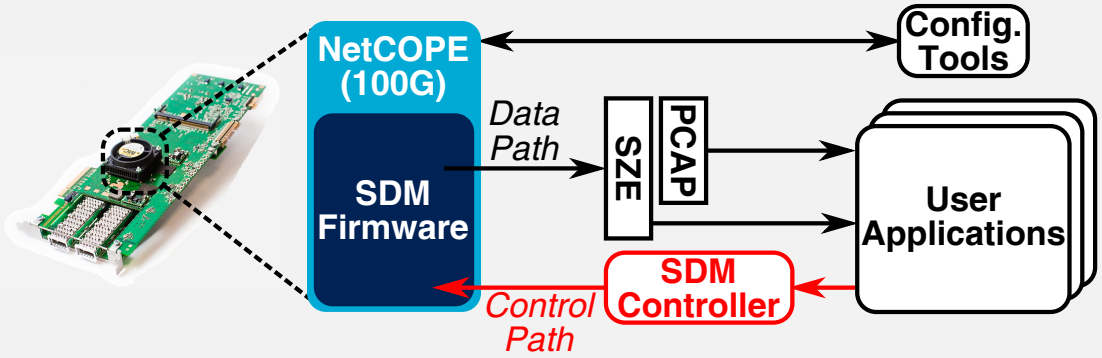
Motivation

- Rapid network bandwidth increase - ***high throughtput*** is imperative.
- Evolving nature of protocol usage and security threats - ***flexibility*** is needed.
- Insufficient ***application protocol support*** in existing monitoring devices.

⇒ *Enable flexible application protocol analysis on high-speeds!*

Designed System

- Acceleration of massively used operations - filtering and agregation.
  - Hardware accelerated, software ***controlled reduction of traffic***.
- Hardware and software are tightly coupled together for maximal efficiency.
- Brand new novel paradigm created: ***Software Defined Monitoring***.



- ***The Performance*** - ***hardware*** performs basic monitoring of uninteresting/ bulk traffic with throughtput sufficient for 100 Gbps networks.
- ***The Controller*** - ***software*** directly controlls acceleration of traffic processing.
- ***The Intelligence*** - ***applications*** perform advanced user specific tasks.
  - Application protocol (Layer 7) parsing and deeper packet inspection.
  - Detailed analysis of suspicious and anomalous traffic for threat detection.

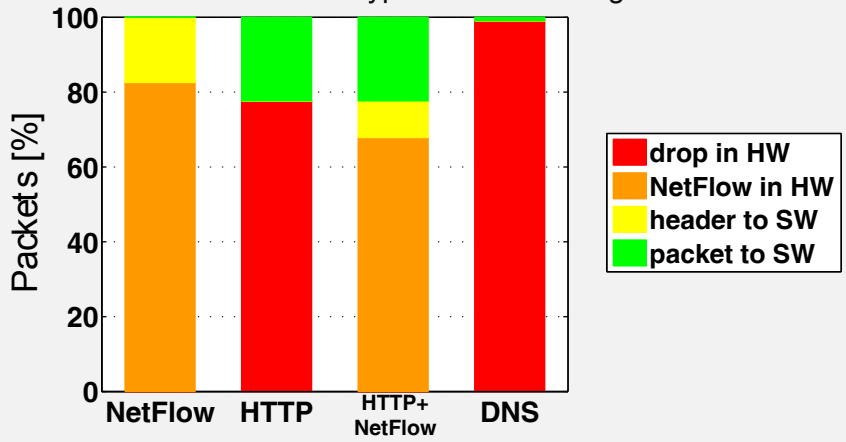
⇒ *User applications can adjust acceleration of traffic processing on fly!*

Principle of Functionality

- Packets from new (unknown) flows are send directly to software.
- User applications decide the traffic type and its accelerated preprocessing:
  - ***Interesting*** => send whole packets (with payload) to software.
  - ***Bulk*** => perform NetFlow in hadrware or send only headers to software.
  - ***Uninteresting*** => drop packets in hardware.

Results

- Results ***measured on real traffic*** from Cesnet high-speed backbone network.
- Achieved application load reduction for various use-cases using SDM system:
  - Standard ***NetFlow*** measurement: reduced to ***17% packets***, ***1% bytes***.
  - Analysis of ***HTTP*** headers: reduced to ***22% packets***, ***17% bytes***.
  - ***HTTP + NetFlow***: reduced to ***32% packets***, ***27% bytes***.
  - Security analysis of ***DNS***: reduced to ***1% packets***, ***0.2% bytes***.
- Usage of hardware acceleration types on incomming traffic:



Contributions and Conclusions

- ***New SDM concept*** of flow based network monitoring acceleration:
  - Flow based network measurements with ***throughput of 100 Gbps***.
  - ***Easy deployment of new tasks*** without hardware modifications.
  - ***Acceleration of application level processing*** and deep packet inspection.

  ⇒*Enables high speed and high quality measurement of network traffic!*
- ***Results published*** on several national and international conferences:
  - ACM/IEEE symposium ***ANCS12***
  - CZ.NIC conference ***IT12***
  - competition ***Student EEICT13***
  - TERENA conference ***TNC13***
  - 87th IETF meeting - ***NMRG Workshop***
- Is ***going to be deployed*** all over the Czech Republic in Cesnet backbone network.