Closing the Network Control Loop

Jennifer Rexford, Princeton University
Programmability From Top-to-Bottom and End-to-End

NIC

5G Mobile Network

SDN Controller

DoS Mitigation
Traffic Engineering
Load Balancing
Overlay Virtualization

...

NIC

P4

P4

P4

P4

DPDK
User space
Kernel stack
XDP/eBPF

ONF

PRONTO
What Will Network Owner’s Do?

• What will network owners do with this new flexibility?

• We believe they will want to run their networks better!
Adding New “Dials”

- Traffic
- Performance
- Cyberattacks
- Failures
- Signal strength
- <Your measurement here>
Adding New “Knobs”

- Drop
- Mark
- Rate-limit
- Reroute
- Hand-off
- <your knob here>
Example #1: Microbursts

- Small timescale traffic bursts
  - Long queues caused by incast, attacks, etc.
  - Lead to high packet delay and loss
  - ... despite low average link utilization
Example #1: Microburst Measurement

- Data-plane measurement and analysis
- Backlog in the queue
- A flow’s own contribution to the queue

ConQuest: "Fine-grained queue measurement in the data plane" in CoNEXT’19.
Example #1: Microburst Mitigation

- Data-plane adaptation
  - Drop or mark an arriving packet probabilistically
  - Based on its flow’s contribution to the queue
Example #2: Distributed Denial-of-Service Attacks

- **DDoS attacks**
  - DNS reflection attack
  - SYN flooding
  - HTTP flooding
  - Slowloris attack
- **Overwhelm the victim**
  - Exhausting network and server resources
Example #2: DDoS Detection

- Data-plane measurement and analysis
  - Identify suspected victim destinations (key DstIP)
  - ... receiving traffic from distinct senders (attribute SrcIP)
  - ... in excess of a threshold (threshold T)

BeauCoup: “Answering many network traffic queries, one memory update at a time” in SIGCOMM’20
Example #3: DDoS Mitigation

- Data-plane adaptation
  - Drop or rate-limit packets to suspected victims
  - Run stateful firewall for suspected victims
  - Pushback upstream toward the senders
Example #3: Path Performance

- Network path diversity

- Load balancing to achieve good performance
  - Track the performance (load, loss, delay) of paths
  - Split traffic effectively over the multiple paths
Example #3: Path Performance Monitoring

- Tracking the best path by some metric
  - E.g., lowest maximum link utilization
  - E.g., minimum end-to-end latency or loss

Probes along reverse path
Example #3: Performance-Aware Load Balancing

- Directing traffic over the best path
  - Sending packets in the forward direction
  - ... along the path with the best performance

Contra: "A programmable system for performance-aware routing" (NSDI'20)
Enabler: Programmable Data Planes

Stages:
- Parser
- Registers
- Memory
- Match-Action Table
- Deparser
Challenges: Resource Limitations

- Limited depth
- Limited # bits
- Limited # rules
- Limited # registers and accesses
- Limited ALU operations

Stages:
- Parser
- Registers
- Match-Action Table
- ALU
- Memory
- Deparser
Solution: Compact Data Structures

- Approximate analysis is fine
  - Microbursts: size estimate for just the large flows
  - DDoS: rough count for large #s of distinct sources
  - Path performance: rough estimates for best paths

- Data structures can fit in data-plane registers
  - Sketch (e.g., Bloom filter, count-min sketch, etc.)
  - Small hash table (e.g., cache of the popular keys)
High-level goals

Compiler

control loop

Distributed software

Controller

vSwitch

Switch OS

Switch OS

vSwitch

P4 NIC

P4 switch

P4 NIC

P4 switch

P4 NIC