



# Security Apps with P4 Programmable Switches

Discussions, applications with  
P4 switches, Tofino pods

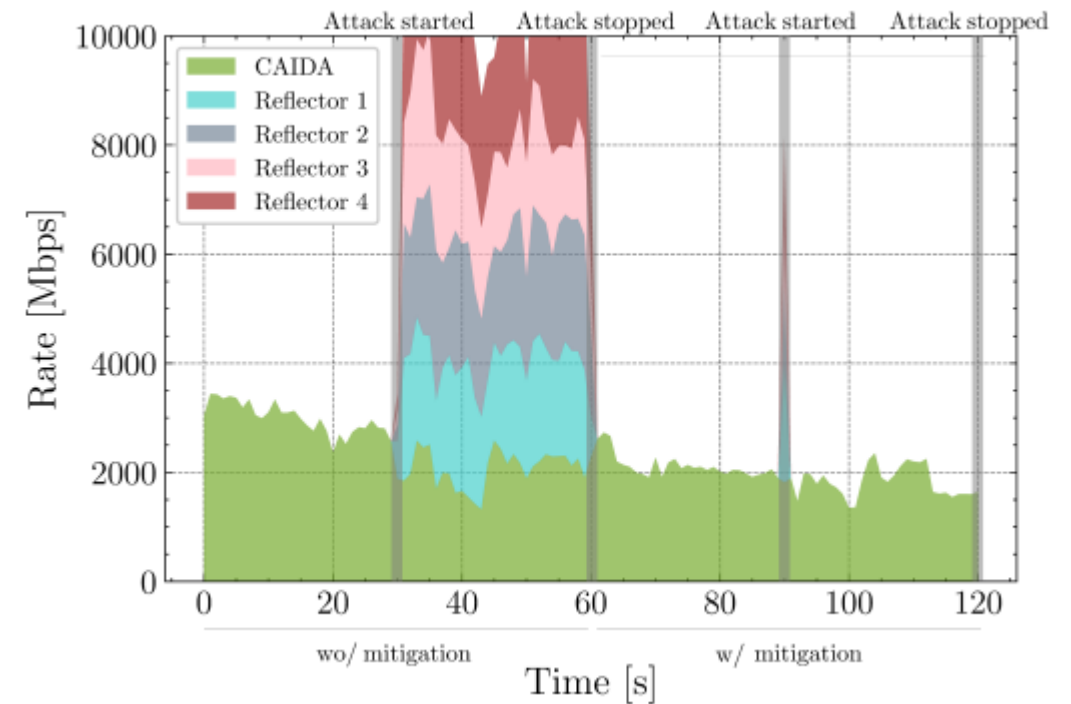
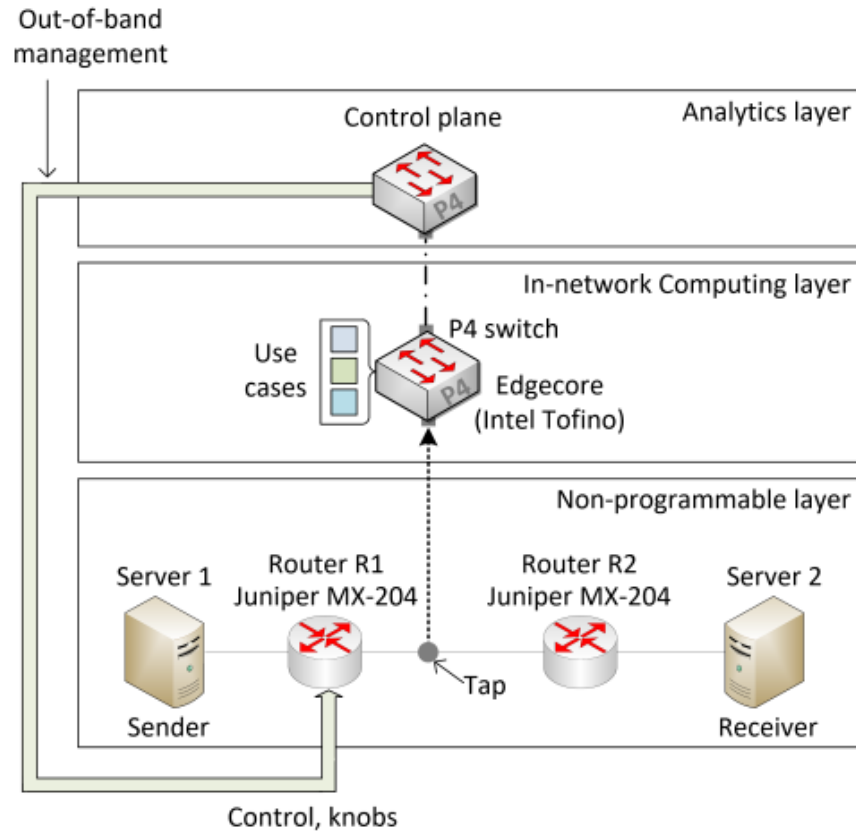
Jose Gomez, Ali AISabeh, Jorge Crichigno  
University of South Carolina  
<http://ce.sc.edu/cyberinfra>

University of South Carolina (USC)  
Energy Sciences Network (ESnet)

September 18, 2023

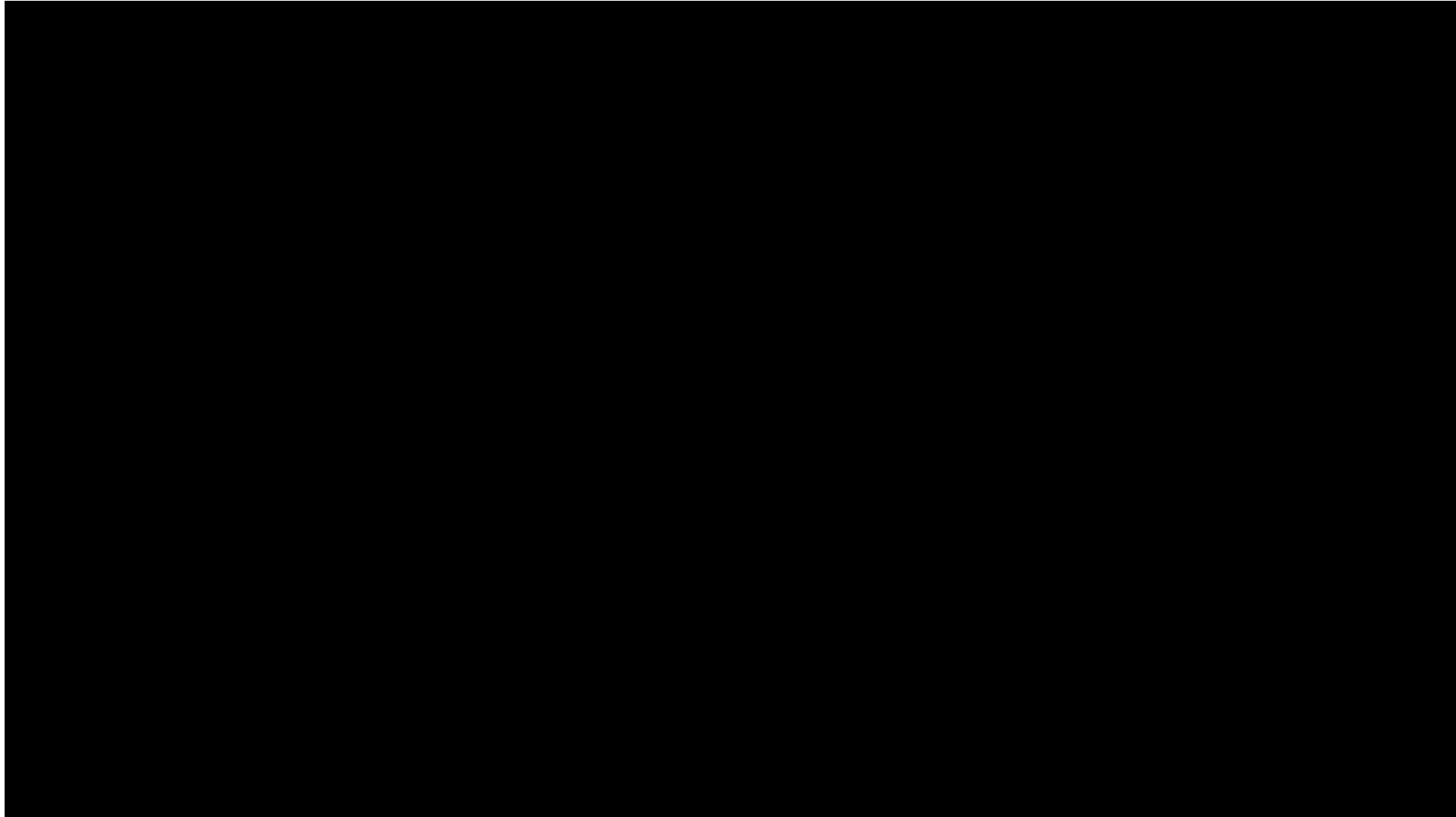
# DDoS Detection and Mitigation

## DDoS detection using passive switch deployment



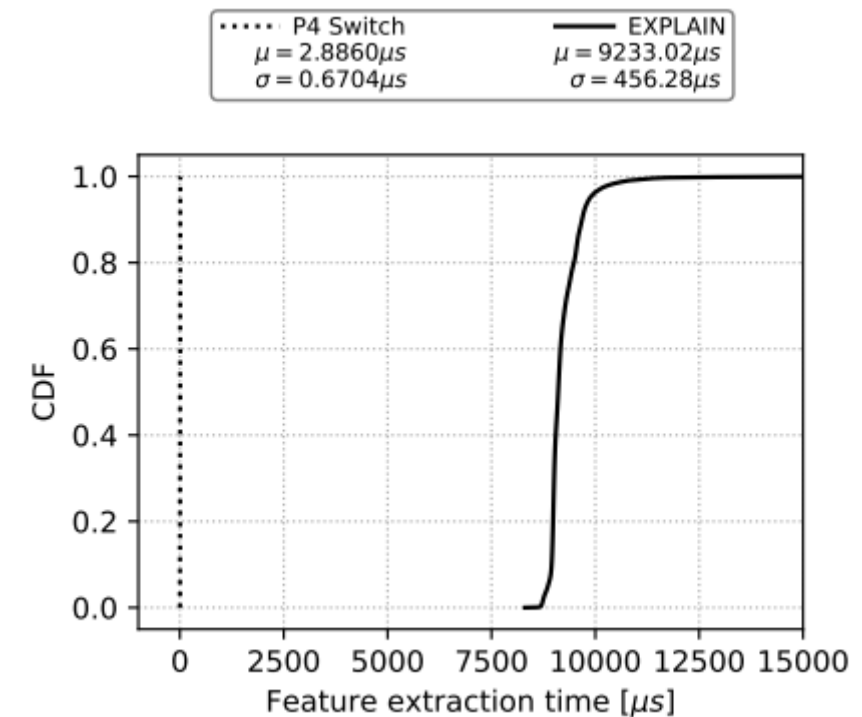
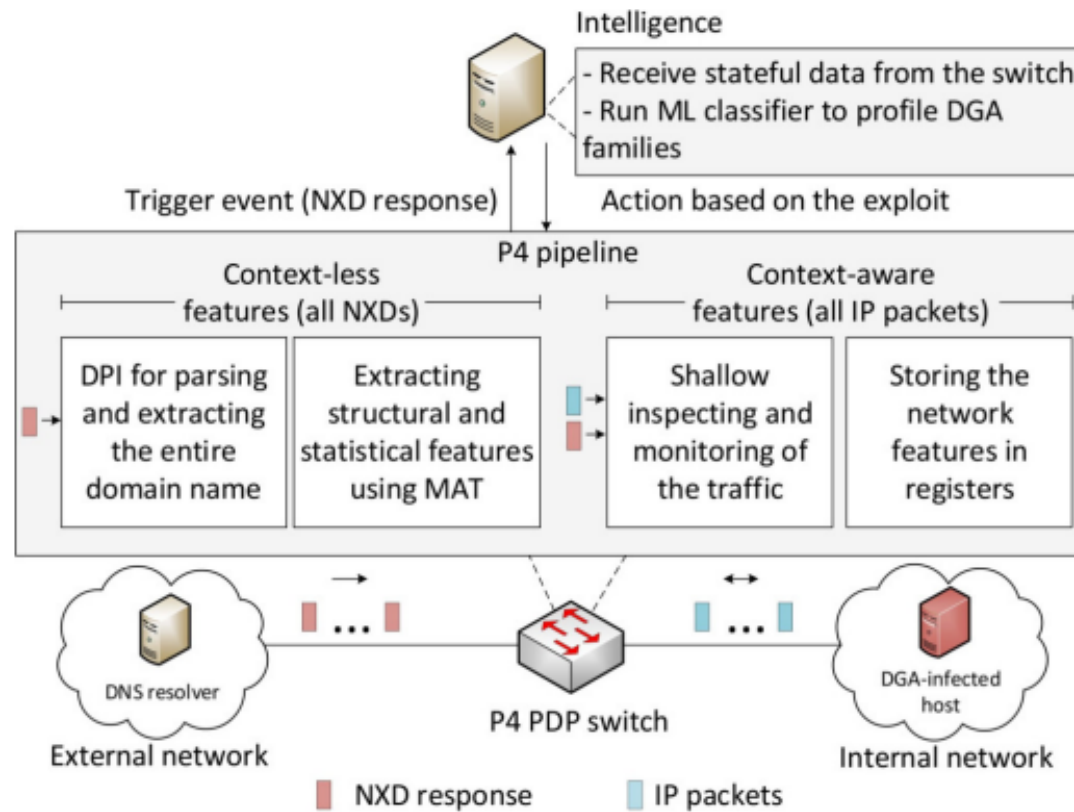
# Fine-grained Measurements

Customized firewall, without adding any additional processing on Science DMZ devices



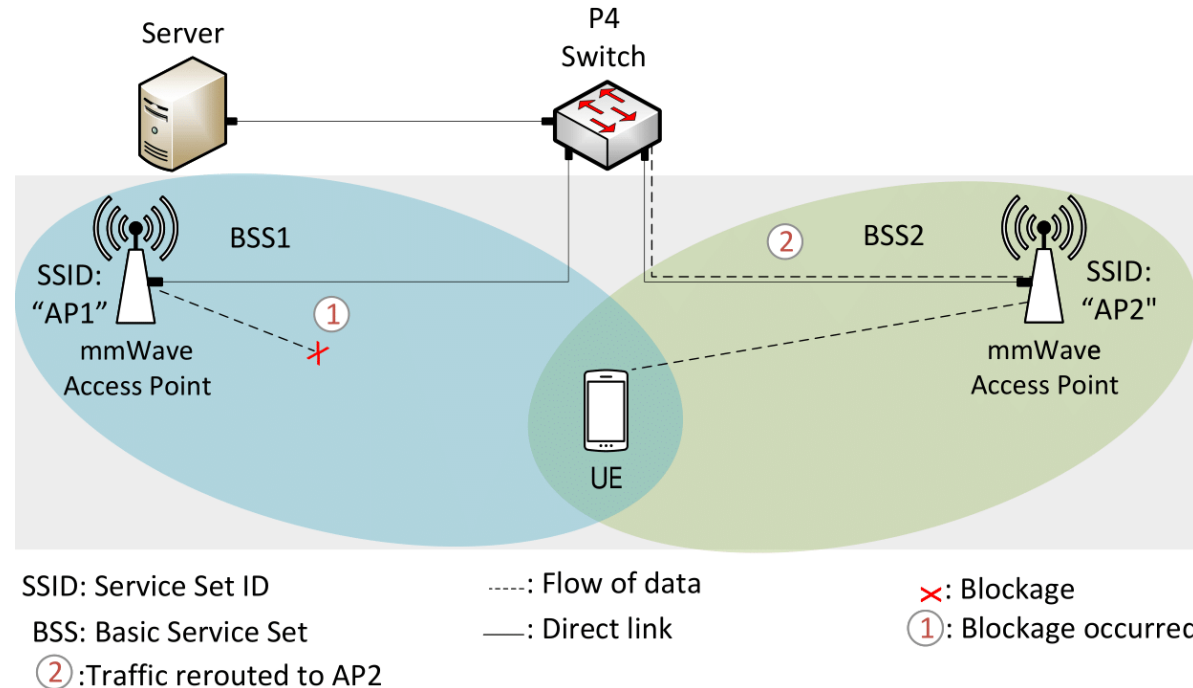
# Domain Name Parsing and Malware Fingerprinting

Domain name inspection and extraction of features for fingerprinting malware in the data plane

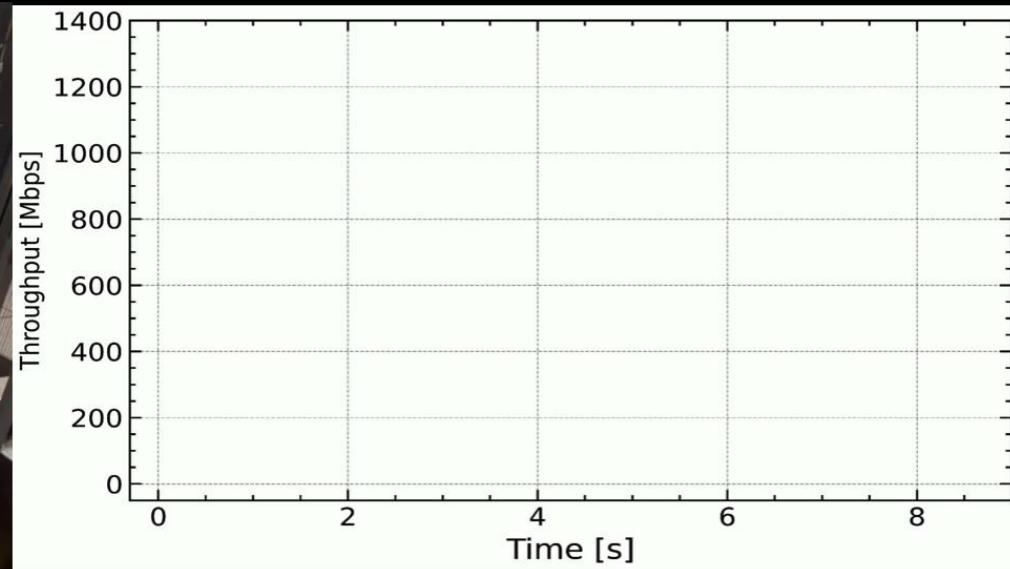


# mmWave Blockage Detection

- Programmable switches monitor the inter-arrival time (IAT) of the packets
- Using the measurements, the programmable switch detects the blockage and then notifies the end user to handover
- The system was implemented and tested on a Tofino hardware switch and off-the-shelf mmWave-compatible devices

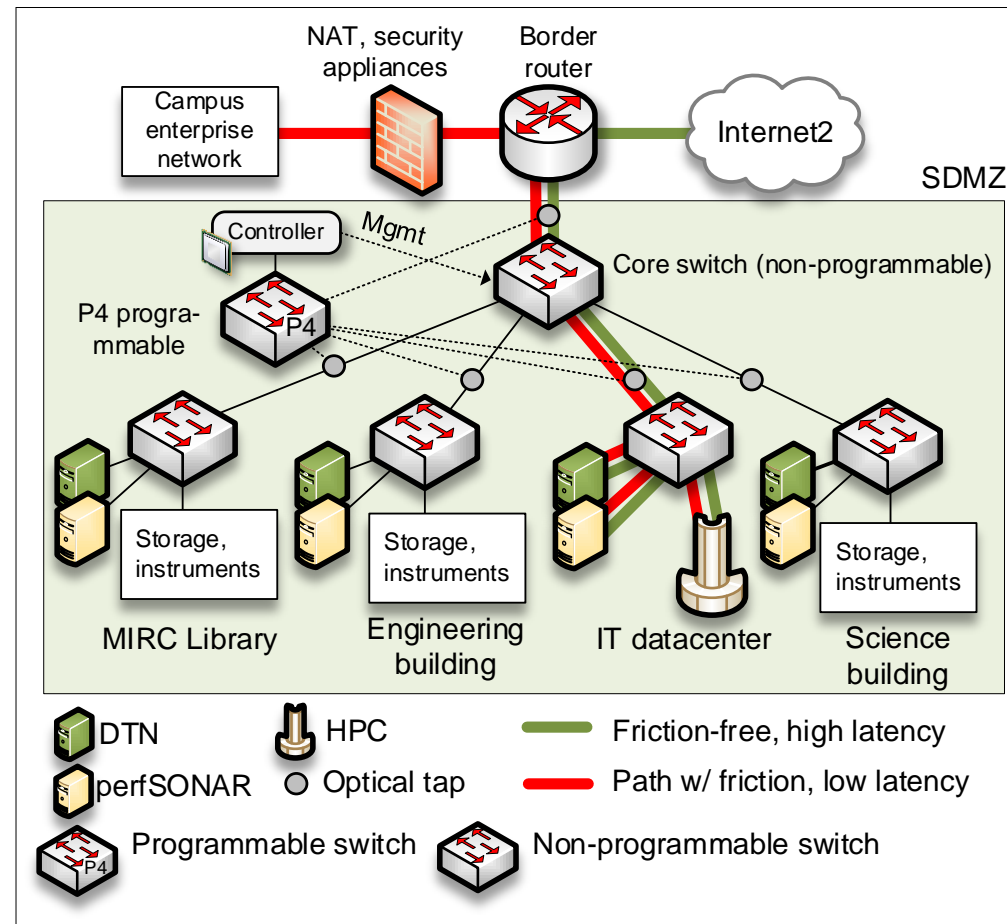


# Proposed System



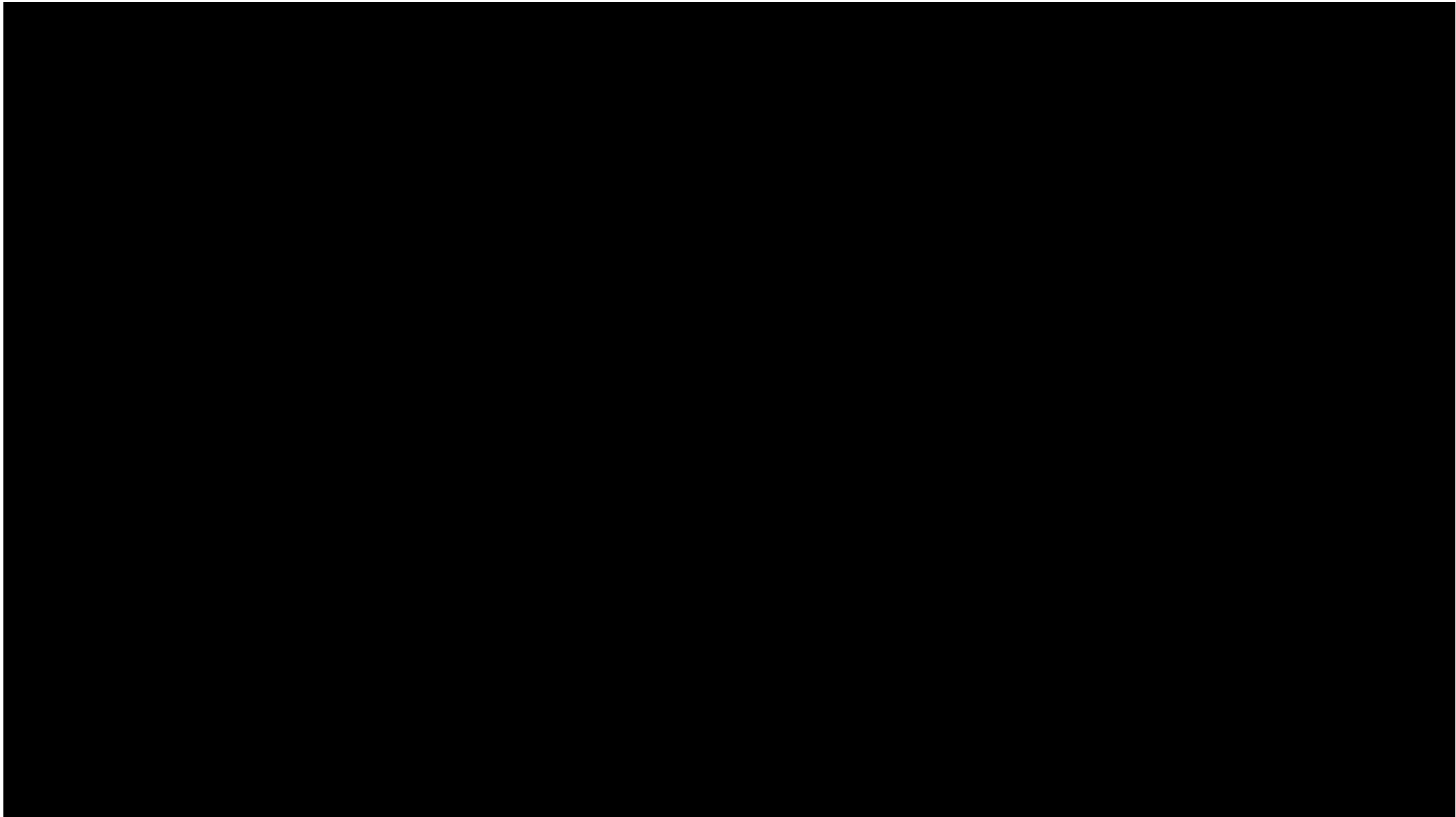
# Fine-grained Measurements

## Granular RTT calculation



# Fine-grained Measurements

---





# Fine-grained Measurements

## Granular RTT calculation - Applications

- Calculating the optimal buffer size (a function of the average RTT of all large flows crossing the switch)
- Detecting bad routing decisions, hijacking, reflected in large RTTs

