vPROM: vSwitch Enhanced Programmable Measurement In SDN

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


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
   - Packet In Table 0 Table 1 ... Table n Monitoring Table Packet Out
   - OpenFlow+
   - Monitoring Table: periodic update monitoring table with kernel flow table info
     1. Monitoring on non-routing fields
     2. Subflow monitoring

5. vPROM architecture
   - High-level Abstraction
     - Routing =⇒ vPROM applications
   - Control Platform
     - Ryu Client
     - Ryu Controller Platform
   - OpenFlow Switches
   - UMON Switches

6. Usecase: vPROM-GUARD
   - Flag Indicators: Potential Attacks
     - Big Flow + CUSUM: TCP SYN Flooding attack
     - 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