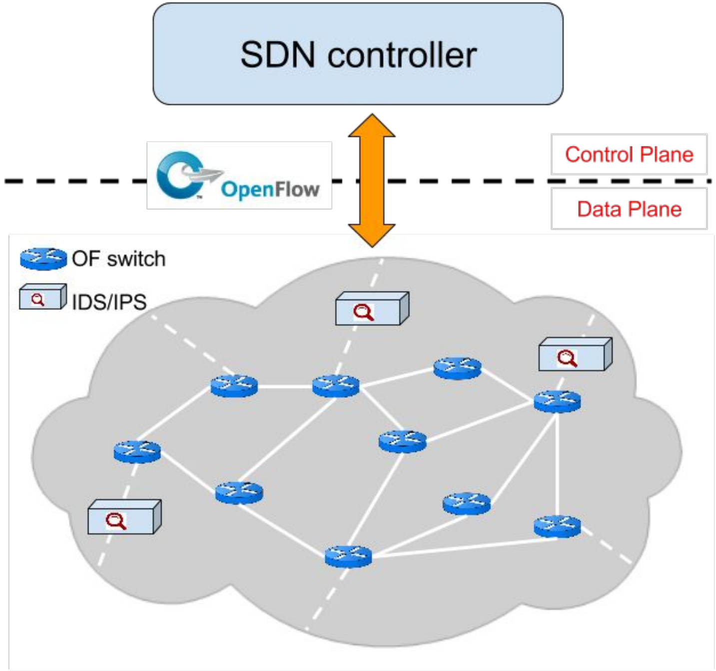
Piggybacking Network Functions on SDN Reactive Routing: A Feasibility Study

Chang Liu, Arun Raghuramu, Chen-Nee Chuah
(UC Davis)

Balachander Krishnamurthy
(AT&T Labs-Research)

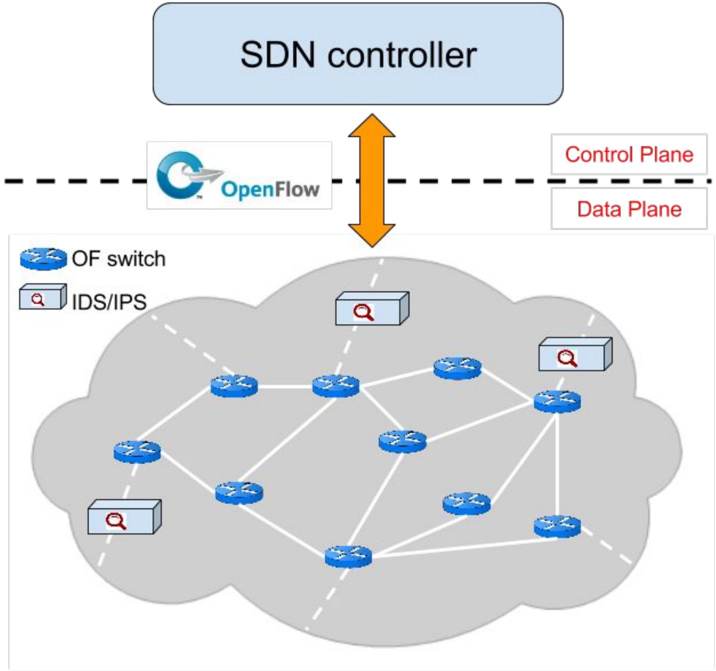
Background and Motivation

- Software-defined Networking (SDN): choice for future networks
- Can we leverage SDN to enhance network security functions?
    - Previous works focus on statistics-based anomaly detection (port scanning, DoS)
    - Can we offload signature-based threat detection to SDN controller/switches?



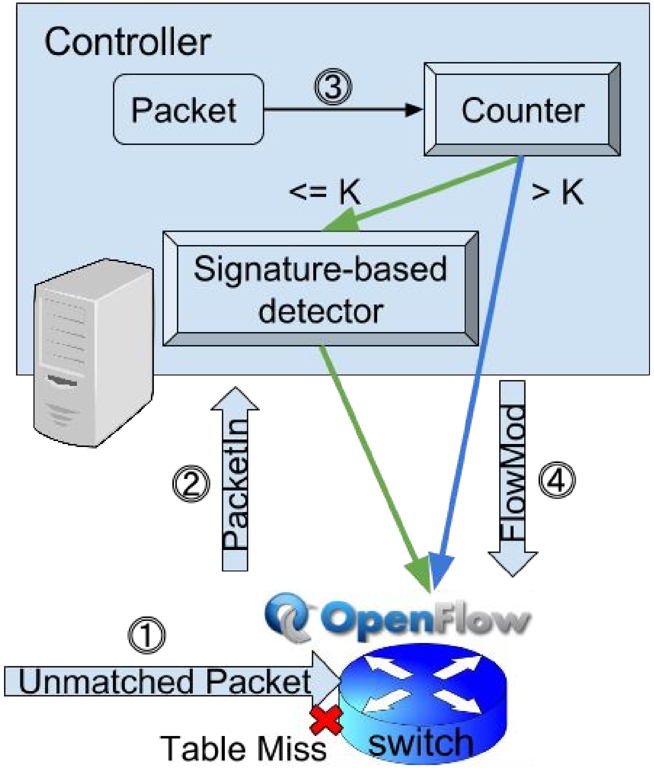
Potential Benefits

- Earlier/faster detection & mitigation
  - Dynamically update flow rules at the data plane to block a malicious flow
- Relieve load on traditional IDS/IPS
- Provide intrusion detection for traffic missed by IDS/IPS middleboxes
- Utilize global view of SDN controller to detect threats not seen by a local vantage point



SDN-Defense

- Piggybacking on reactive routing
  - The first packet of a new flow is sent to the controller for forwarding decisions
  - Inspect the first packet:
    - IP firewall
- Selective K packets inspection at controller
  - Delay installation of forwarding rules
  - Inspect first K packets of a flow at the controller site
  - K is a design parameter tunable by the SDN controller



Feasibility Study: Campus WiFi Traffic

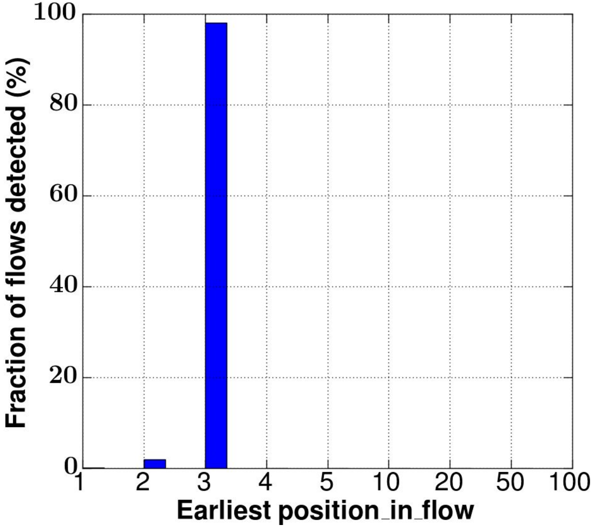
- Traffic
  - Collected on 05/30/2014
  - 296GB, 10.67hours
  - 269M packets, 5M flows
- A TCP flow is uniquely identified by a unidirectional 5-tuple

- Alerts (running traffic against Snort)
  - 1770 TCP alerts
  - 44 rules (Signature IDs)
  - 1145 malicious flows
- Top 4 most-frequently-triggered rules detect more than 75% of the malicious flows

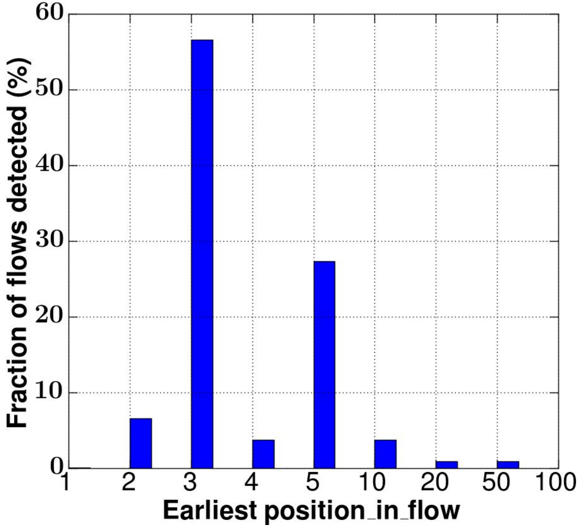
- *Earliest position in flow*
  - The earliest packet position in a TCP flow that triggers a specific security alert
  - Counted within unidirectional traffic of a flow

Feasibility Study: Which packet triggers an alert?

- SID: 24111
  - Most frequently occurring rule
  - 44.2% of malicious flows caught by this rule
  - Match against the http header of a packet
- 100% of malicious flows could be detected within the first 3 packets



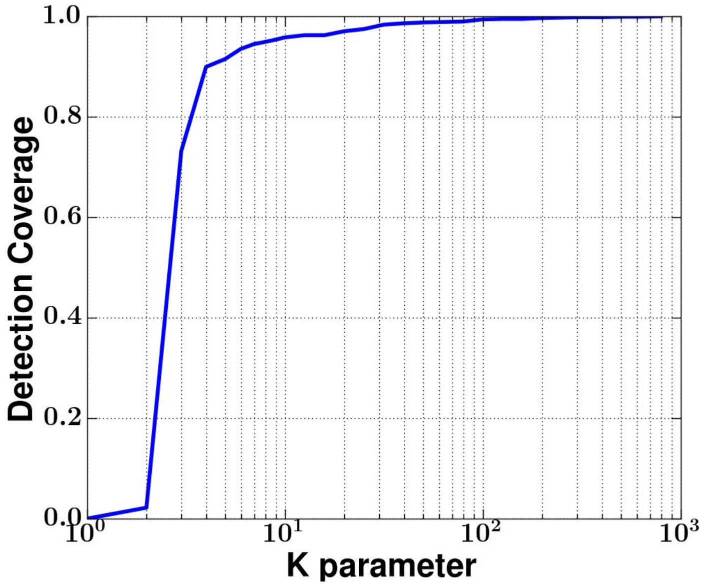
- SID: 16301
  - 2nd most frequently occurring rule
  - 18.2% of malicious flows caught by this rule
  - Match against payload
- 60% of malicious flows could be detected within the first 3 packets



Feasibility Study: Which packet triggers an alert?

- Detectability vs K
  - *Detection coverage*: fraction of the number of malicious flows detected within the first K packets over the total number of malicious flows
  - K: number of packets per flow examined

- 73% of malicious flows are detected within the first 3 packets
- 90% of malicious flows are detected within the first 4 packets



Fraction of flows detected within first K packets

Cost Analysis

- Vanilla SDN reactive routing (SDN-RR)
- SDN-Defense with varying parameters
    - K: number of packets per flow examined
    - M_i: subset of rules offloaded to the SDN controller

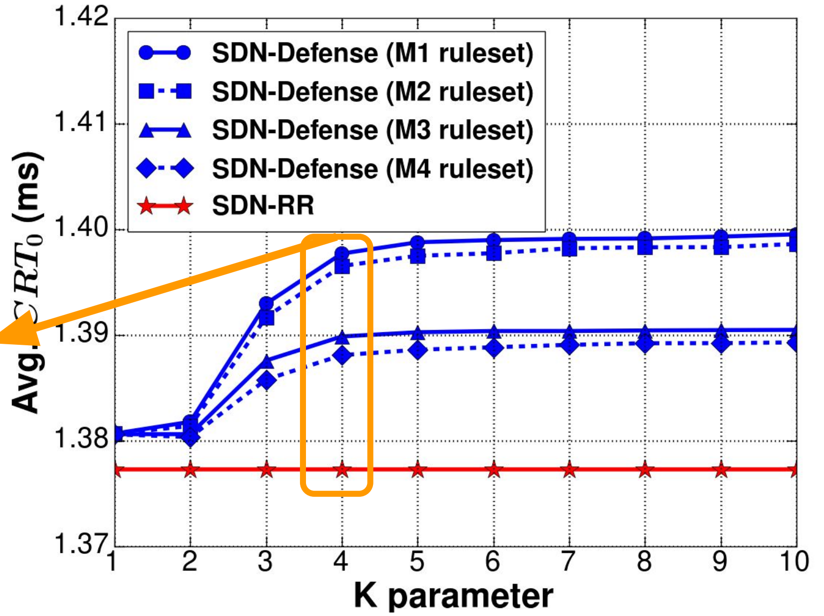
M_i	Description	$\|M_i\|$	%Coverage*
M_1	All Snort 2.9.8.3 rules	12.3k	100
M_2	Highest priority rules	11k	89.9
M_3	Rules scanning http headers	1750	79.7
M_4	Rules triggered by WiFi traffic	53	100

*: the percentage of malicious flows detected by a given rule subset.

Cost Analysis: Controller Response Time

- Metric: zero-load controller response time (CRT_0)
  - Controller's processing time for handling a single PacketIn message at minimum load

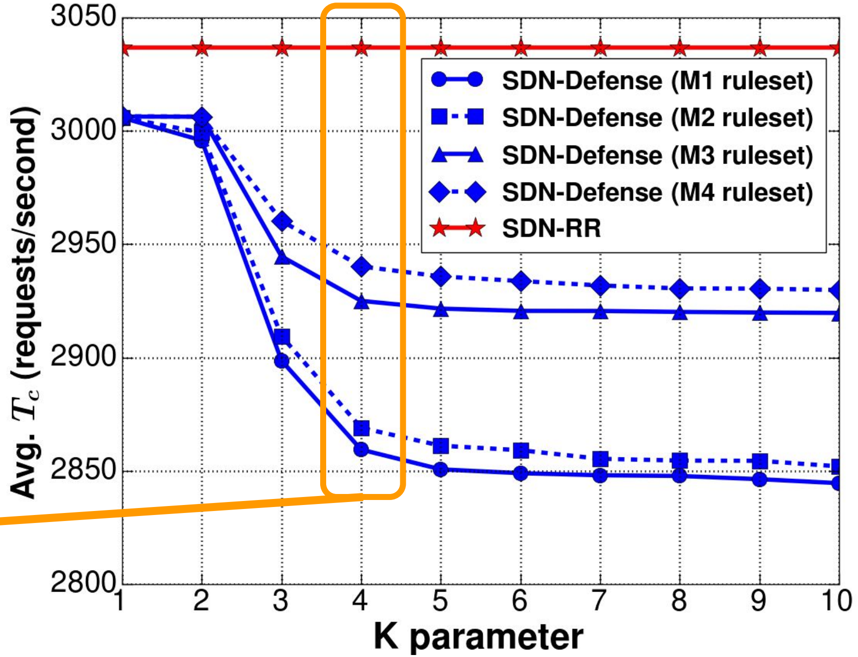
- CRT_0 increases as K increases
- SDN-Defense introduces
  - 1.5% CRT_0 overhead, while achieving up to 90% detection coverage with M_1 ruleset offload
  - ~0.94% CRT_0 overhead and up to 78% detection coverage with M3 ruleset offload.



Cost Analysis: Controller Throughput

- Metric: controller throughput (T_c)
  - The maximum number of requests the controller can handle per unit time

- The throughput decreases as K increases
- SDN-Defense introduces
  - 5.8% throughput drop, while achieving up to 90% detection coverage with M_1 ruleset offload
  - 3.6% throughput drop and up to 78% detection coverage with M3 ruleset offload.



Discussion

- The framework is not limited to security applications. Other potential applications include:
    - Traffic classification
        - Early application identification with high accuracy using only the first four or five packets
        - Network administrators gain immediate visibility into the traffic and react to changes via dynamically managing the data plane.
    - Traffic dispersion graph (TDG) generation
        - Answer questions about “Who talks to whom” utilizing the first flow packets available via reactive routing
        - Comprehensive picture of the network leveraging SDN controller’s global view

Discussion & Future Work

- Motivation of piggybacking on reactive routing:
  - Access to initial packets @ the controller site
- Reactive routing is not scalable
  - The SDN controller becomes the bottleneck under large traffic load
  - Introduce additional end-to-end latency due to the switch-controller-switch loop
- Alternative solutions:
  - Packet mirroring*
  - Programmable switches with P4 support
  - Sampling flows to accommodate large traffic load
- Future Work:
  - Explore potential of P4-enabled switches to solve scalability issues

*:Y. Wang, C. Orapinpatipat, H. Gharakheili, et al. Telescope: Flow-level video telemetry using sdn. In Proc. of EWSDN, The Hague, Netherlands, 2016.

Thank You!