vPROM: vSwitch Enhanced Programmable Measurement In SDN

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

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.*
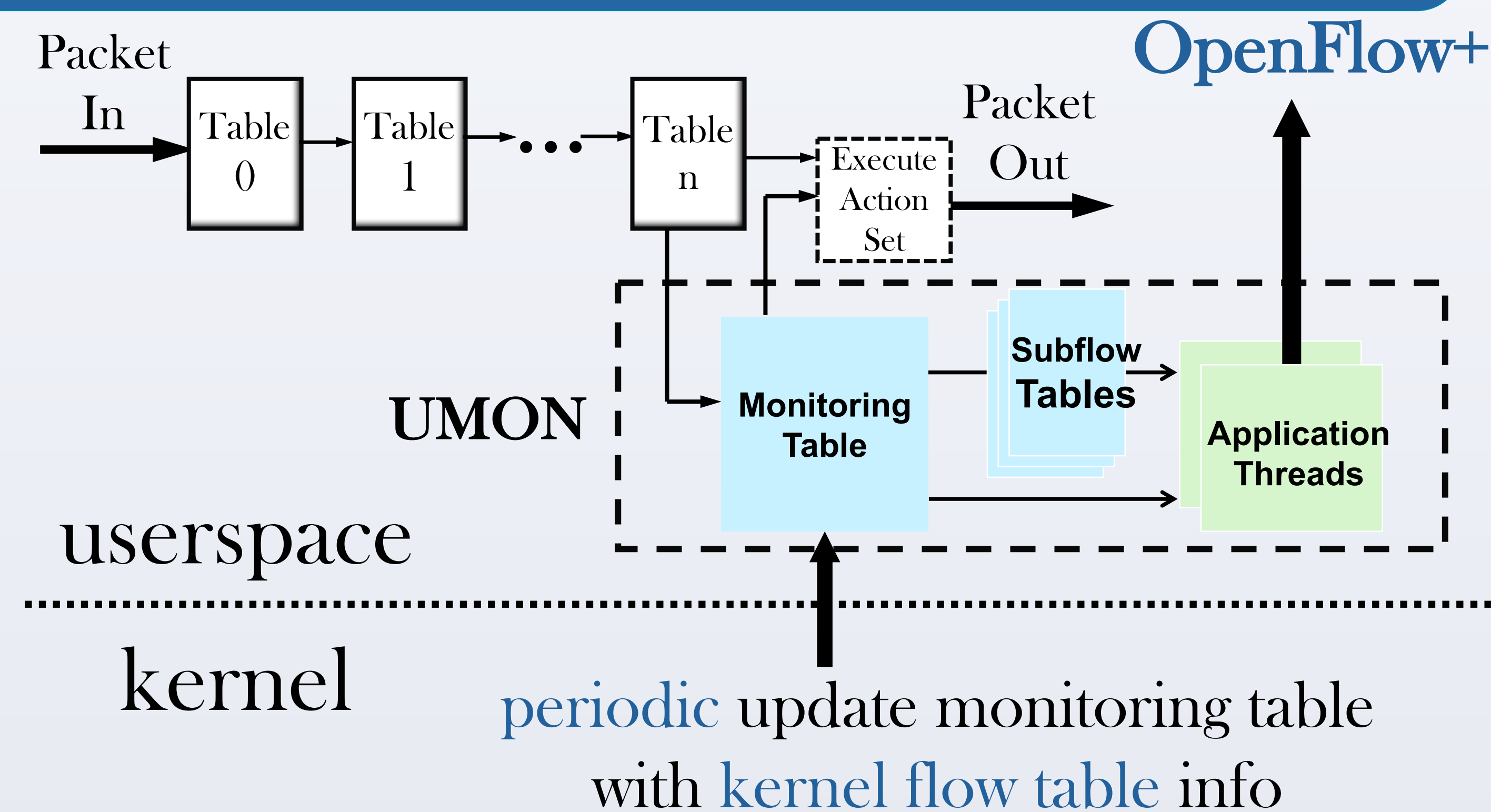
② Challenges

- ❑ 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

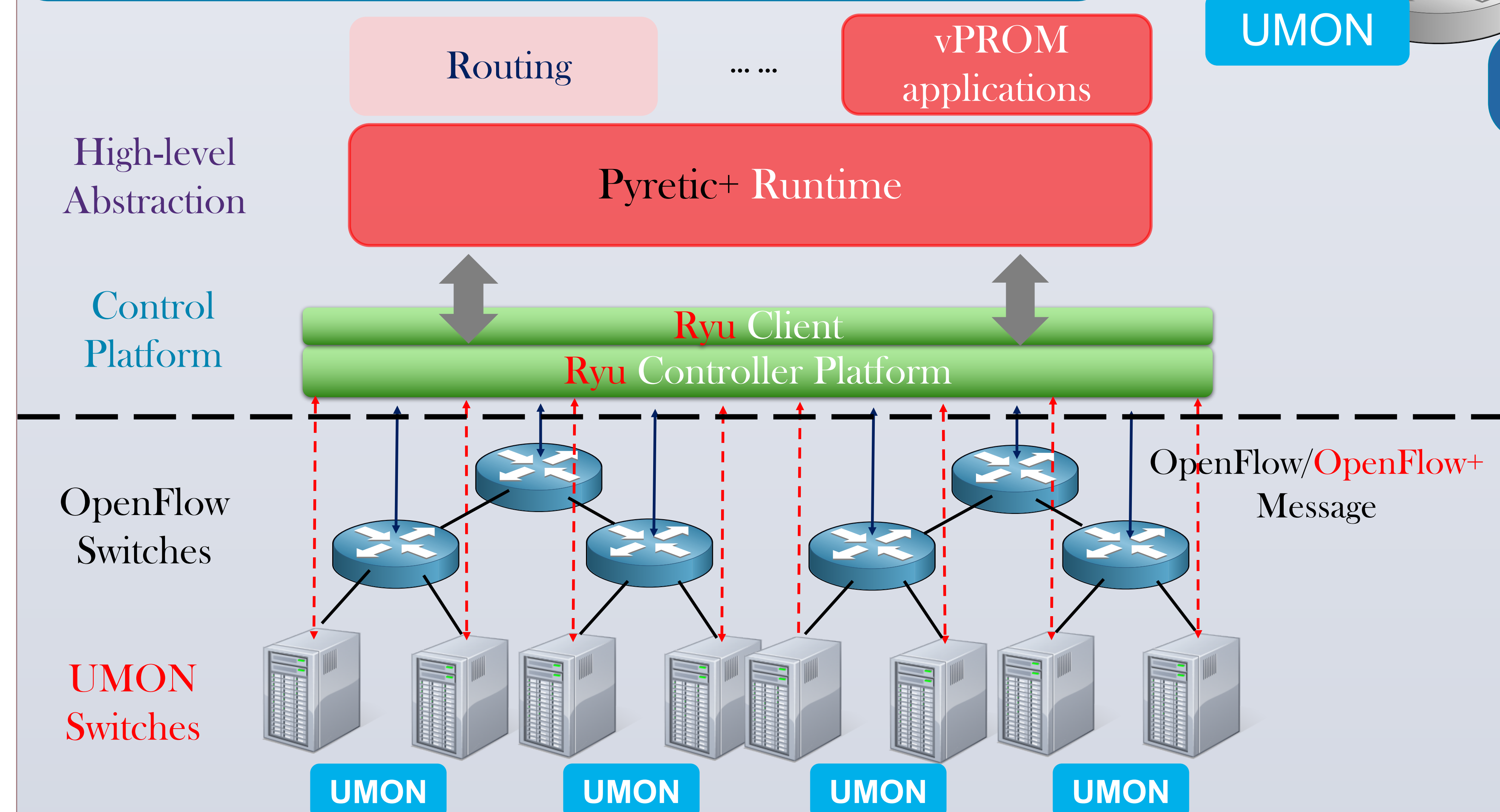**Decouple monitoring function from forwarding function in both data and control plane**

- ❑ 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

OpenFlow+

Packet In → Table 0 → Table 1 → ... → Table n → Execute Action Set → Packet Out

UMON: Monitoring Table → Subflow Tables → Application Threads

userspace

kernel

periodic update monitoring table with *kernel flow table* info

① Monitoring on **non-routing** fields
② **Subflow** monitoring

⑤ vPROM architecture

Routing ... ... vPROM applications

High-level Abstraction — Pyretic+ Runtime

Control Platform — **Ryu** Client / **Ryu** Controller Platform

OpenFlow Switches

UMON Switches

OpenFlow/OpenFlow+ Message

UMON UMON UMON UMON

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

UMON

UMON

Pyretic+ Controller

⑦ Evaluations

SYN Flooding attacks

137 — 1.97s
138 — 3.01s
143 — 2.40s
161 — 6.11s

150 200 250 300 350

21 — 2.91s
22 — 2.76s
23 — 2.69s
80 — 5.48s

550 600 650 700 750
Time (s)

Port scanning attacks

Vertical Detection

178.45.71.66 — 10.22s
178.45.66.41 — 8.10s
178.45.66.22 — 8.19s

0 50 100 150 200

Horizontal Detection

214.210.24.105 — 24.78s
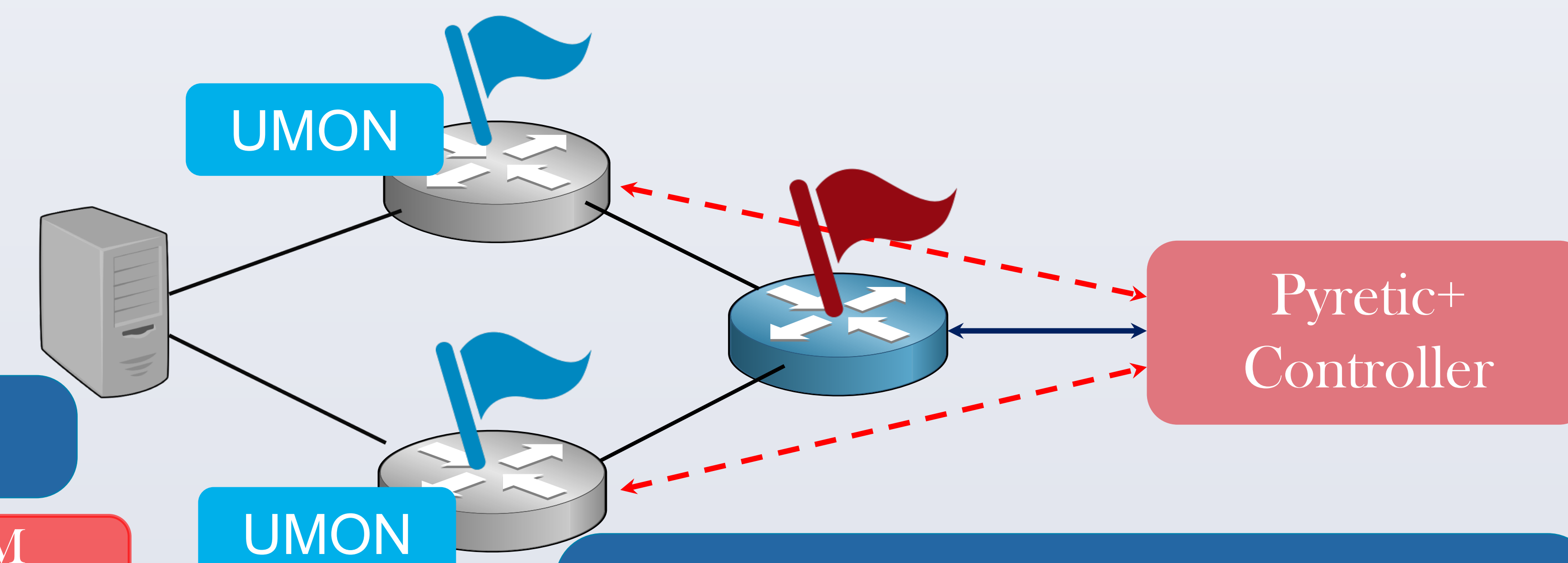
800 1000 1200 1400 1600 1800
Time (s)

⑧ Conclusions

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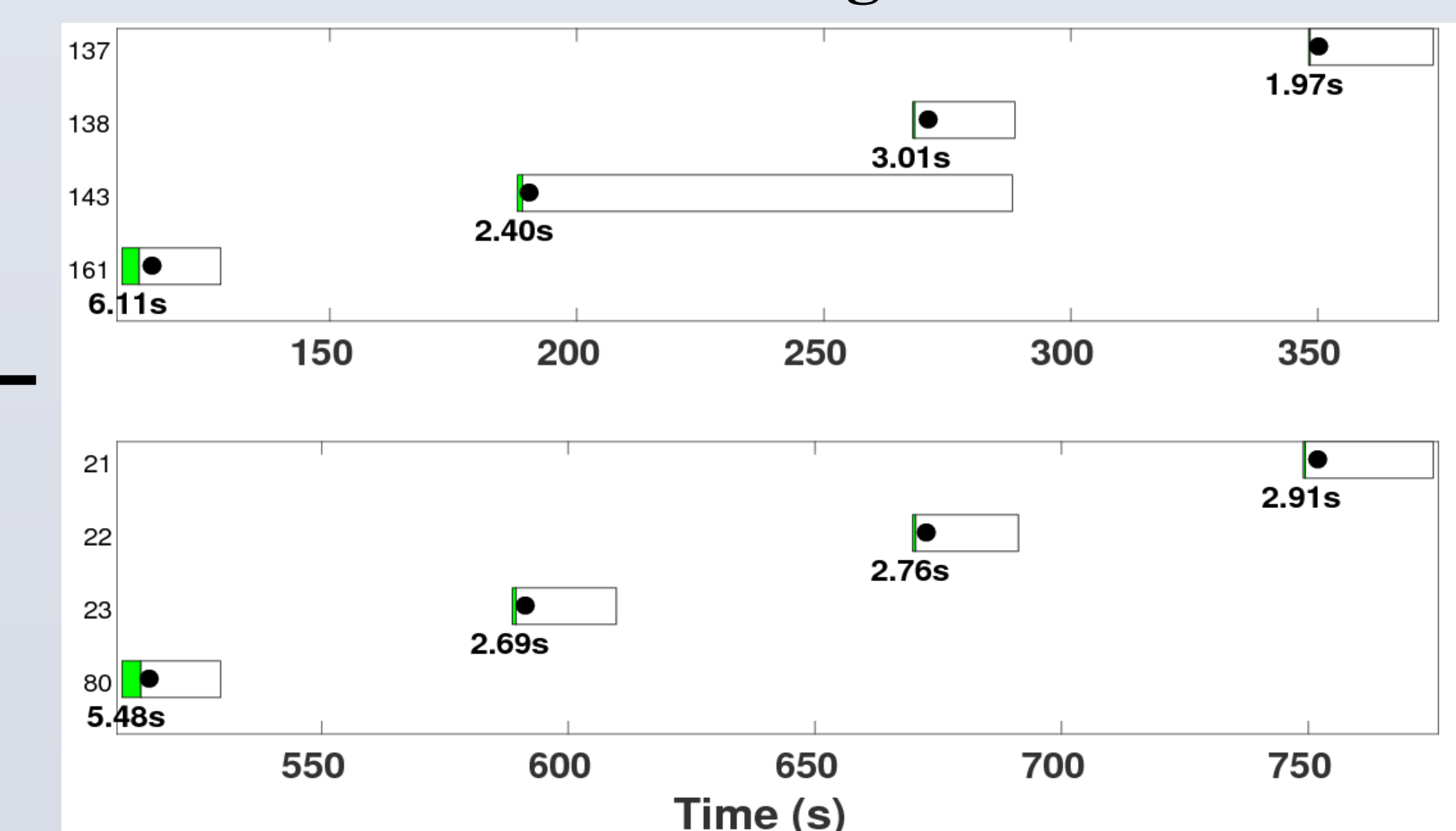- ❑ vPROM-GUARD detect **DDoS and port scanning attacks efficiently**