NIST National Institute of Standards and Technology U.S. Department of Commerce

vPROM: vSwitch Enhanced Programmable Measurement In SDN

Software Defined Virtual Networks

An Wang, Yang Guo, Doug Montgomery, Kotikalapudi Sriram, Songqing Chen, Fang Hao, T.V. Lakshman

https://www.nist.gov/programs-projects/software-defined-virtual-networks

① Motivations

- ❑ SDN is a **new networking paradigm** with separated control and data plane
- ❑ **Network programmability**: ability to program the network with perception that underlying network is a single device
- ❑ Benefits: **Program and automate** *network measurement, cyber security, anomaly detection, network management, etc.*

② Challenges

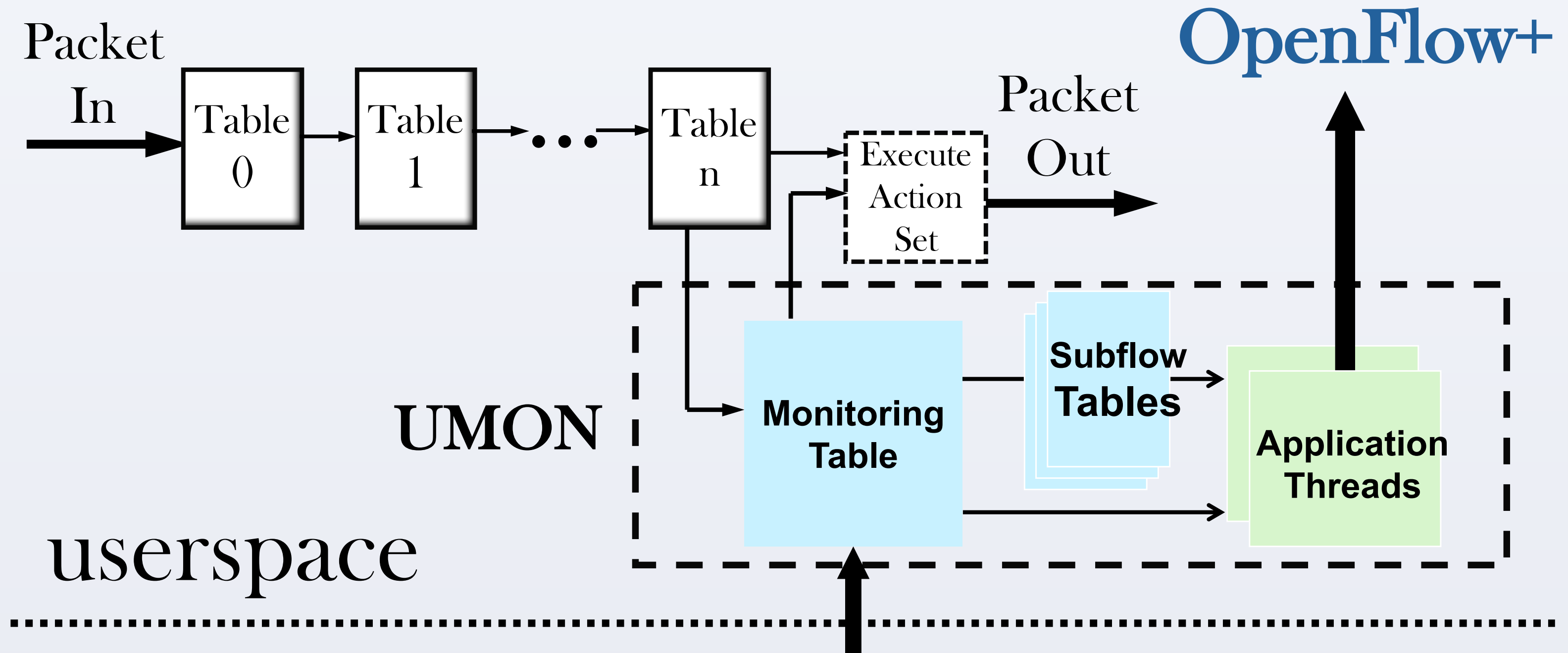
- ❑ Interference between monitoring and other applications
  - ➢ Rule overlapping and conflicts
- ❑ Continuous involvement of the controller may be required
  - ➢ Sub-flow collection
- ❑ Using forwarding table for monitoring is neither flexible nor sufficient
  - ➢ Forwarding and monitoring applications have different header fields of interest

③ Solutions

Decouple monitoring function from forwarding function in both data and control plane

- ❑ Data plane:
  - ➢ instrumented Open vSwitches (**UMON**)
- ❑ Control Plane
  - ➢ Pyretic => **Pyretic+** to generate different rule sets for monitoring and network anomaly detection
  - ➢ OpenFlow => **OpenFlow+** to enable direct configuration of monitoring rules

④ UMON workflow

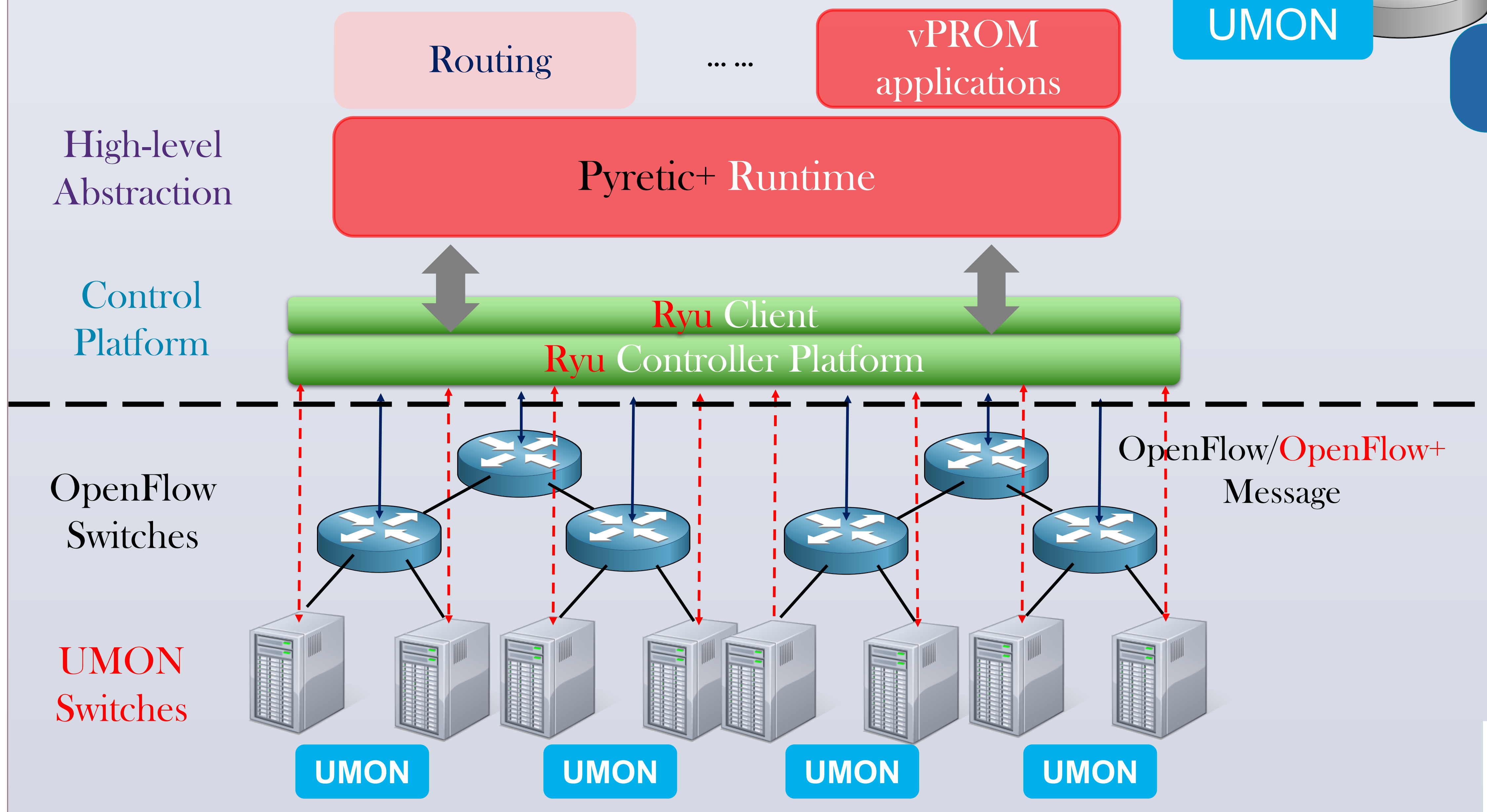


periodic update monitoring table with kernel flow table info

① Monitoring on **non-routing** fields

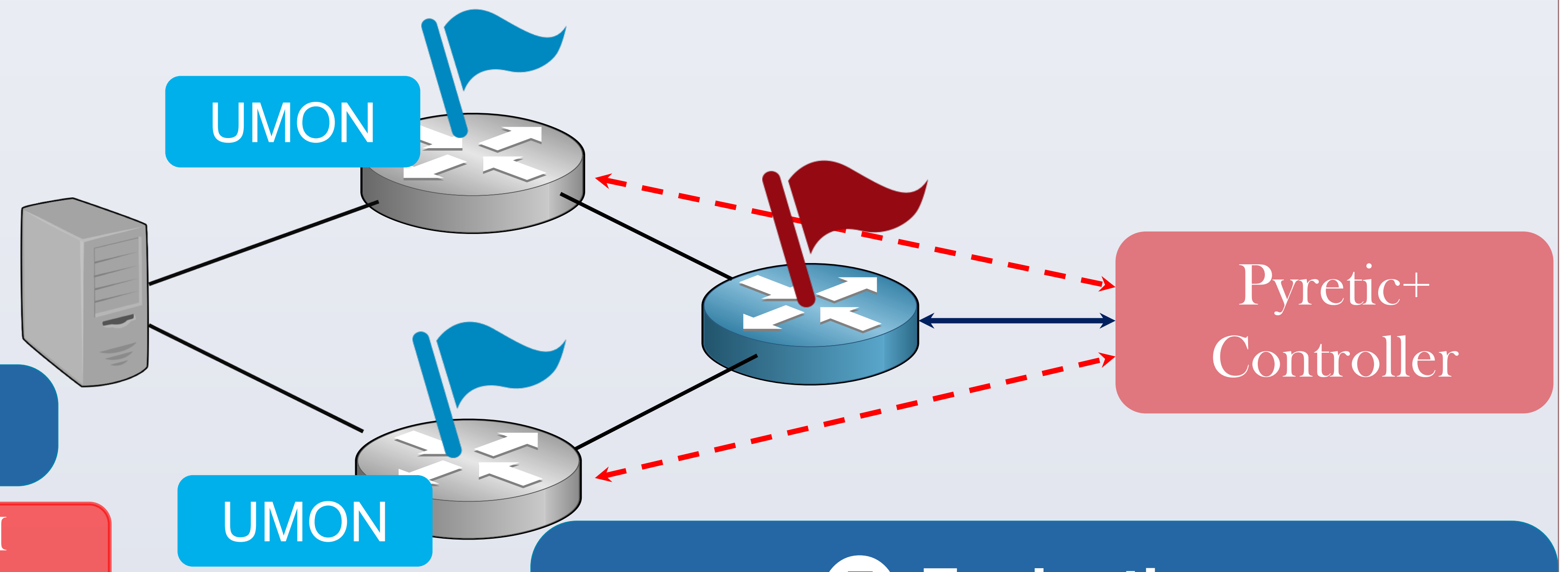
② **Subflow** monitoring

⑤ vPROM architecture



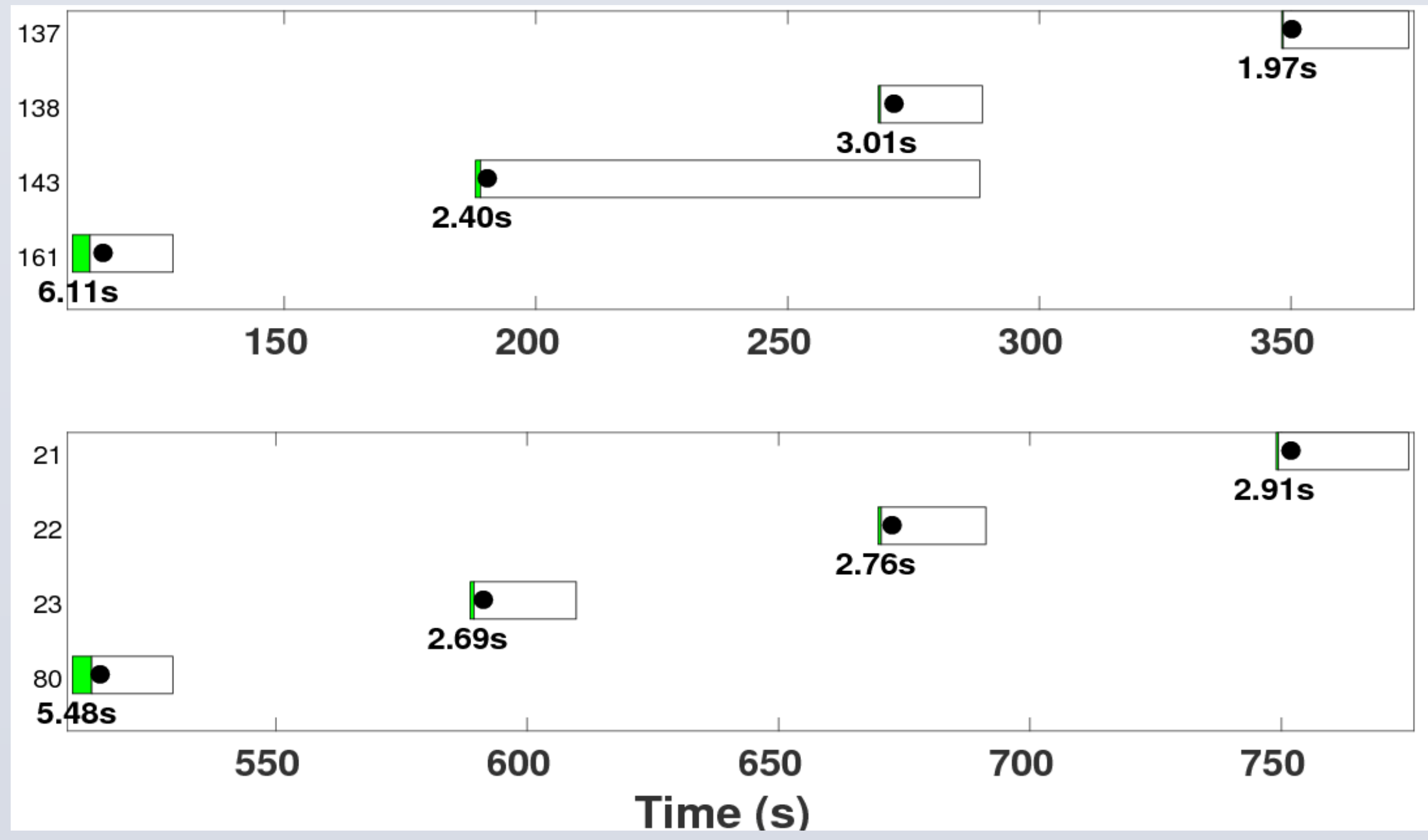
⑥ Usecase : vPROM-GUARD

Flag Indicators	Potential Attacks
Big Flow + CUSUM	TCP SYN Flooding attack
Big Flow	Large flow DDoS attack
CUSUM	Collecting finer grained sub-flows & detecting scanning attacks

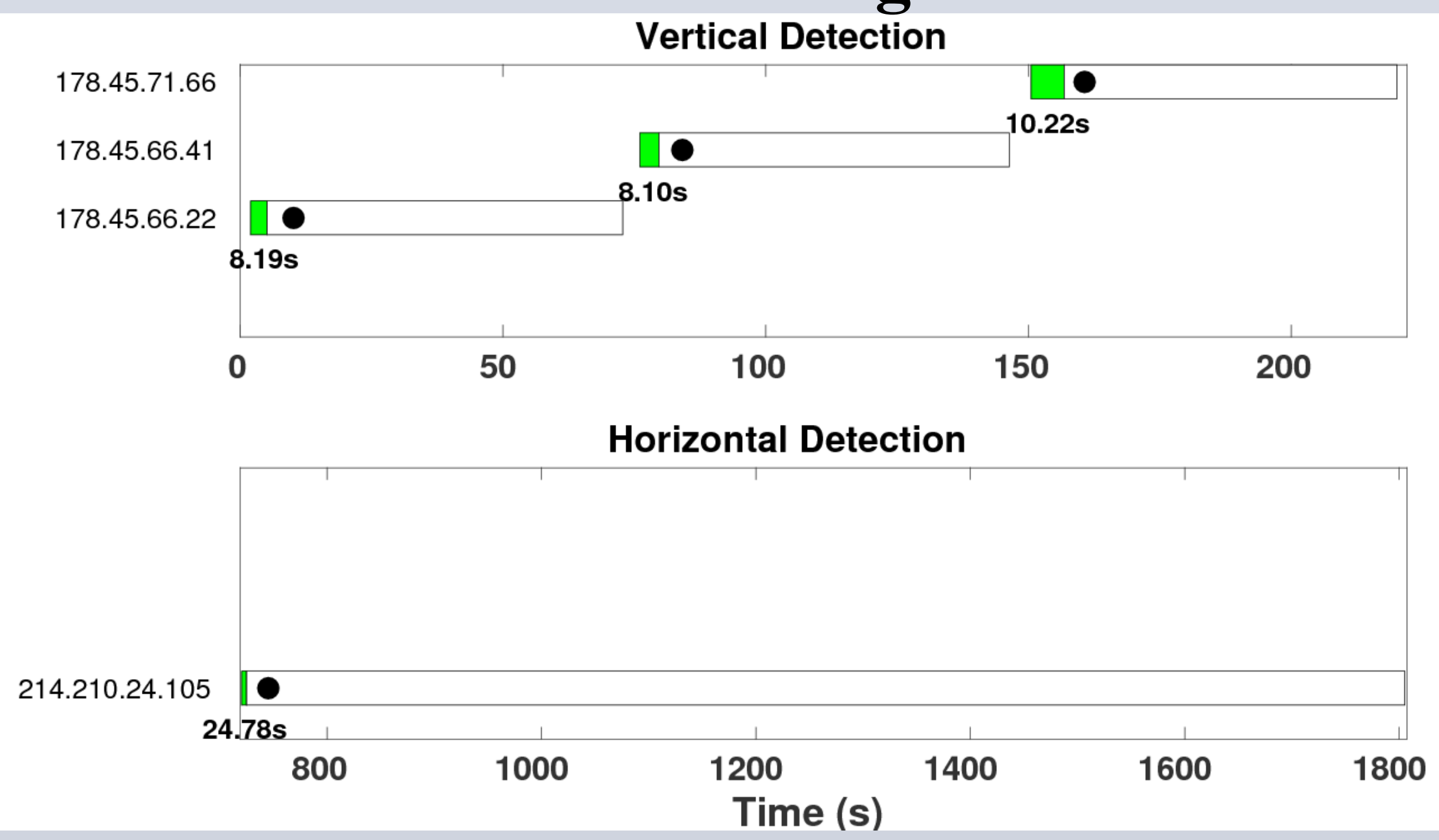


⑦ Evaluations

SYN Flooding attacks



Port scanning attacks



⑧ Conclusions

- ❑ Decoupling monitoring from forwarding is the **KEY** to address challenges
- ❑ **vPROM** offer a new programmable network measurement and anomaly detection framework
- ❑ vPROM-GUARD detect **DDoS and port scanning attacks efficiently**