Balancing between Power Efficiency and High Performance on Software-based Intrusion Detection Systems

Muhammad Jamshed, Jaehyun Nam, Byungkwon Choi, Dongsu Han and KyoungSoo Park
Electrical Engineering Dept., KAIST, {ajamshed, namjh, cbkbrad}@kaist.ac.kr, {dongsuh, kyoungsoo}@ee.kaist.ac.kr

Motivation

- **Fast growth of Internet traffic**
  - » 54.3 EB/Month (2013) → 117.8 EB/Month (2017) [Cisco VNI, 2013]
- **Various security threats**
  - » Targeted attacks, mobile vulnerabilities, spam, etc. [Symantec, 2013]
- **Problems in the state-of-the-art IDS appliances**
  - » High power consumption
  - » Inflexibility

Existing S/W-based IDS (Kargus, CCS '12)

- High performance
  - » ~ 33 Gbps
- Poor power efficiency
  - » ~ 900 W (2 CPUs + 2 GPUs)

Many-Core Processors (MCPs)

- **Highly-scalable general-purpose processors**
- **Low power consumption (~400 mW per core)**
- **Each core capable of running independent applications**

Objectives

- **Power-efficient, highly-scalable IDS**
  - » Main IDS engine on MCP
  - » Use host machine when MCP is under stress
  - » Opportunistically offload subtasks to host
- **Goal: High performance per power**

Key Insight

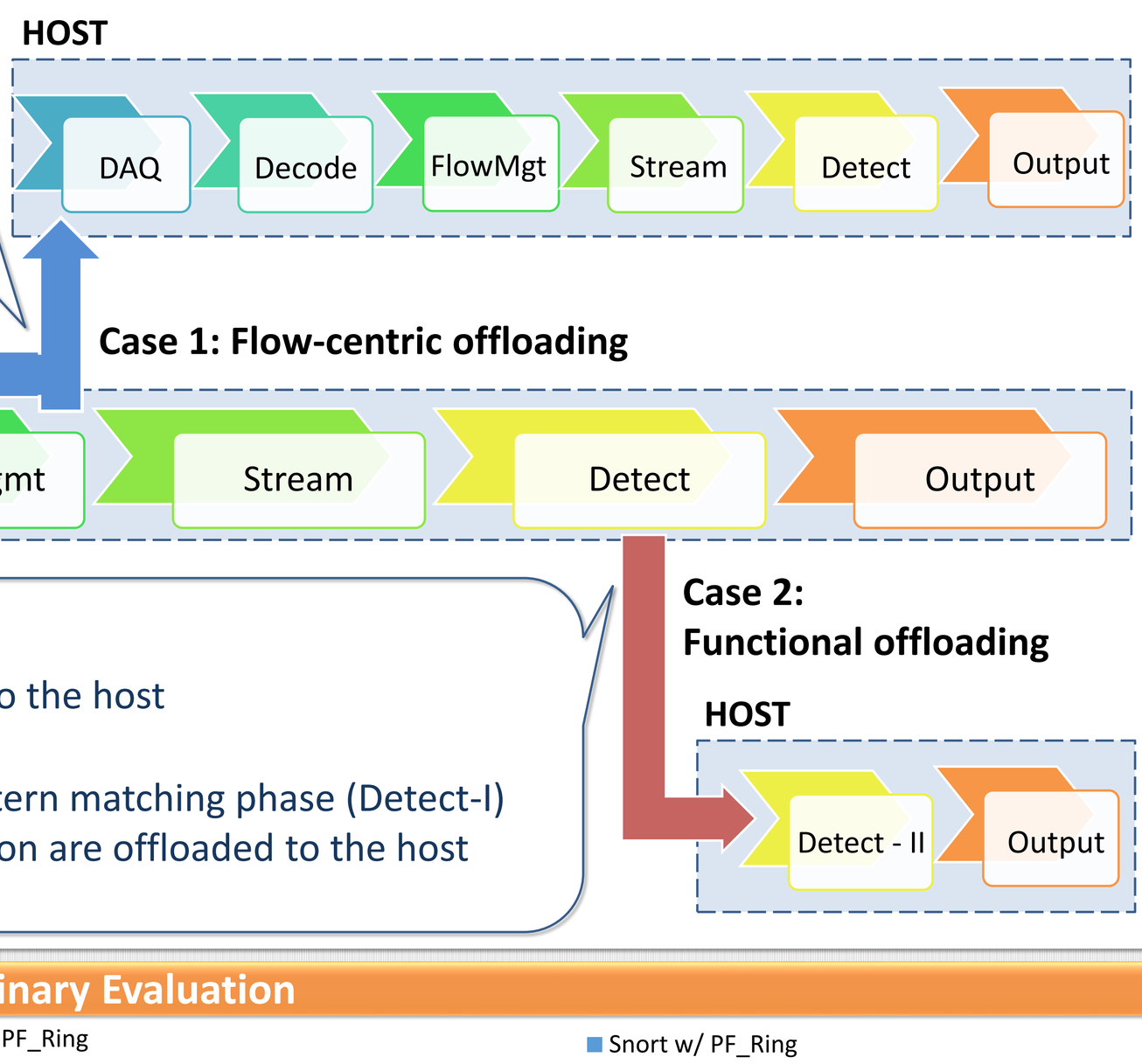
"Enforce dynamic IDS subtask offloading techniques while minimizing overall power usage"

Design

Flow-centric offloading

- Offloading Scheme
  - » Forward packets of new connections to the host
- Key Idea

  MCP continues managing the existing flows
  - » offload packets from Packet Rx module, or
  - » offload packets after flow management



Functional offloading

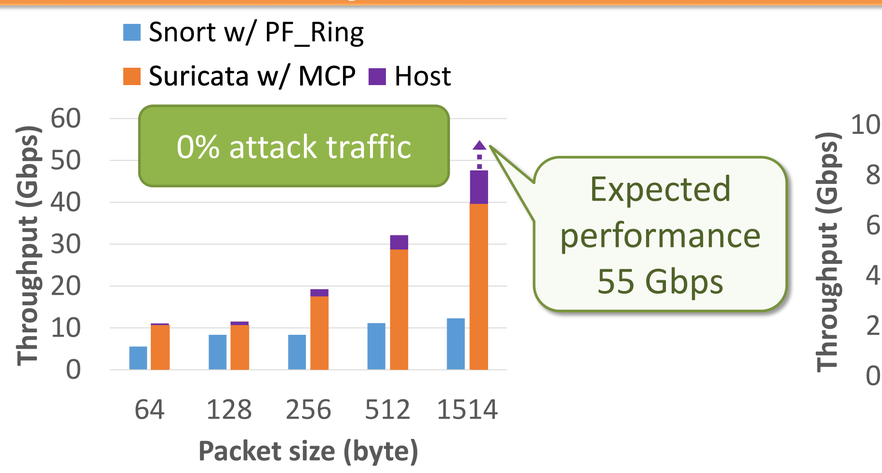
- Offloading Scheme
  - » Traffic that requires detailed analysis is forwarded to the host
- Key Idea
  - » Process incoming packets until the multi-string pattern matching phase (Detect-I)
  - » Suspected flows that pass the first phase of detection are offloaded to the host for further analysis (Detect-II)

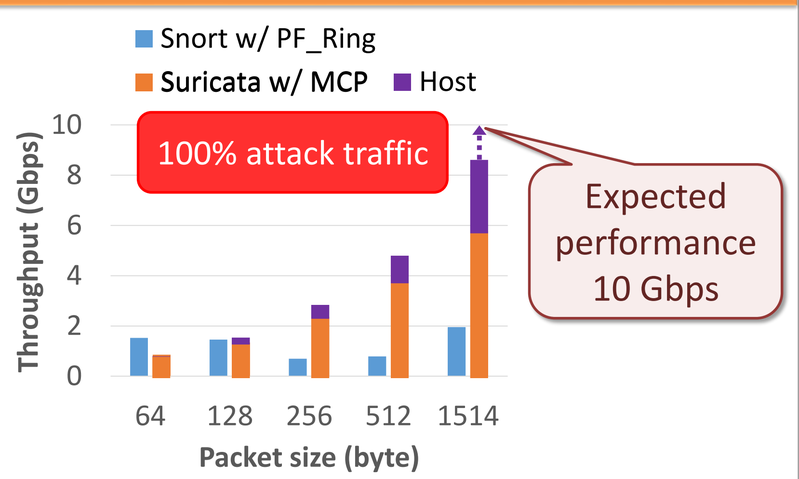
Preliminary Evaluation

- Experimental environment
  - » 50 Gbps transmission rate (synthetic traffic)
  - » Snort HTTP rules v2.9.2.1 (2433 rules)

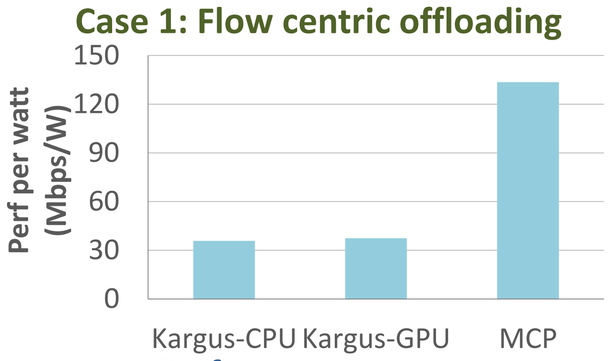
MCP: Tilera TILE-Gx72 (72 cores)	
Clock speed	1.0 GHz
Cache size	L1: 32KB/ L2: 256KB
Mem size	12 GB
IDS	Suricata

Host: Intel Xeon (8 cores)	
Clock speed	3.33 GHz
Cache size	L3: 12MB
Mem size	24 GB
IDS	Multi-threaded Snort





Case 1: Flow centric offloading



Case 2: Functional offloading

- Current Status
  - » Offloading statically
  - » Analyzing stress-specific parameters
- TODO
  - » Develop dynamic offloading schemes
  - » Optimize offloading techniques (e.g., zerocopy)