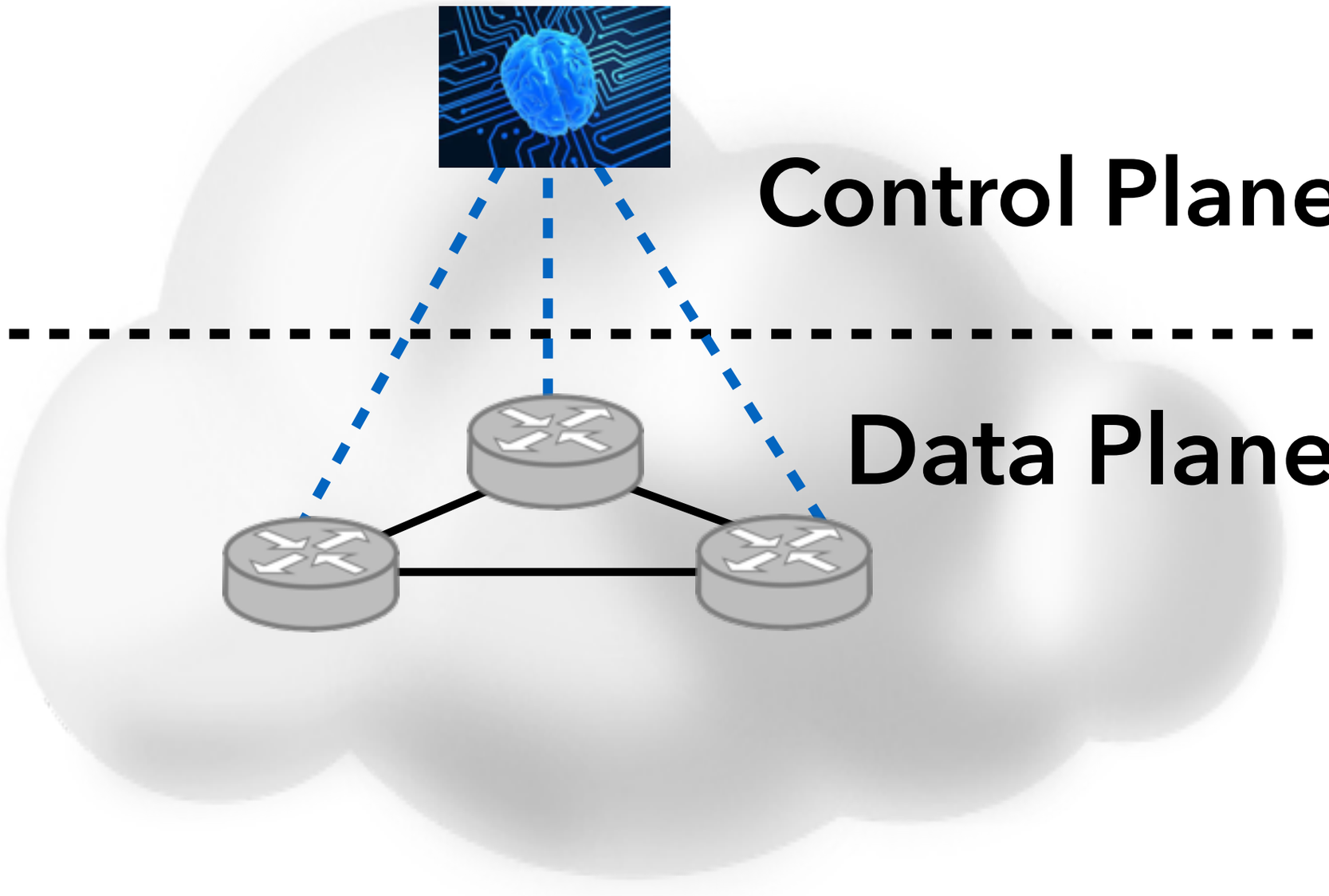
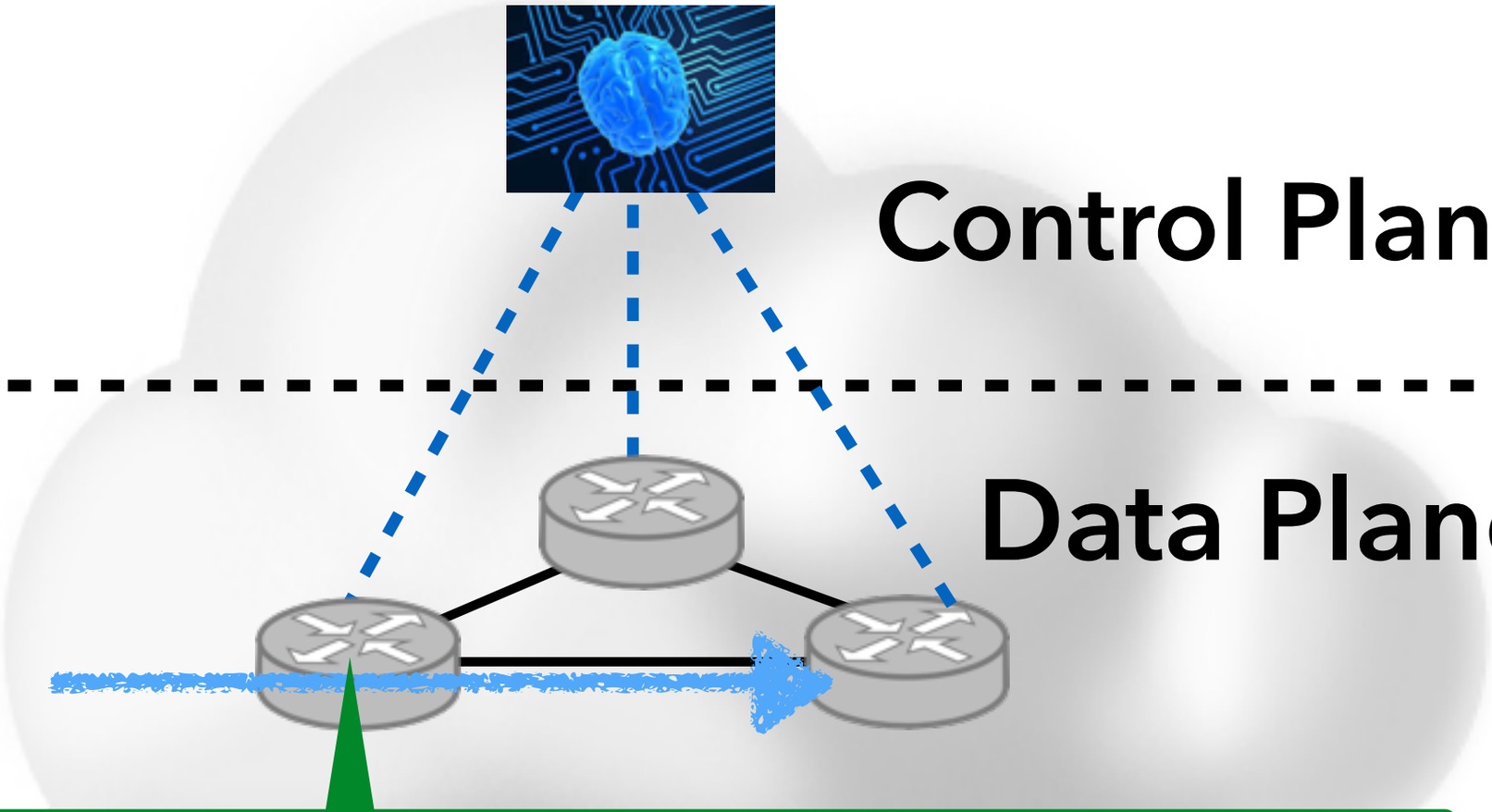
Timing-based Reconnaissance and Defense in Software-defined Networks

John Sonchack, *Anurag Dubey,*
Adam J. Aviv, Jonathan M. Smith, and Eric Keller

Software Defined Networks (SDNs)



Software Defined Networks (SDNs)

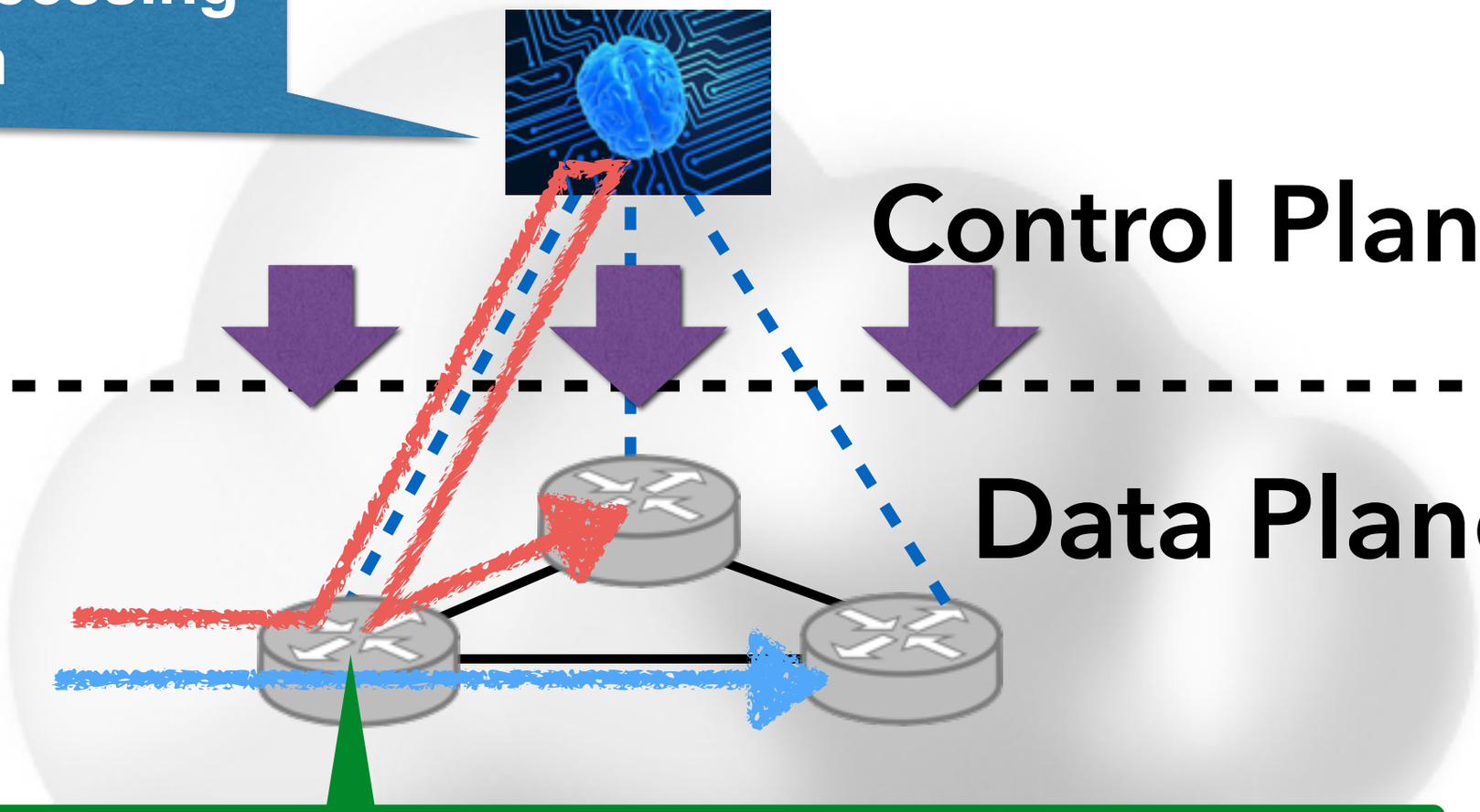


Fast, flow-based packet forwarding

MAC Src	MAC Dst	IP Src	IP Dst	…	Timeout	action
00:…:00:06	00:…:00:01	*	*	…	1	Out 1
*	*	*	*	*	-	Control

Software Defined Networks (SDNs)

Complex packet processing
New flow installation



Fast, flow-based packet forwarding

MAC Src	MAC Dst	IP Src	IP Dst	…	Timeout	action
00:…:00:06	00:…:00:01	*	*	…	1	Out 1
00:…:00:03	00:…:00:02	*	*	…	1	Out 2
*	*	*	*	*	-	Control

Software Defined Networks (SDNs)

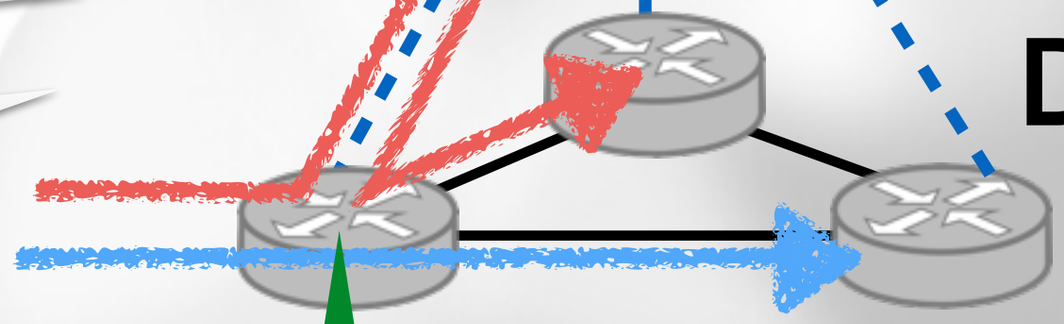
Complex packet processing
New flow installation

Control Plane

Access Control

Dynamic Routing

Monitoring

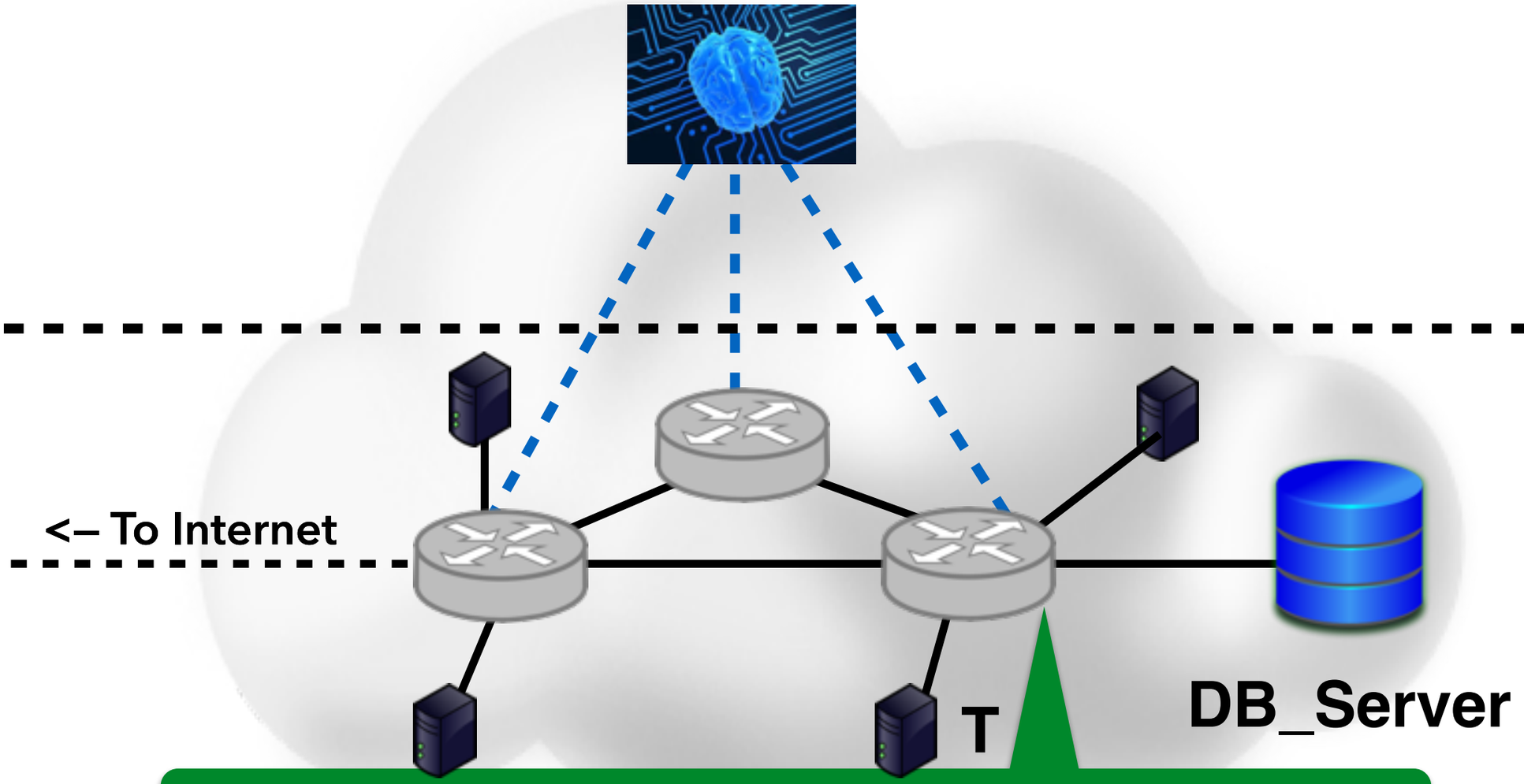


Data Plane

Fast, flow-based packet forwarding

MAC Src	MAC Dst	IP Src	IP Dst	…	Timeout	action
00:…:00:06	00:…:00:01	*	*	…	1	Out 1
00:…:00:03	00:…:00:02	*	*	…	1	Out 2
*	*	*	*	*	-	Control

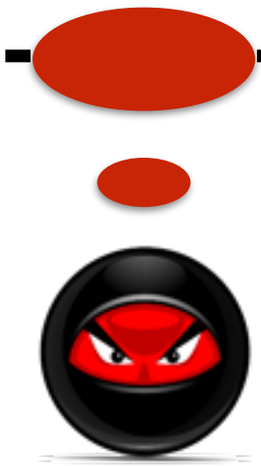
SDN Flow Tables Reveal Sensitive Information

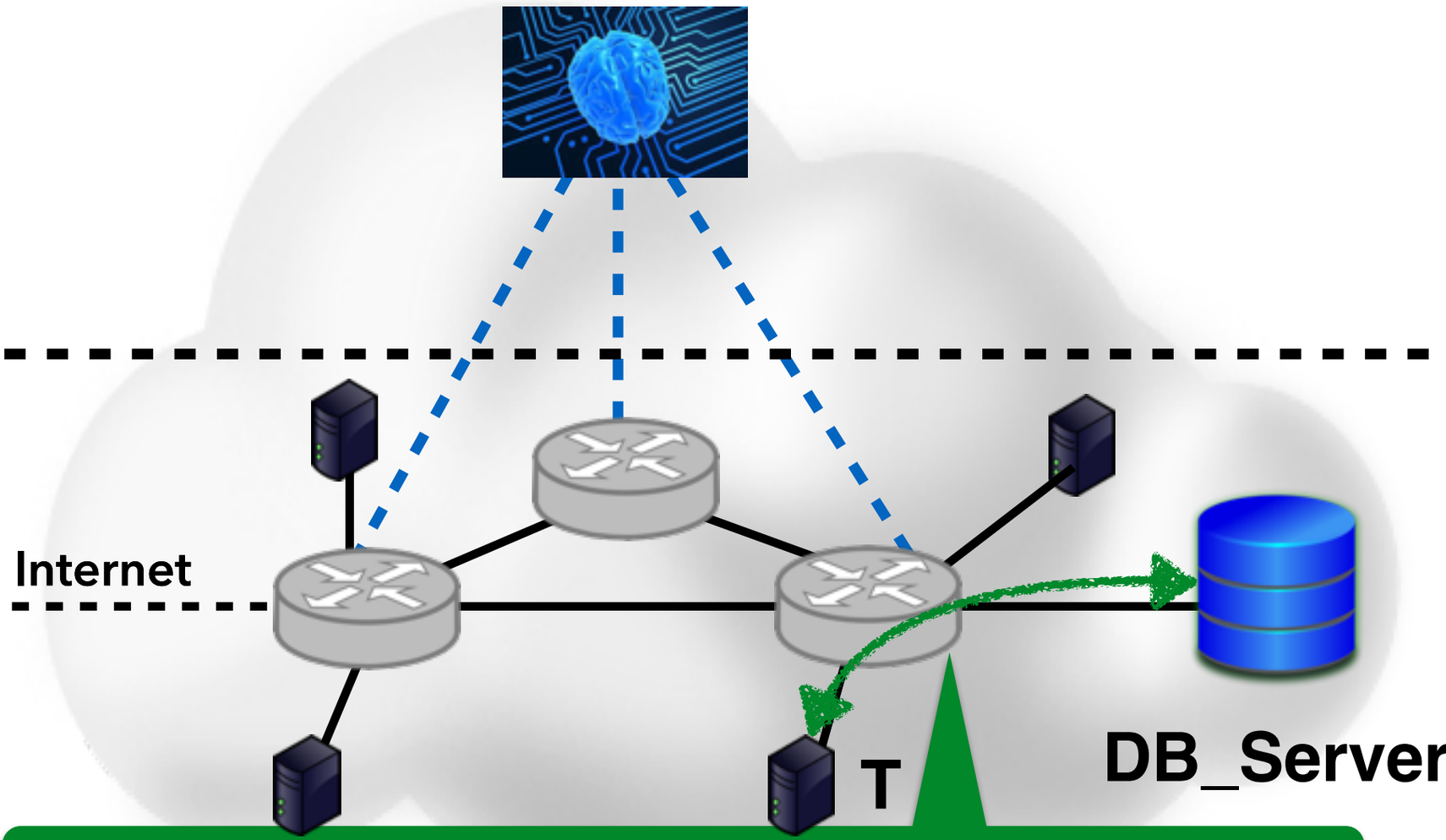


IP Src	IP Dst	…	Timeout	Action
T	DB_Server		1	ALLOW
*	DB_Server		1	DROP
DB_Server	*			ALLOW
*	*	…	-	Controller

SDN Flow Tables Reveal Sensitive Information

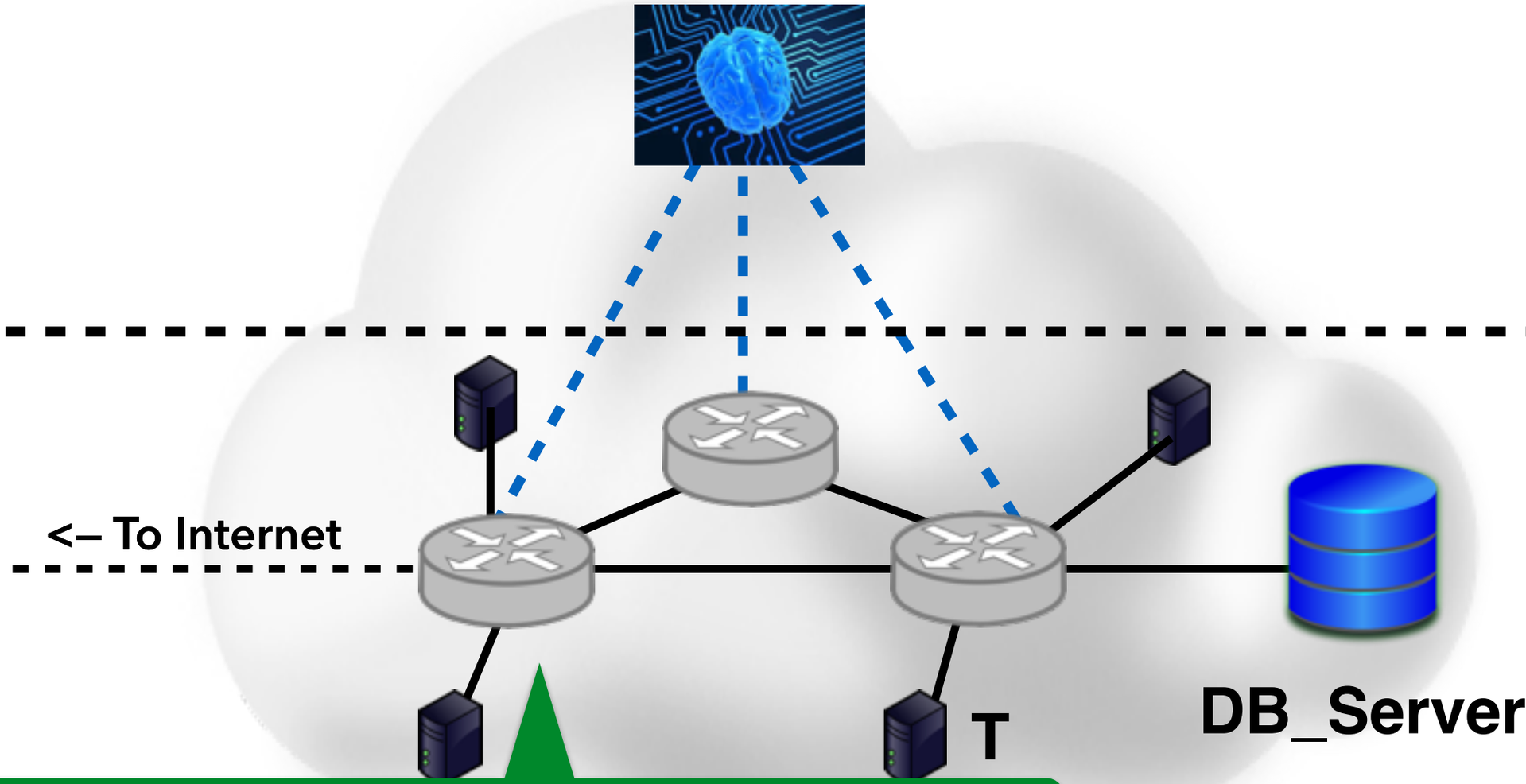
DB_Server exists, and only T can communicate with it.





IP Src	IP Dst	...	Timeout	Action
T	DB_Server		1	ALLOW
*	DB_Server		1	DROP
DB_Server	*			ALLOW
*	*	...	-	Controller

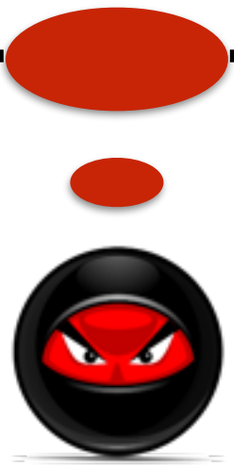
SDN Flow Tables Reveal Sensitive Information

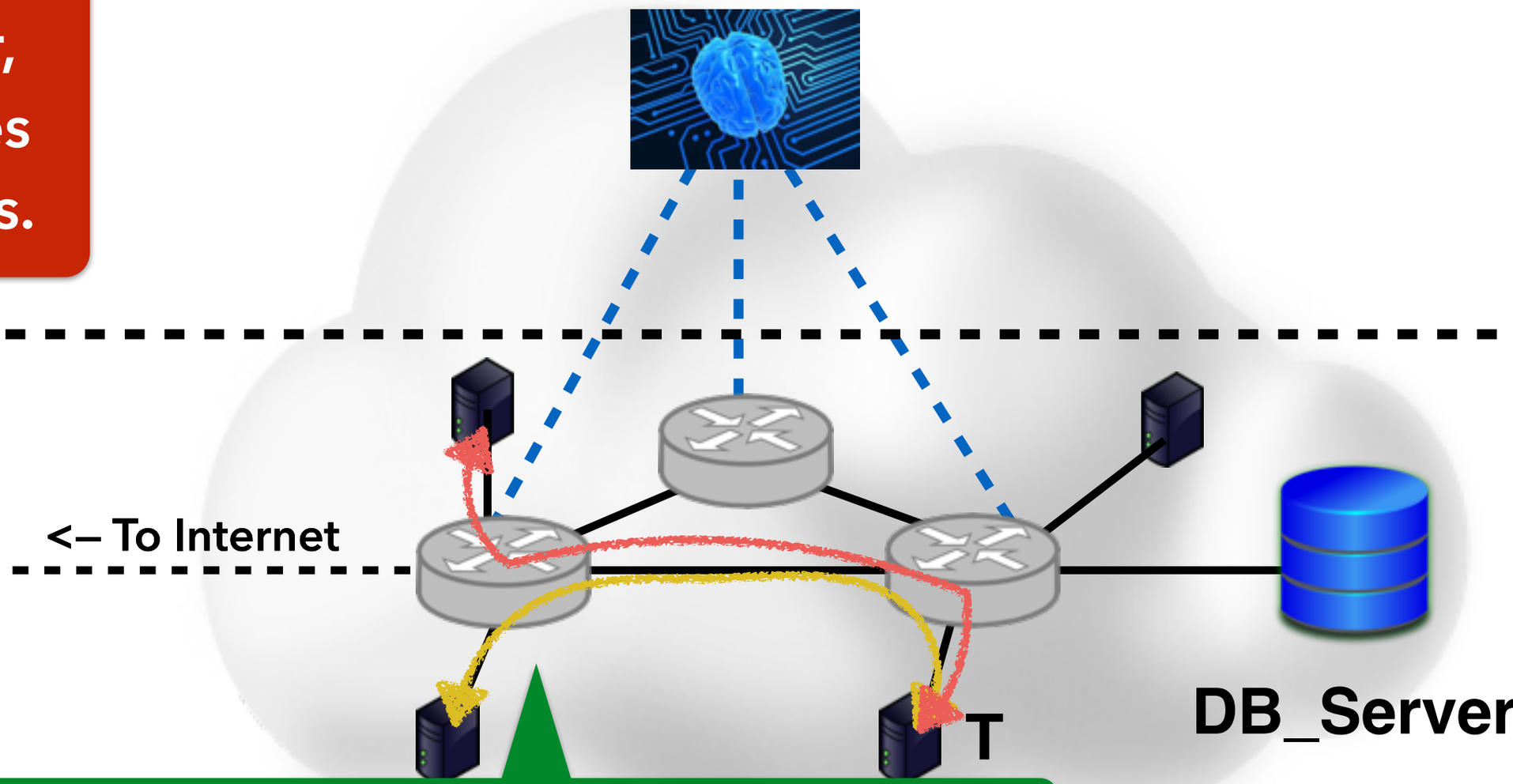


MAC Src	MAC Dst	…	Timeout	action
00:…:05	00:…:03		1	Output:3
00:…:03	00:…:05		1	Output:5
00:…:01	00:…:03		1	Output:3
00:…:03	00:…:01		1	Output:1
*	*	…	-	Controller

SDN Flow Tables Reveal Sensitive Information

T behaves like an application server, and communicates with many devices.



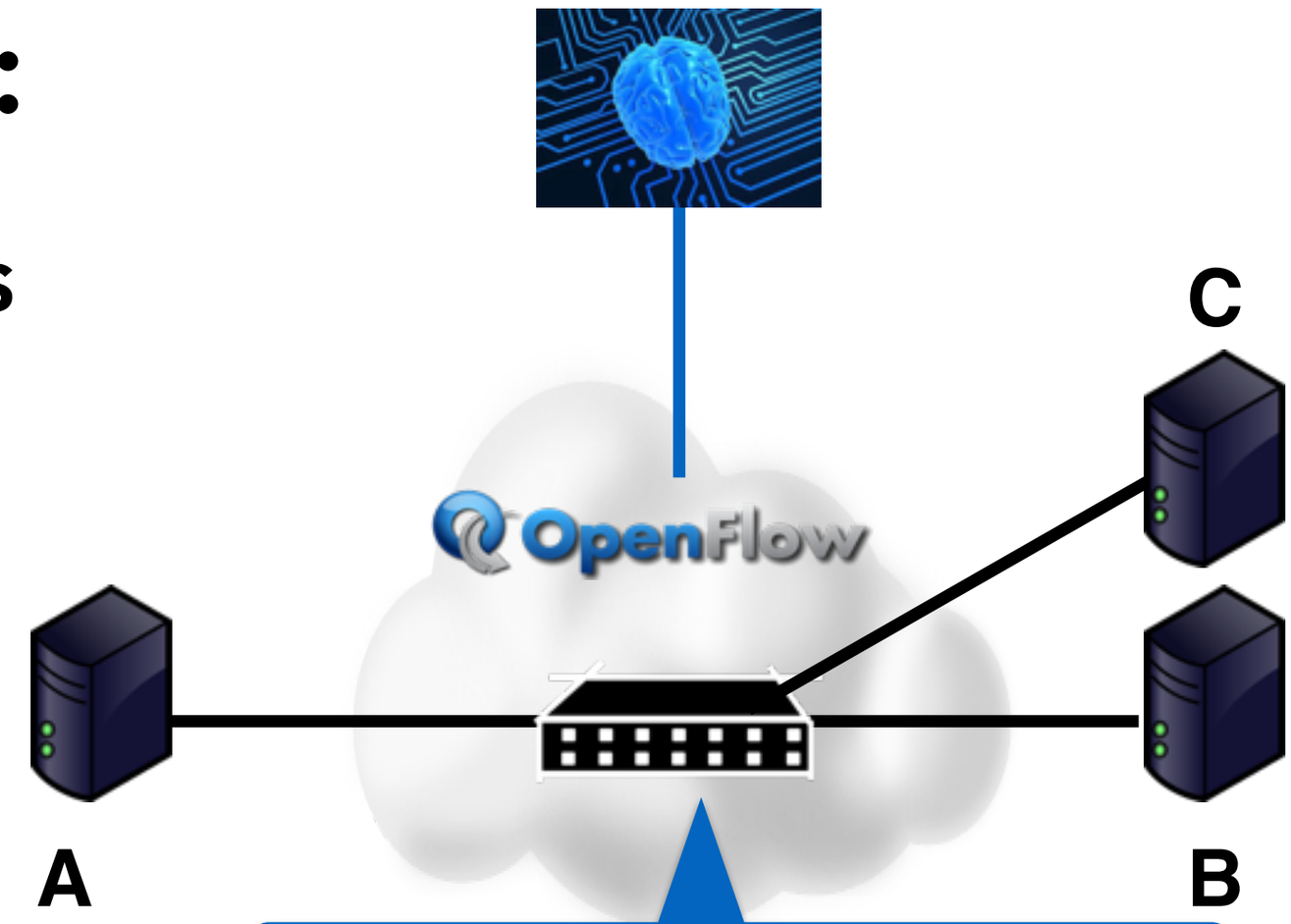


MAC Src	MAC Dst	...	Timeout	action
00:...:05	00:...:03		1	Output:3
00:...:03	00:...:05		1	Output:5
00:...:01	00:...:03		1	Output:3
00:...:03	00:...:01		1	Output:1
*	*	...	-	Controller

SDN Flow Tables Reveal Sensitive Information

Flow tables reveal:

Communication patterns
Access control policies
Network monitoring
Much more

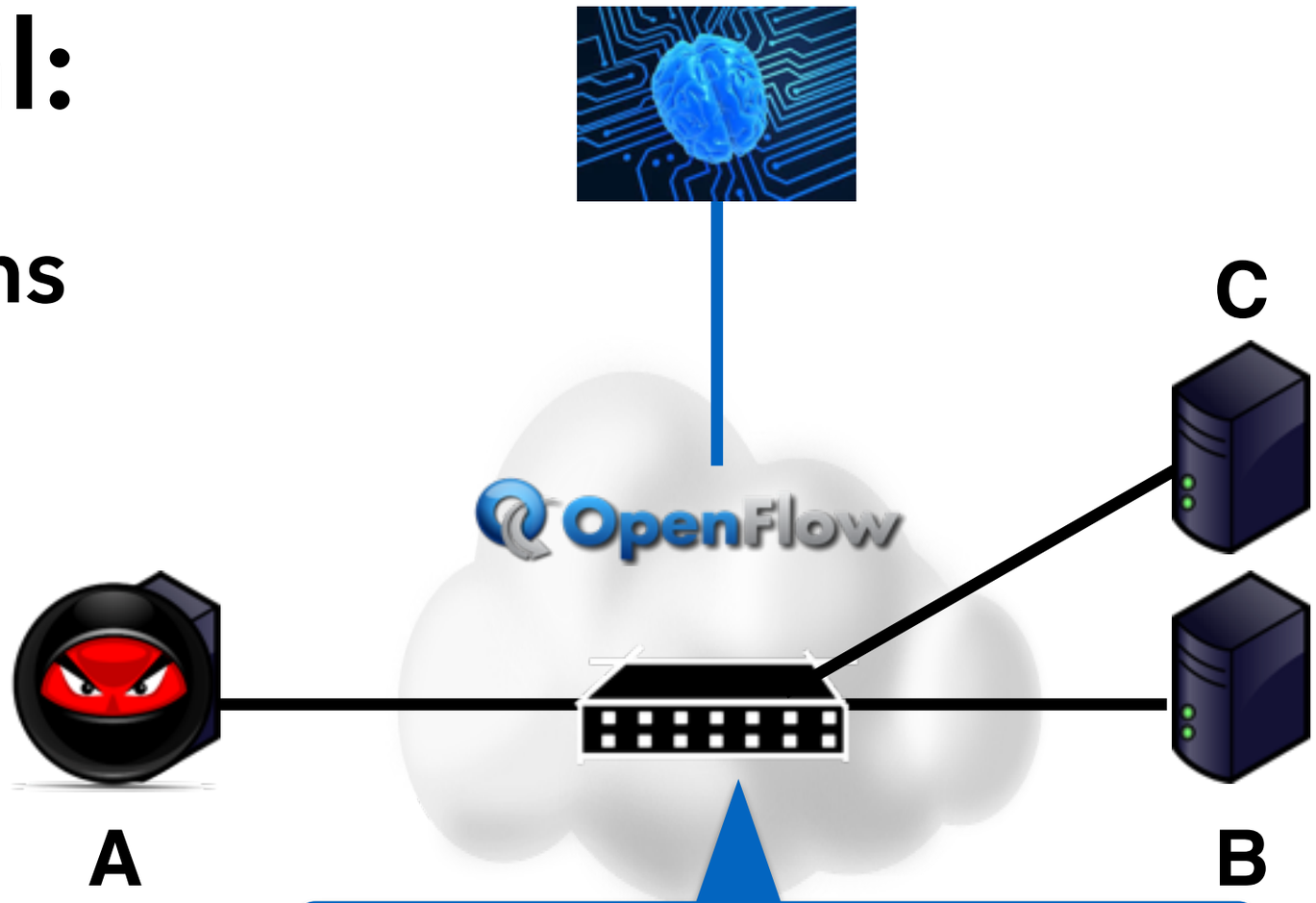


Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

SDN Flow Tables Reveal Sensitive Information

Flow tables reveal:

Communication patterns
Access control policies
Network monitoring
Much more

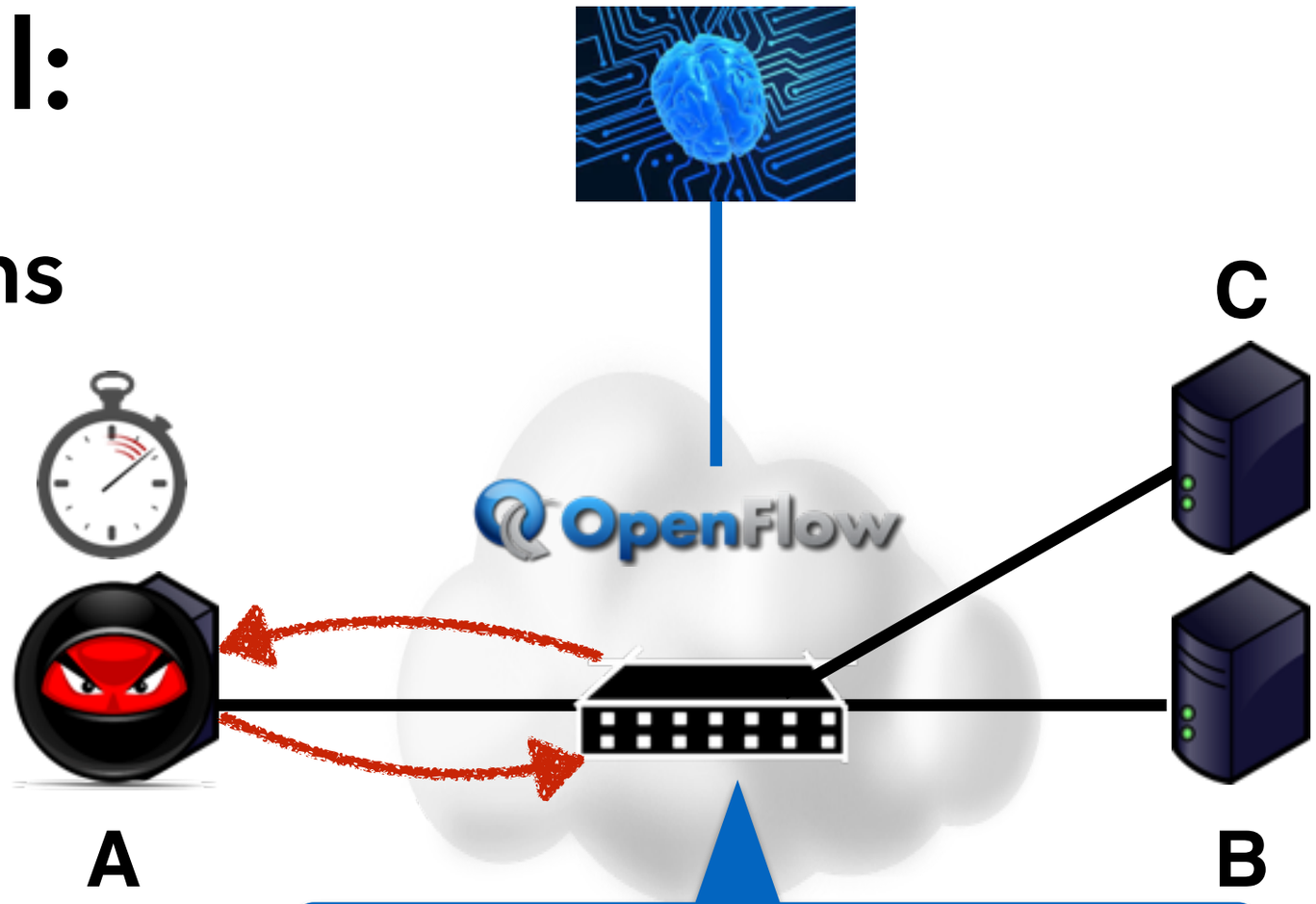


Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

SDN Flow Tables Reveal Sensitive Information

Flow tables reveal:

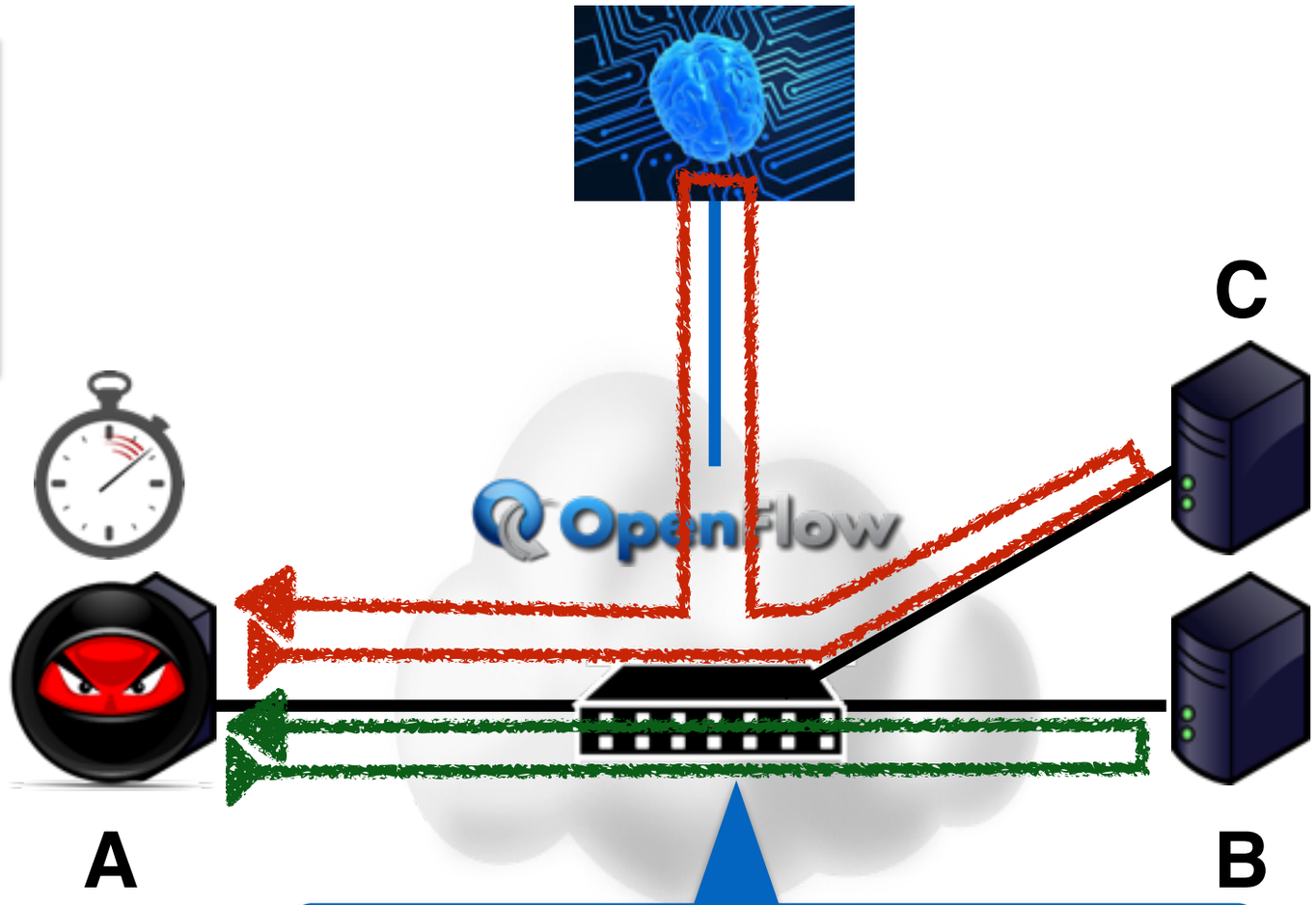
- Communication patterns
- Access control policies
- Network monitoring
- Much more



Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

Previous SDN Timing Attacks

<u>SDN Timing Property:</u>
RTT is much higher when the controller is on the path.

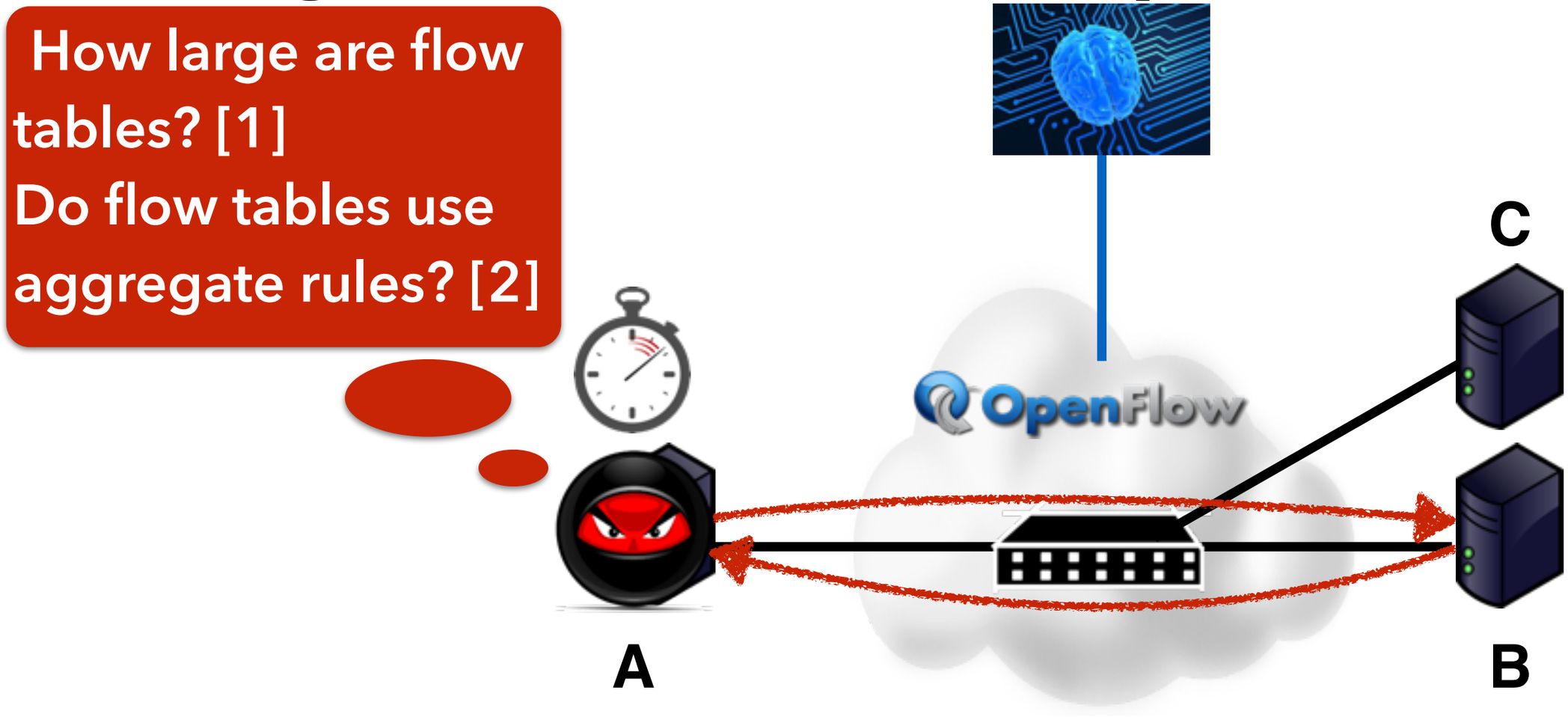


Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

```
PING SERVER_B (1.1.1.2) 56(84) bytes
64 bytes from 1.1.1.2: time=0.34 ms

PING SERVER_C (1.1.1.3) 56(84) bytes
64 bytes from 1.1.1.3: time=2.64 ms
```

Previous SDN Timing Attacks: Learning Flow Table Properties

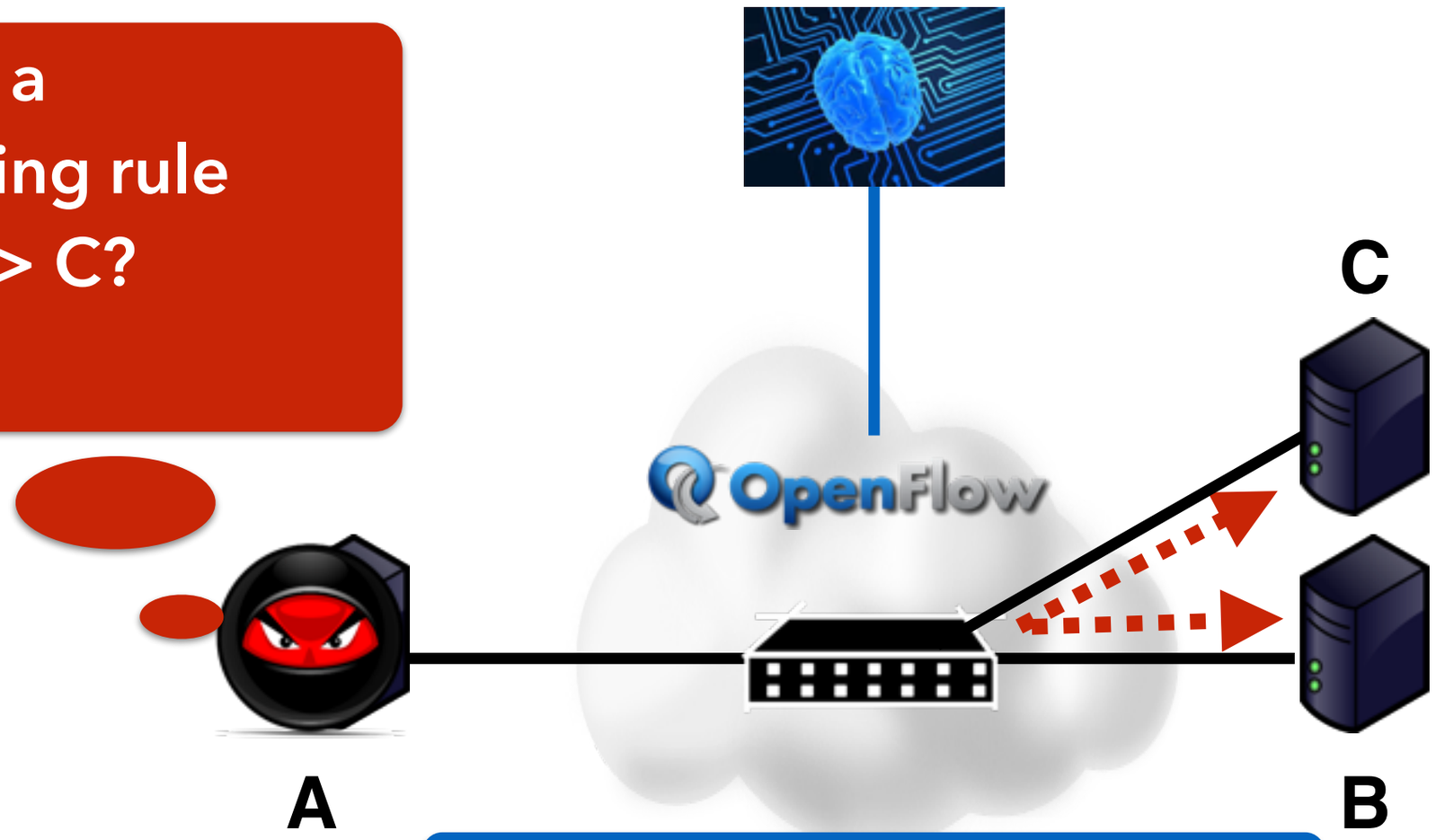


[1] J. Leng, Y. Zhou, J. Zhang, and C. Hu. **An inference attack model for flow table capacity and usage: Exploiting the vulnerability of flow table overflow in software-defined network.** *arXiv preprint arXiv:1504.03095*, 2015.

[2] R. Kloti, V. Kotronis, and P. Smith. **Openflow: A security analysis.** In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–6. IEEE, 2013.

Previous SDN Timing Attacks: Limitations

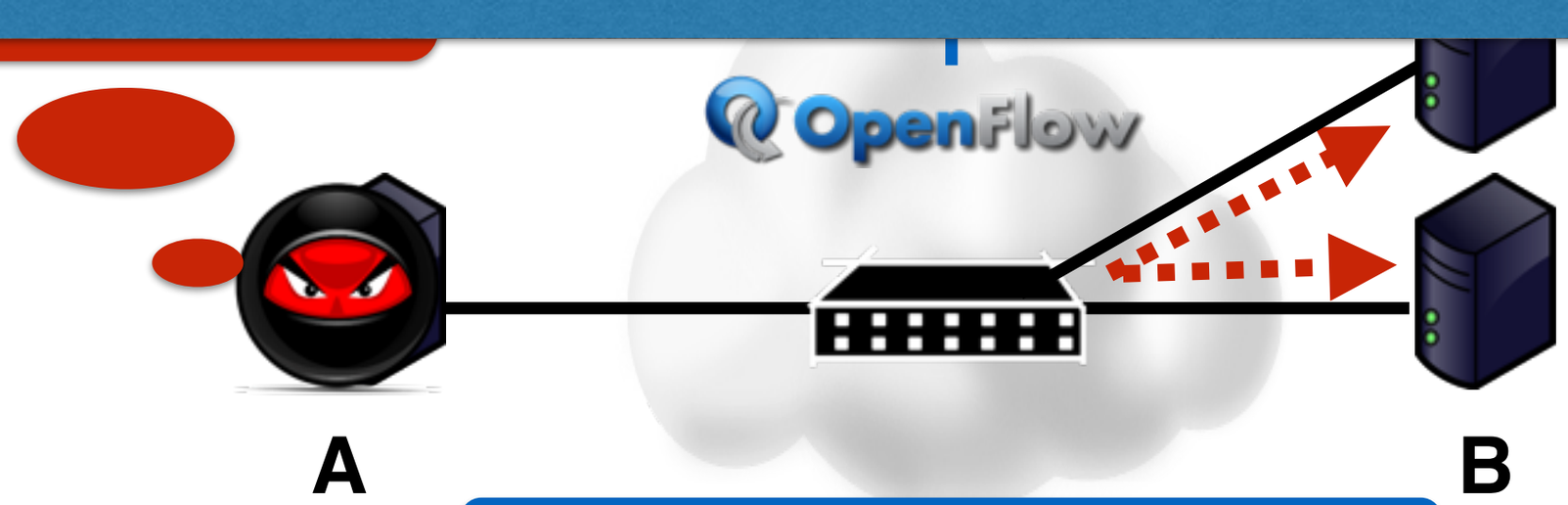
Is there a forwarding rule from B -> C?



Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

Previous SDN Timing Attacks: Limitations

Research question: is there a **more powerful timing side channel** that can leak **flow rules?**

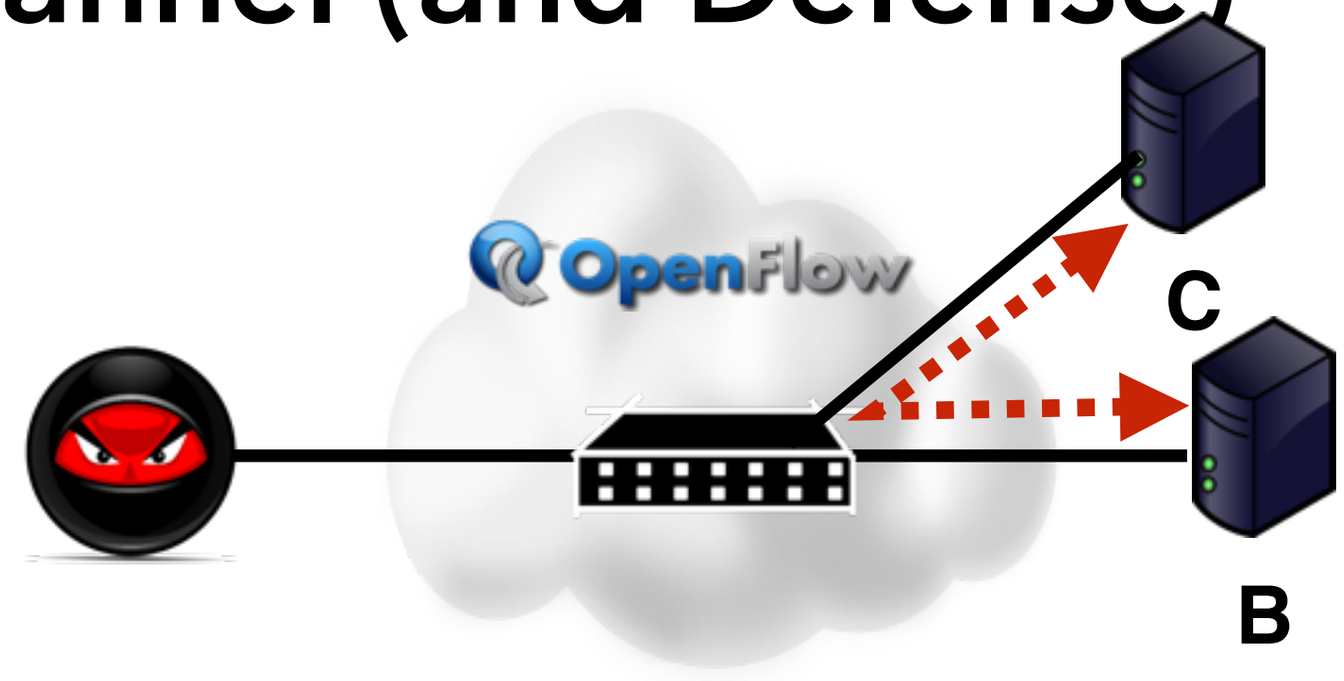


Src	Dst	…	Action
A	B		2
B	A		1
B	C		3
*	*	…	Controller

Our Work: A More General SDN Timing Side Channel (and Defense)

Contributions:

A **general timing attack** to learn about **any** flow rule.

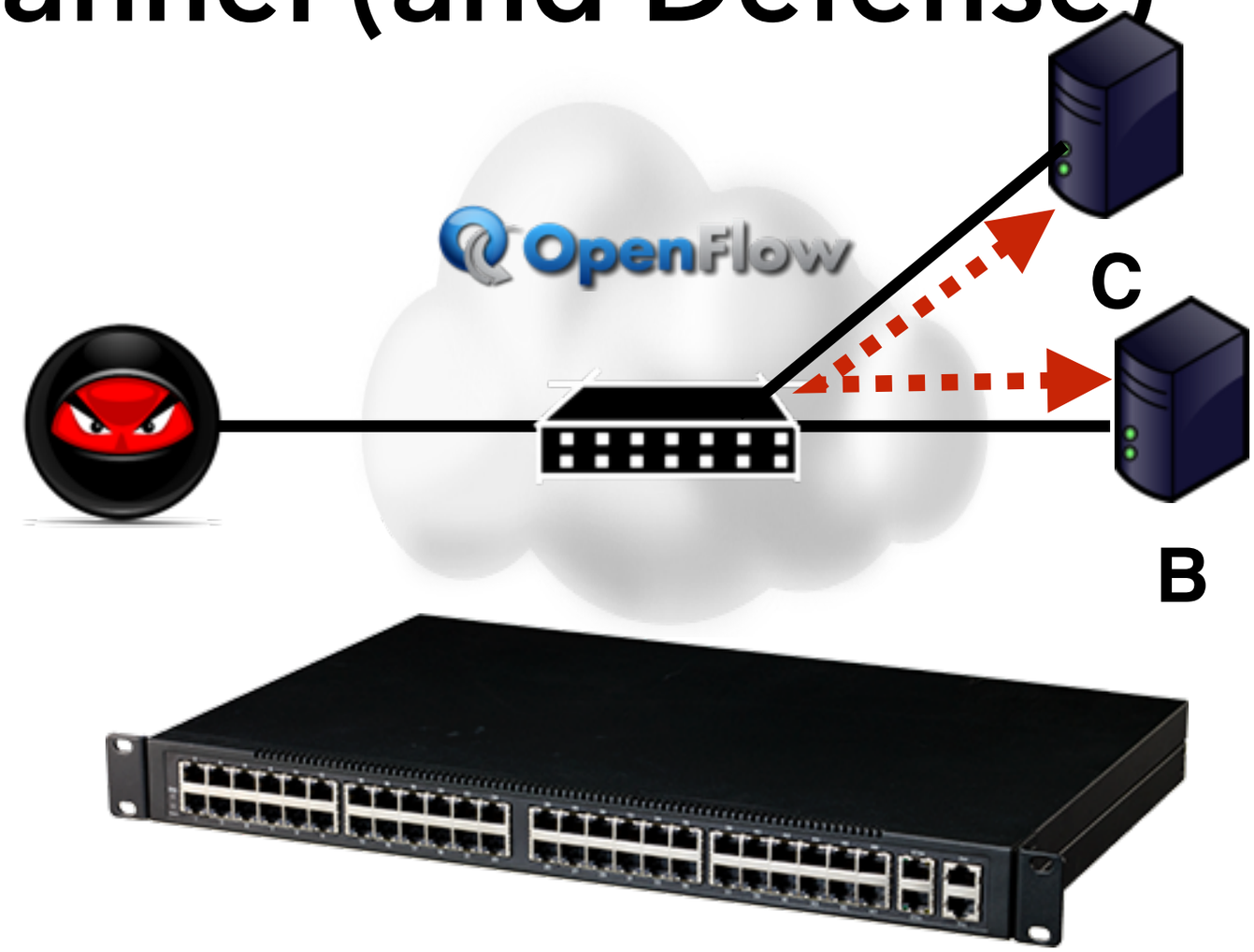


Our Work: A More General SDN Timing Side Channel (and Defense)

Contributions:

A **general timing attack** to learn about **any** flow rule.

Evaluation on **real hardware.**



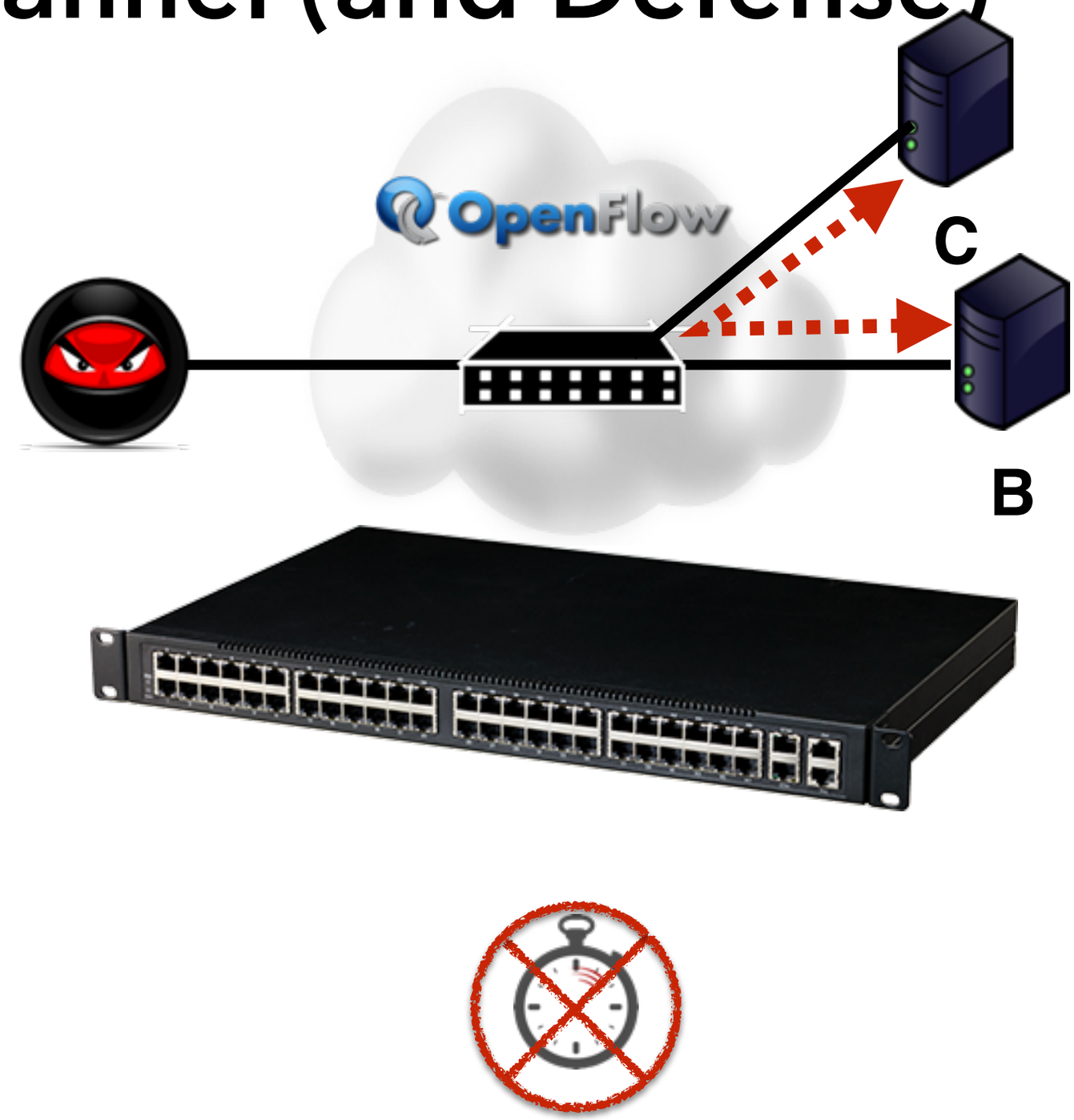
Our Work: A More General SDN Timing Side Channel (and Defense)

Contributions:

A **general timing attack** to learn about **any** flow rule.

Evaluation on **real hardware.**

A working **timing attack defense.**



Outline

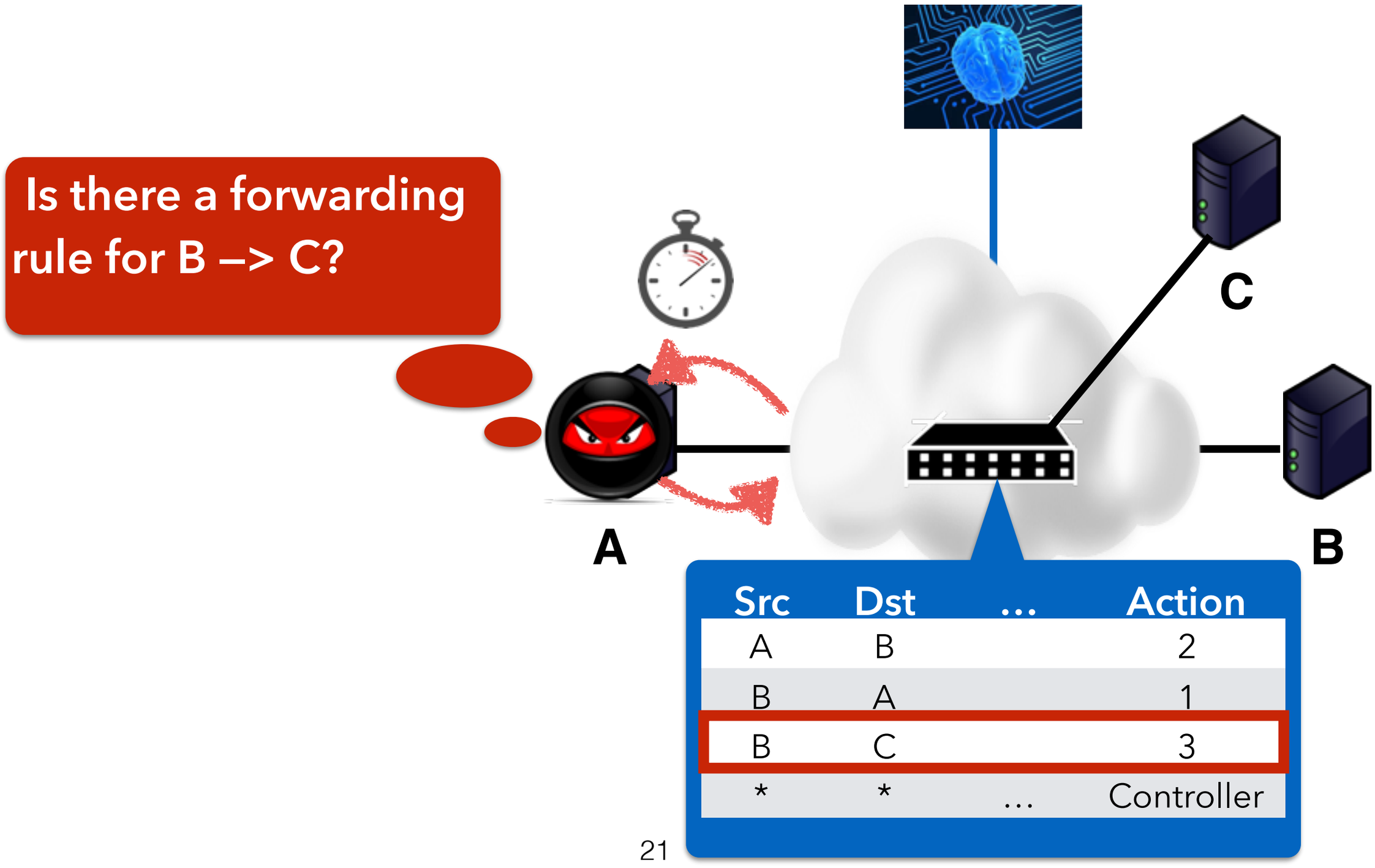
Timing Side Channels in SDNs

A More General Timing Attack

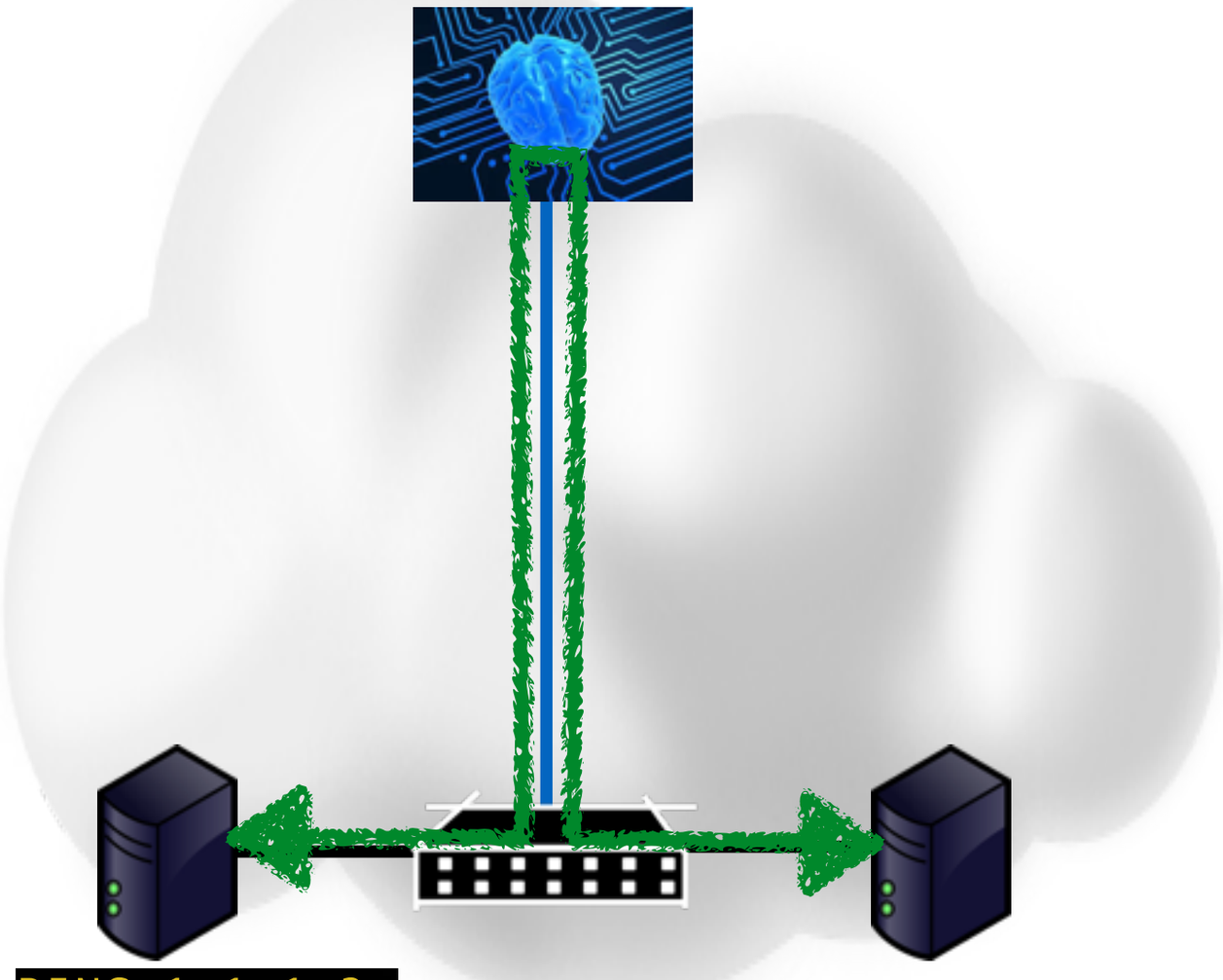
Evaluation on Real Hardware

Defense

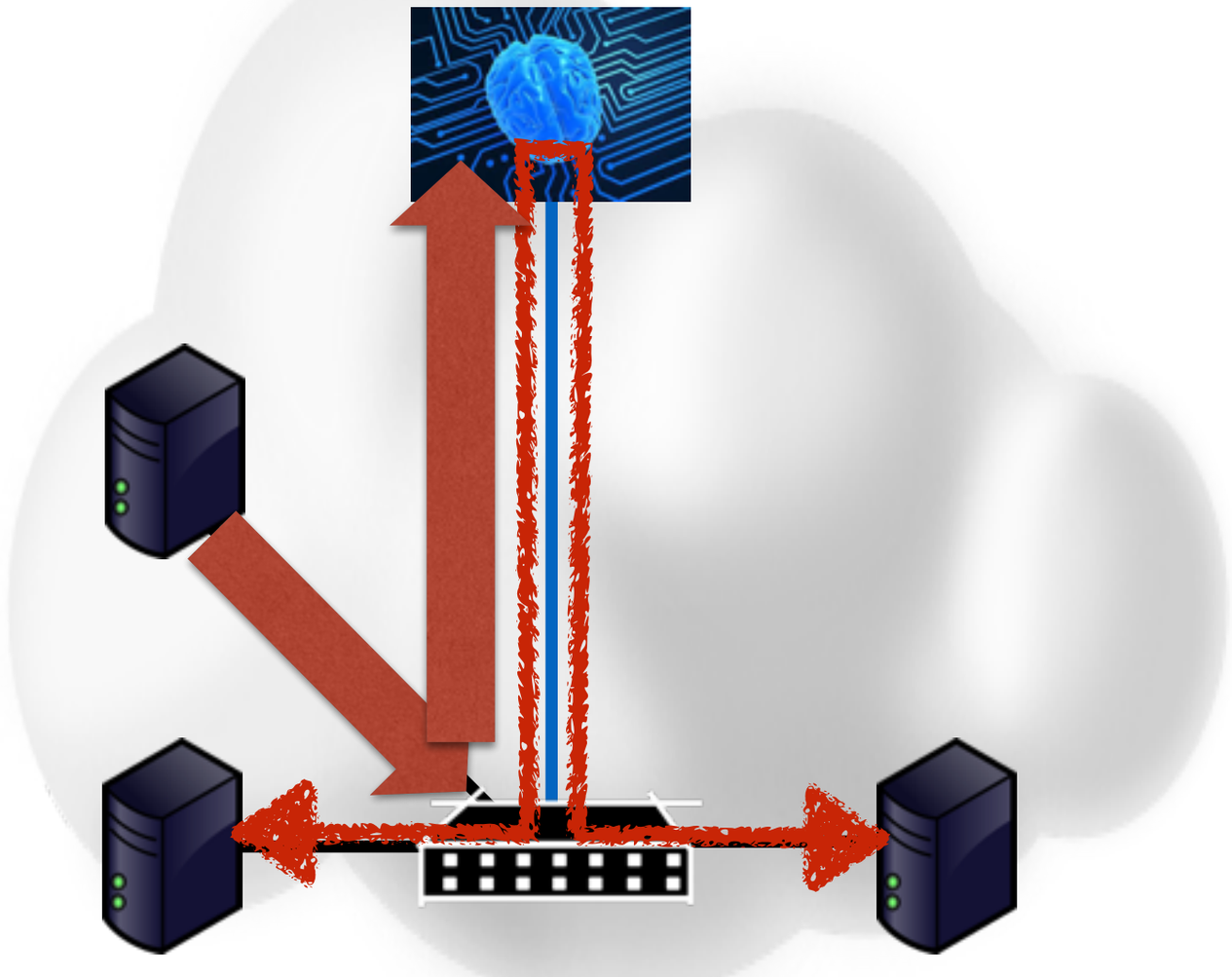
Timing an SDN To Learn Flow Rules



SDN Timing Property: Correlation Between Control Plane Load and Response Time

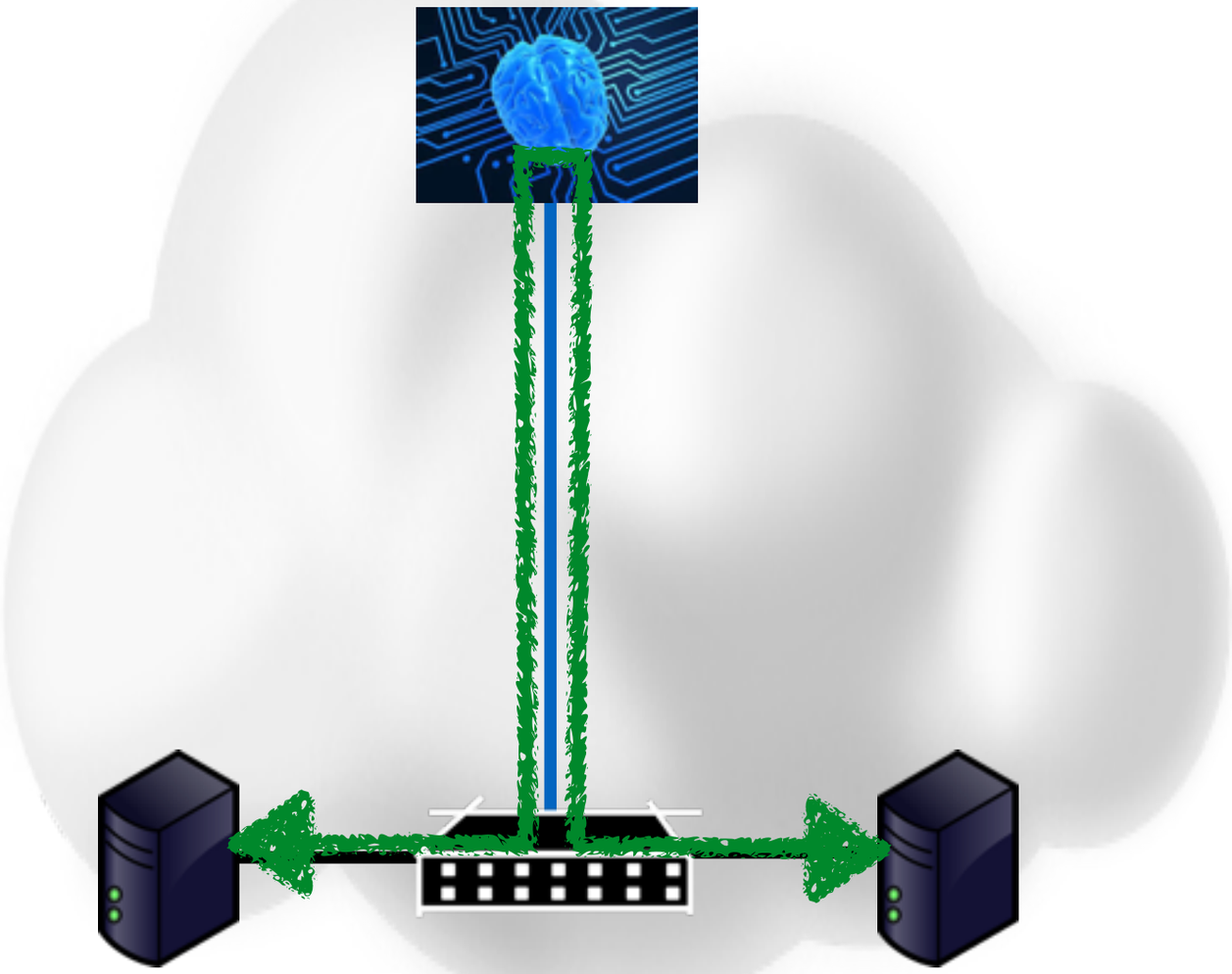


```
PING 1.1.1.2
64 bytes from 1.1.1.2:  time=2.56 ms
64 bytes from 1.1.1.2: time=0.345 ms
64 bytes from 1.1.1.2: time=0.044 ms
```

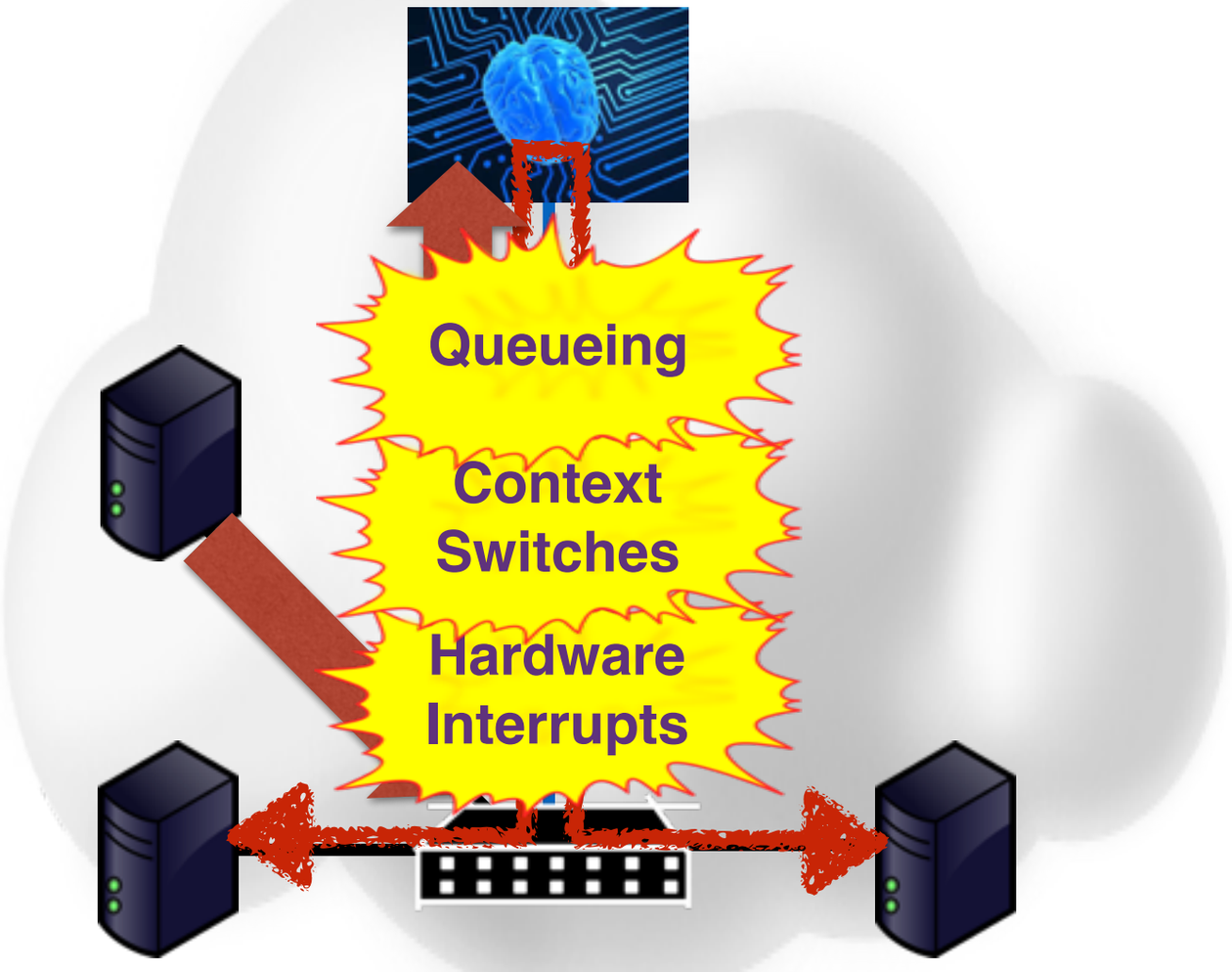


```
PING 1.1.1.2
64 bytes from 1.1.1.2:  time=10.8 ms
64 bytes from 1.1.1.2: time=0.345 ms
64 bytes from 1.1.1.2: time=0.044 ms
```

SDN Timing Property: Correlation Between Control Plane Load and Response Time

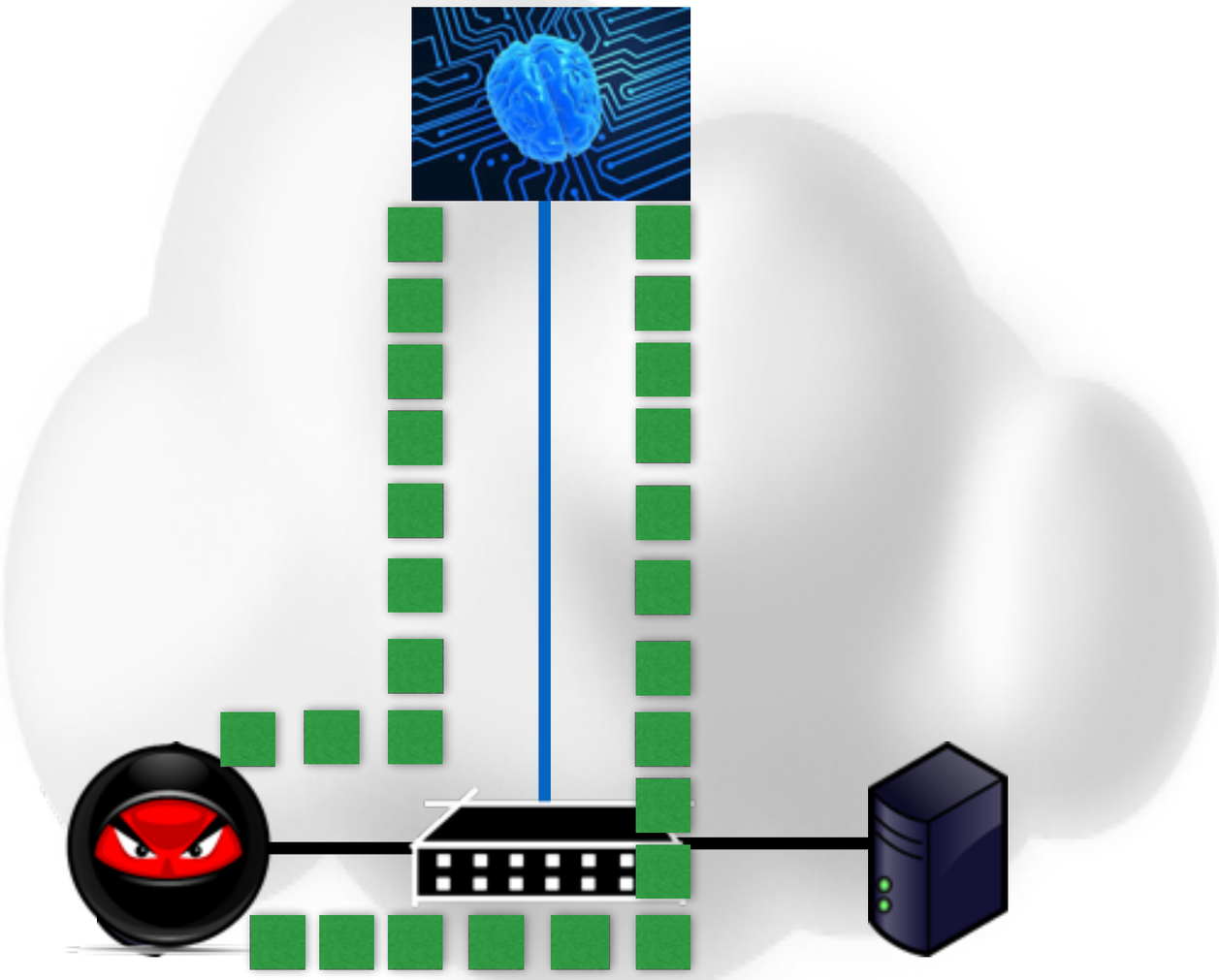


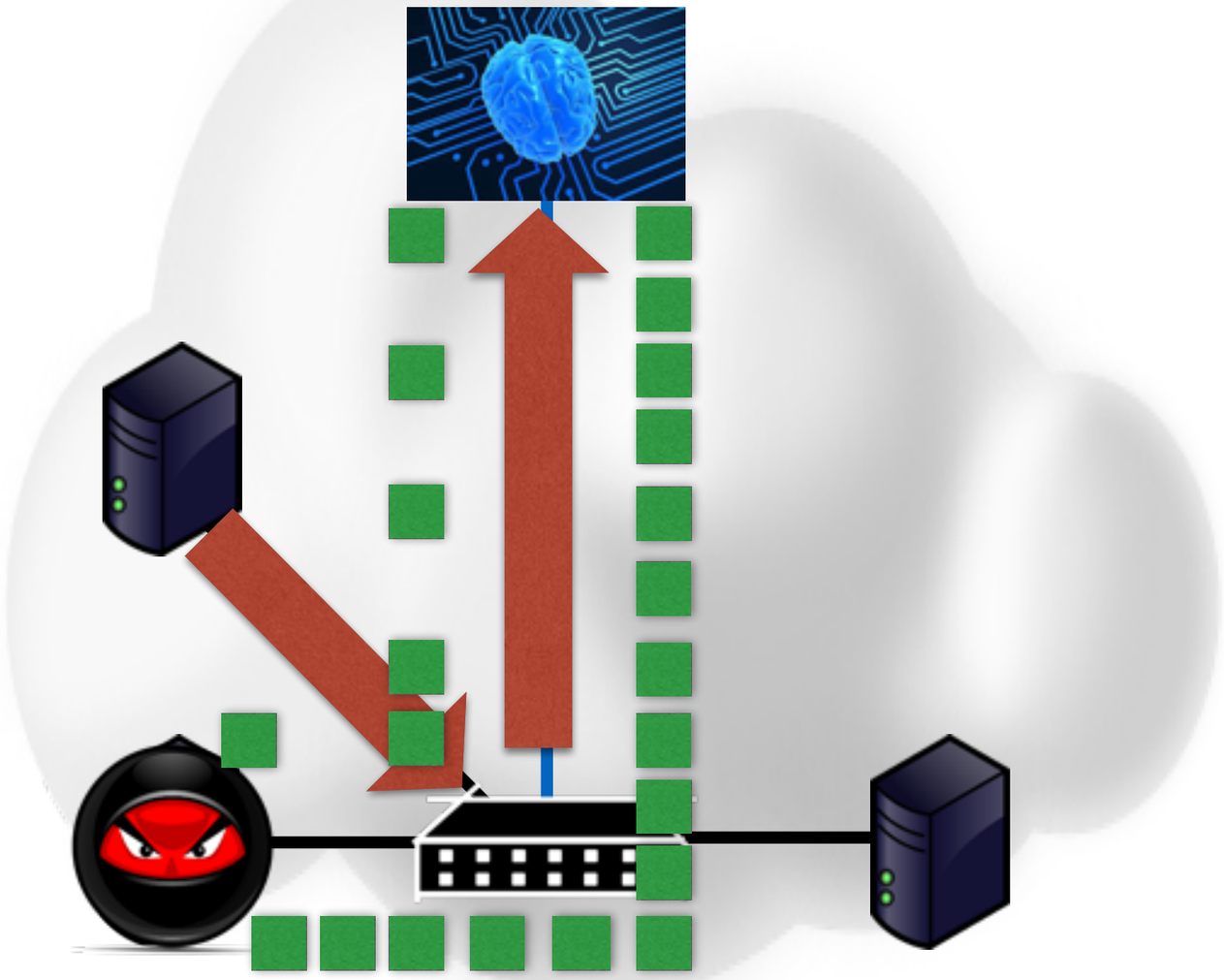
```
PING 1.1.1.2
64 bytes from 1.1.1.2  time=2.56 ms
64 bytes from 1.1.1.2: time=0.345 ms
64 bytes from 1.1.1.2: time=0.044 ms
```




```
PING 1.1.1.2
64 bytes from 1.1.1.2  time=10.8 ms
64 bytes from 1.1.1.2: time=0.345 ms
64 bytes from 1.1.1.2: time=0.044 ms
```

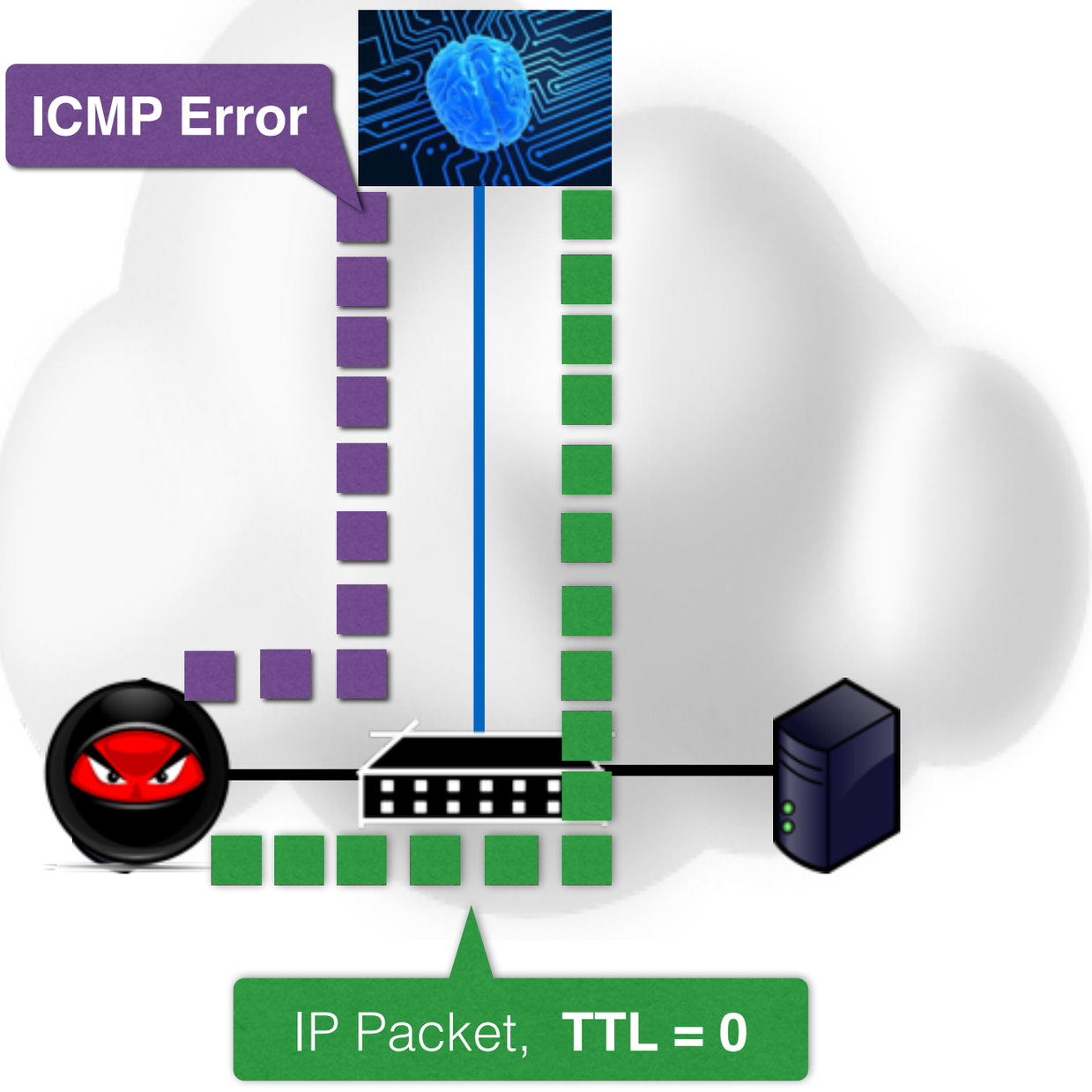
Timing The Control Plane to Estimate Load



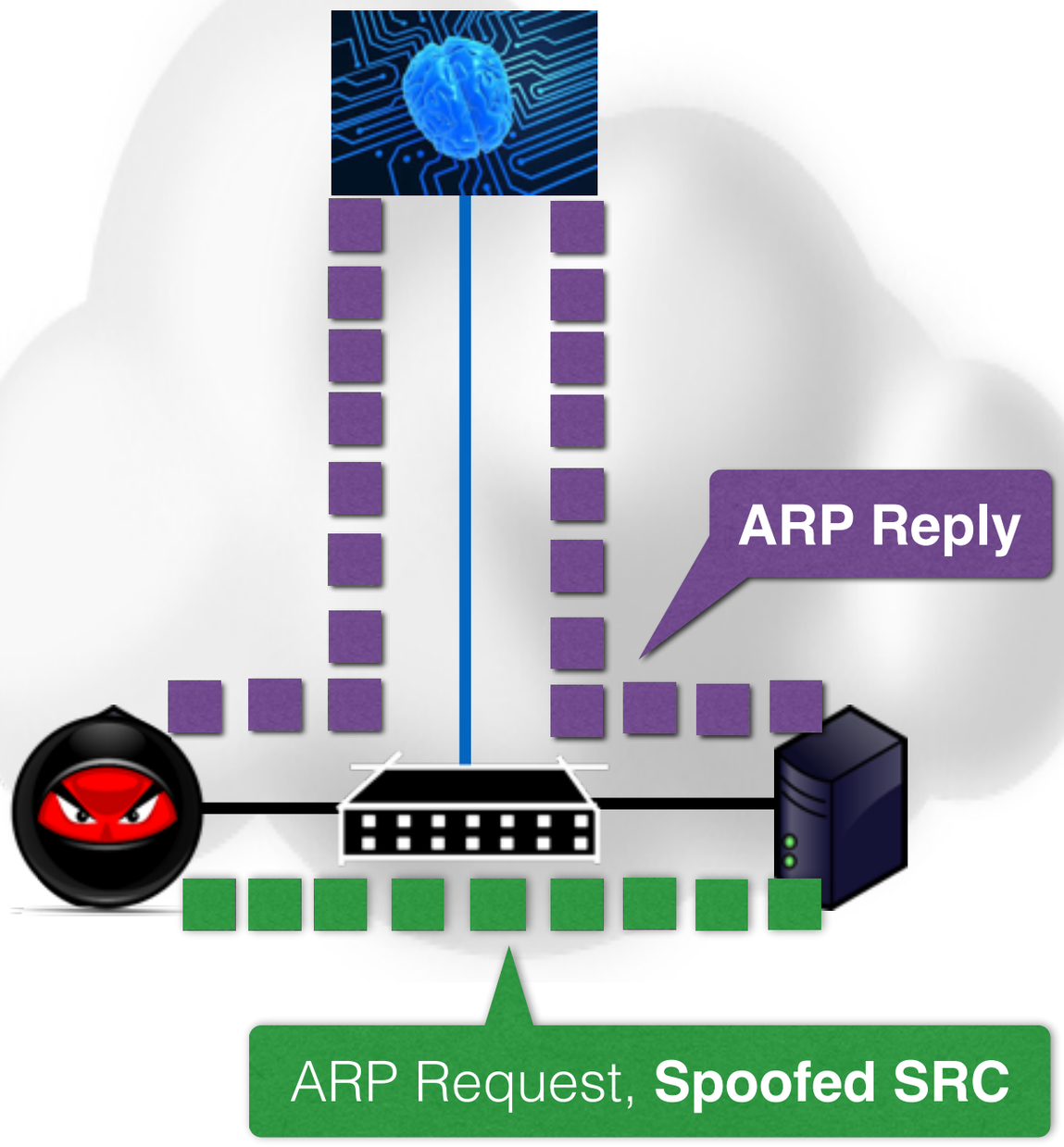


Timing The Control Plane to Estimate Load

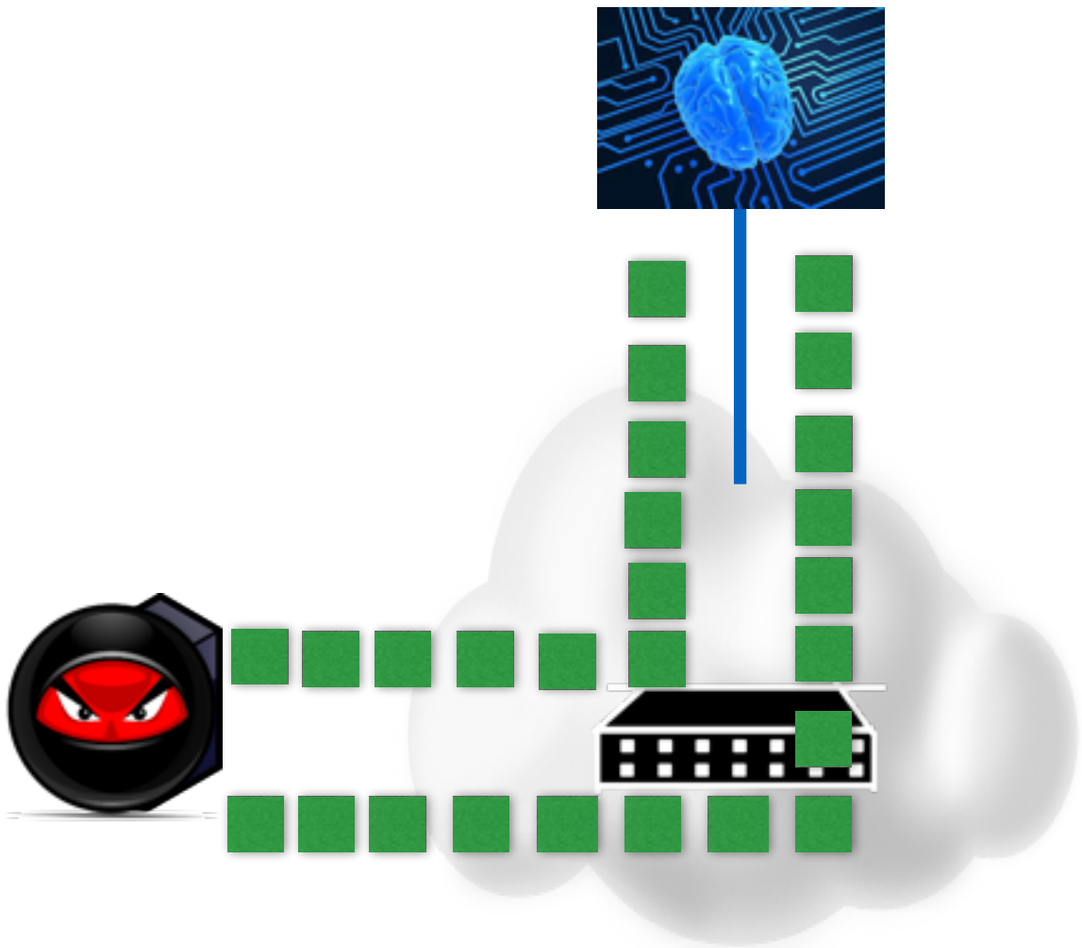
IP Network



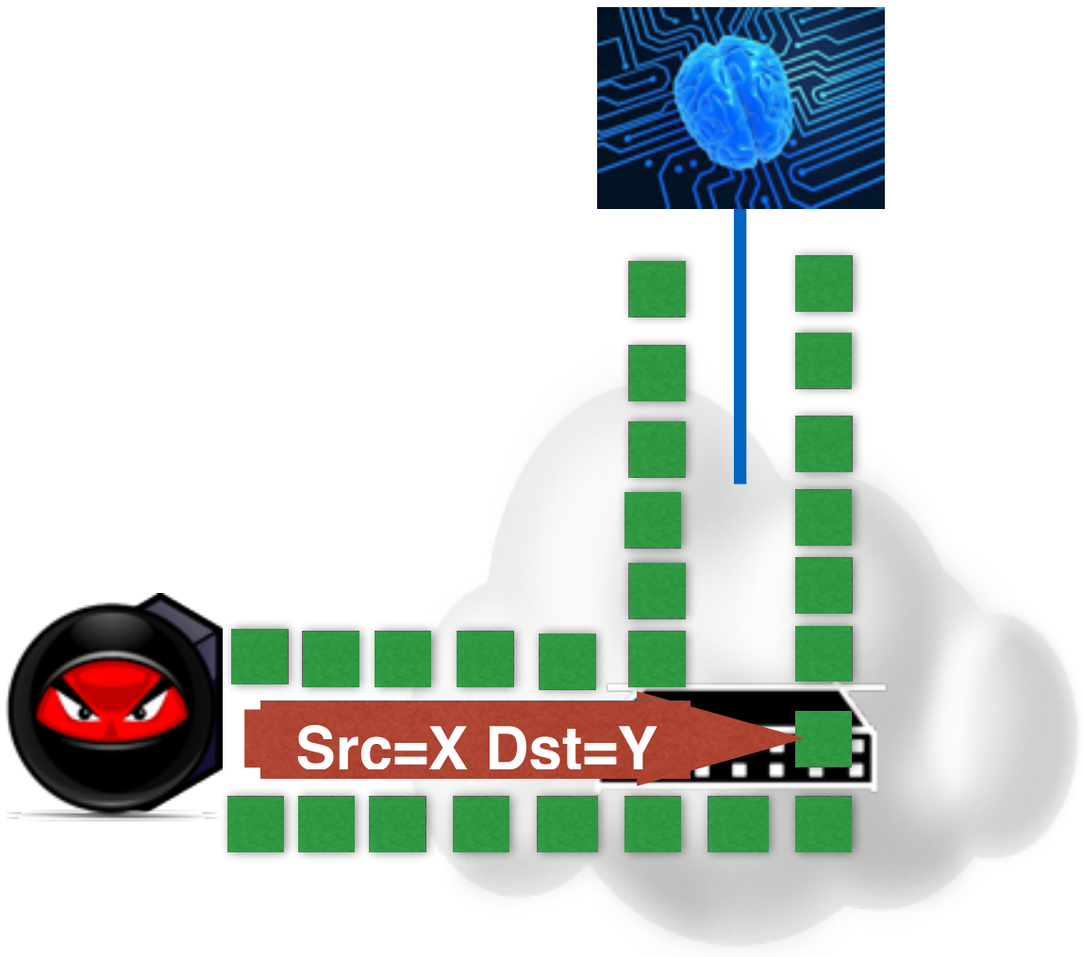
Ethernet Network



Timing the Control Plane to Learn Flow Rules

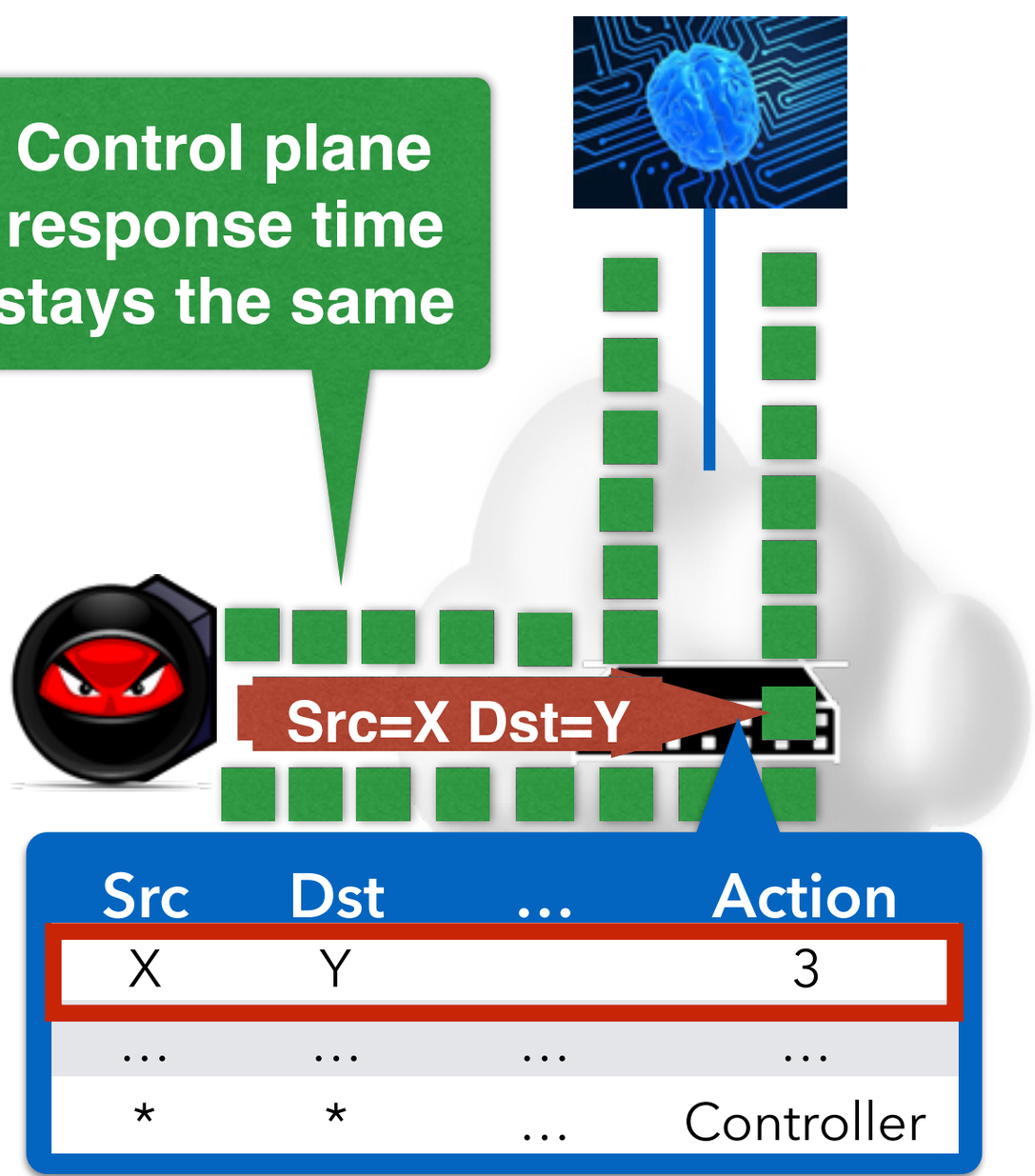


Timing the Control Plane to Learn Flow Rules



Timing the Control Plane to Learn Flow Rules

Matching Rule



Timing the Control Plane to Learn Flow Rules

Matching Rule

Control plane response time stays the same

Src	Dst	…	Action
X	Y		3
…	…	…	…
*	*	…	Controller

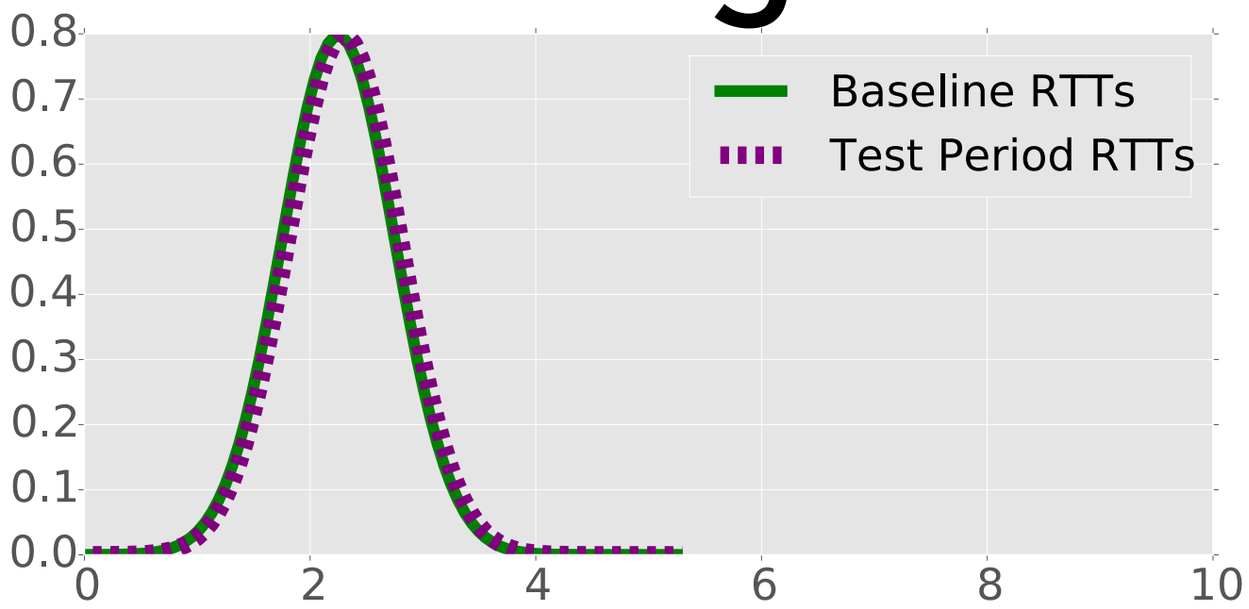
No Matching Rule

Control plane response time increases

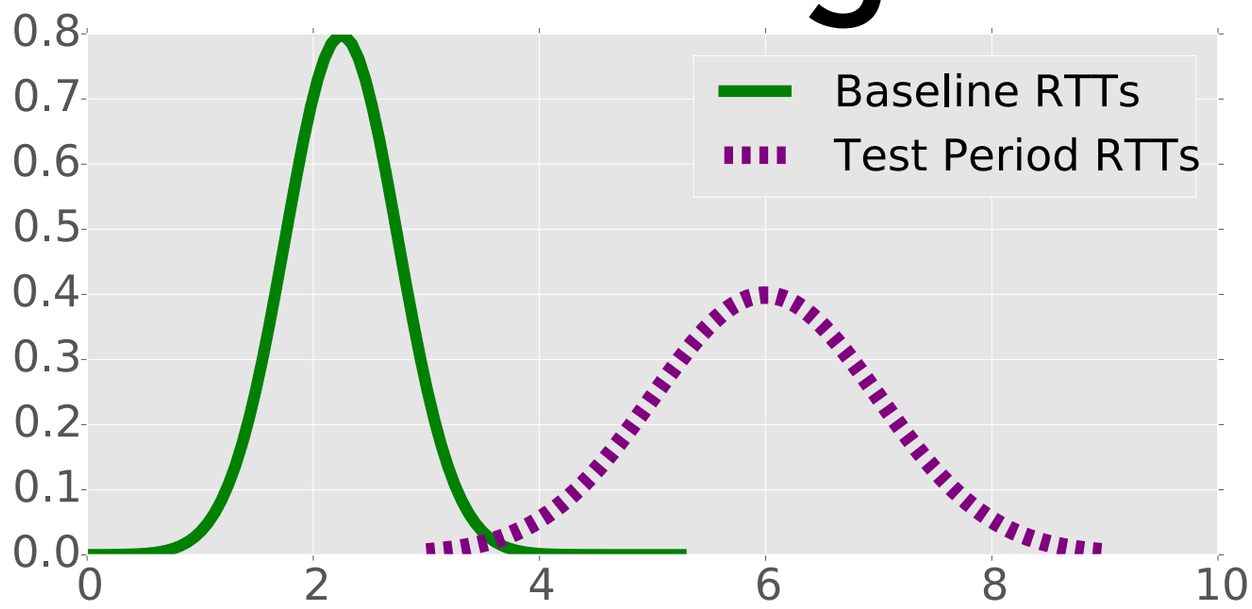
Src	Dst	…	Action
…	…	…	…
*	*	…	Controller

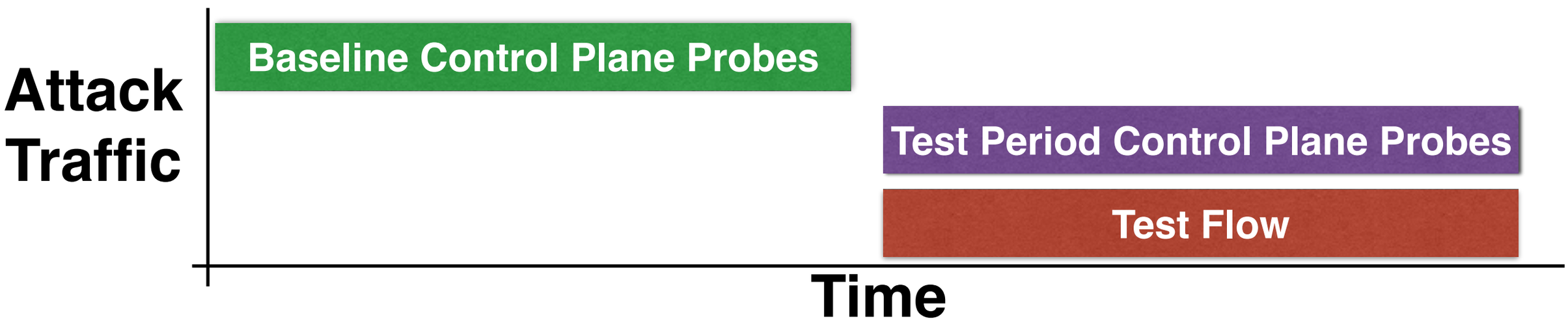
Timing the Control Plane to Learn Flow Rules

Matching Rule

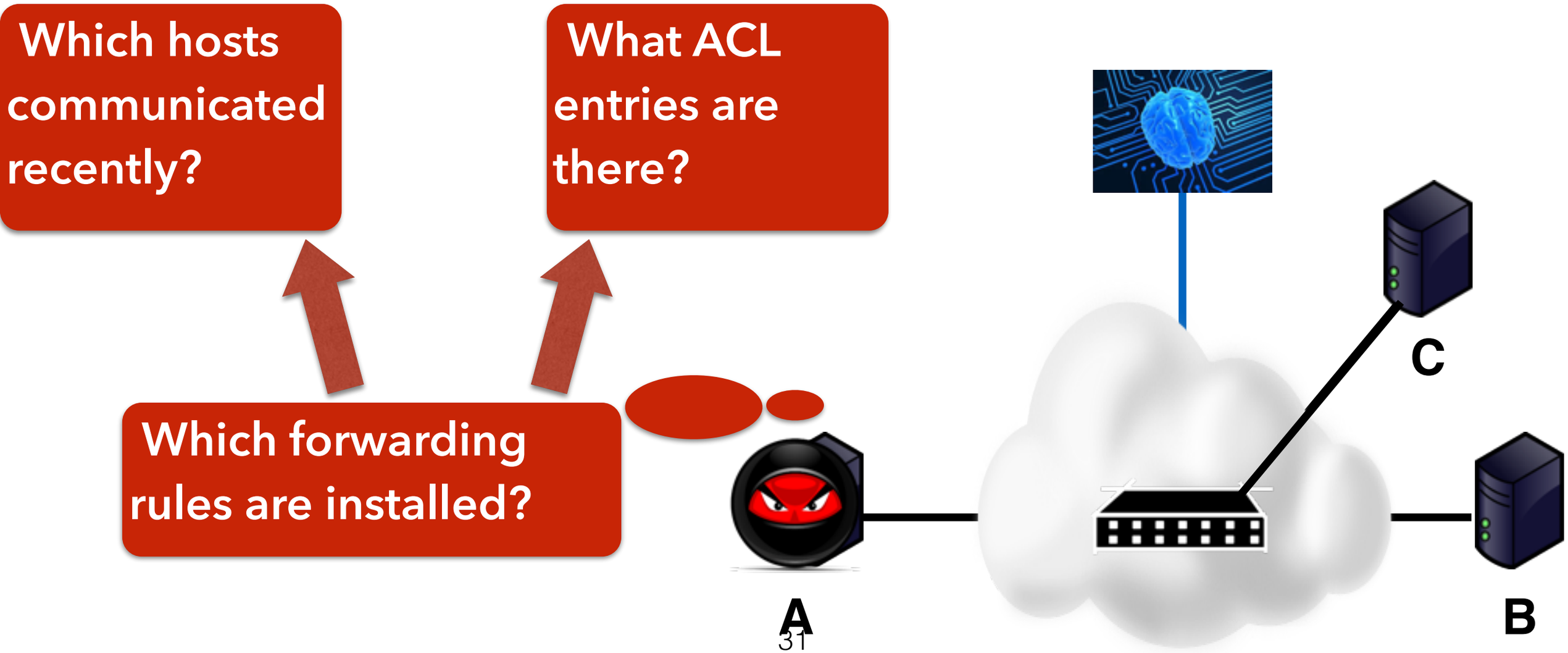


No Matching Rule





Timing the Control Plane to Learn Flow Rules: Applications



Outline

Timing Side Channels in SDNs

A More General Timing Attack

Evaluation on Real Hardware

Defense

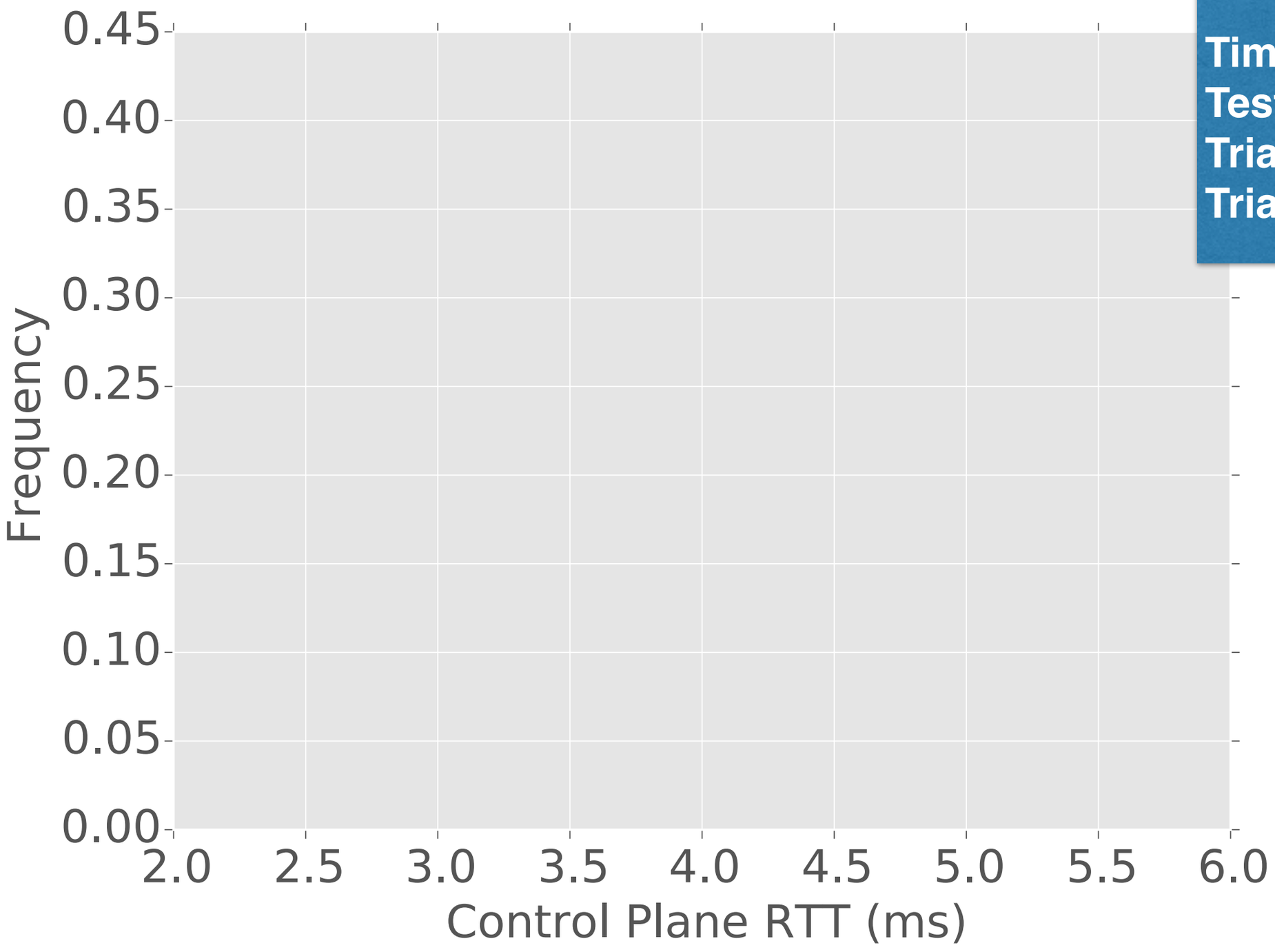
Timing Attack Evaluation

Attack Effectiveness } This Presentation

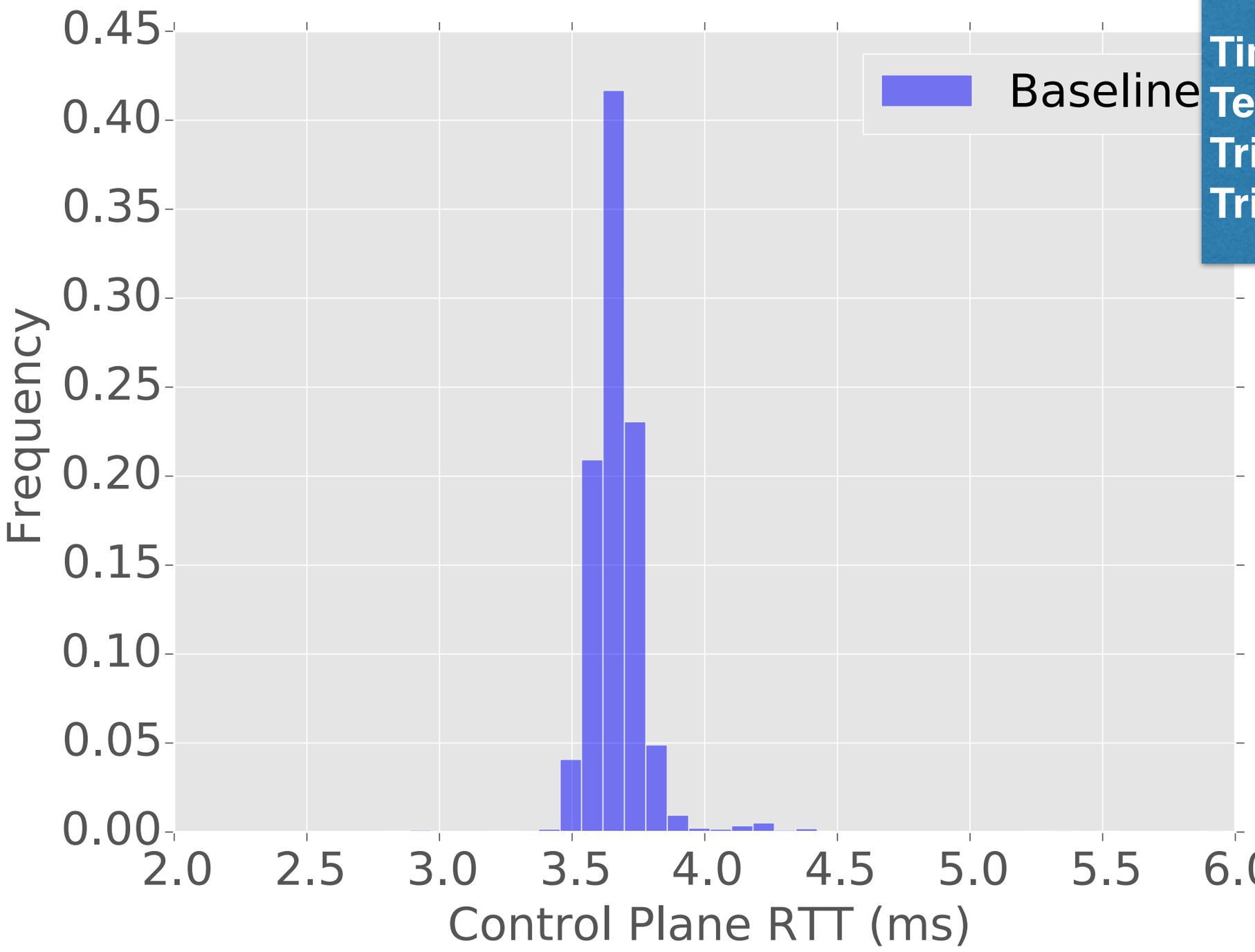
The Paper { Root Causes
Impact of Background Traffic
Attack Application Effectiveness

Attack Effectiveness

Parameters:
Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100



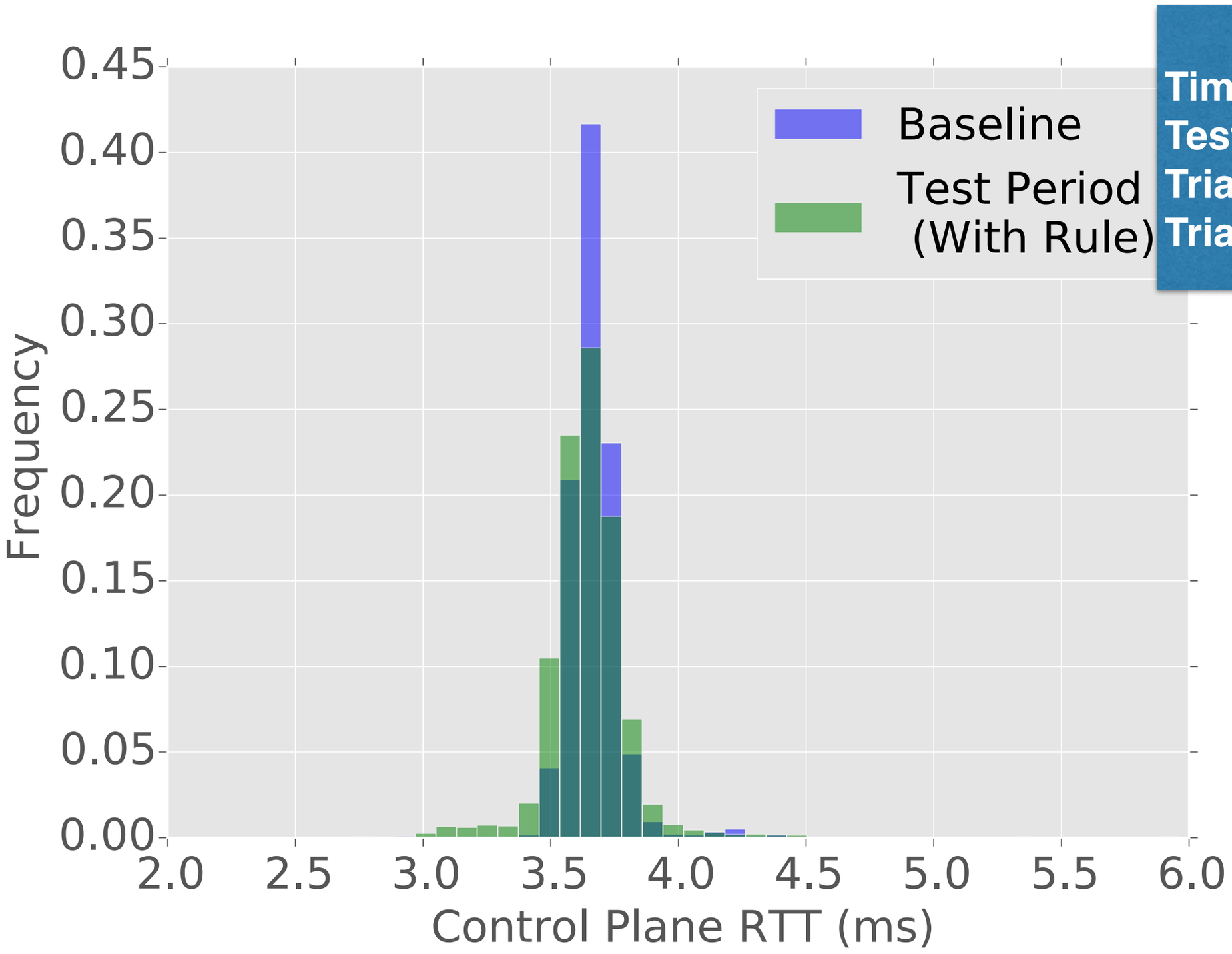
Attack Effectiveness



Parameters:

Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100

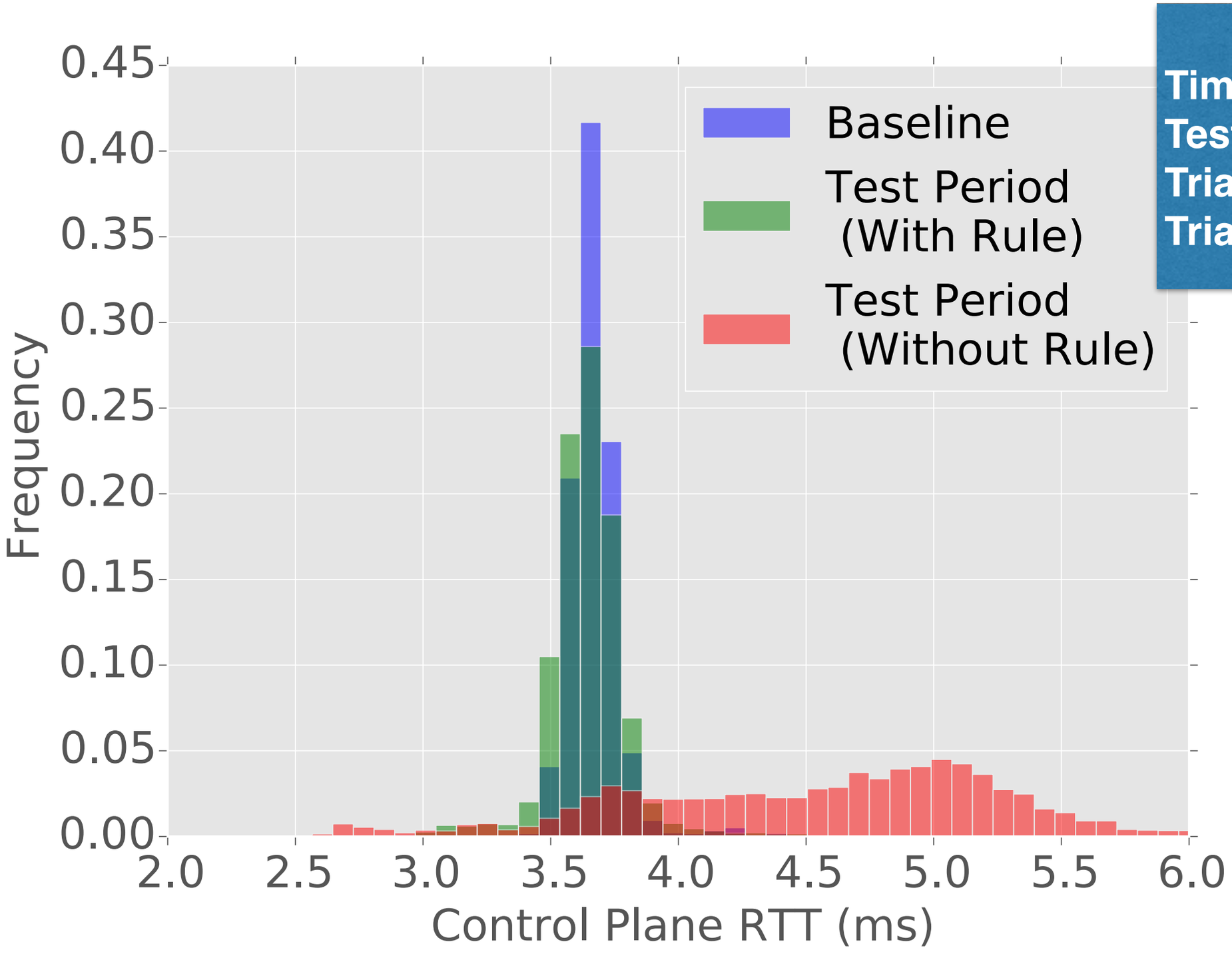
Attack Effectiveness



Parameters:

Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100

Attack Effectiveness

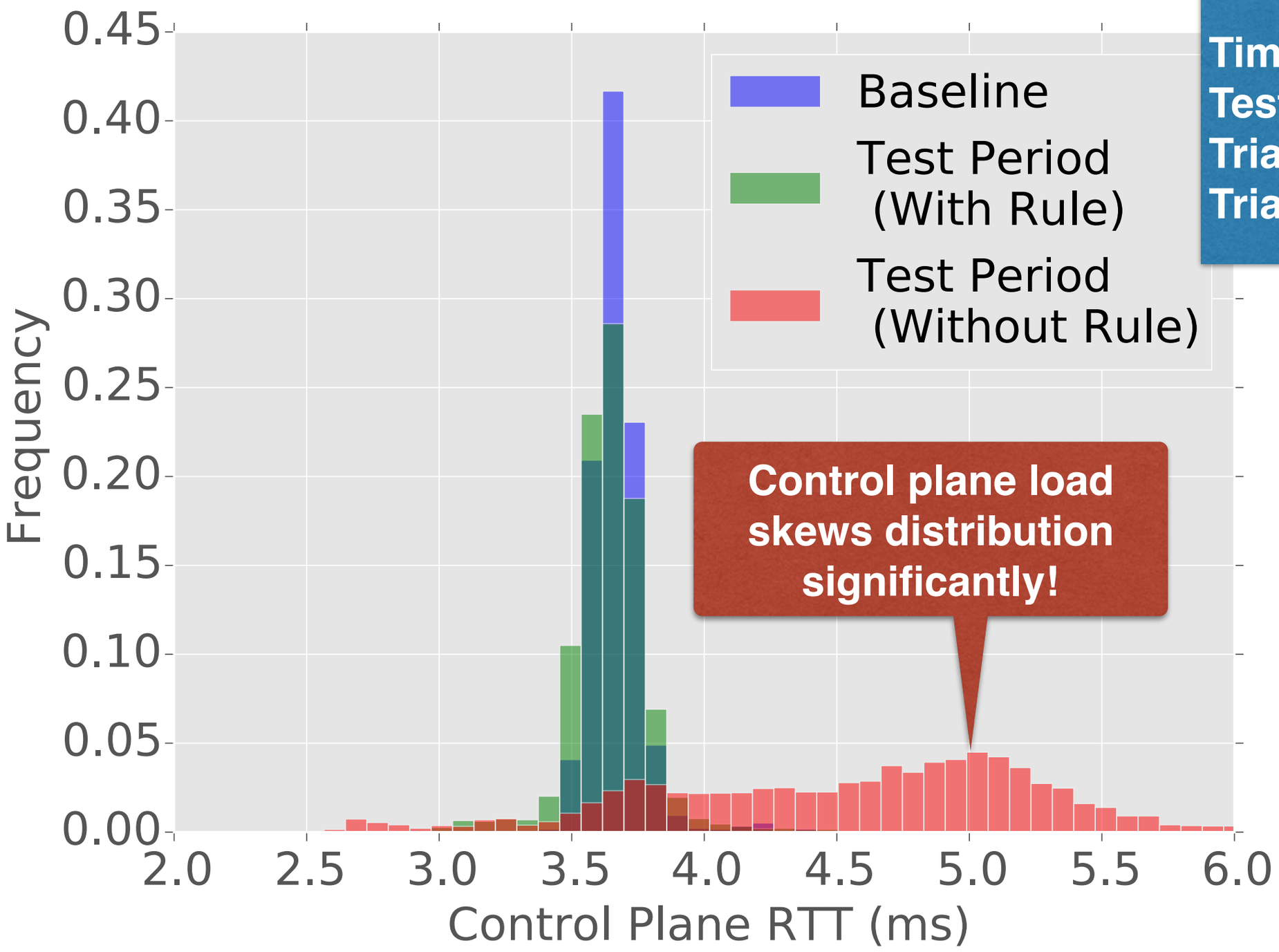


Parameters:

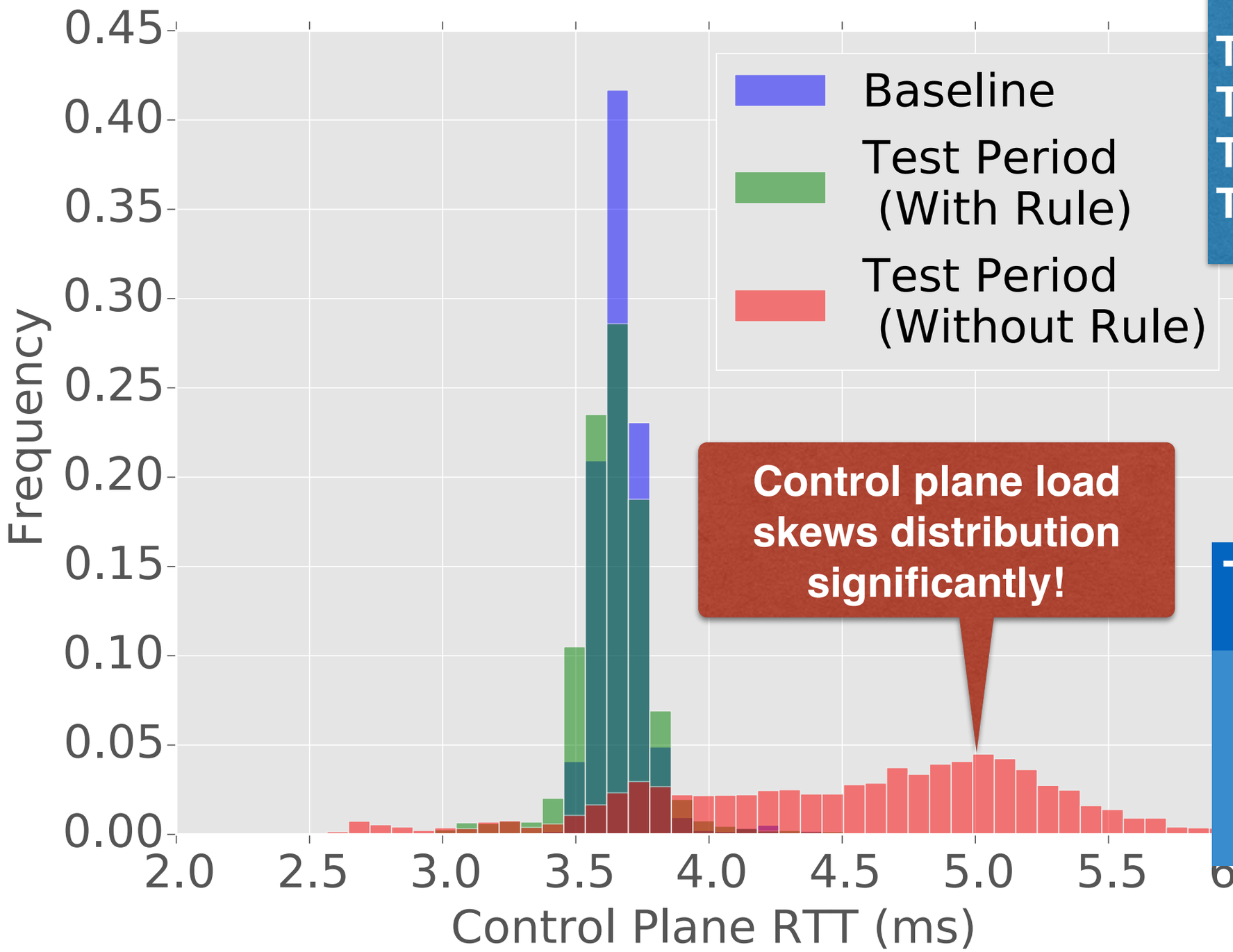
Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100

Attack Effectiveness

Parameters:
Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100



Attack Effectiveness



Parameters:

Timing Probe Rate: 10
Test Flow Packet Rate: 500
Trial Duration: 10 seconds
Trial Count: 100

Compares Baseline with Test Period to Predict "rule" or "no rule"

Test Packet Rate	*T*-test Accuracy
500	100%
50	89%

Outline

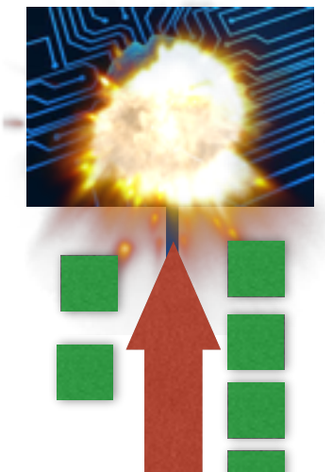
Timing Side Channels in SDNs

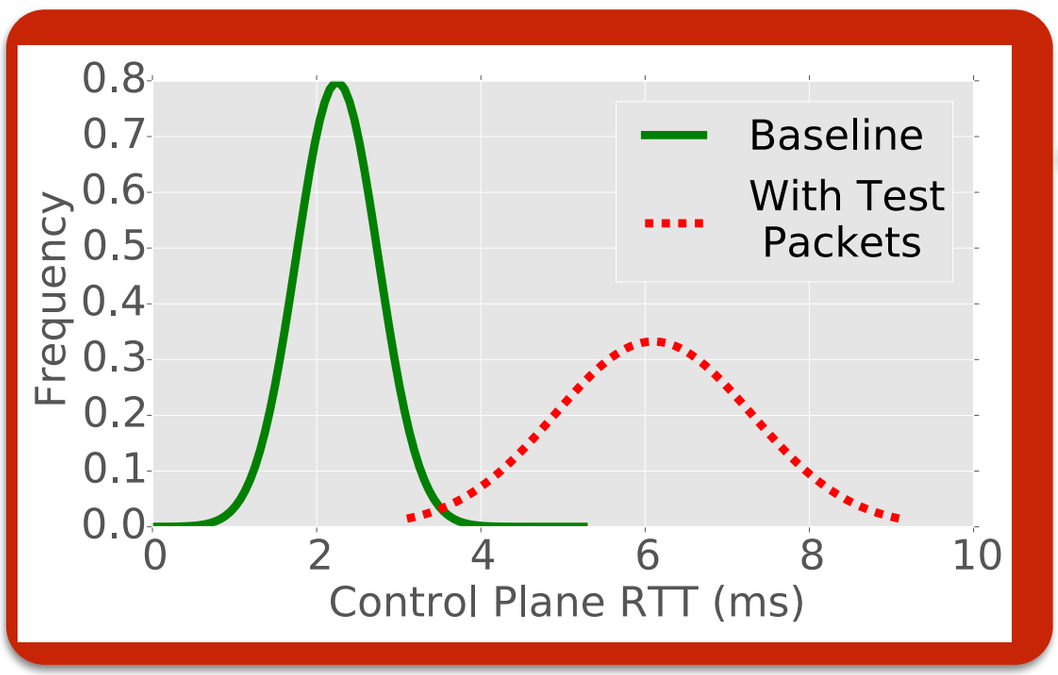
A More General Timing Attack

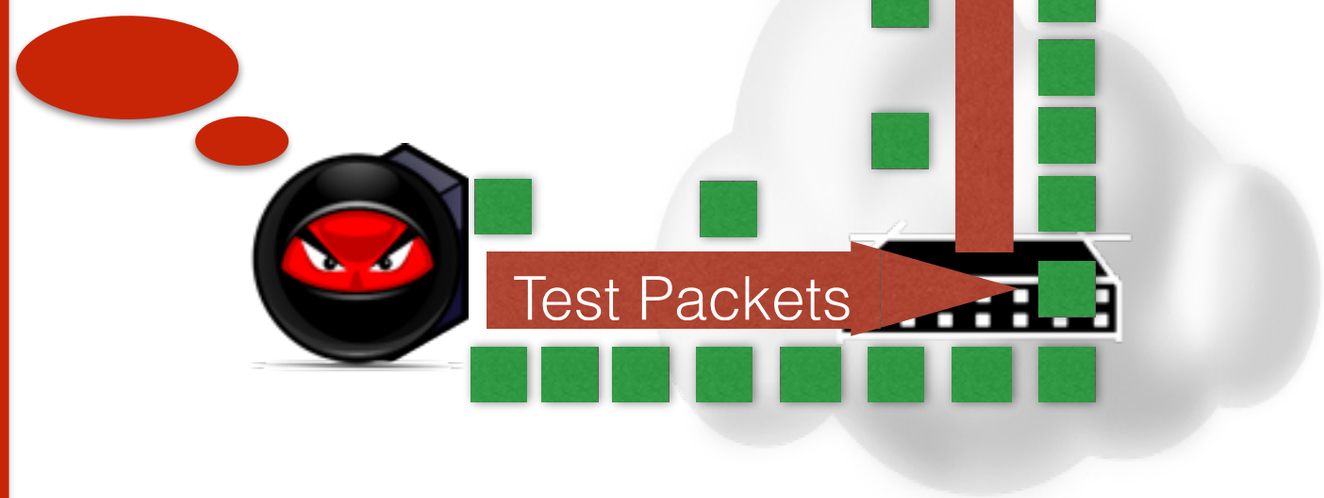
Evaluation on Real Hardware

Defense

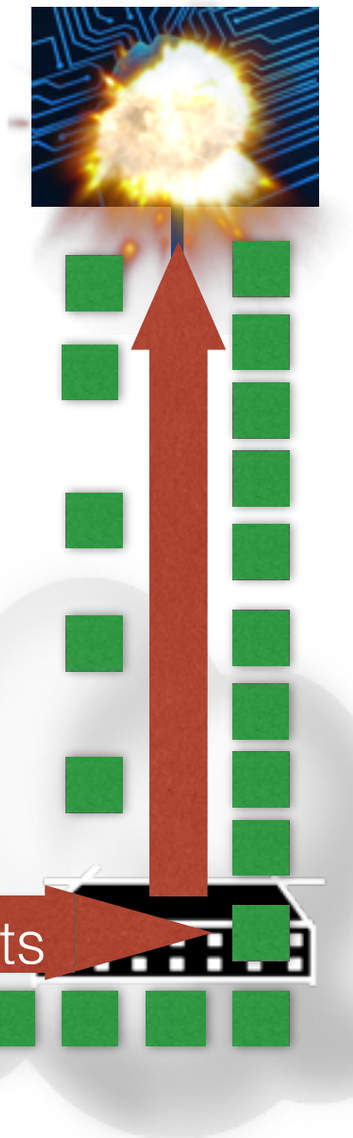
Defending Against Control Plane Timing Attacks

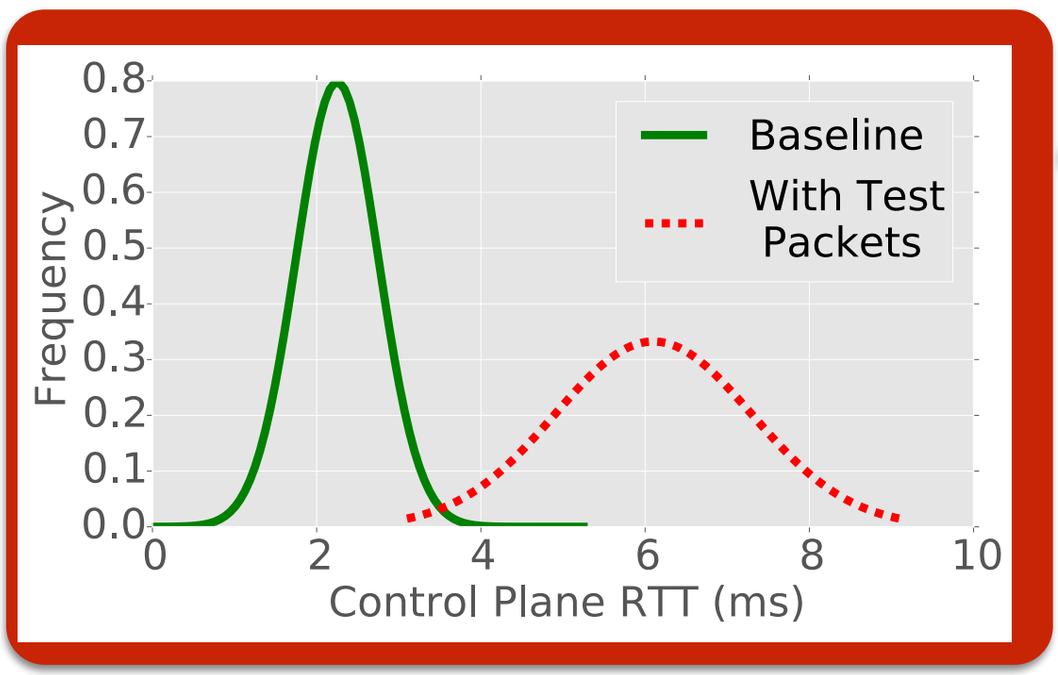




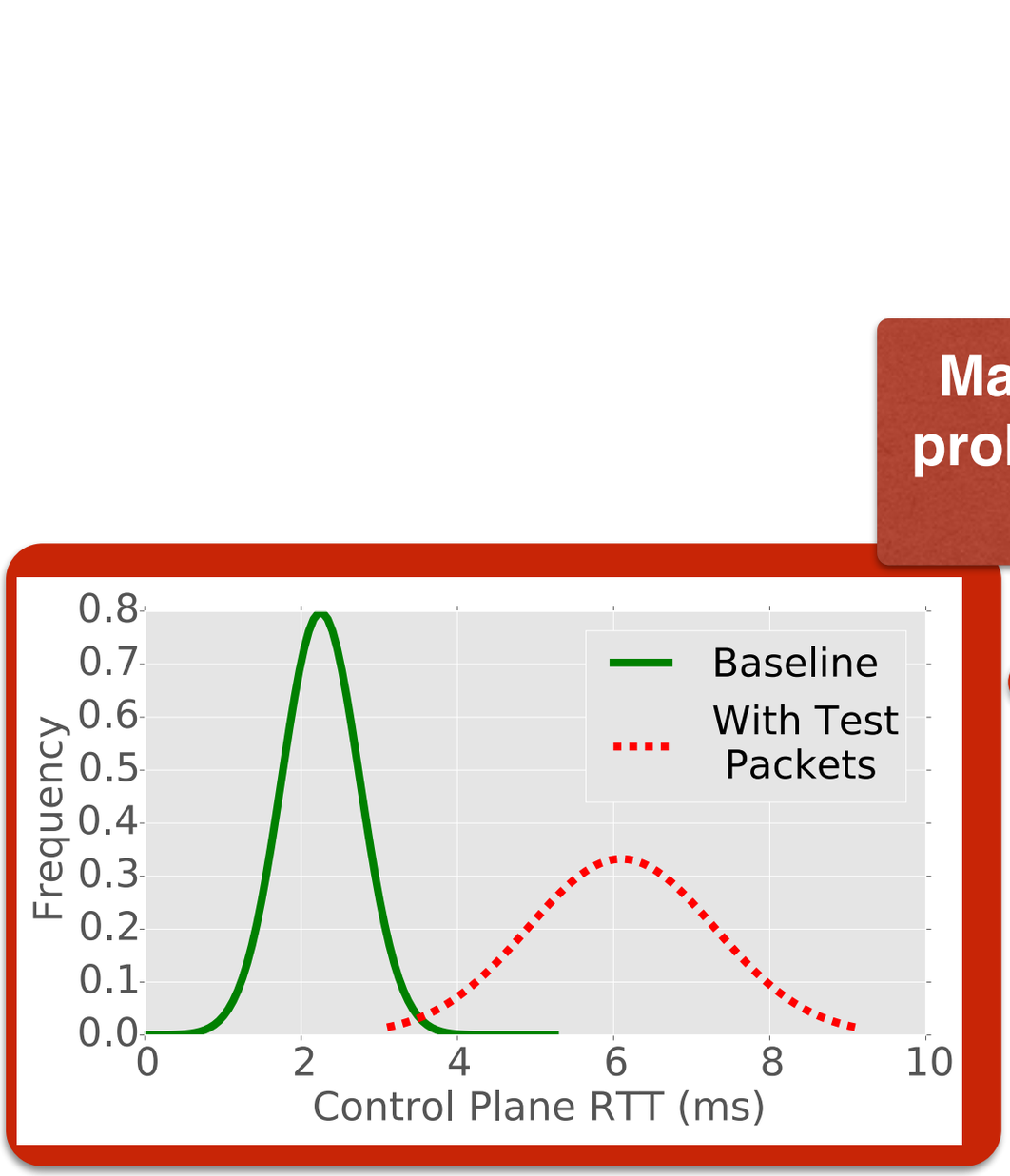


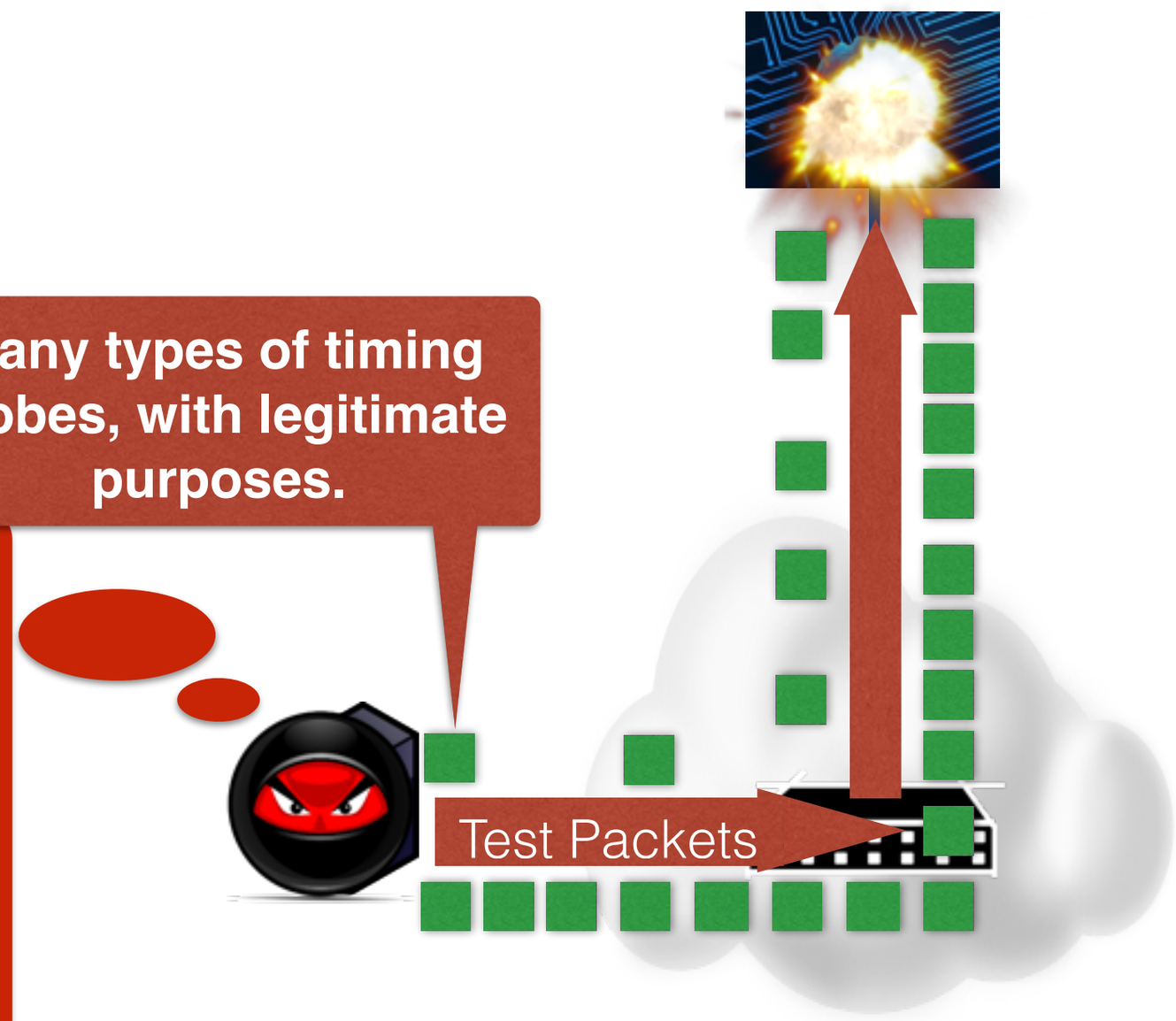
Defending Against Control Plane Timing Attacks: Challenges



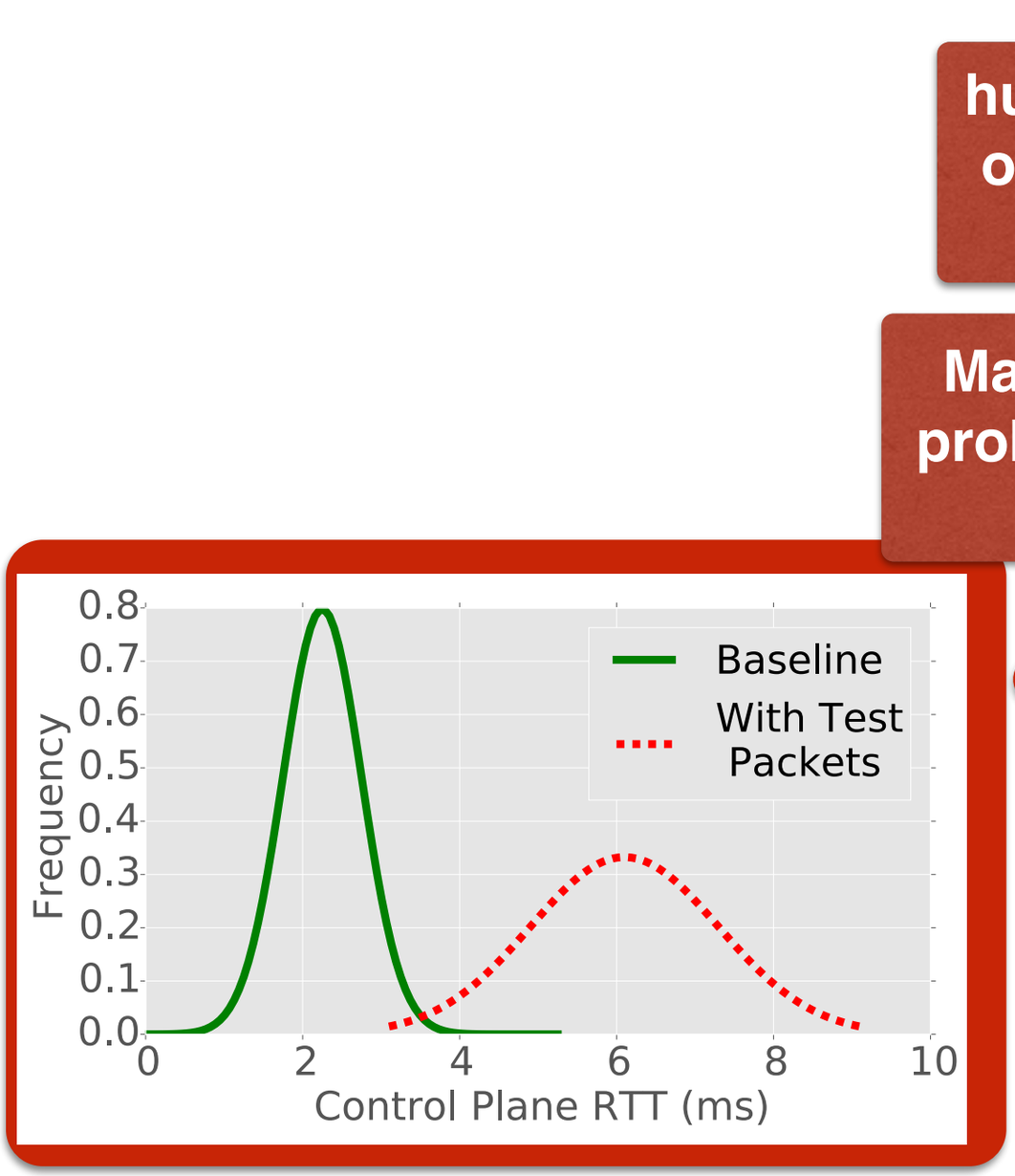


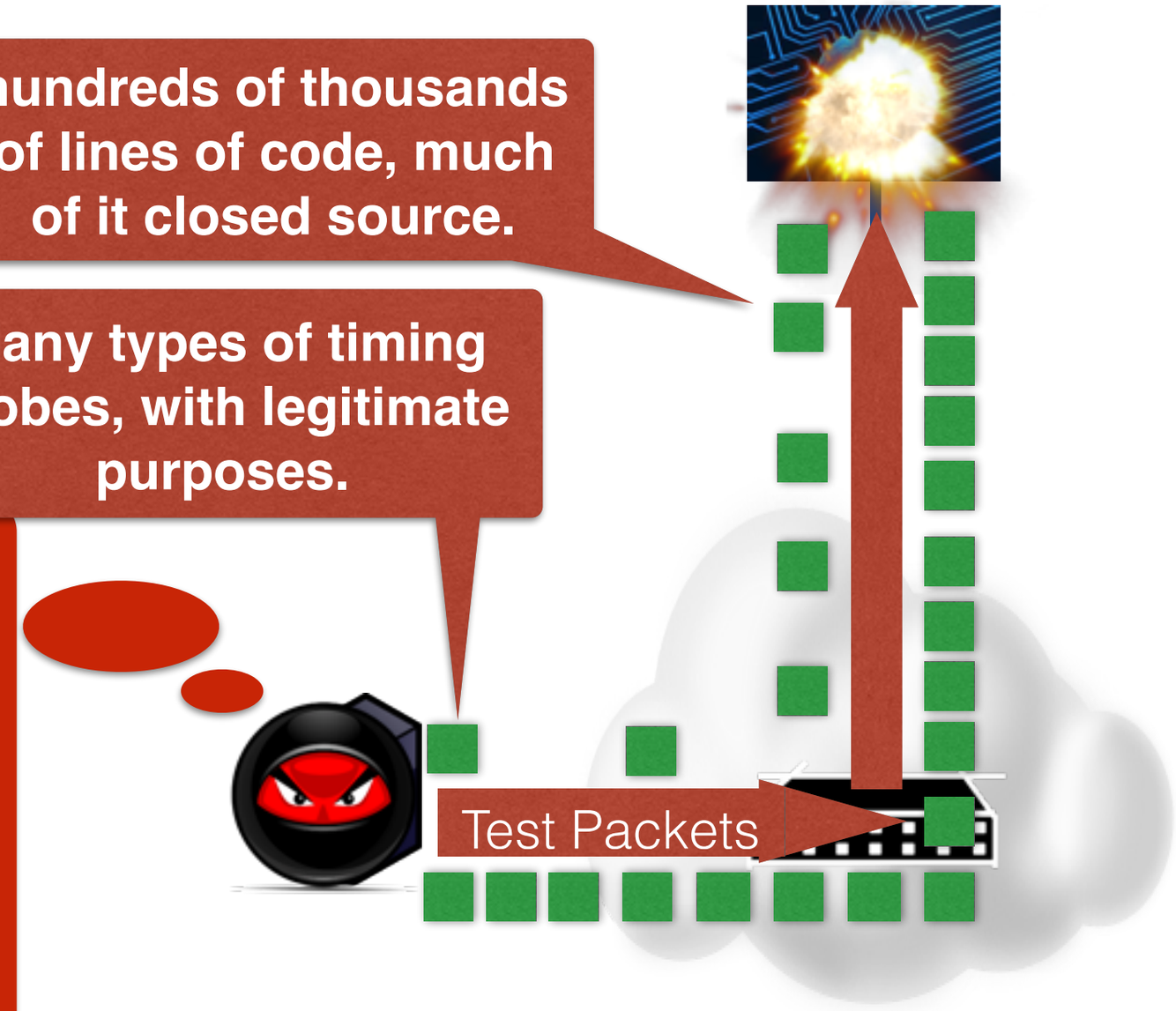
Defending Against Control Plane Timing Attacks: Challenges





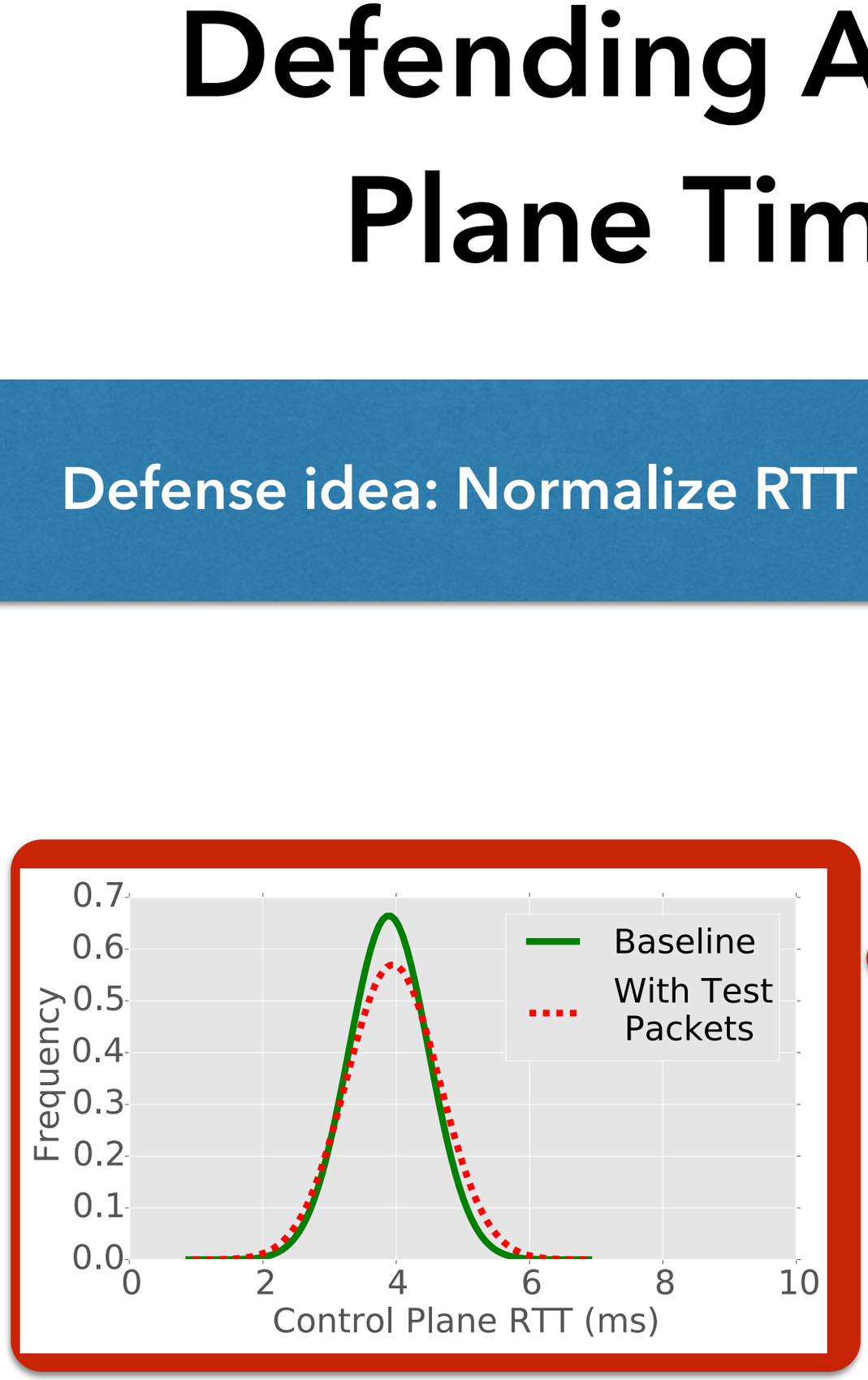
Defending Against Control Plane Timing Attacks: Challenges

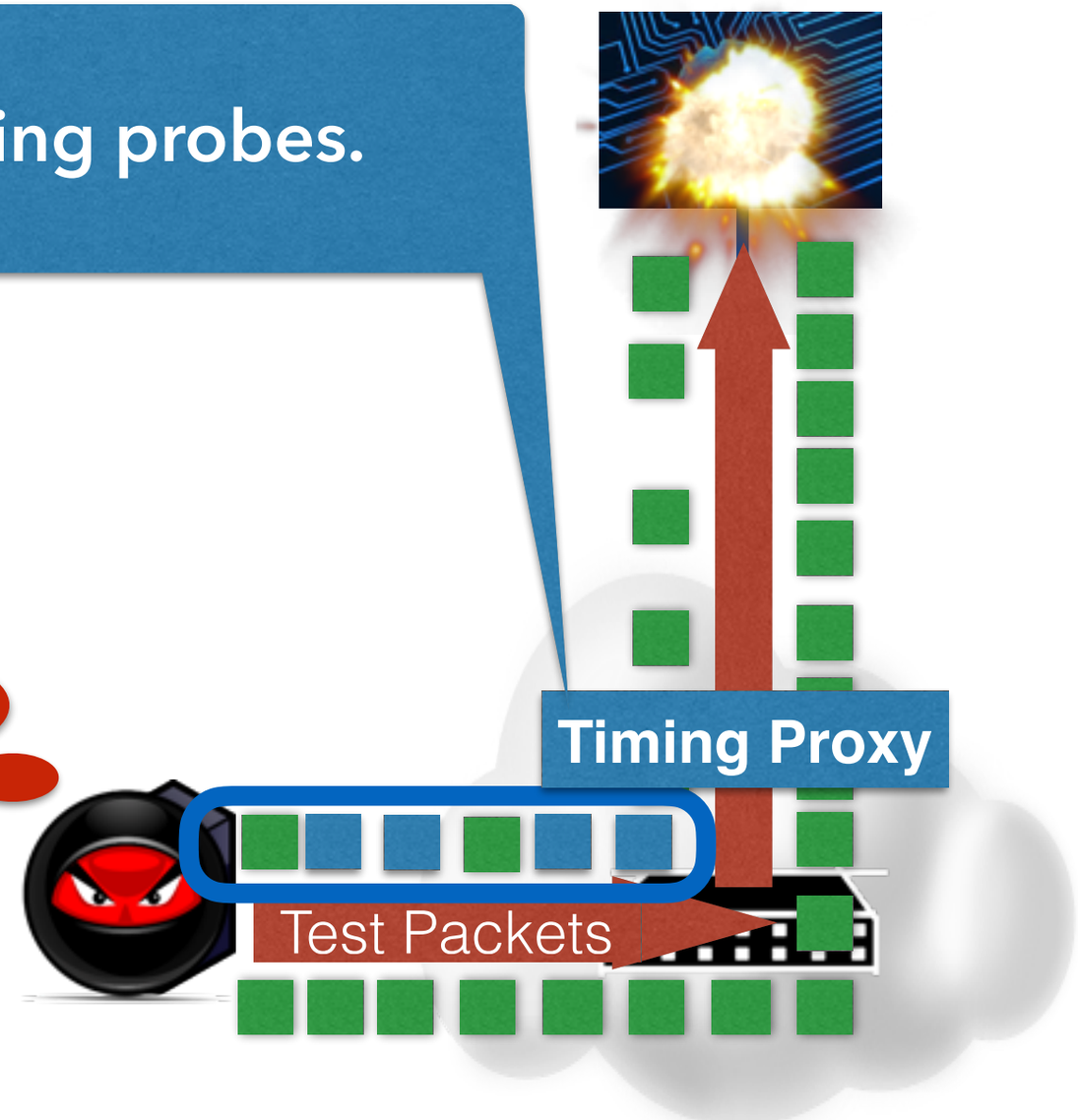




Defending Against Control Plane Timing Attacks

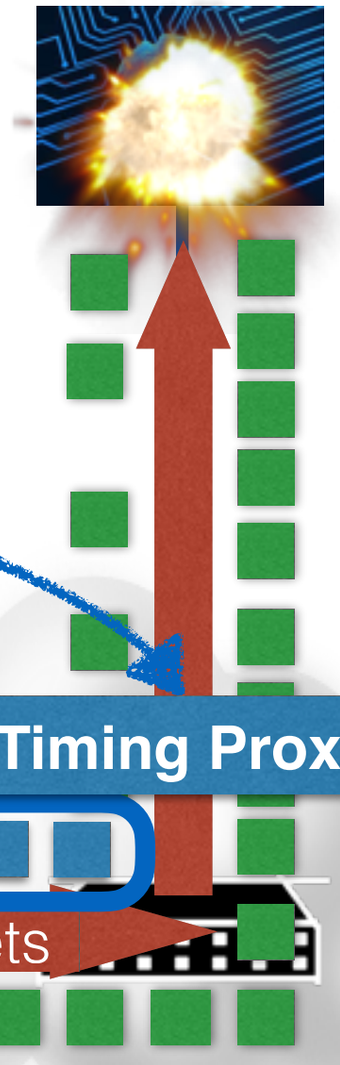
Defense idea: Normalize RTT of timing probes.

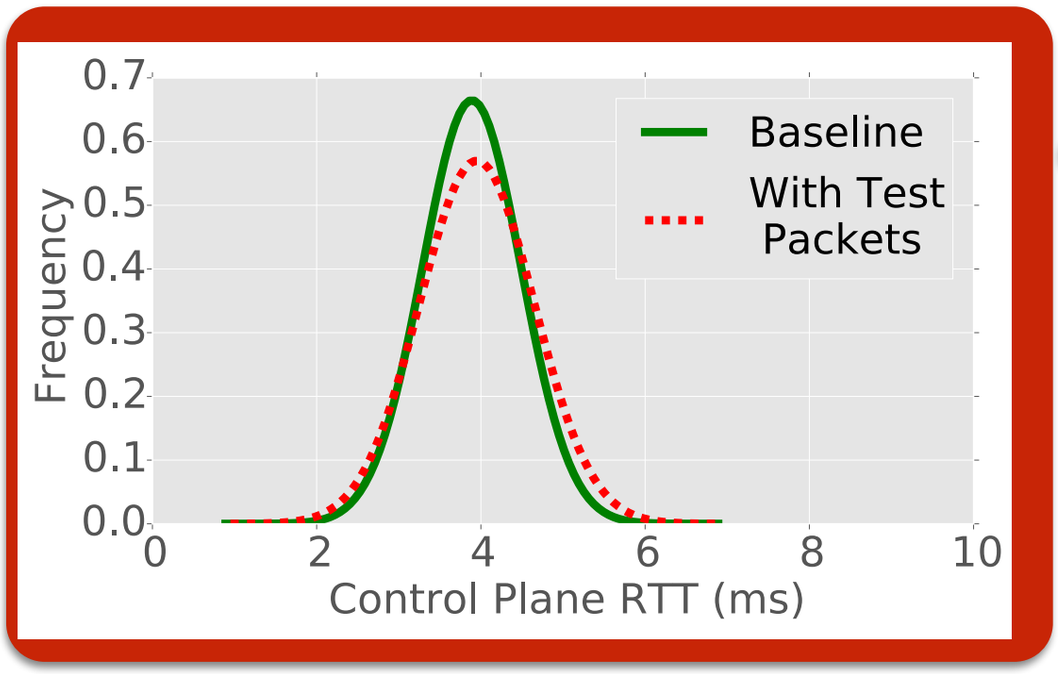




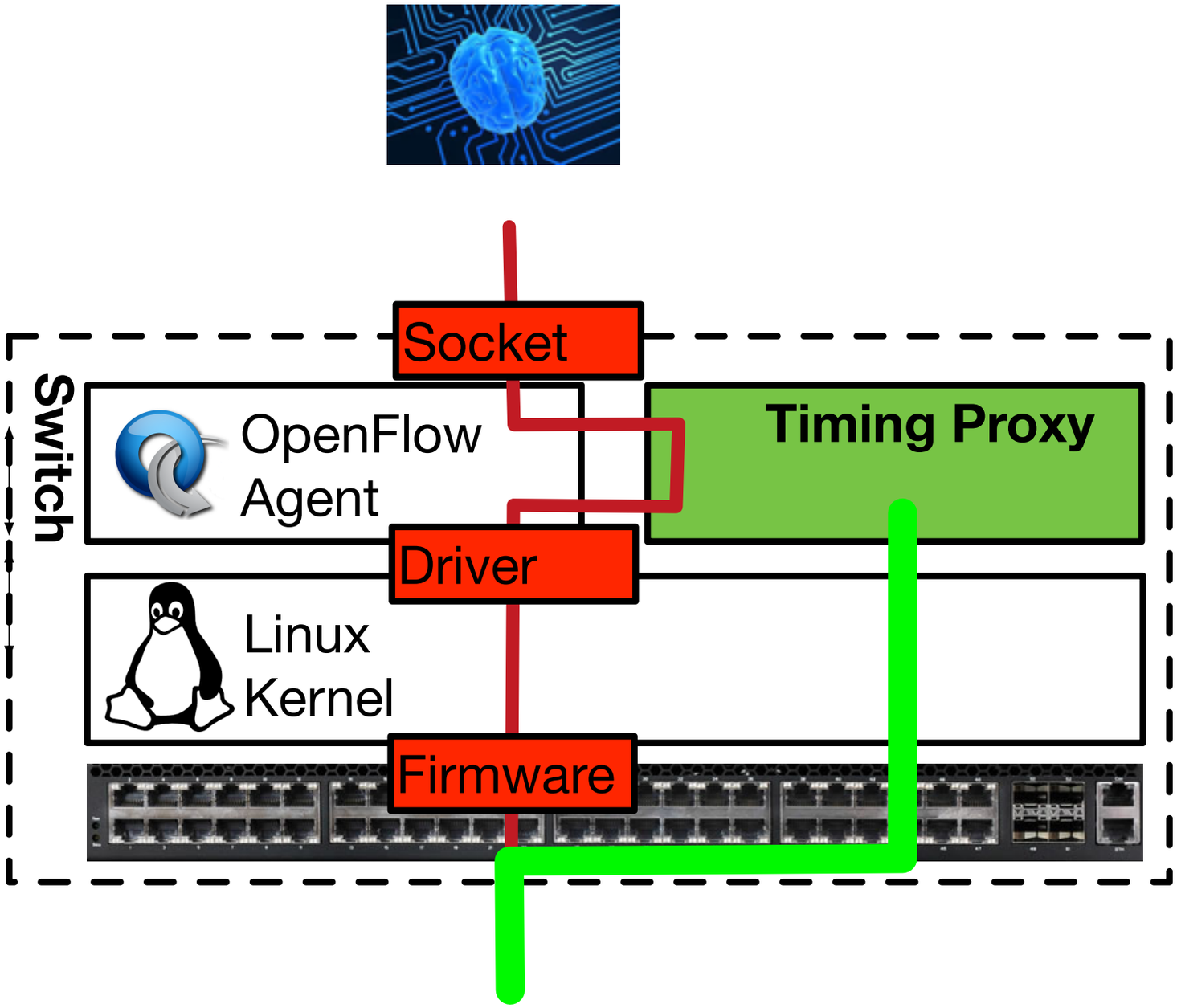
Defending Against Control Plane Timing Attacks

Time Bound: 3.5 - 4.5ms
Timeout Action: Flood

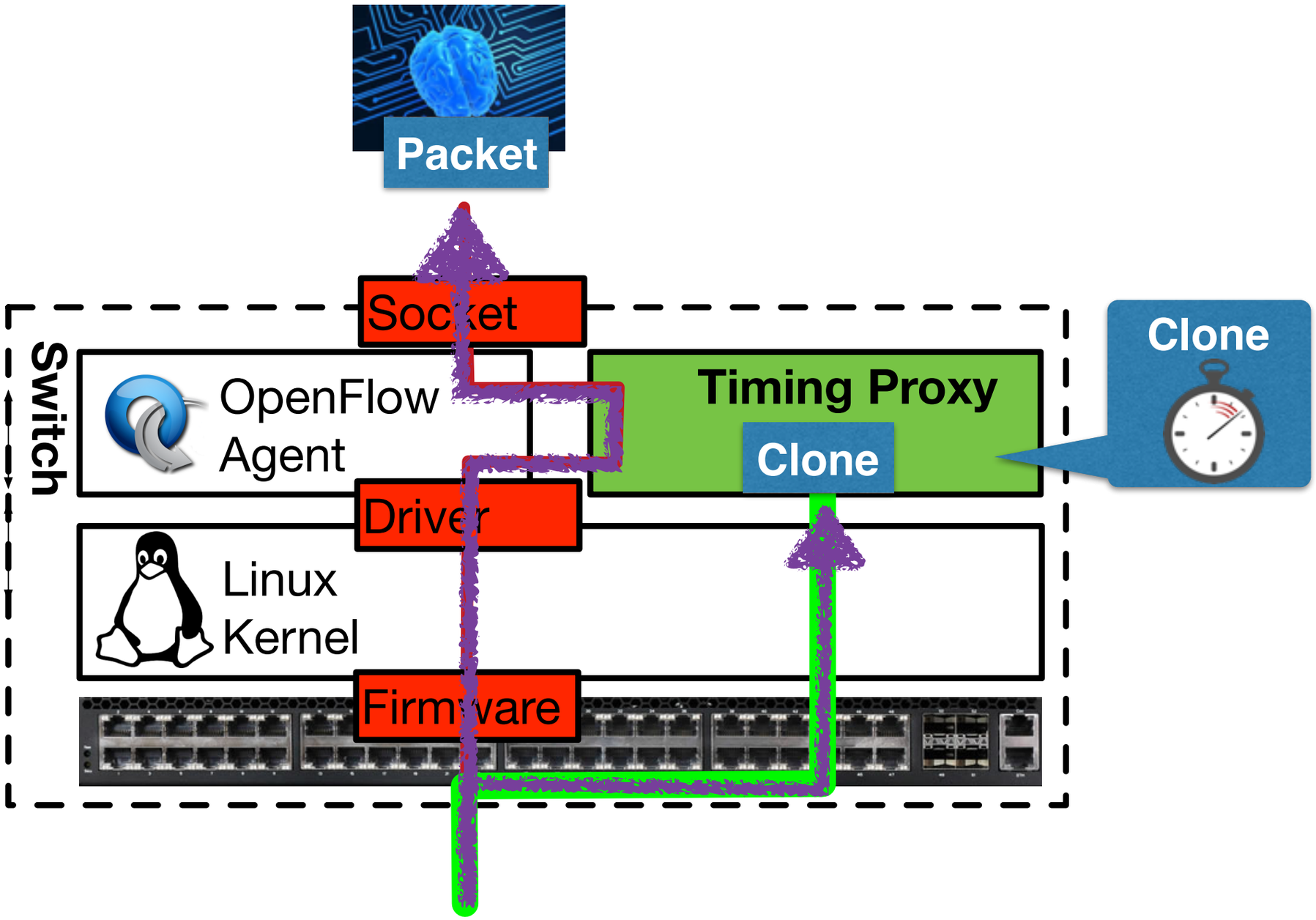




Timing Proxy Implementation

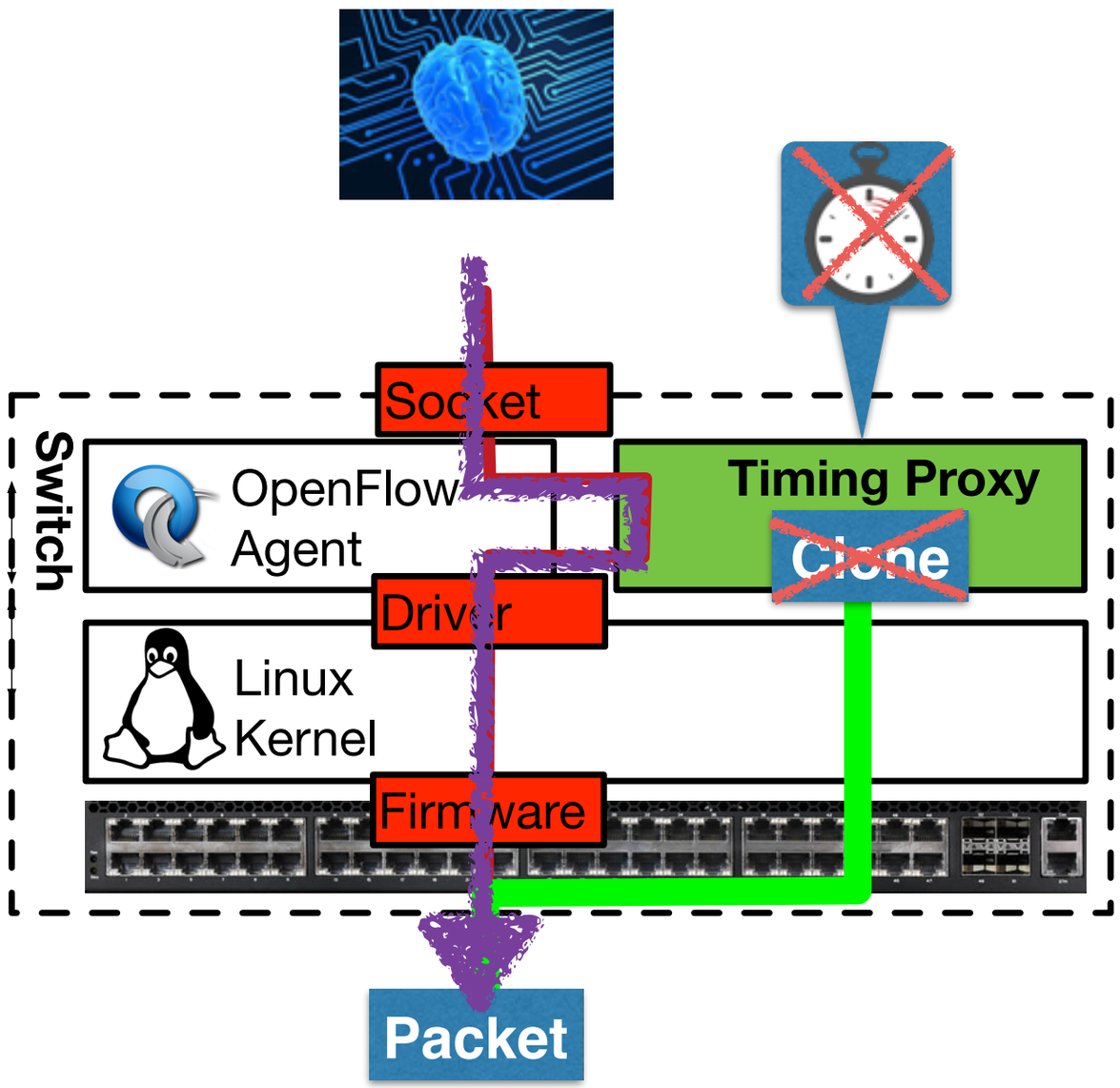


Timing Proxy Implementation

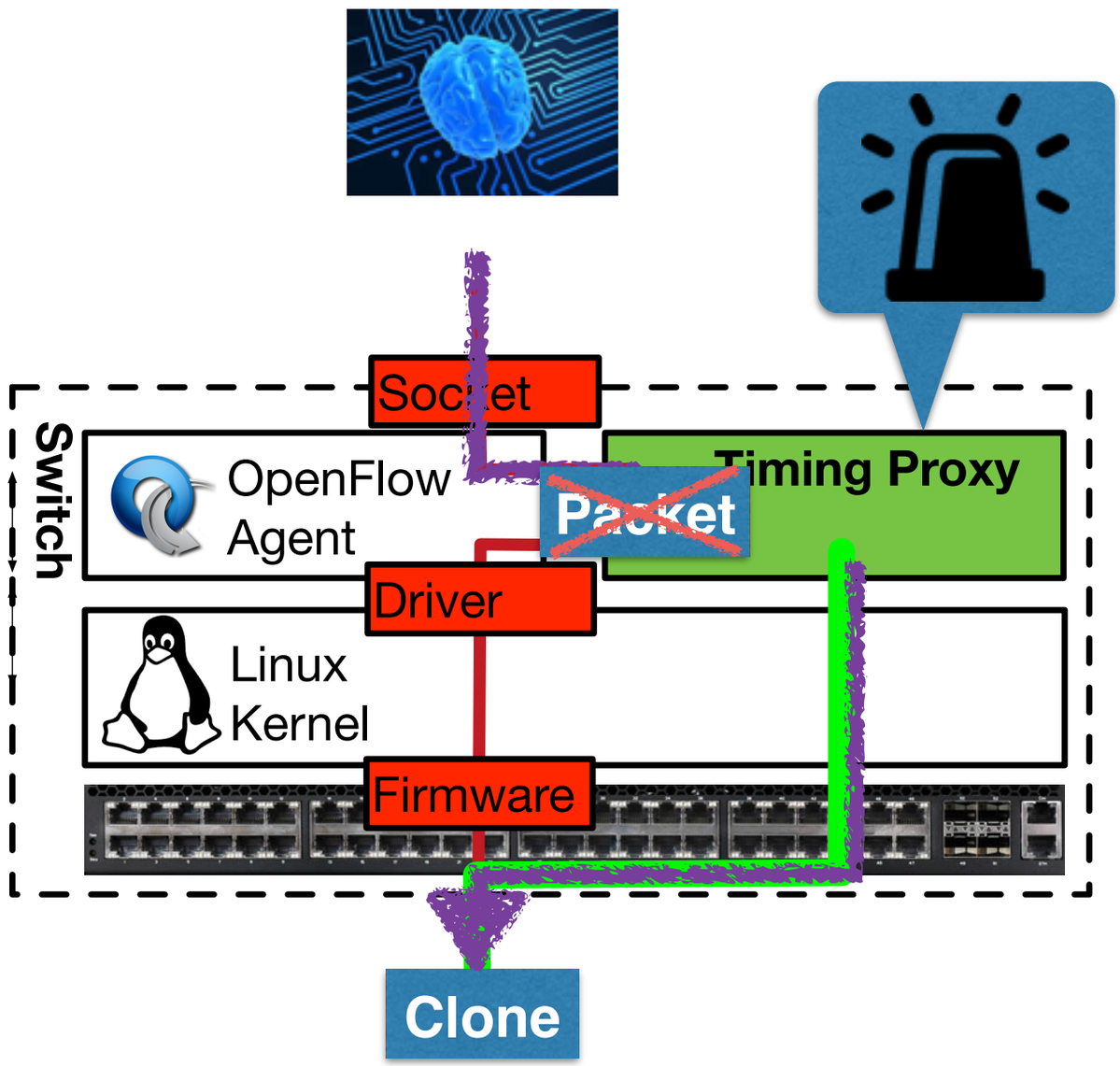


Timing Proxy Implementation

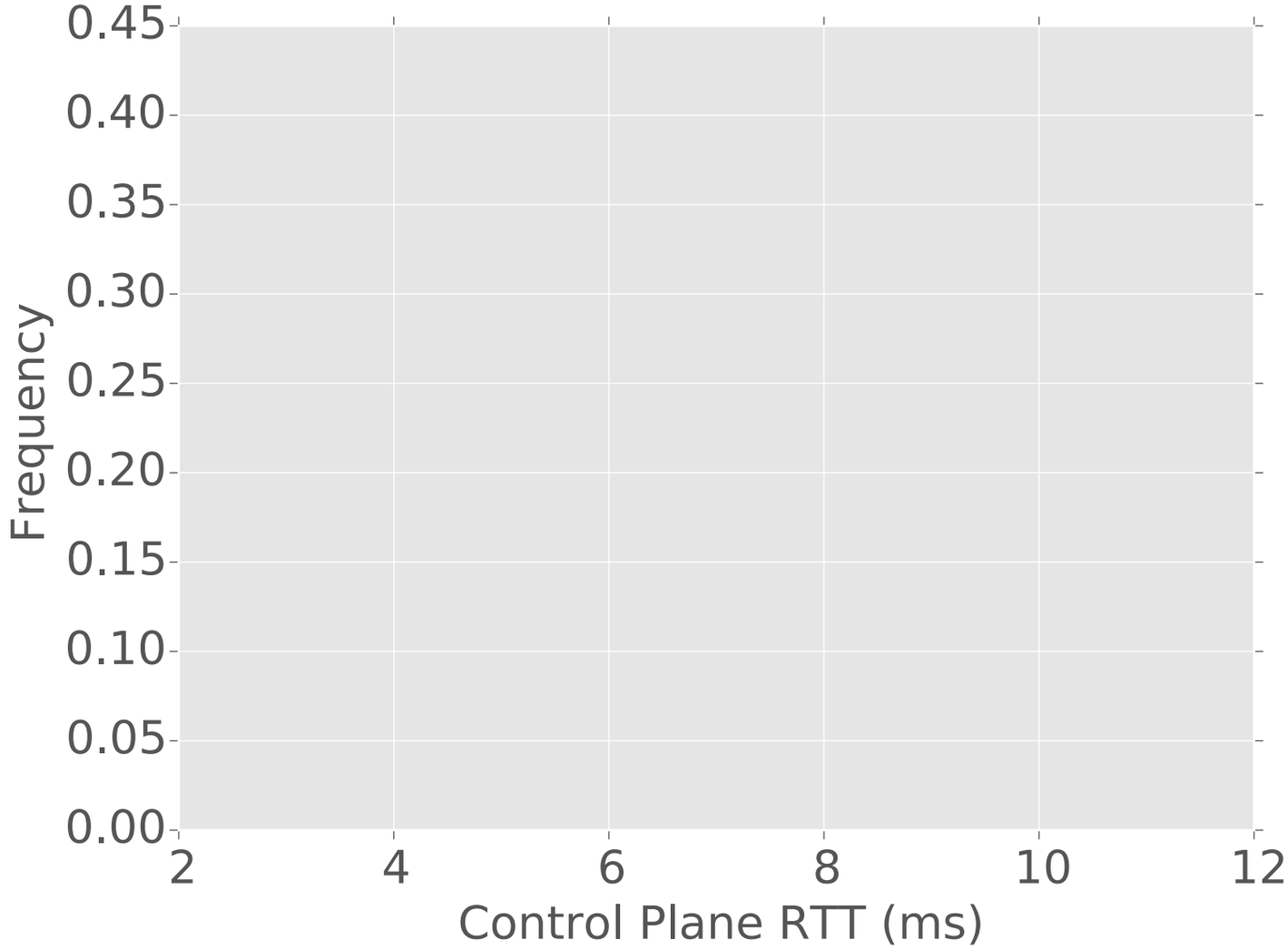
Controller responds in time



Controller times out



Timing Proxy Evaluation

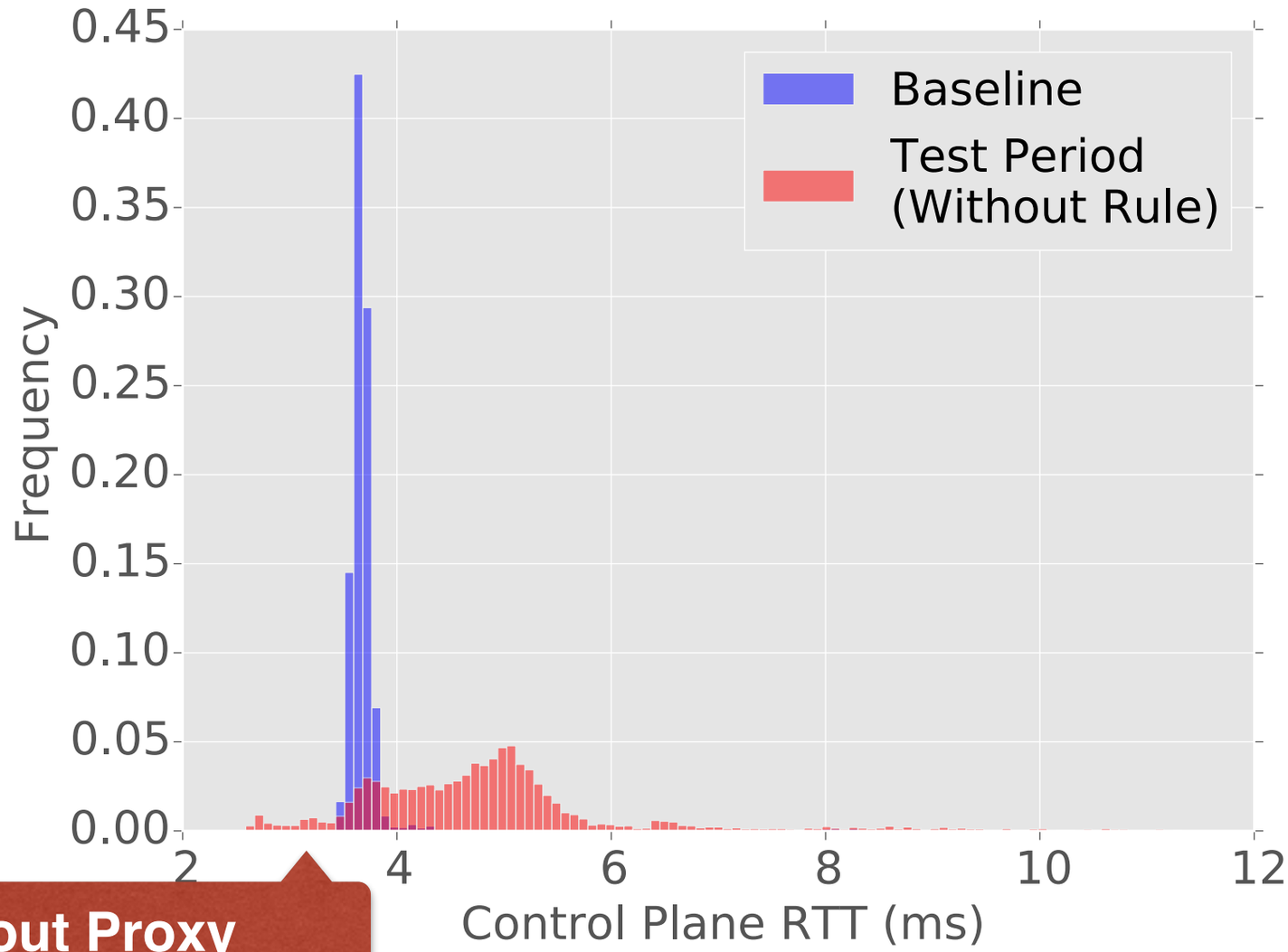


Parameters:

Timing Probe Rate: 10 **Test Flow Packet Rate**: 500

Trial Duration: 10 seconds **Trial Count**: 100 **Timing Bound:** 10-12 ms

Timing Proxy Evaluation



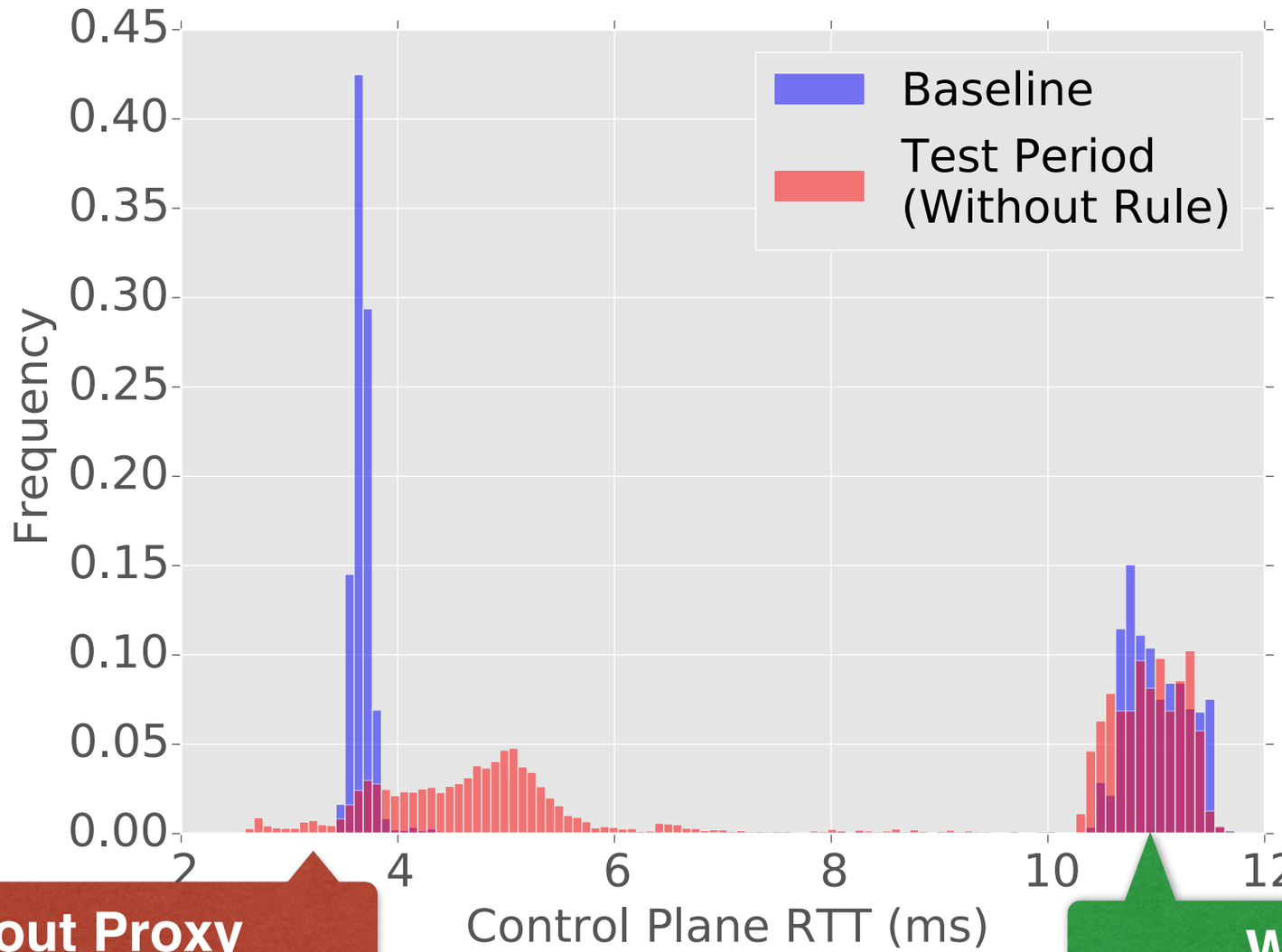
Without Proxy
(test flow changed timing distribution)

Parameters:

Timing Probe Rate: 10 **Test Flow Packet Rate**: 500

Trial Duration: 10 seconds **Trial Count**: 100 **Timing Bound:** 10-12 ms

Timing Proxy Evaluation



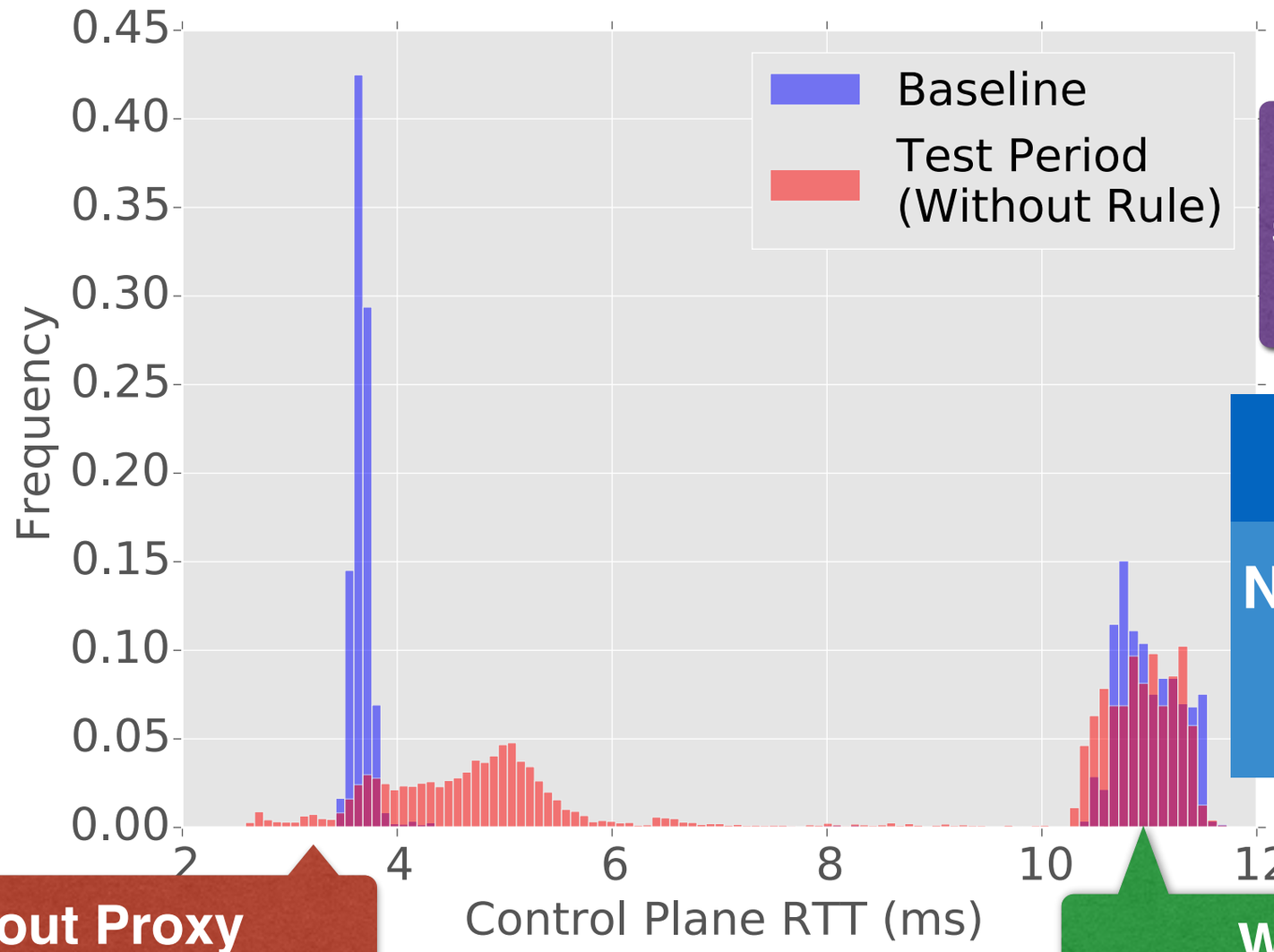
Without Proxy
(test flow changed timing distribution)

With Proxy
(test flow did not change timing distribution)

Parameters:

Timing Probe Rate: 10 **Test Flow Packet Rate**: 500
Trial Duration: 10 seconds **Trial Count**: 100 **Timing Bound:** 10-12 ms

Timing Proxy Evaluation



Attack is only slightly better than random guessing!

T-test	Accuracy
No Proxy	100%
Proxy	**59%**

Without Proxy
(test flow changed timing distribution)

With Proxy
(test flow did not change timing distribution)

Parameters:

Timing Probe Rate: 10 **Test Flow Packet Rate**: 500
Trial Duration: 10 seconds **Trial Count**: 100 **Timing Bound:** 10-12 ms

Outline

Timing Side Channels in SDNs

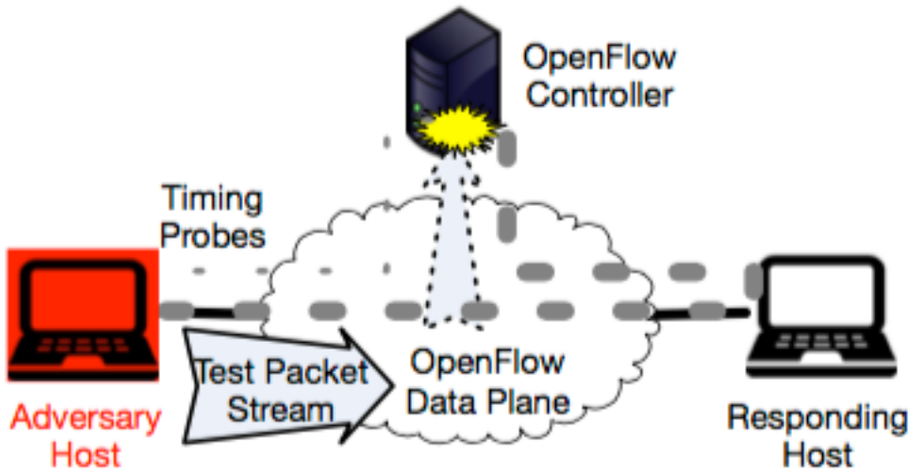
A More General Timing Attack

Evaluation on Real Hardware

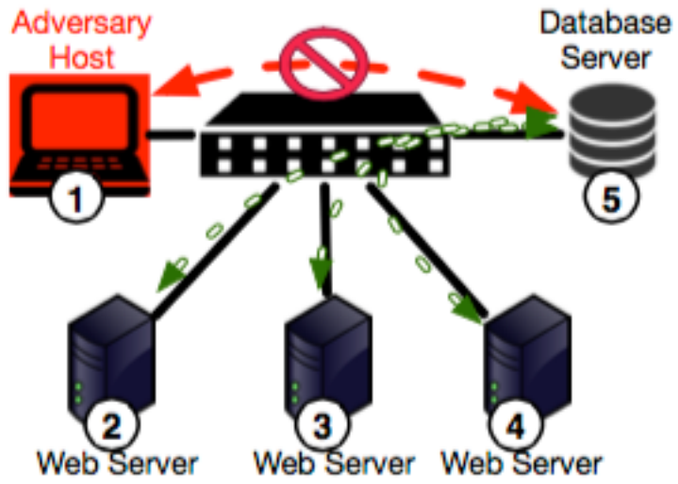
Defense

In The Paper

Attack Details

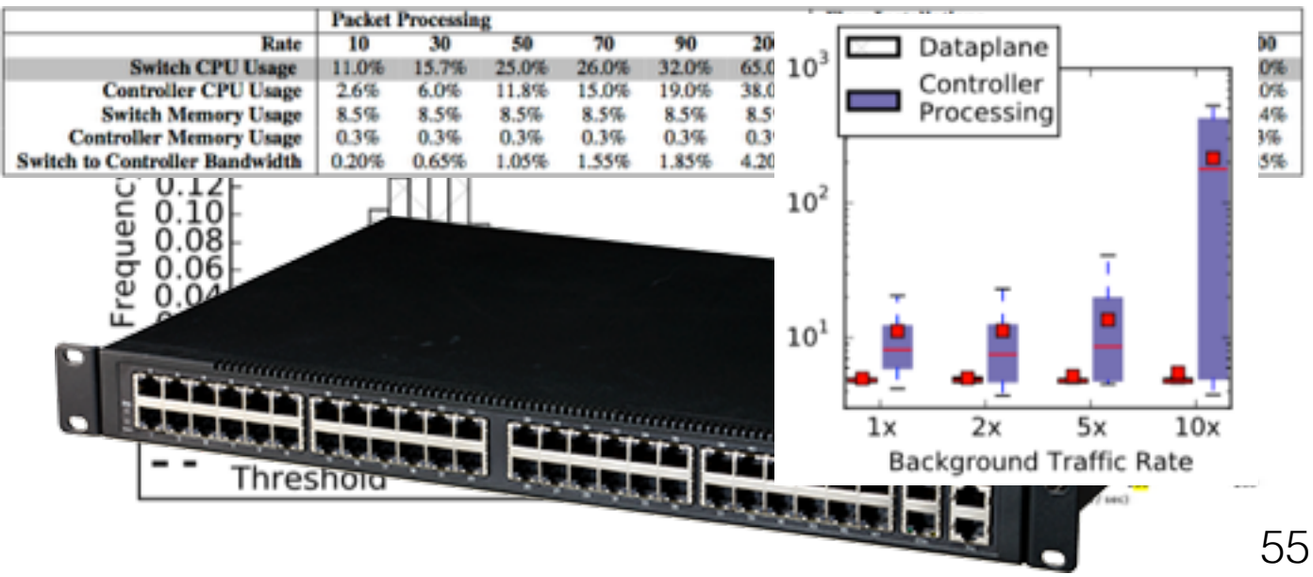


Attack Applications

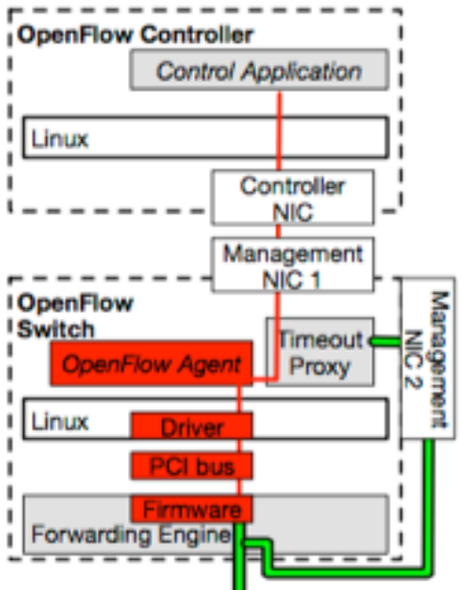


Measurements

	Packet Processing					
Rate	10	30	50	70	90	20
Switch CPU Usage	11.0%	15.7%	25.0%	26.0%	32.0%	65.0
Controller CPU Usage	2.6%	6.0%	11.8%	15.0%	19.0%	38.0
Switch Memory Usage	8.5%	8.5%	8.5%	8.5%	8.5%	8.5
Controller Memory Usage	0.3%	0.3%	0.3%	0.3%	0.3%	0.3
Switch to Controller Bandwidth	0.20%	0.65%	1.05%	1.55%	1.85%	4.20



Defense Details



Thank You!

Timing-based Reconnaissance and Defense in Software-defined Networks

- **SDNs have timing side-channels** that leak sensitive information about networks.
- Timing attacks are **effective against real SDN switches**, with background traffic present.
- Timeout rules plug the side channel, and **can be implemented on existing switches** as a proxy.

Penn
University of Pennsylvania

University of Colorado Boulder