Network Technologies for Secure Data Movement

Emerging Topics on Packet Processing Acceleration

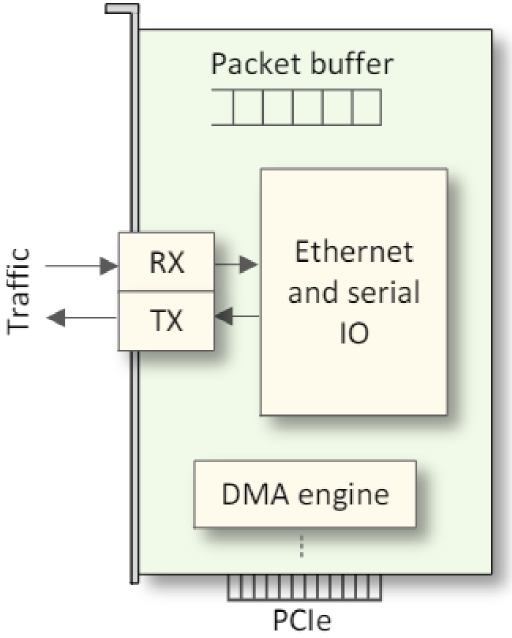
Elie Kfoury[1], Ali Mazloum[1], Jennifer Kim[2]
[1]University of South Carolina (USC)
[2]Internet2
https://research.cec.sc.edu/cyberinfra/

Boston, MA
December 9, 2024

Packet processing on Network Interface Cards (NICs)

Evolution of Network Interface Cards (NICs)

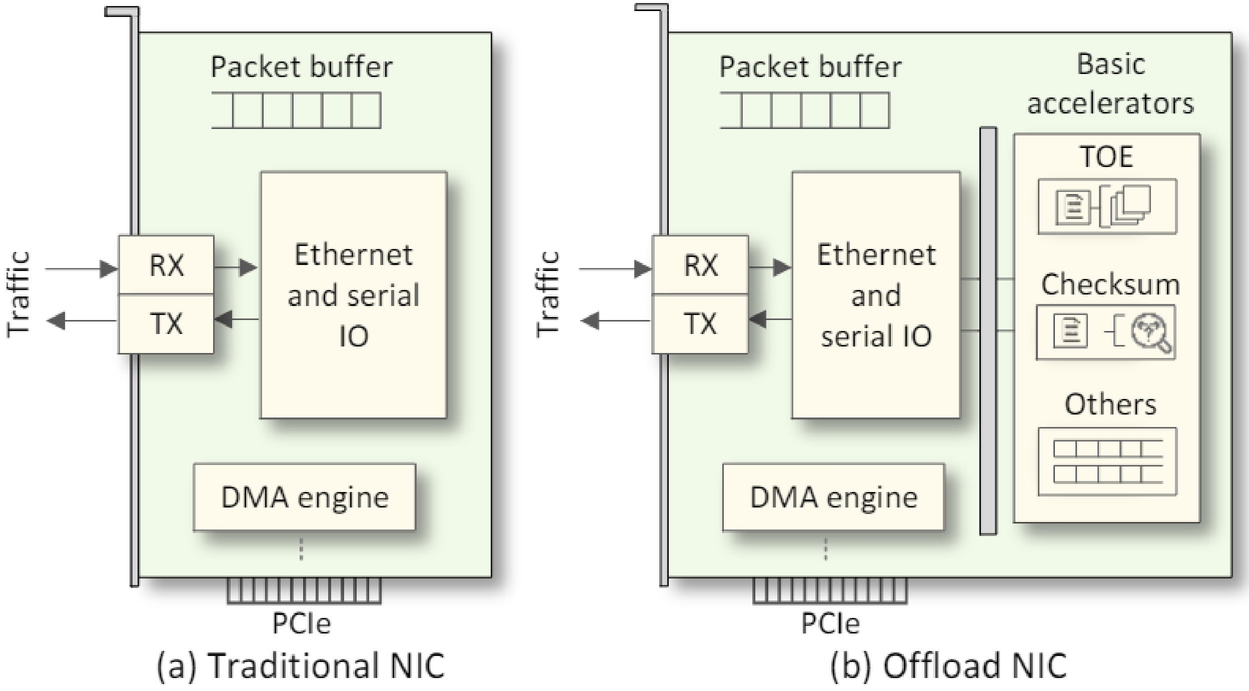
- Network Interface Cards (NICs) have evolved over the years
- Traditional NICs use fixed-function components to implement basic physical and data-link layer services



(a) Traditional NIC

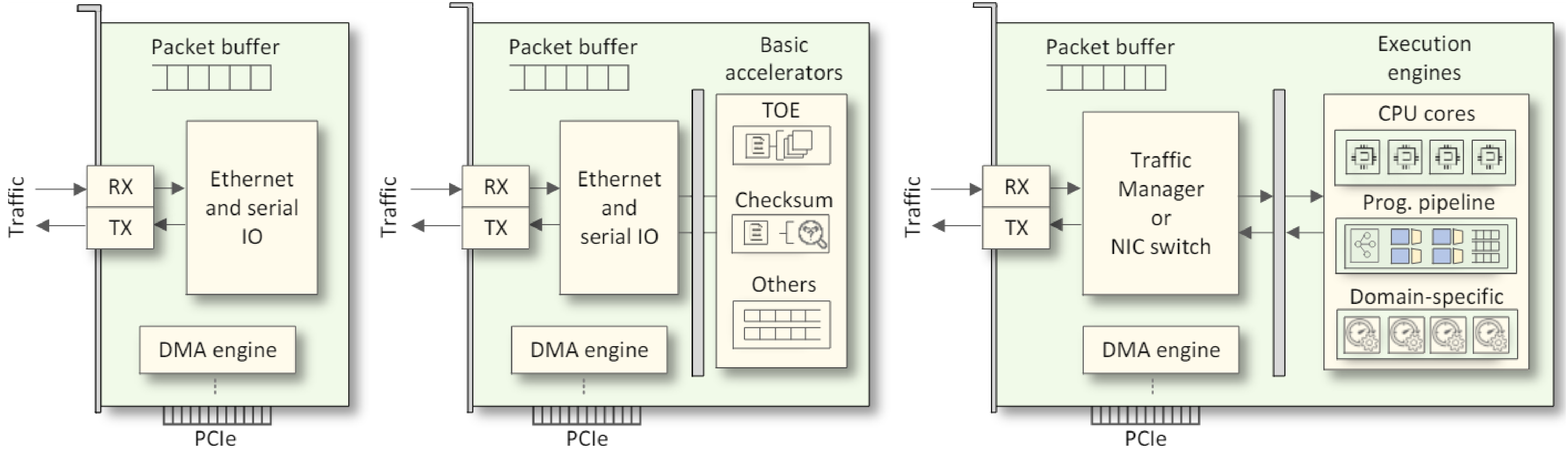
Evolution of Network Interface Cards (NICs)

- Network Interface Cards (NICs) have evolved over the years
- Traditional NICs use fixed-function components to implement basic physical and data-link layer services
- Offload NICs use fixed-function components to offload basic infrastructure functions
  - Computing IP checksums, encapsulating/de-encapsulating segments, etc.



Evolution of Network Interface Cards (NICs)

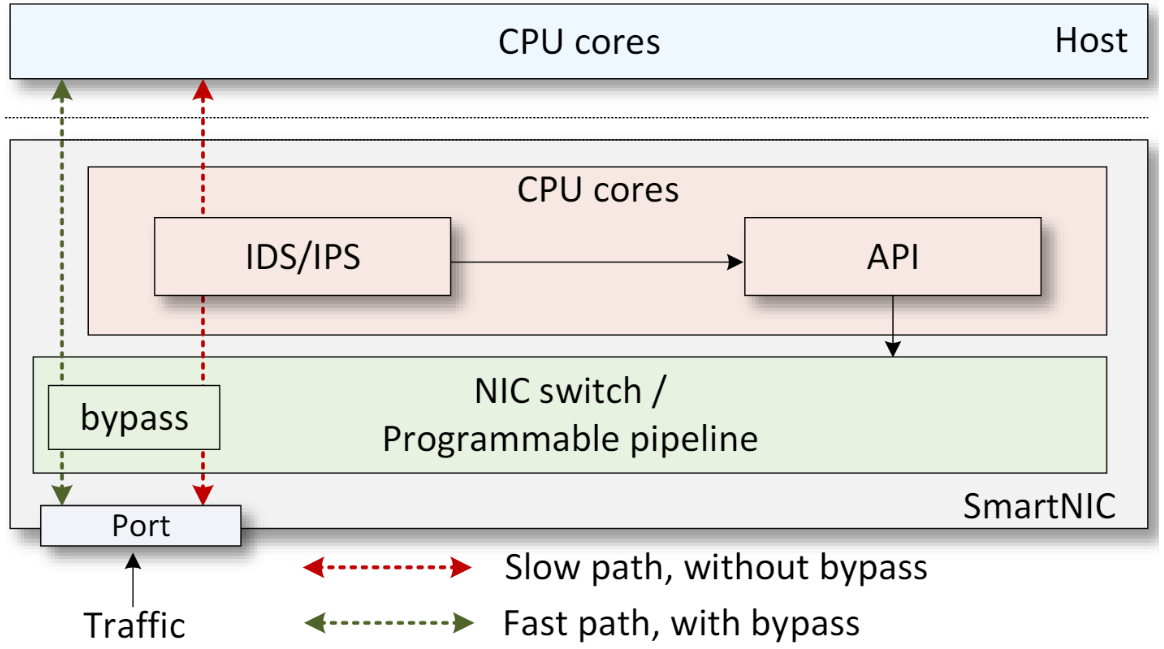
- SmartNICs use domain-specific processors to customize packet processing
  - Programmable packet processing pipeline, regular expression, encryption/decryption, etc.
- The domain-specific processors are typically ASIC or FPGA-based
- SmartNICs also include general-purpose CPU cores for managing the system



(a) Traditional NIC (b) Offload NIC (c) SmartNIC

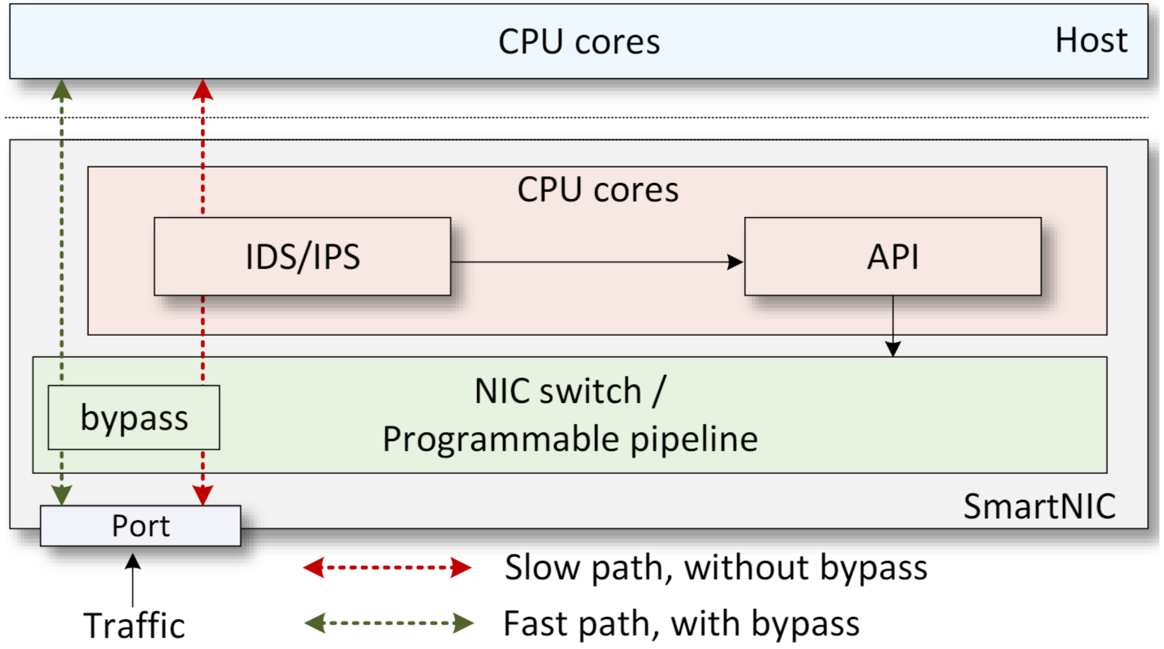
Accelerating IDS/IPS Functions

- Intrusion Detection/Prevention System (IDS/IPS) functions can be offloaded to the SmartNIC
  - ➢ Traffic bypass, Deep Packet Inspection (DPI), signature matching, etc.

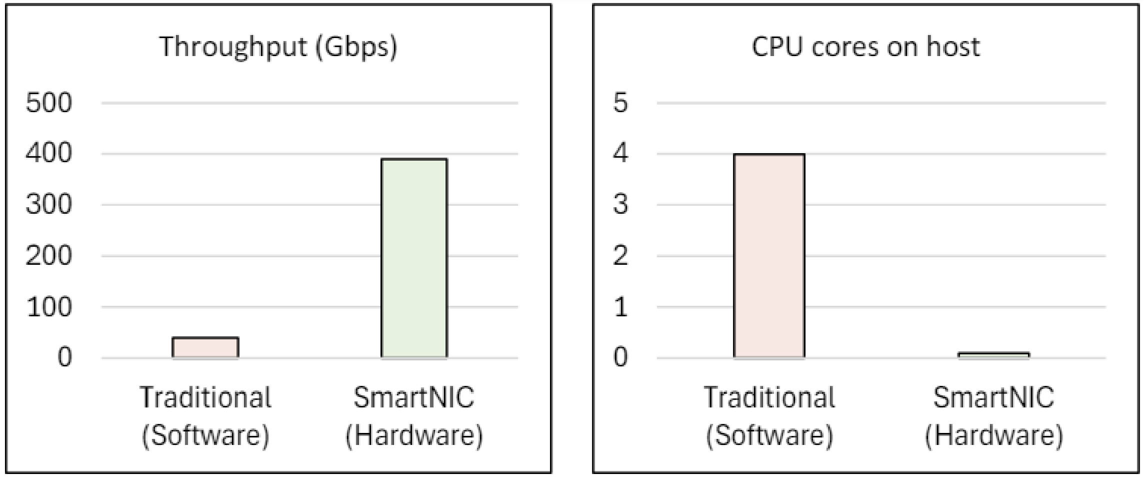


Accelerating IDS/IPS Functions

- Intrusion Detection/Prevention System (IDS/IPS) functions can be offloaded to the SmartNIC
  - ➢ Traffic bypass, Deep Packet Inspection (DPI), signature matching, etc.



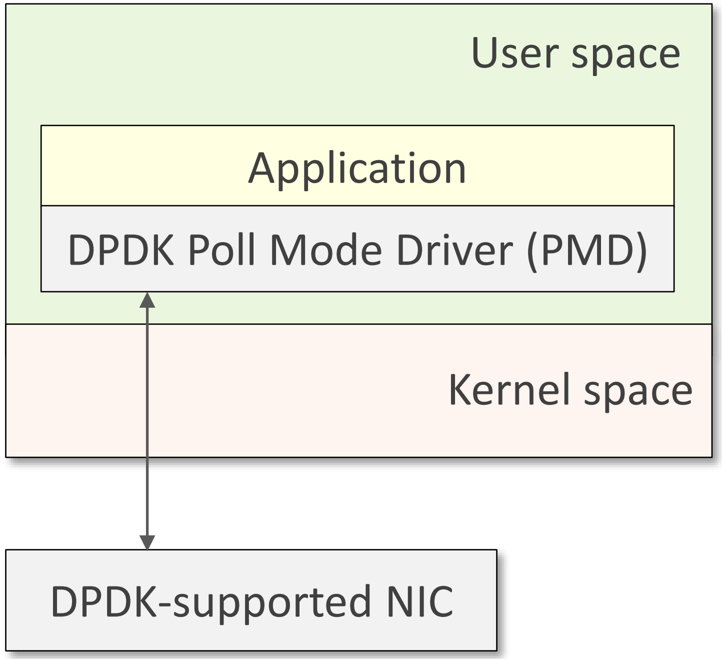
Suricata bypass function



Packet Processing on End-hosts

Data Plane Development Kit (DPDK)

- One approach to avoid the overhead is to bypass the kernel
- DPDK is a set of optimized libraries for processing packets in the user space
- DPDK bypasses the kernel
- DPDK uses Poll Mode Drivers (PMD) which constantly poll the NICs for new packets
- This avoids the overheads resulting from interrupts



P4-DPDK

- Programming using DPDK is not straightforward and presents barrier to entry
- P4 is a domain-specific language for packet processing
- P4 was originally designed for programmable data plane switches
- Recently, P4 has been used to program other packet processing datapaths

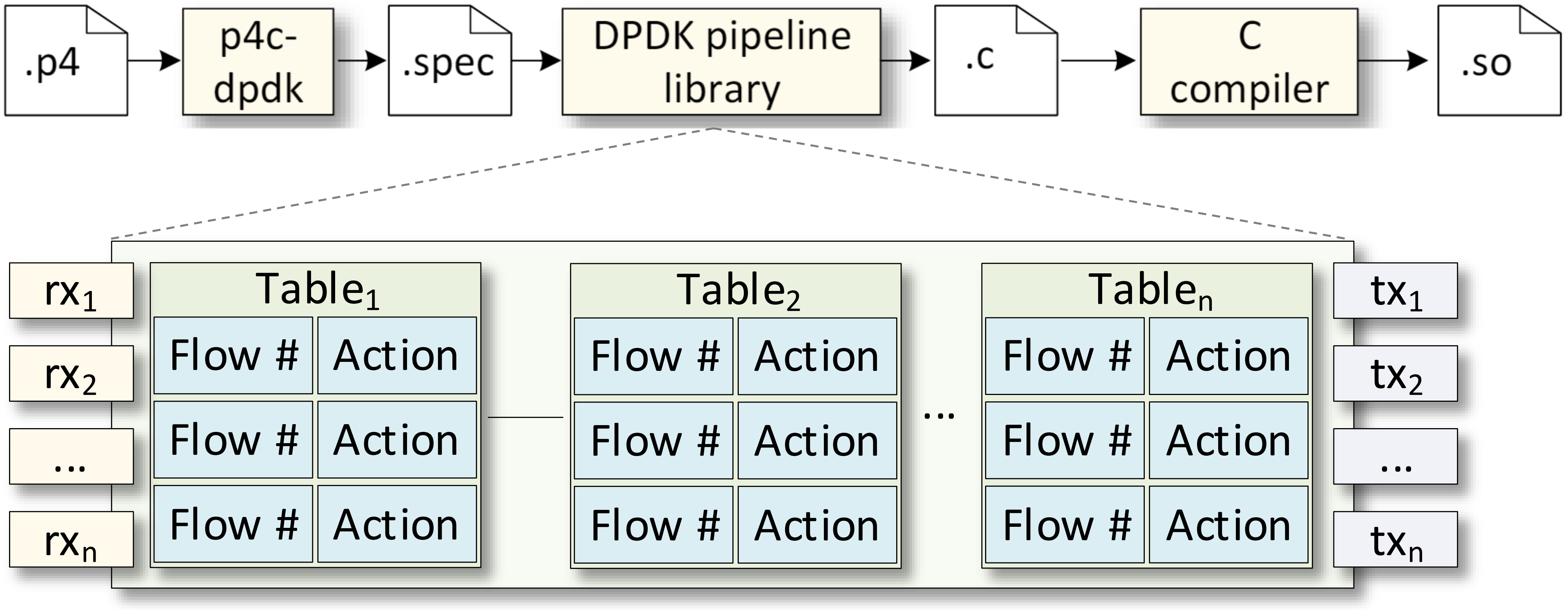
Lines of code (LOC) for implementing defenses against common cyberattacks[1]

Attack	DPDK	P4
DNS amplification	898	255
HTTP flood	1184	354
SlowLoris	995	513
UDP flood	911	376
Elephant flow (heavy hitter)	903	373

[1] Zhang, Menghao, et al. "Poseidon: Mitigating volumetric DDoS attacks with programmable switches." *NDSS, 2020.*

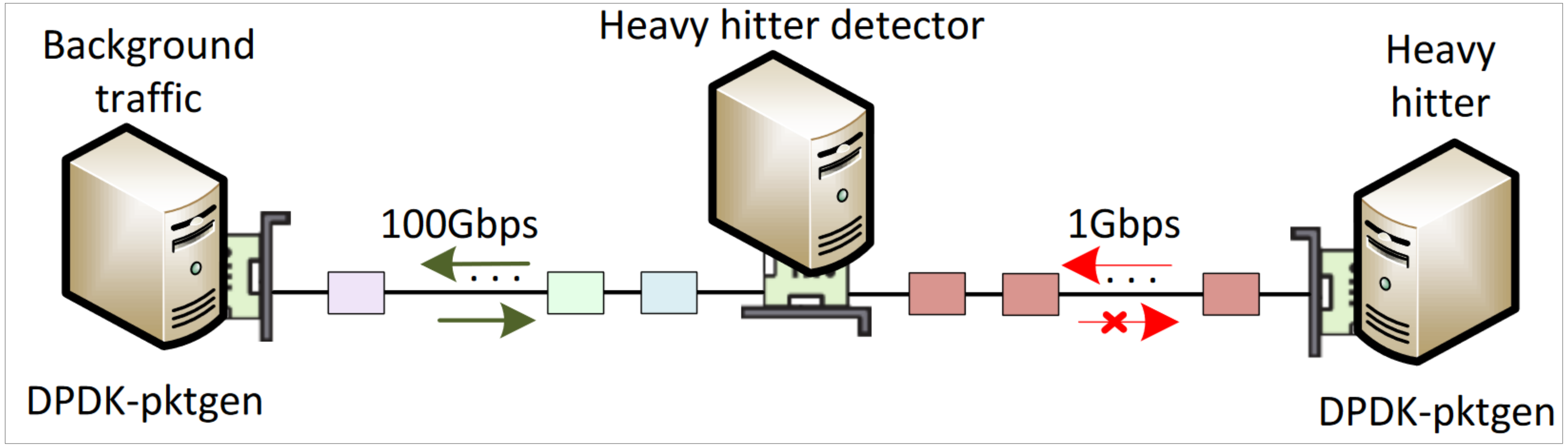
P4-DPDK

- P4-DPDK is an initiative that translates P4 code to DPDK



Heavy Hitter Detection

- Heavy hitters are flows that contribute a significant amount of traffic to a link
- Detecting heavy hitters is crucial across various applications:
  - Congestion control
  - Intrusion detection and prevention
  - Traffic rerouting
  - Network capacity planning
  - etc.
- DPDK-based heavy hitter detection using P4



Scalable Heavy Hitter Detection in Cloud Environments: A DPDK-based Software Approach with P4 Integration

Samia Choueiri, Ali Mazloum, Elie Kfoury, Jorge Crichigno

Integrated Information Technology Department, University of South Carolina, Columbia, South Carolina