DPDK
SUMMIT
APAC • 2021

Introducing Hardware Content Inspection Accelerator Into the Network Security Applications

KUN QIU, HARRY CHANG

NPG-PRC-SW NETWORK APPLICATION TEAM, INTEL R&D APAC

Agenda

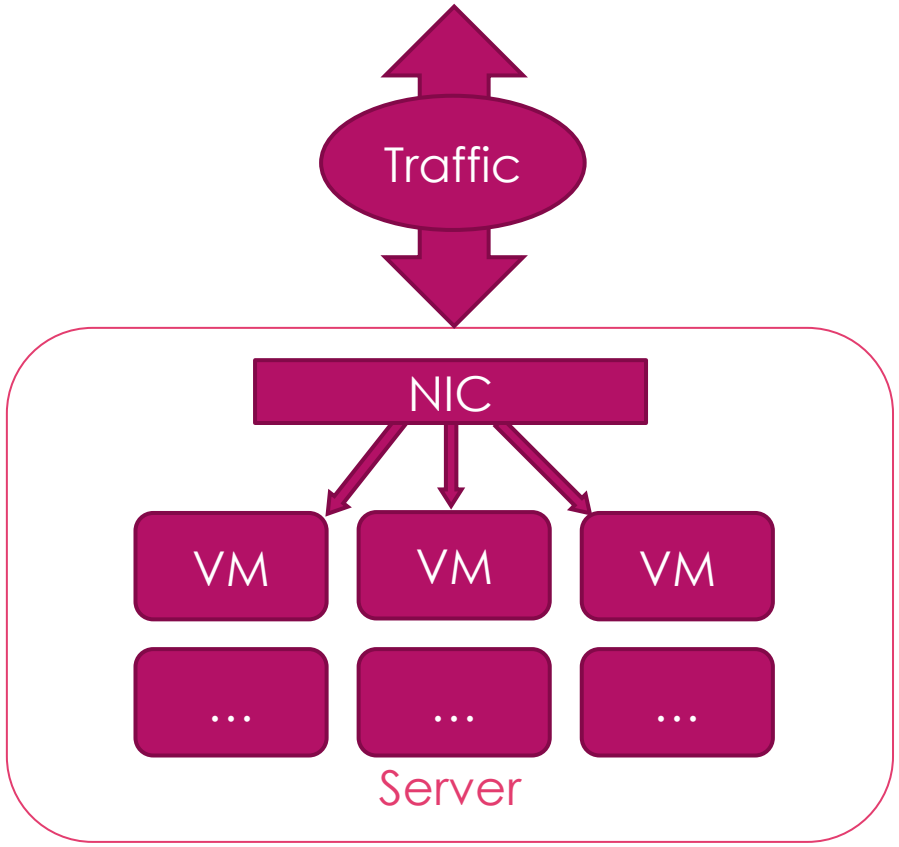
DPDK SUMMIT APAC•2021

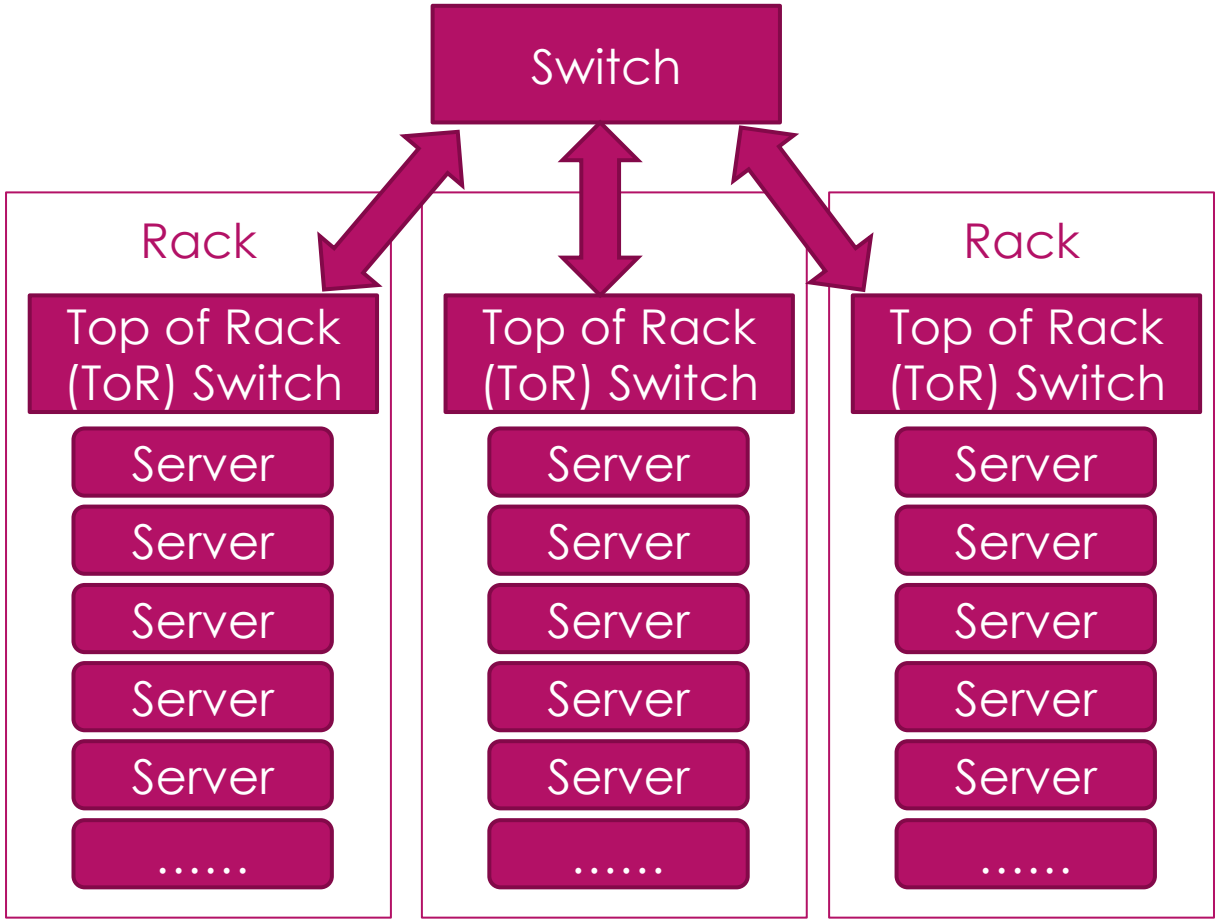
- Introduction
- Background
- Problem
- Challenge
- Solution
- Acknowledgement
- Reference & QA

Introduction

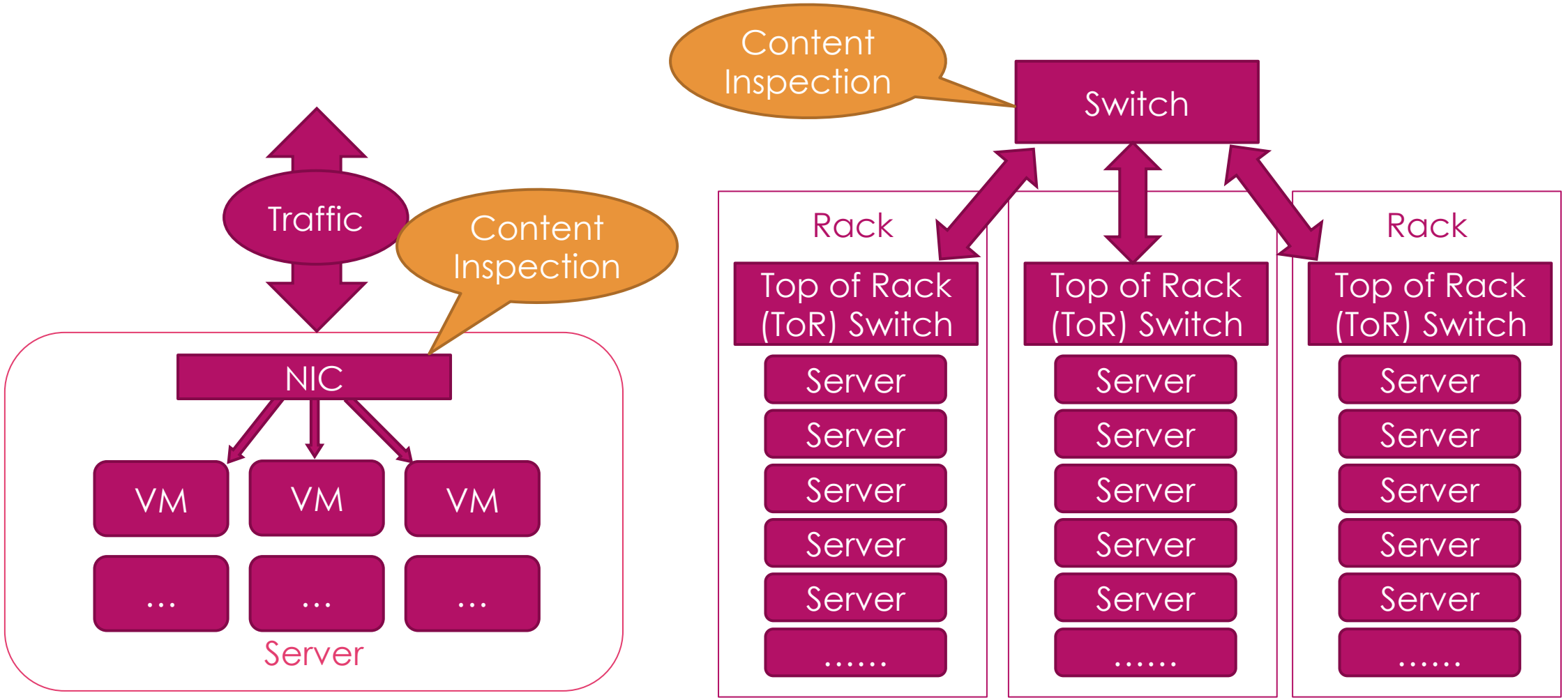
- Content Inspection
  - Literal Matching
    - Regular Expression (Regex)
- Regex Matching
  - "ARGS_NAMES:/^video\[[0-9]*\]\[\]/"
    - Searching video ID only composed by number
- High Performance Regex Matching
  - Software-based
  - Hardware-based
- Hardware Accelerator
  - NIC/Switch
    - Load balance
    - Flow director
    - …
  - …
- Network Security
  - Firewall
    - Web Application Firewall (WAF)
    - …
  - Network Intrusion System (IDS)
    - Deep Packet Inspection (DPI)
    - …

Background


Traffic
NIC
VM
VM
VM
...
...
...
Server


Switch
Rack
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....
Rack
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....

Background


Content Inspection
Switch
Traffic
Content Inspection
NIC
VM
VM
VM
...
...
...
Server
Rack
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....
Rack
Top of Rack (ToR) Switch
Server
Server
Server
Server
Server
.....

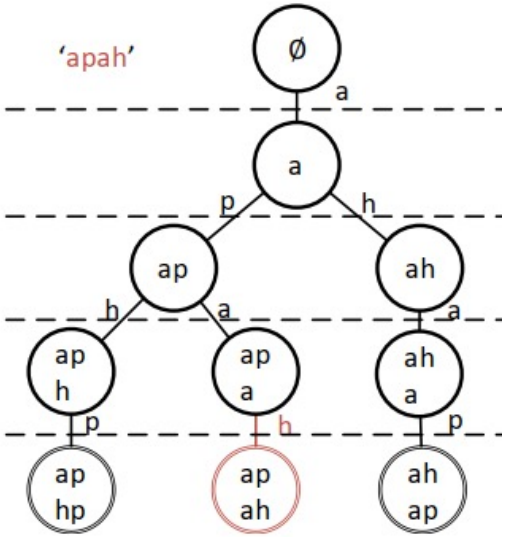
Problem

- Flexibility
  - Software
    - Easy to configurate
  - Hardware
    - FPGA/ASIC-based
      - SmartNIC
      - Configurable Switch
- Performance
  - Software
    - Hyperscan
  - Hardware
    - One order of magnitude (or two) larger than software
- CPU
  - Paying the levitation cost
    - Get data off the NIC through PCI-Express
- GPU/FPGA Acceleration[1,2]
  - Cannot catch up with the dramatic increase of the network traffic (e.g., multi-100s of Gbps) [3]
- PISA
  - Protocol Independent Switch Architecture
    - Tofino

Challenge

- Tofino
  - Programmable Switch[4]
  - SmartNIC[5]
  - …
- Protocol Independent
  - Match anything in any offset of the packet
    - Self-defined protocol
    - Traffic monitoring
    - …
- Content Inspection?

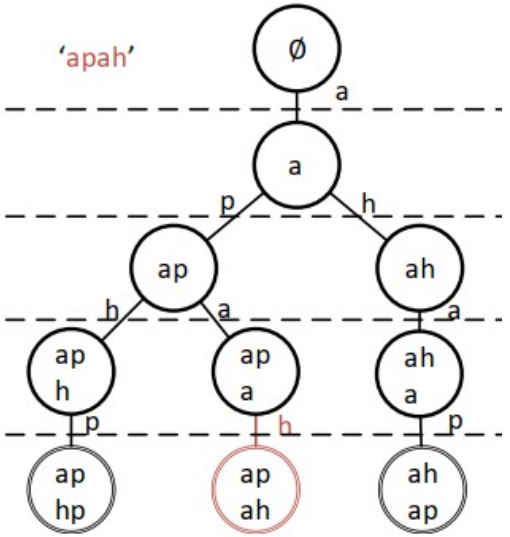
- State Machine
  - Deterministic finite automaton (DFA)



Challenge

- Regex → DFA
  - Regex Compiler
- Intel Hyperscan
  - High performance regex engine
  - Compiler (Regex→DFA)
  - Running time (DFA on CPU)
    - Optimized for CPU

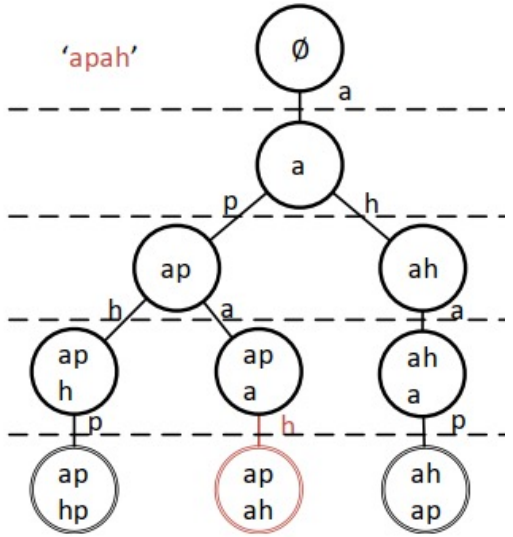
- State Machine
  - Deterministic finite automaton (DFA)



Challenge

- Regex → DFA
  - Regex Compiler
- Intel Hyperscan
  - High performance regex engine
  - Compiler (Regex→DFA)
  - ~~Running time (DFA on CPU)~~
    - ~~Optimized for CPU~~
- DFA→PISA (DFA on Tofino)
  - Limited Memory
    - Several hundred MB

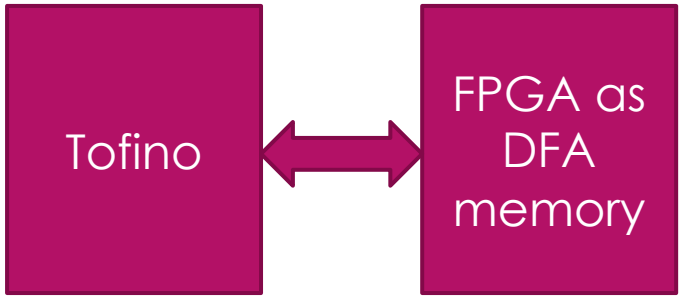
- State Machine
  - Deterministic finite automaton (DFA)



Solution

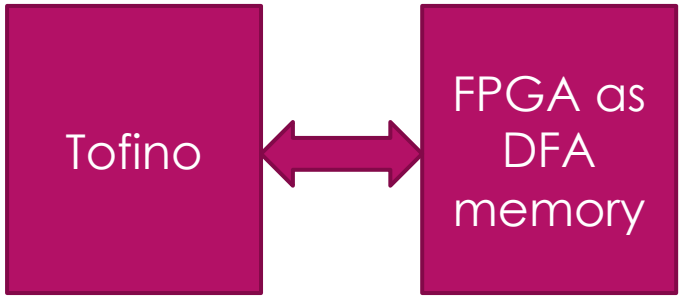
- **Hardware**
- FPGA-based Extended Memory

server-other	string	2118	100%	100%	86837	44460544	EMEM
emerging-trojans	string	9608	100%	100%	412676	211290112	EMEM
emerging-trojans	regex	1496	30%	96%	742765	380295680	EMEM
server-mail	regex	93	91%	95%	3642492	1864955904	EMEM
emerging-pop3	regex	16	100%	100%	34524	17676288	EMEM
community all	string	134	100%	100%	3464	1773568	IMEM
emerging threats all	string	5546	100%	100%	243857	124854784	EMEM
community all	regex	546	54%	84%	3631070	1859107840	EMEM
emerging threats all	regex	5159	32%	90%	2121305	1086108160	EMEM



Solution

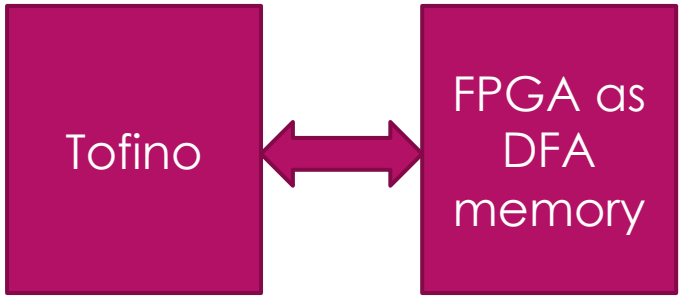
- **Hardware**
- FPGA-based Extended Memory
  - Utilized in Tofino-based load balance solution
  - Existing→Too large [6]



- **Software**
- Sub-ruleset
  - SQL-injection/Cross-site script
    - Over 70%
  - Tokenization
    - Modsecurity/libinjection
  - **‘ and 1=1**
  - **s & 1 o 1**
  - **(quote) (and) (num) (oper) (num)**
- SQL DFA tokenization states
  - Based on Hyperscan compiler
  - Only 9000+ states
  - (less then 8MB)

Solution

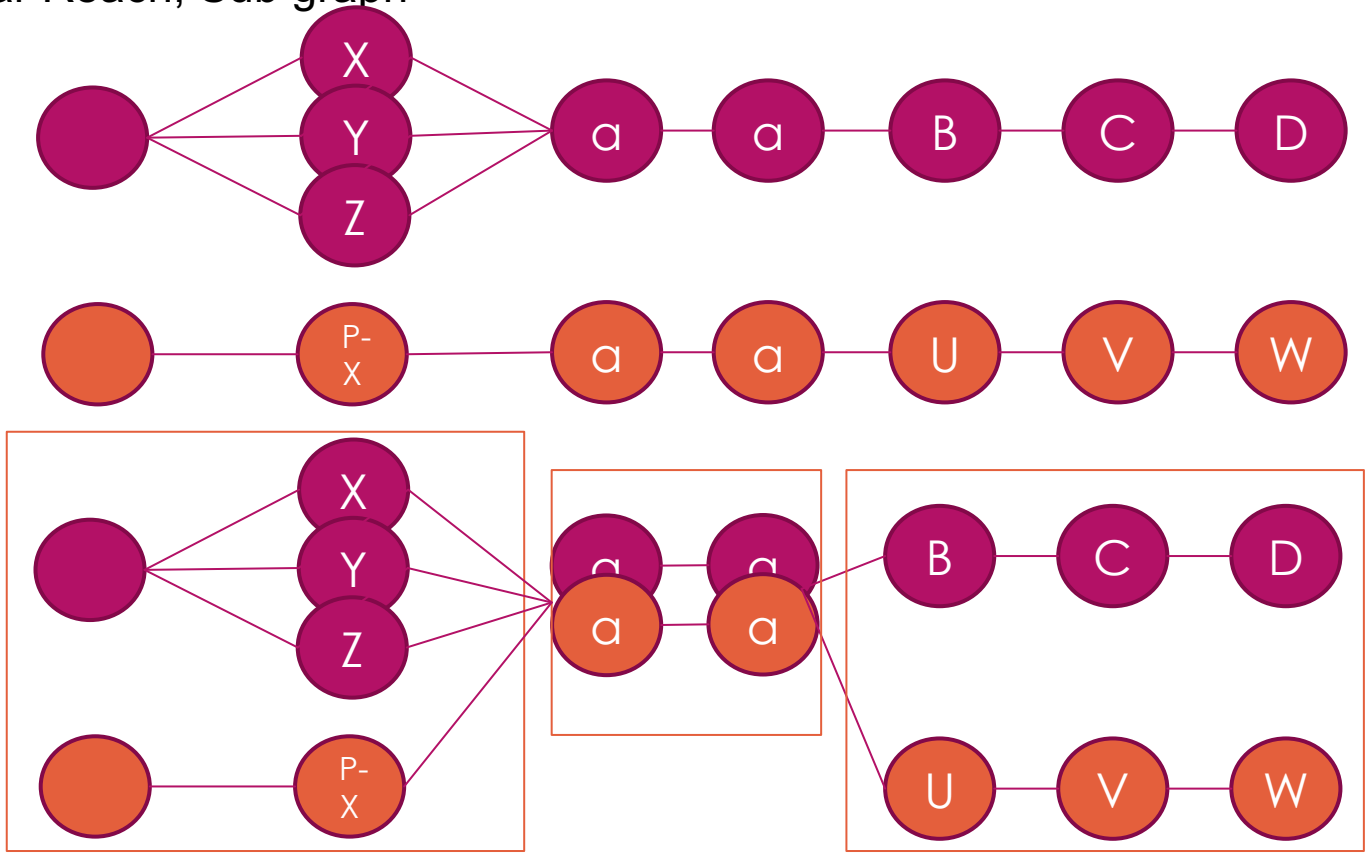
- **Hardware**
- FPGA-based Extended Memory
  - Utilized in Tofino-based load balance solution
  - Existing→Too large [6]



- **Software**
- RuleTailor (WIP)
  - Full snort rule set is too large
  - Decreasing the number of DFA states
    - Longest-prefix-based:
      - abc,abcde,abcfg:A
      - abf,abg:B
      - abc*:A
      - ab*:B
    - Non-prefix-based
      - (X|Y|Z)aaBCD: A
      - (P-X)aaUVW: A
      - *aa*: A
      - Graph-based compression
  - Intel Hyperscan Compile time
    - DFA Compression

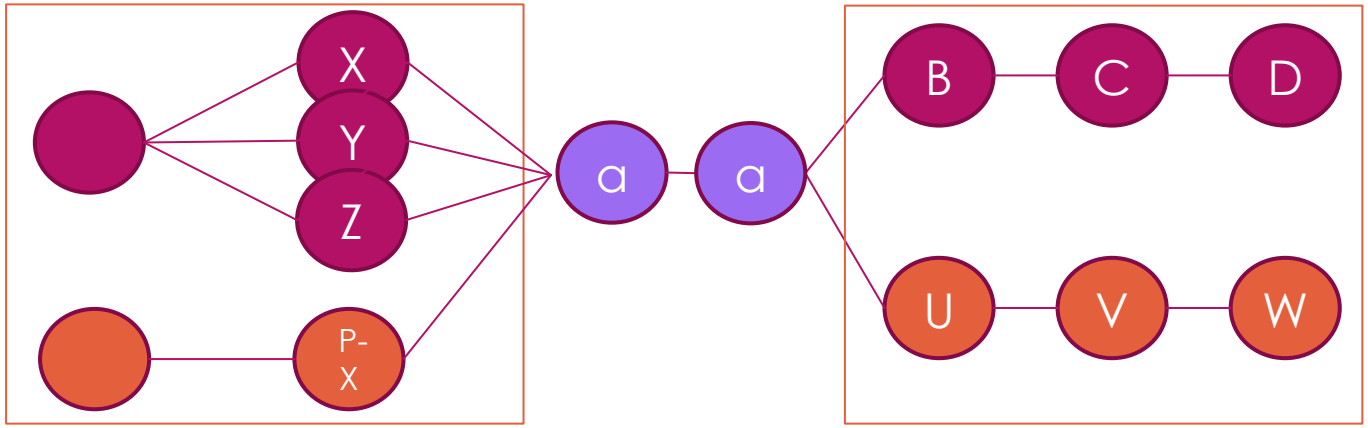
Solution

- RuleTailor
  - Innovative from Intel Hyperscan
  - Graph Computation
    - Char Reach, Sub graph



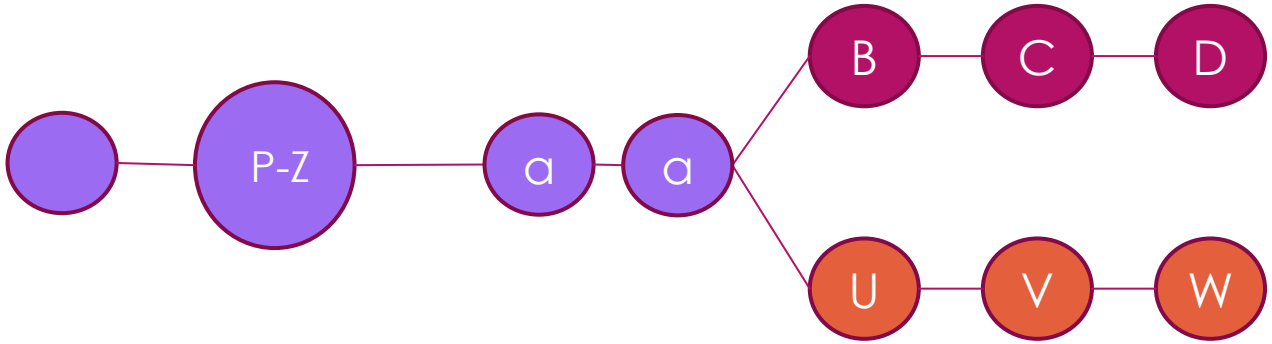
Solution

- RuleTailor
  - Innovative from Intel Hyperscan
  - Graph Computation
    - Char Reach, Sub graph

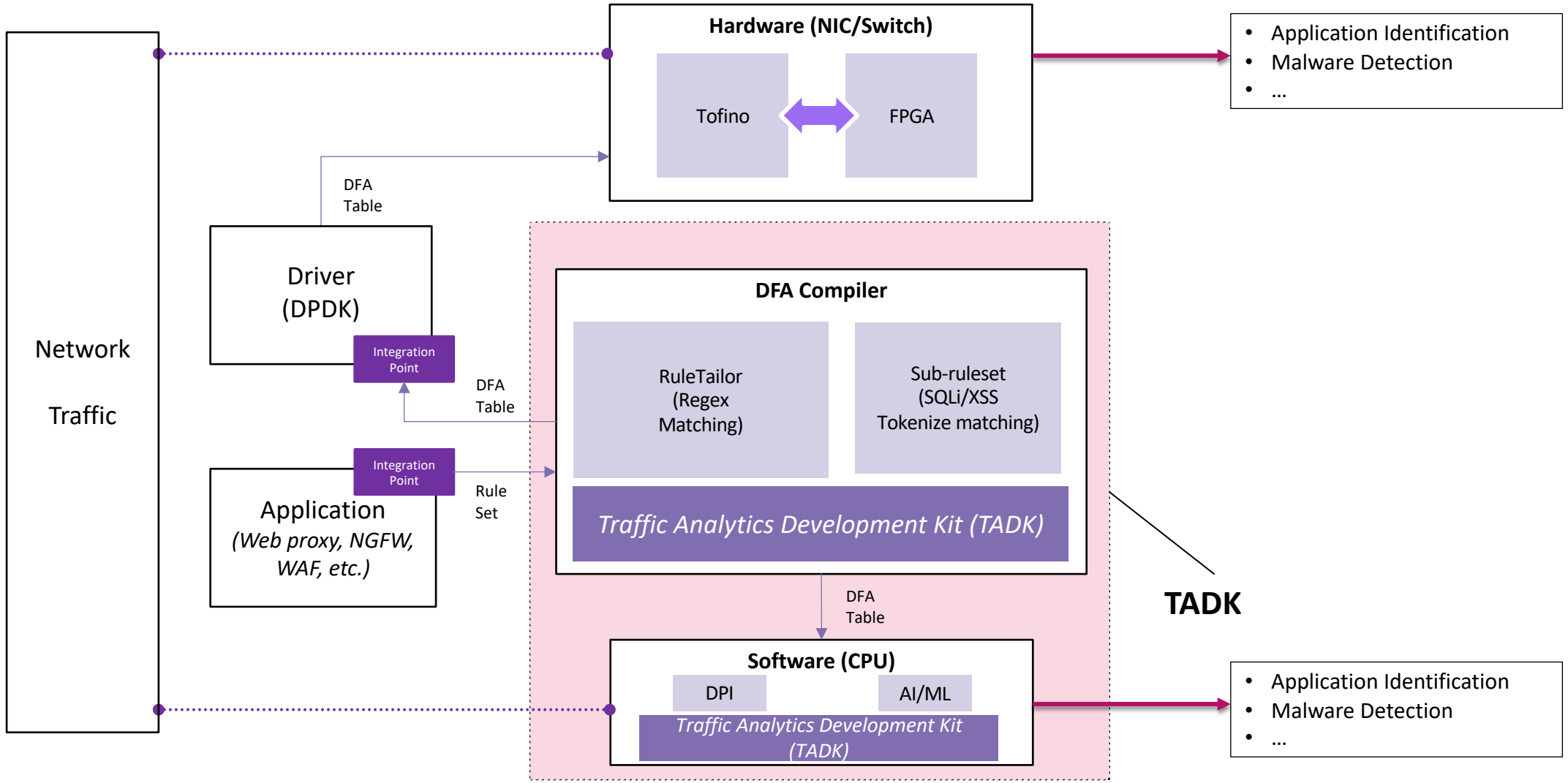


Solution

- RuleTailor
  - Innovative from Intel Hyperscan
  - Graph Computation
    - Char Reach, Sub graph



Solution


Hardware (NIC/Switch)
Tofino
FPGA
Application Identification
Malware Detection
…
DFA Table
Driver (DPDK)
Integration Point
Network Traffic
DFA Compiler
RuleTailor (Regex Matching)
Sub-ruleset (SQLi/XSS Tokenize matching)
Traffic Analytics Development Kit (TADK)
DFA Table
Integration Point
Application (Web proxy, NGFW, WAF, etc.)
Rule Set
TADK
DFA Table
Software (CPU)
DPI
AI/ML
Traffic Analytics Development Kit (TADK)
Application Identification
Malware Detection
…

Acknowledgement

- Network Application Team
  - Ying Wang, Wenjun Zhu, Xiahui Yu, Chenmin Sun,
- Hongjun Ni, Xiang Wang, Weigang Li, Baoqian Li, Haitao Kang
- Intel Barefoot Team
  - Robert Soule, Changhoon Kim

Reference & QA

- [1] Reetinder Sidhu and Viktor K Prasanna. 2001. Fast regular expression matching using FPGAs. In FCCM. IEEE, 227–238.
- [2] Muhammad Asim Jamshed and et al. 2012. Kargus: a highly-scalable softwarebased intrusion detection system. In *CCS*. ACM, 317–328.
- [3]Wang, Shicheng, et al. Fast Multi-string Pattern Matching using PISA. In CoNEXT. 2019.
- [4] https://www.intel.com/content/www/us/en/products/network-io/programmable-ethernet-switch/tofino-series/tofino.html
- [5] https://www.nextplatform.com/2020/10/15/intel-networking-not-just-a-bag-of-parts/
- [6] Hypolite, J., Sonchack, J., Hershkop, S., Dautenhahn, N., DeHon, A., & Smith, J. M. (2020, November). DeepMatch: practical deep packet inspection in the data plane using network processors. In *Proceedings of the 16th CoNEXT*


DPDK
SUMMIT
APAC•2021