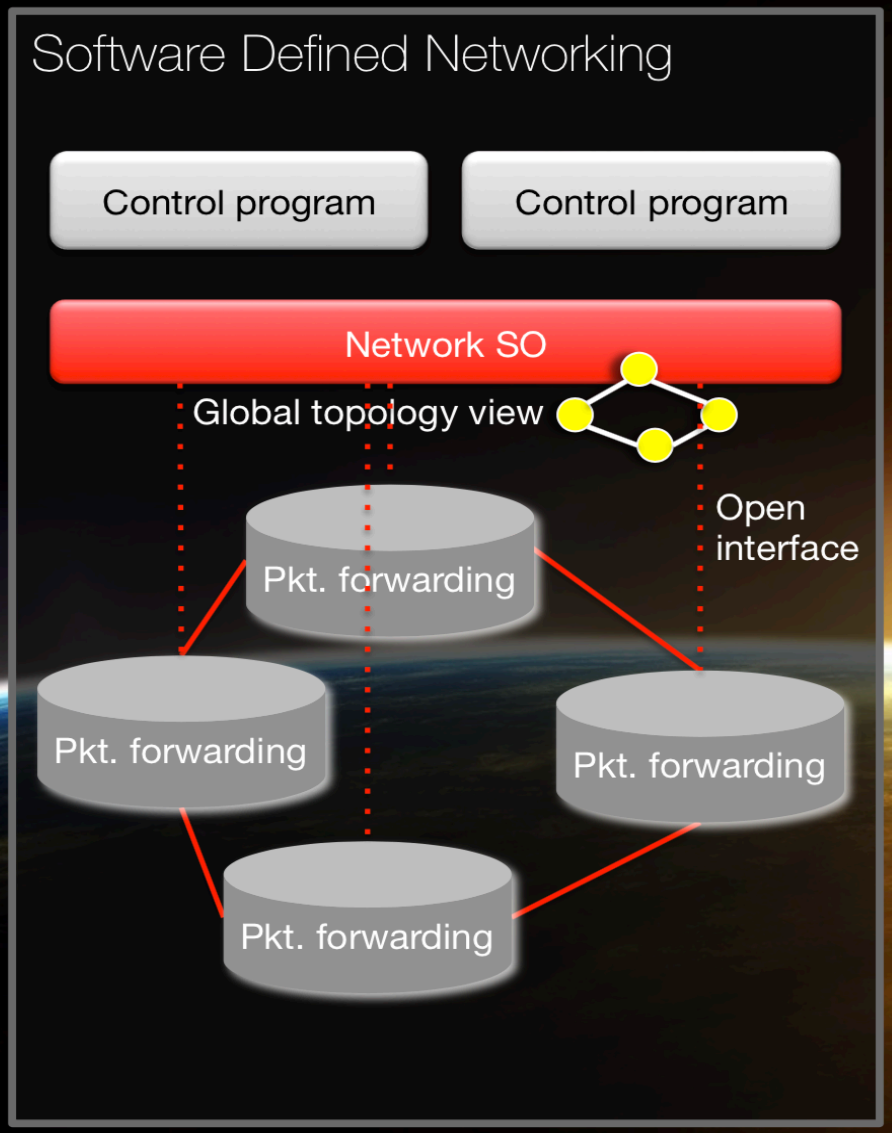
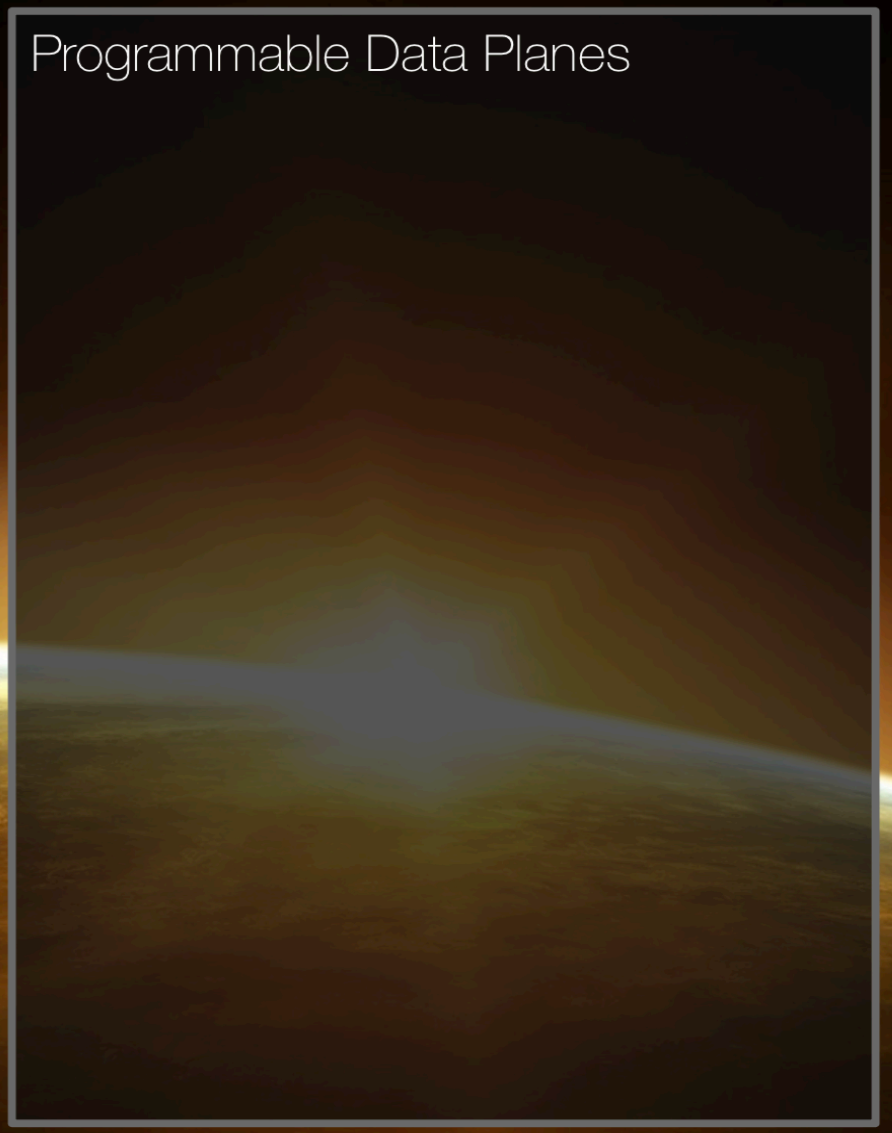
Securing Networks in the Programmable Data Plane Era

Luciano Gaspary
paschoal@inf.ufrgs.br
Instituto de Informática – UFRGS

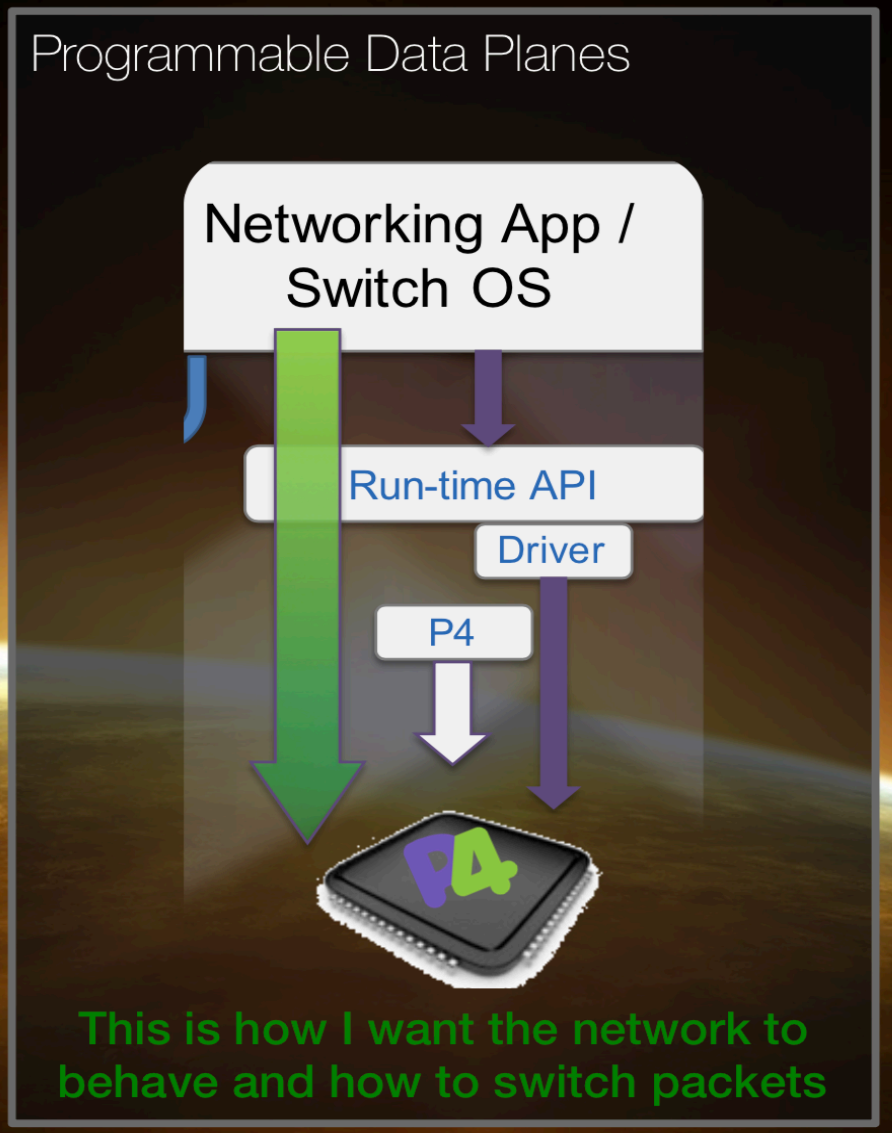
Securing Networks in the Programmable Data Plane Era

Network *softwarization*: the first wave





Network *softwarization*: the second wave



Source: https://github.com/p4lang/tutorials/blob/master/SIGCOMM_2016/p4-tutorial-slides.pdf

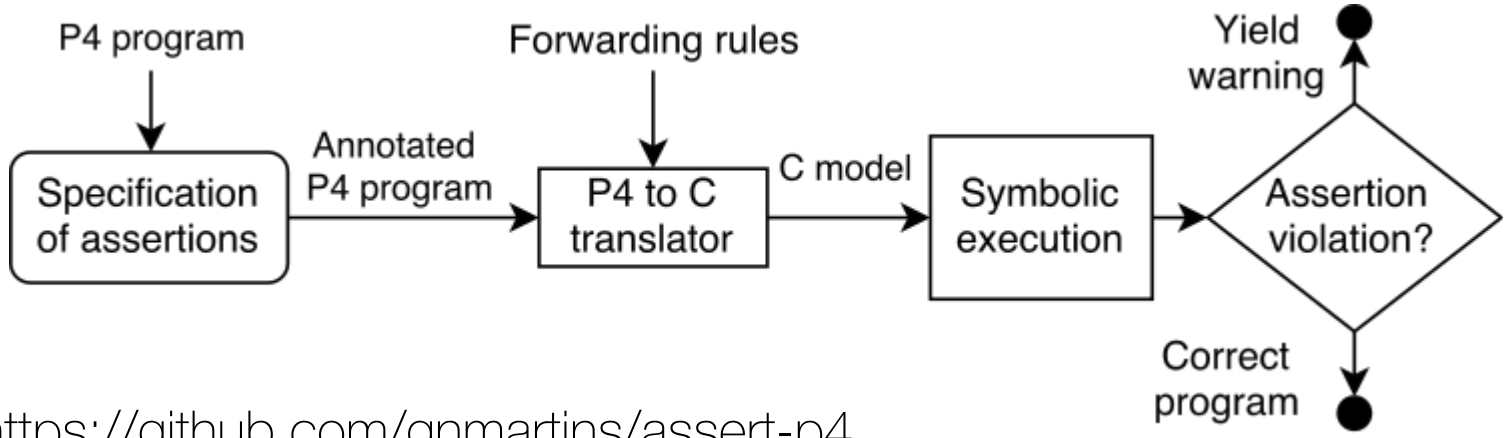
Problems and opportunities

- P4 programs are subject to bugs
  - Nonconformity with RFCs
  - Malformed packets
  - Use of uninitialized variables
- Correctness and security properties can be violated
- Existing tools are incapable of timely verifying P4 code
- We have an unprecedented opportunity to devise new security services

W. L. C. Cordeiro, J. A. Marques, L. P. Gaspary. **Data Plane Programmability Beyond OpenFlow: Opportunities and Challenges for Network and Service Operations and Management**. J. Netw. Syst. Manage., v. 25, n. 4, p. 784-818, 2017.

Assert-p4

- Efficient verification of programmable data planes
- Use of assertions and symbolic execution
- Capable of verifying properties in the order of seconds

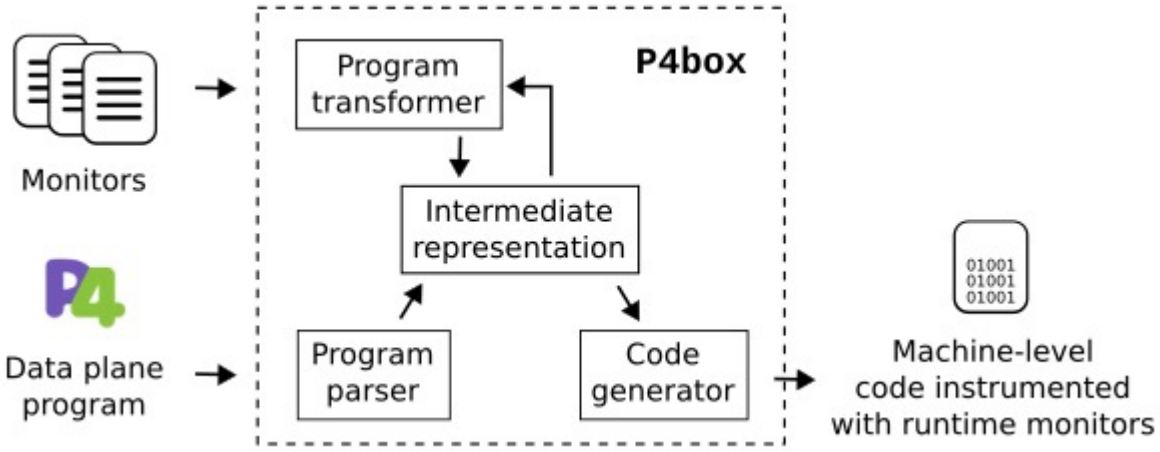


- https://github.com/gnmartins/assert-p4

M. Neves, A. Schaeffer-Filho, M. Barcellos. **Verification of P4 programs in feasible time using assertions**. ACM CoNEXT 2018.

P4box

- P4 program monitor (guarantees properties at runtime)
- Useful for cases where verification is impracticable
- Instrumentation of P4 programs during compilation
- Low networking device overhead



- https://github.com/mcnevesinf/p4box

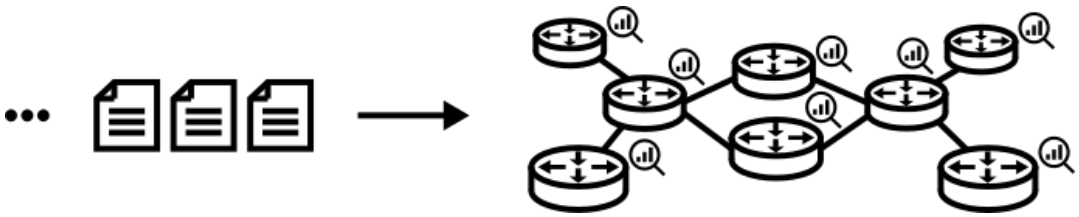
M. Neves, B. Huffaker, K. Levchenko, M. Barcellos. **Dynamic property enforcement in programmable data planes**. IFIP NETWORKING 2019. (*To appear*) (**3rd prize of the ACM SIGCOMM student research competition 2017**)

Offloading anomaly detection to P4

Packet Processing Programming Language

- Protocol independent
- Target independent
- Field reconfigurable

In-network monitoring program



Fine-grained measurements

Real-time inspection

Challenges: line rate execution (programmable hardware switch)

Time budget: ~ dozens of nanoseconds per packet

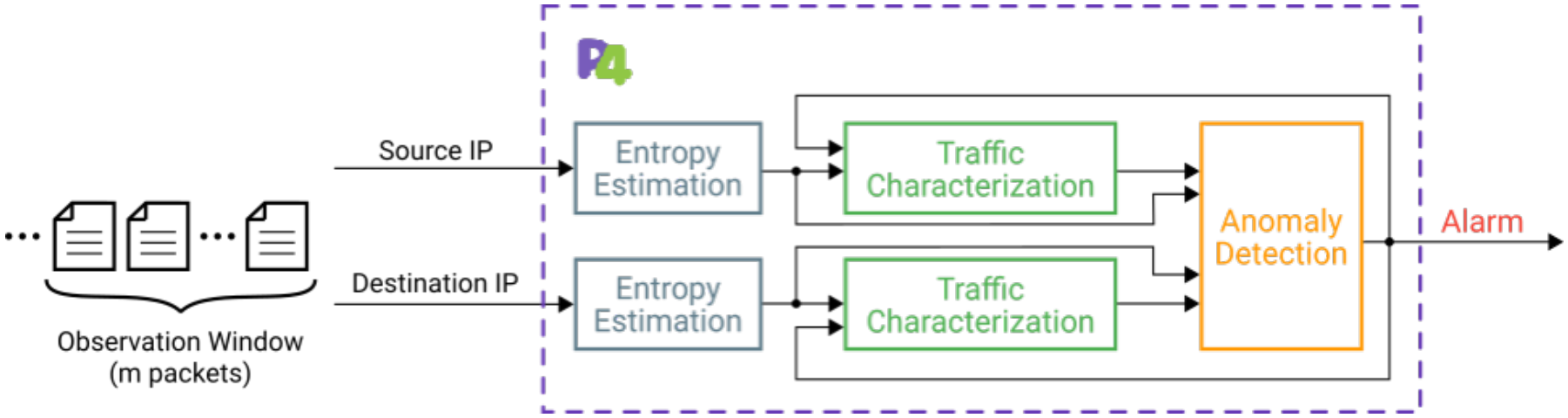
Memory space: ~50 MB SRAM, ~ 5 MB TCAM

Limited programming primitives
Elementary arithmetic
Table lookups

How to overcome such challenges to reap the benefits of an in-network, programmable design?

A. Lapolli, J. A. Marques, L. P. Gaspary. Offloading real-time DDoS attack detection to programmable data planes. IFIP/IEEE IM 2019. (Best student paper award)

Offloading anomaly detection to P4

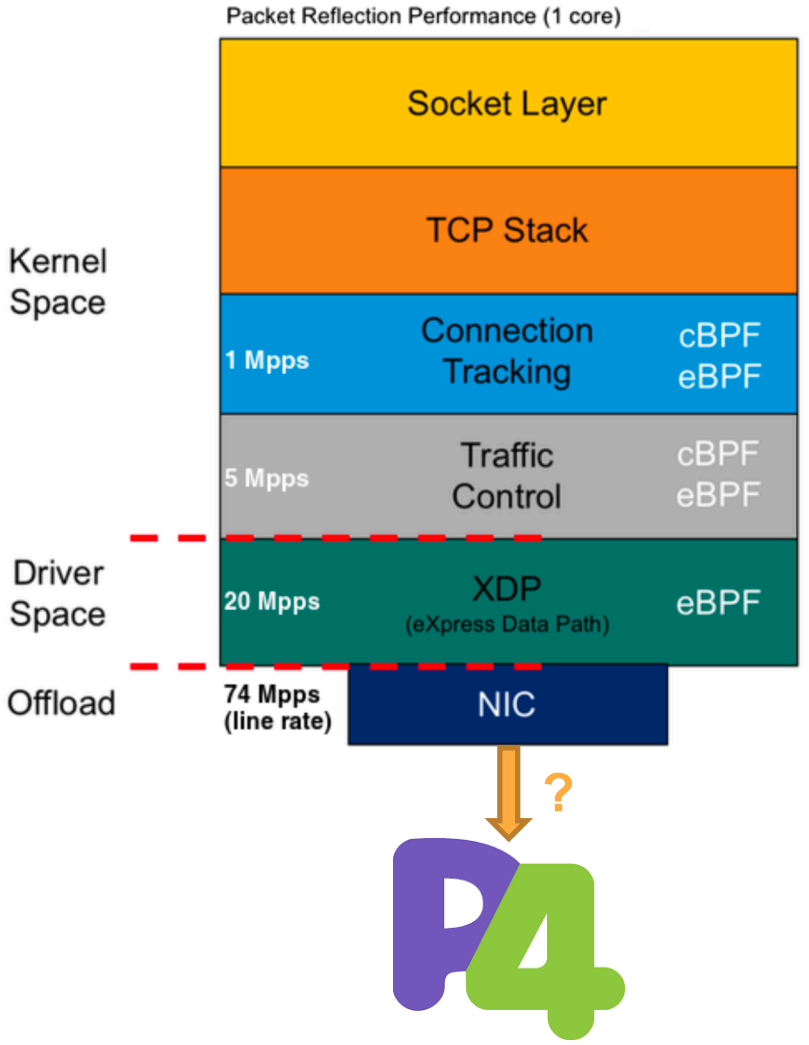


- Entropy estimation over observation windows
- Real-time traffic characterization based on the entropy values of the legitimate traffic
- In-network anomaly detection
- https://github.com/aclapolli/ddosd-p4

A. Lapolli, J. A. Marques, L. P. Gaspary. **Offloading real-time DDoS attack detection to programmable data planes**. IFIP/IEEE IM 2019. (**Best student paper award**)

Ongoing/future work

- Offloading traffic filters to programmable switches for a more efficient strategy to triage the packets submitted to Zeek (Bro)
- Proposal of more sophisticated reasoning mechanisms (ML-based) for intrusion detection
- Proposal of attack mitigation mechanisms



Thank you ;-)

Luciano Gaspary
paschoal@inf.ufrgs.br
Instituto de Informática – UFRGS