\Orchestrating a brighter world NEC

Fingerprinting Software-defined Networks

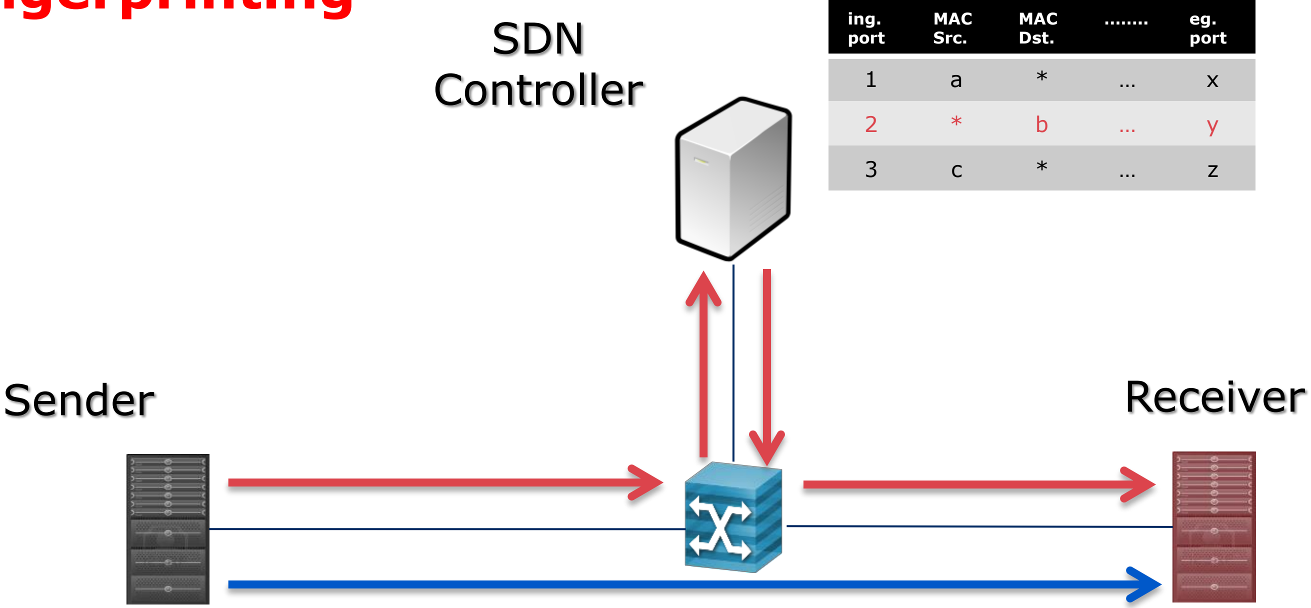
Roberto Bifulco, Heng Cui, Ghassan Karame, Felix Klaedtke
NEC Laboratories Europe, Heidelberg, Germany

CoolSDN 2015, ICNP

Introduction

- Software-defined networking (SDN):
  - Separates data plane from control plane.
  - Software controls the network.
- Packet processing
  - **Fast** at data plane (hardware)
  - **Slow** at control plane (software)
- An attacker can measure packet processing times

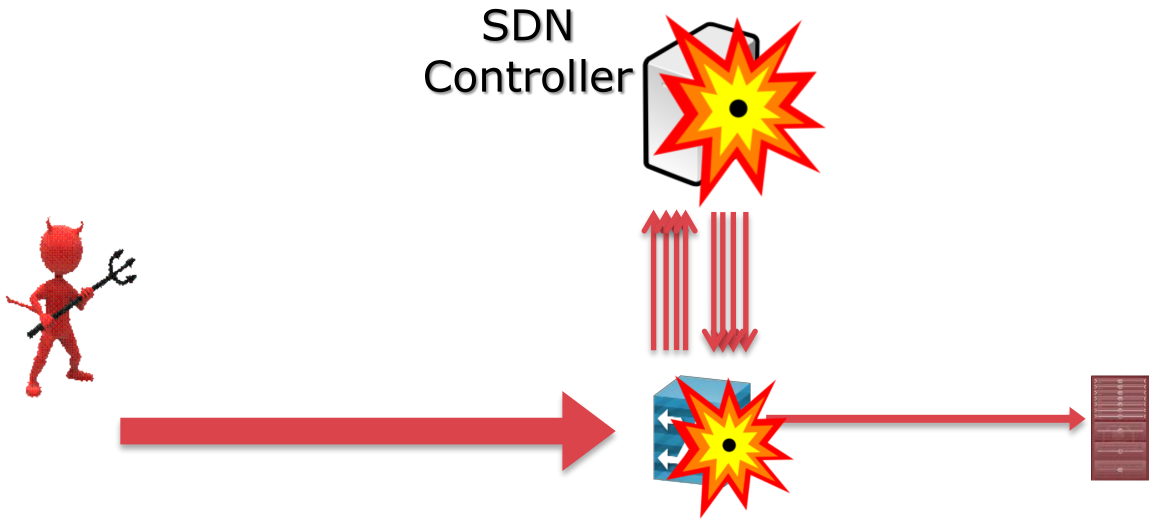
  → **Fingerprinting**



ing. port	MAC Src.	MAC Dst.	....	eg. port
1	a	*	...	x
2	*	b	...	y
3	c	*	...	z

Introduction (cont.)

- Knowing controller-switch interaction:
  - Better understanding of the network's forwarding logic.
  - Makes DoS attacks more powerful/effective.



- No feasibility study of fingerprint **realistic** SDN deployments.

Problem Statement

- Feasibility of fingerprinting an SDN network?
- Accuracy of fingerprinting an SDN network?
- Impact of number of switches in an SDN network?
- Attack models:

Active

- Compromise a remote client.
- Inject probe packets.

Passive

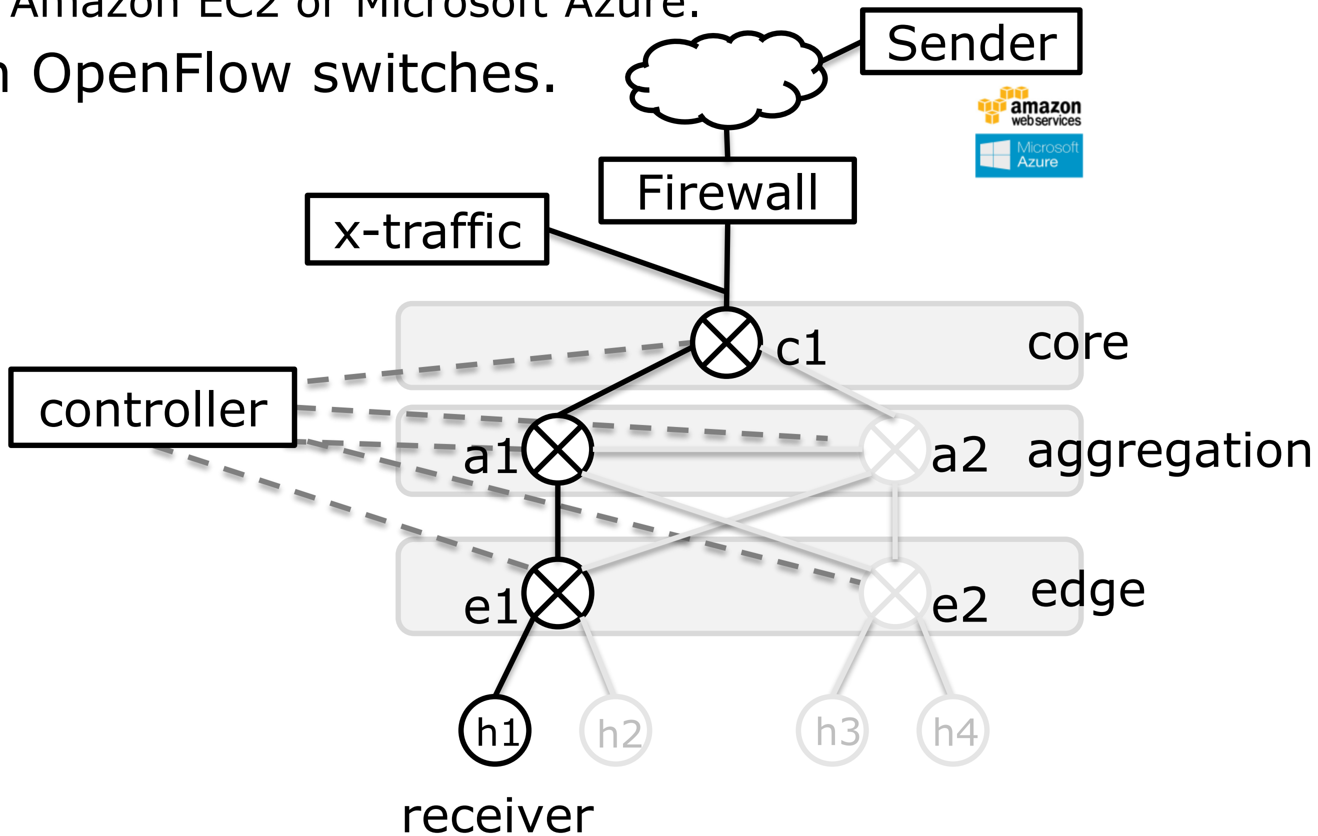
- Passively monitor traffic between client and server.

Roadmap

- Part I
  - Introduction and Motivation
  - Problem Statement
- Part II
  - Testbed
  - Measured Features
  - Results
- Part III
  - Related Works
  - Conclusions

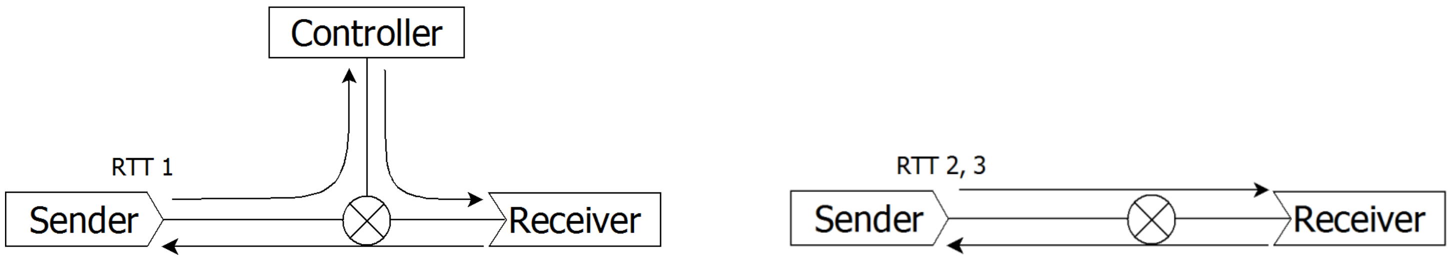
Testbed

- Three NEC PF5240 OpenFlow switches
  - Conventional data center typically consists of 3-tier switches.
- Floodlight controller.
- Probe: internet → firewall → OpenFlow switches → receiver.
  - Probe sender at Amazon EC2 or Microsoft Azure.
- Cross-traffic in OpenFlow switches.



Measured Feature: Round Trip Time (RTT)

- Compute δ_{RTT} based on two RTT measurements:
  - $\delta_{RTT} = RTT_1 - RTT_2$ is mainly dominated by controller-switch interaction delay.
  - $\delta'_{RTT} = RTT_2 - RTT_3$ represents delay variances along the network path.

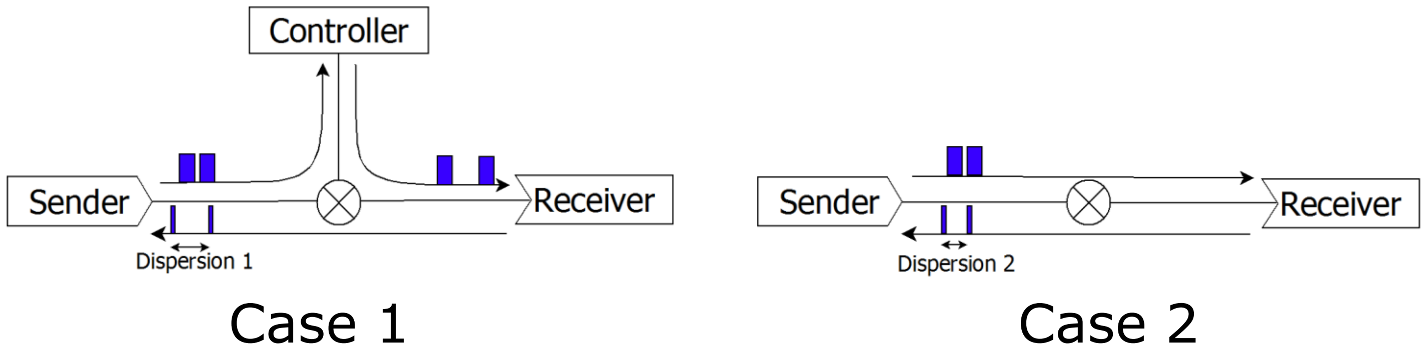


Case 1   Case 2

- Active/Passive attacker.

Measured Feature: Dispersion

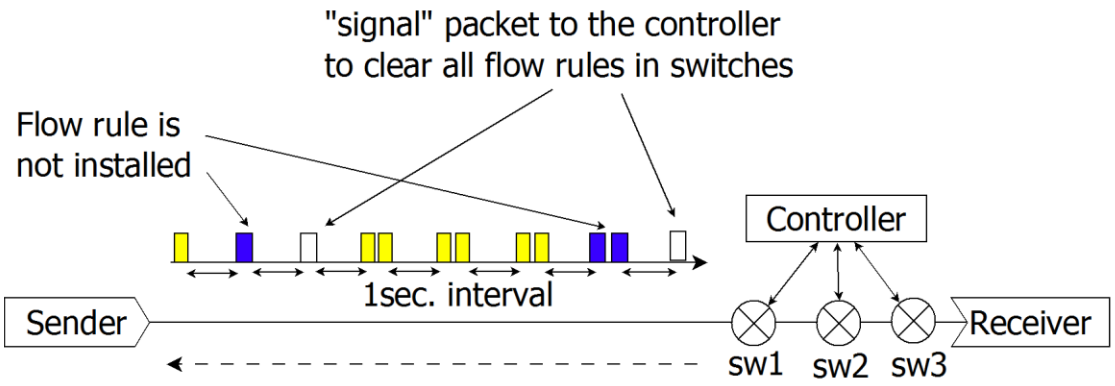
- Dispersion in case 1:
  - Limited by the delay of the controller-switch interaction.
  - Typically in the order of milliseconds.
- Dispersion in case 2:
  - Represents the network bottleneck bandwidth.
  - Typically in the order or microseconds.



- Active attacker.

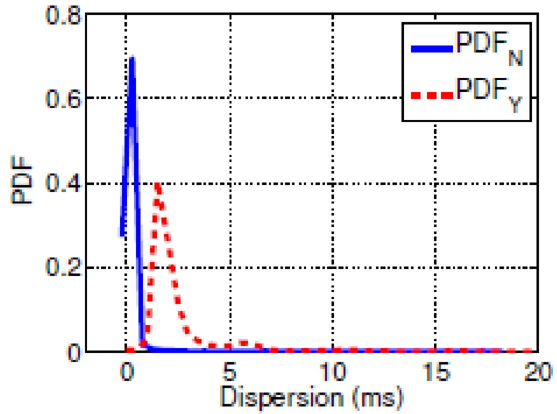
Conducted Experiment

- 20 machines around the globe.
  - Probing spanning two weeks.
- UDP probe packets (echoed by receiver).
- Use a pre-defined type of packet as “signal” to controller to clear flow rules.
- Reconfigure number of switches which are involved in the controller/switch interaction (k=1,2,3).
  - By installing static forwarding rule to the rest of switches.

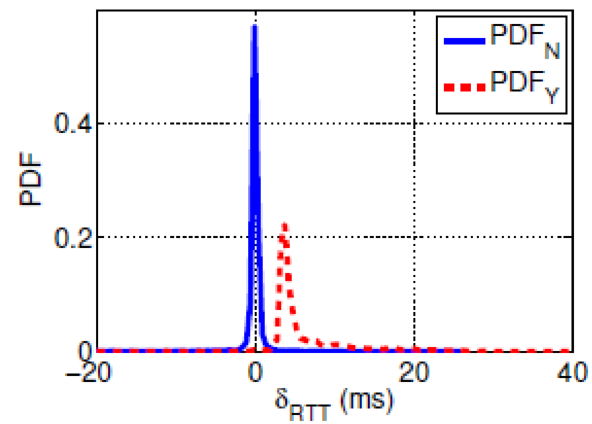


Measurement Results in PDF

- PDF_Y: probe triggers rule installation (red).
- PDF_N: no rule installation is performed (blue).
- Distributions of PDF_Y and PDF_N significantly differ.



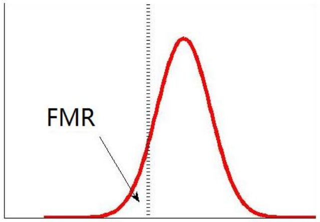
(c) $k = 1$

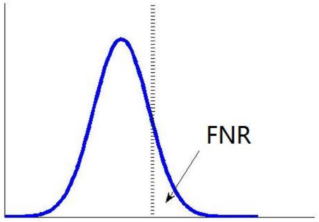


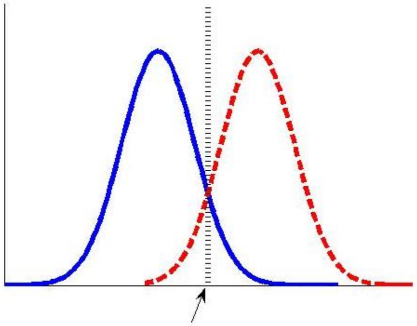
(c) $k = 1$, time span 1 second

Quantitative Interpretation of Results

- False Match Rate (FMR)
  - Decision: no rule was installed
  - In reality: there is a rule installation.
- False Non-match Rate (FNR)
  - Decision: a new rule was installed.
  - In reality: no rule was installed.
- Equal Error Rate (EER)
  - Error rate at which both FMR and FNR are equal.
  - Widely accepted as a single metric for the accuracy of an identification system.







			$k=1$	$k=2$	$k=3$
Packet-pair Dispersion		EER	1.59%	1.46%	1.46%
		Threshold	1.07 ms	1.42 ms	1.45 ms
δ_{RTT}	1 second	EER	2.64%	1.26%	1.27%
		Threshold	2.20 ms	4.67 ms	5.71 ms
	10 minutes	EER	7.50%	5.00%	2.50%
		Threshold	3.23 ms	3.99 ms	7.62 ms
	3 weeks	EER	19.17%	11.83%	10.83%
		Threshold	0.99 ms	3.65 ms	3.74 ms

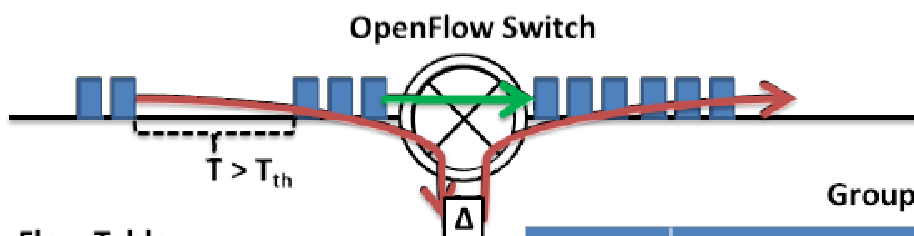
Implications

- Fingerprinting an SDN network is feasible.
  - Dispersion:
    - stable over time
  - δRTT:
    - can be extracted by passive measurement

- Our setting emulates a case which is hard to fingerprint:
  - Controller CPU was idle most of the time.
  - Pre-computed logic to issue forwarding decision.
  - Our hardware switches are among the fastest ones on the market.

Countermeasure

- Delay each packet at a switch before forwarding.
  - Harms network performance
- Delay the first few packets of old flows.
  - Minor impact on network performance.
  - The amount of delay can be determined from our observations.
  - Obscure attacker whether additional delay is caused by controller-switch interaction or by delay element Δ.



Flow Table

Match set	Action set
Destination IP = 1.2.3.4	Group(3)
*	To Controller
...	...

Group Table

Group Identifier	Buckets	
	Description	Action set
3	Active flows bucket	Forward to port 2
	Inactive flows bucket	Delay and forward to port 2
	...	...

Related Work

- Prior work hints at the possibility of fingerprinting an SDN network [ShinHotsdn13].
  - We provide two possible features.
  - We demonstrate the feasibility of fingerprinting SDN networks.
- Other related works on network fingerprint/characterization.
  - RTT is relatively stable in backbone networks [MarkopoulouComComm06].
  - Residential network features (RTT, dispersion) mainly depend on “last-mile hops” [DischingerIMC07].
  - Dispersion is widely used in bandwidth estimation.
    - Available bandwidth or bottleneck bandwidth along the path.

Conclusion

- It is feasible to fingerprint SDN networks.
  - Overwhelming probability of predicting controller-switch interactions.
  - Feasible for both active and passive attackers.
    - \+ Active probing has more stable accuracy
- *but* can be deterred by anomaly detection systems.
    - \- Passive measurement accuracy depends on network conditions
+ *but* passively measuring the network traffic is hard to detect.
- Countermeasure against fingerprinting.
  - Evaluation of the effectiveness is current work.

Thank you

&&

Questions

\Orchestrating a brighter world

NEC