Timing SDN Control Planes to Infer Network Configurations

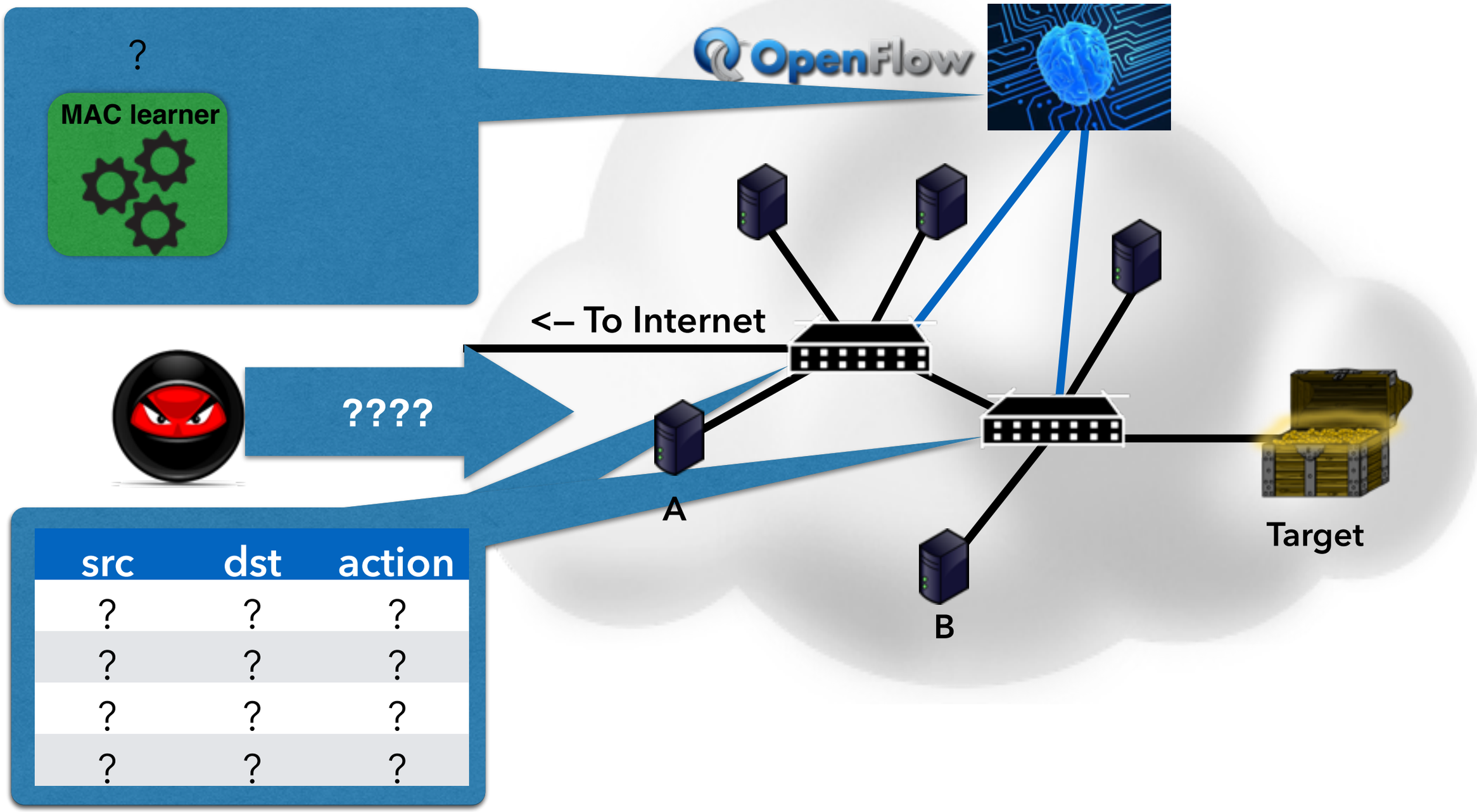
John Sonchack, *Adam J. Aviv and Eric Keller*

Penn
University of Pennsylvania

University of Colorado
Boulder

SCIENTIA UT AMICOS SERVEMUS
USNA
{0,1}
Computer Science and Information Technology
SCIENTIA UT HOSTES VINCAMUS

Attack Goal: Probe An OpenFlow Network to Learn its Configuration



Outline

Introduction

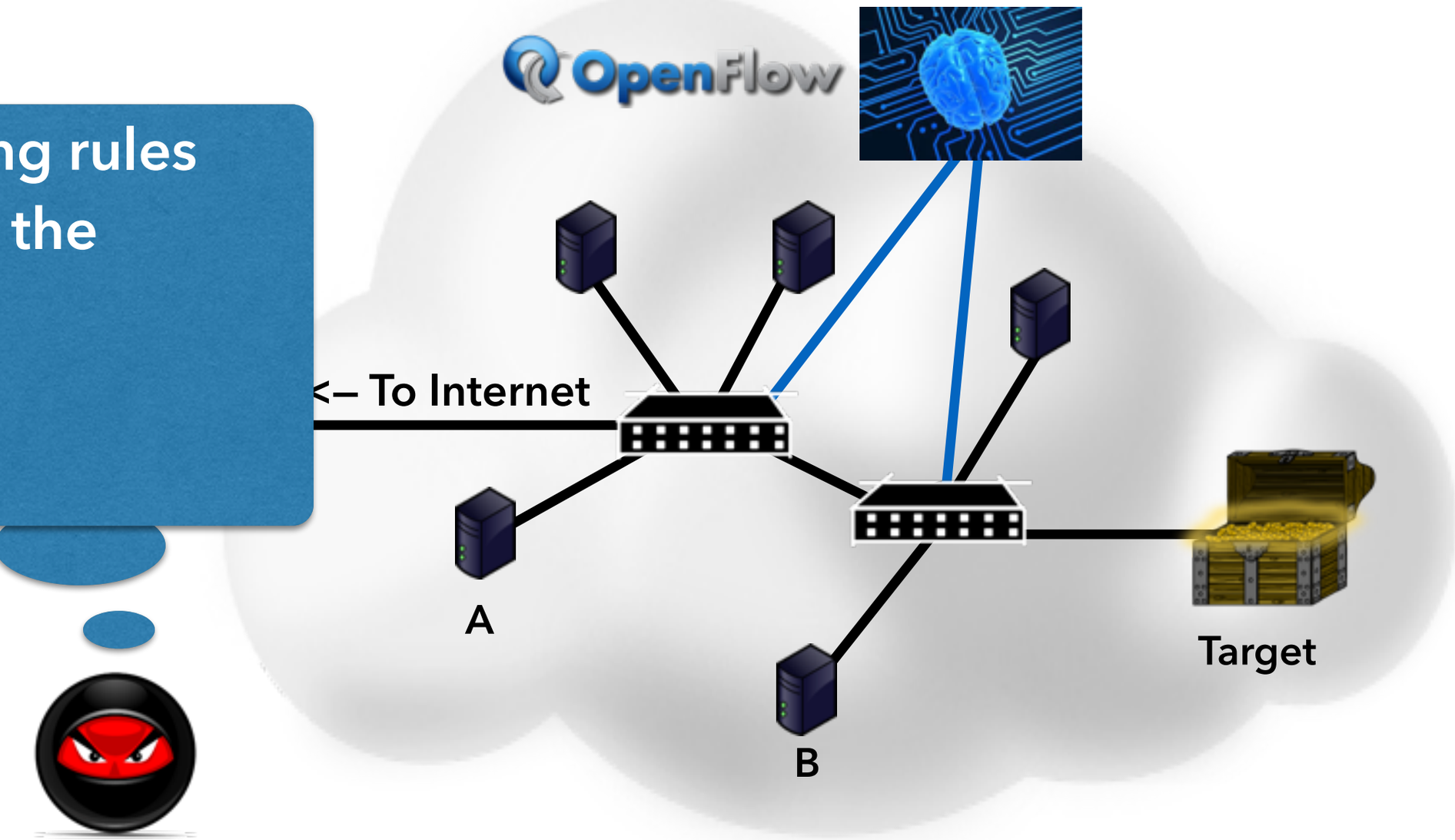
OpenFlow Timing Attacks

A More General OpenFlow Timing Attack

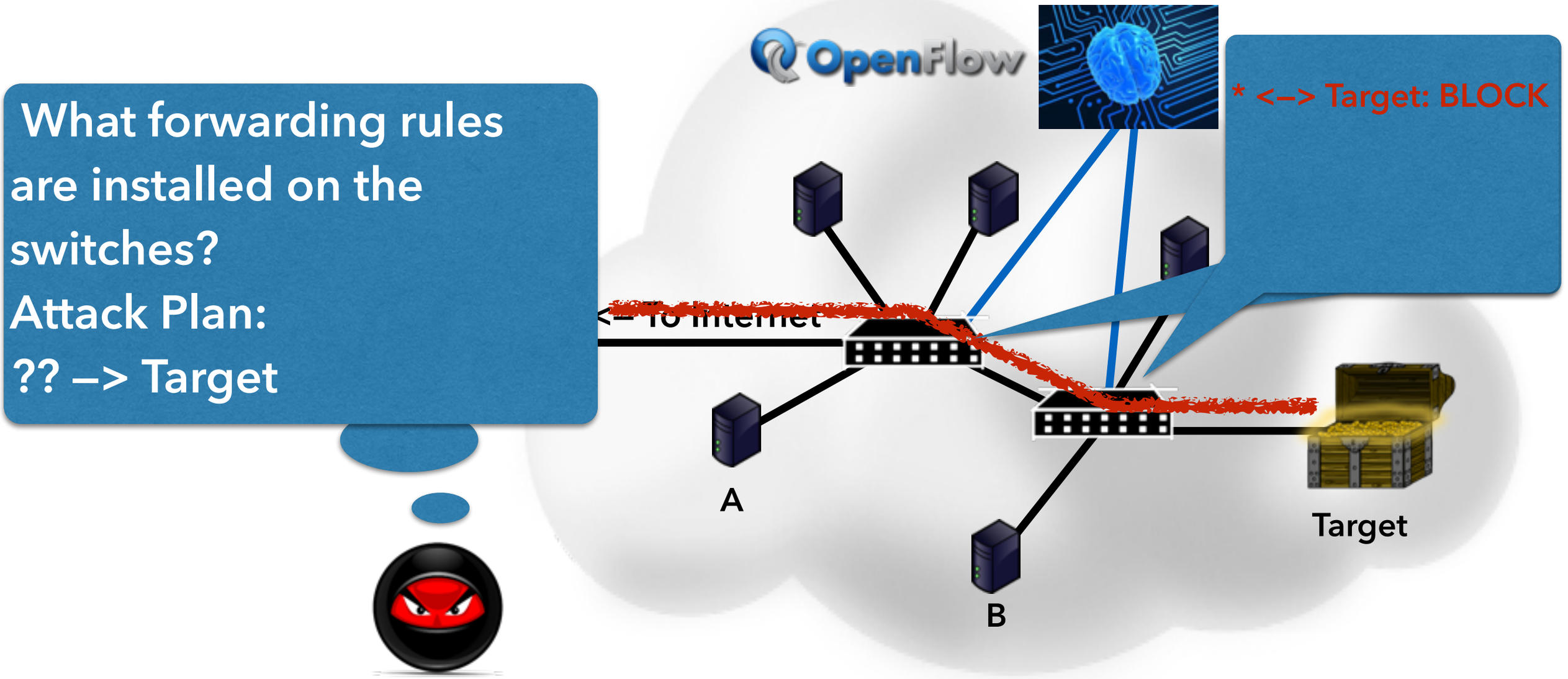
Preliminary Results

Motivation: Plan Multi-Staged Attacks

What forwarding rules are installed on the switches?



Motivation: Plan Multi-Staged Attacks

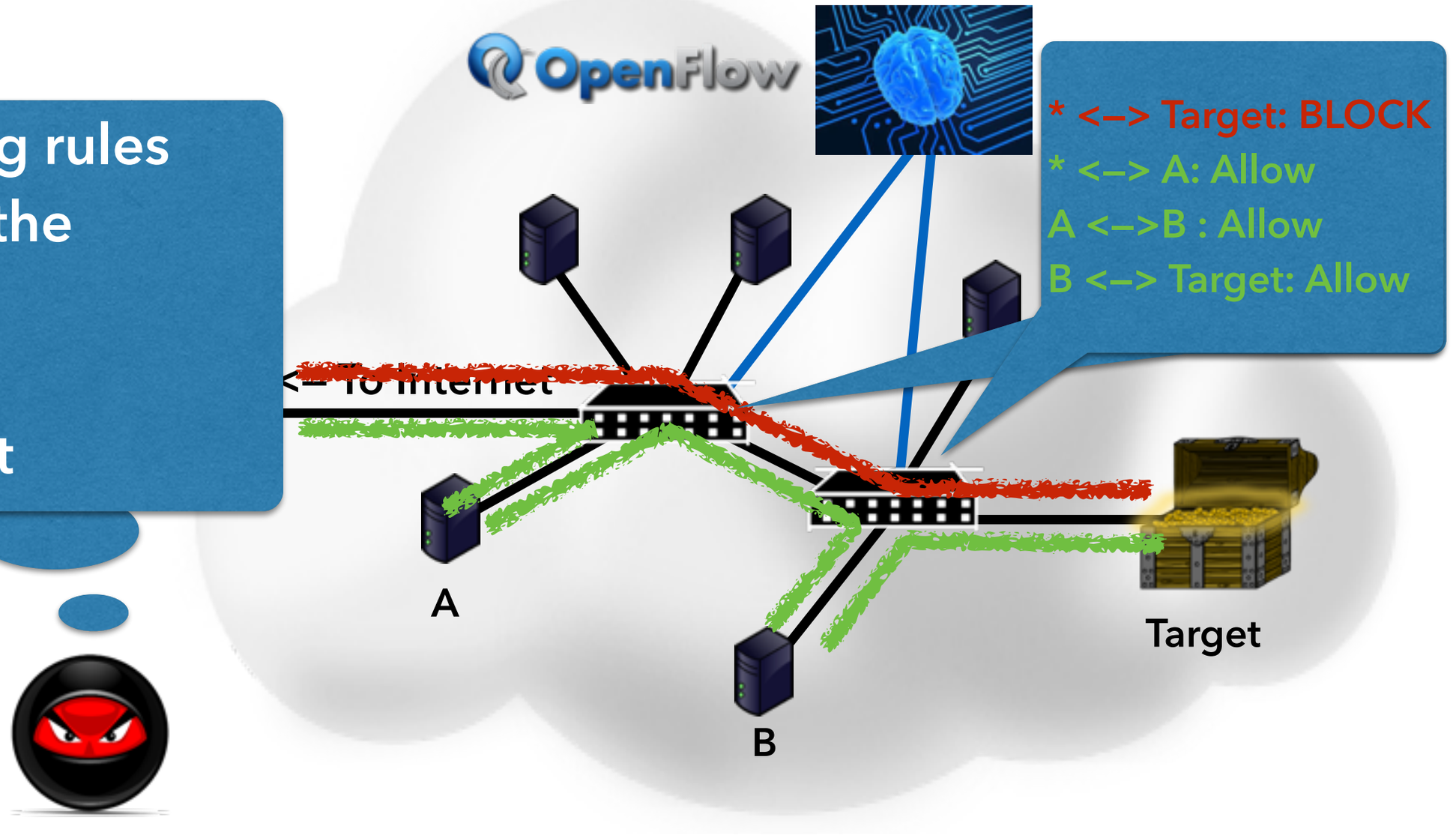


Motivation: Plan Multi-Staged Attacks

What forwarding rules are installed on the switches?

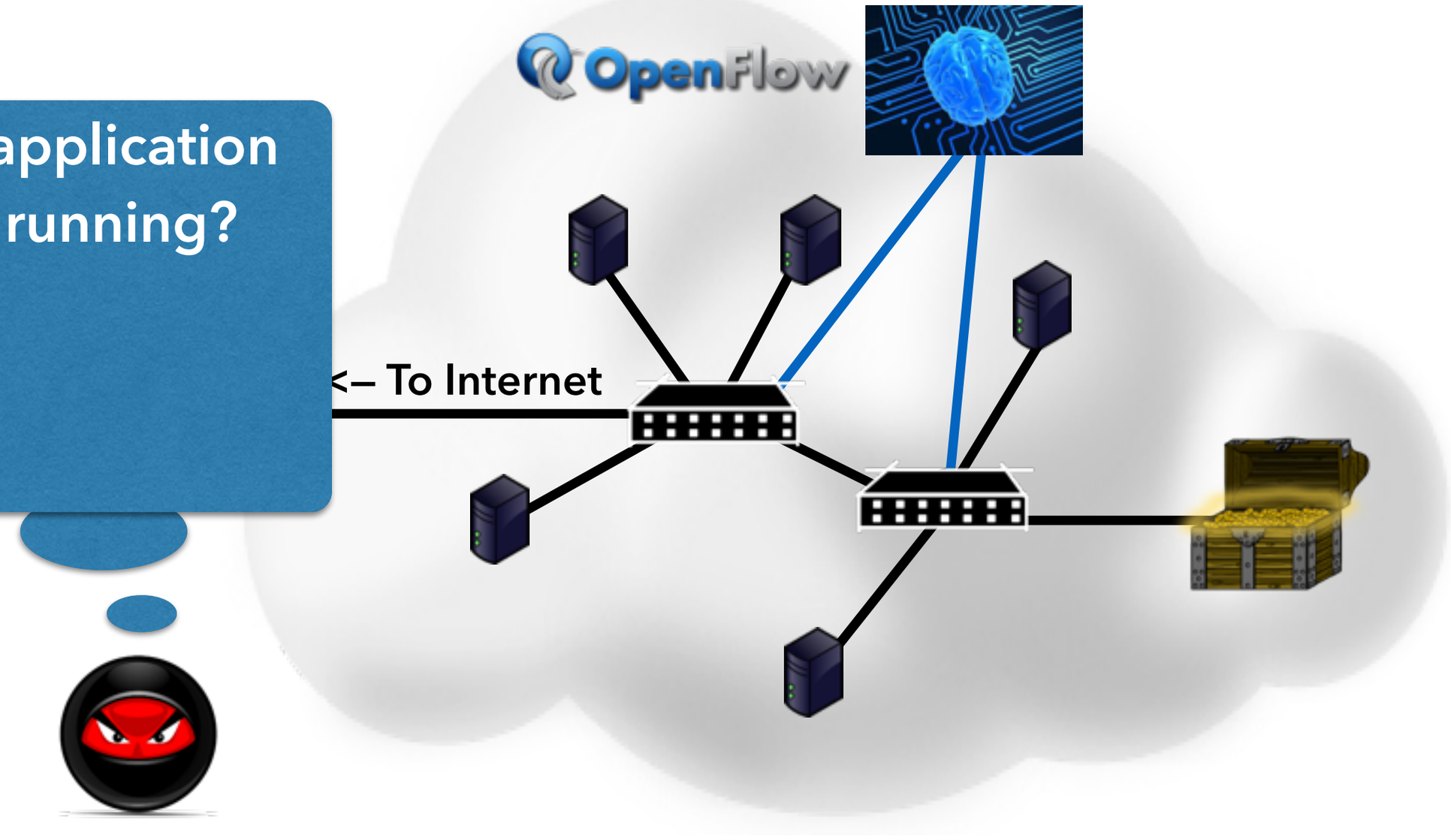
Attack Plan:

A –> B –> Target

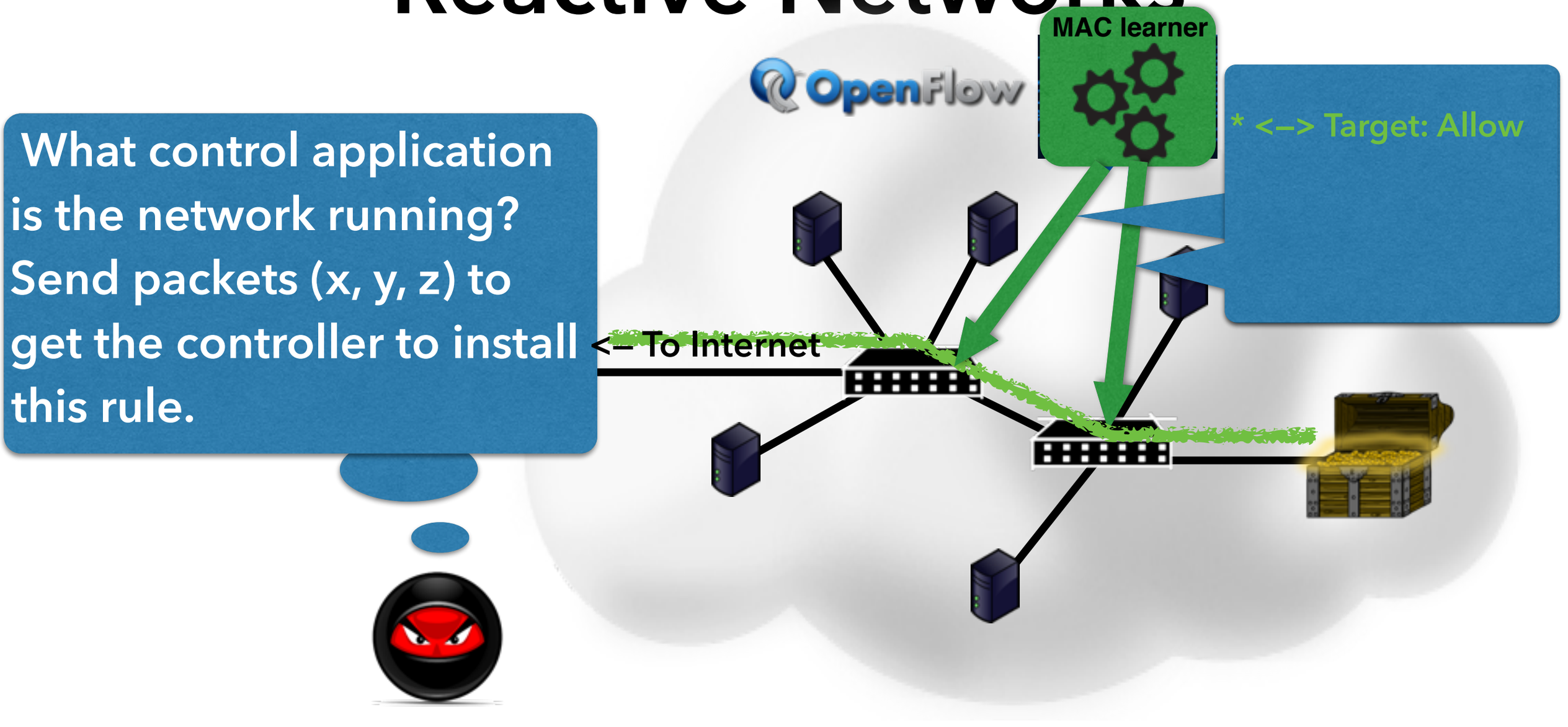


Motivation: Reprogramming Reactive Networks

What control application is the network running?



Motivation: Reprogramming Reactive Networks



Attack Goal: Probe An OpenFlow Network to Learn its Configuration

- **Which forwarding rules are installed?**

Motivation: makes multi-stage attacks easier to plan

- **When do new forwarding rules get installed?**

Motivation: makes reactive networks easier to reprogram for adversaries

Outline

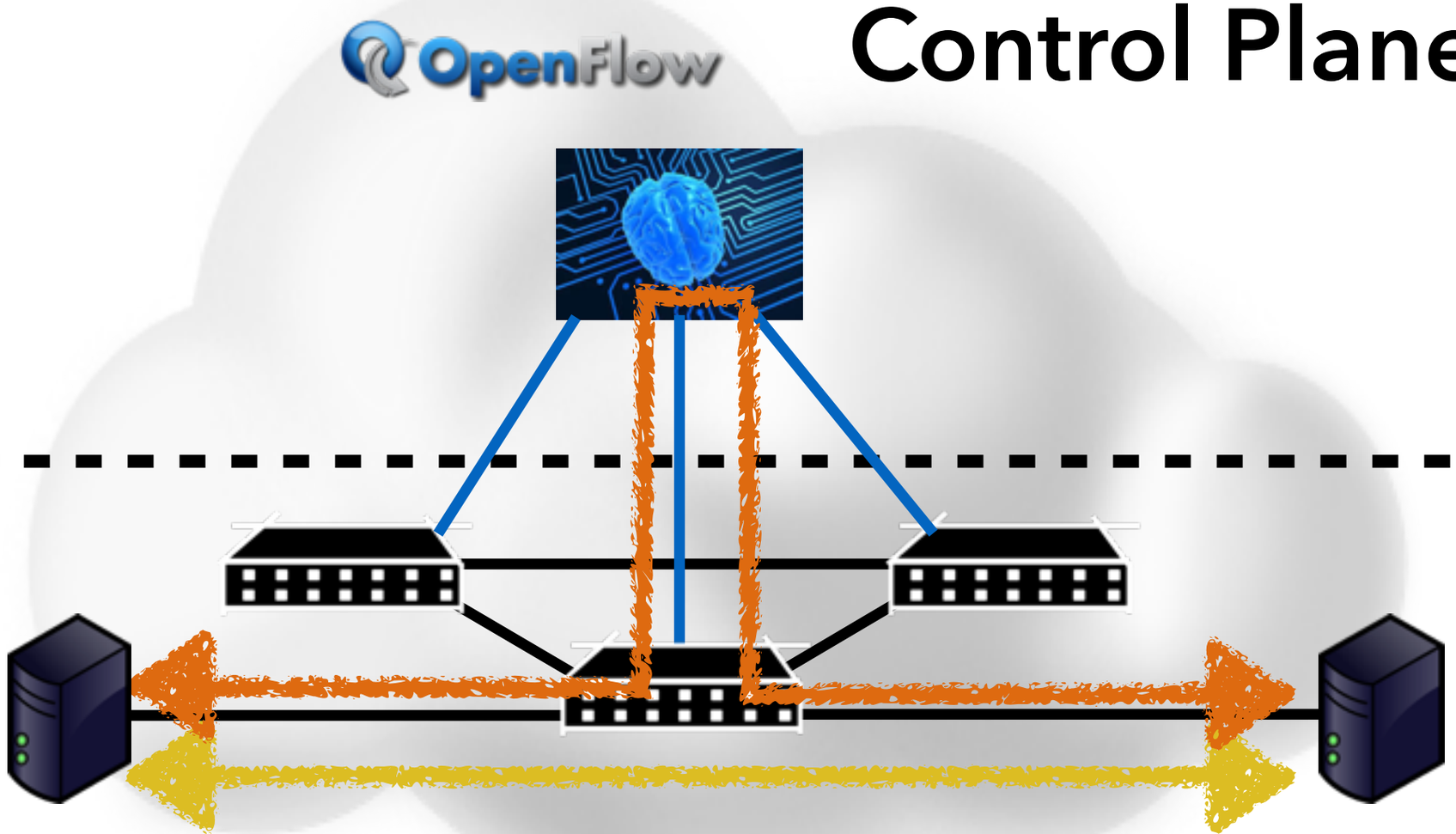
Introduction

OpenFlow Timing Attacks

A More General OpenFlow Timing Attack

Preliminary Results

A Simple OpenFlow Timing Property



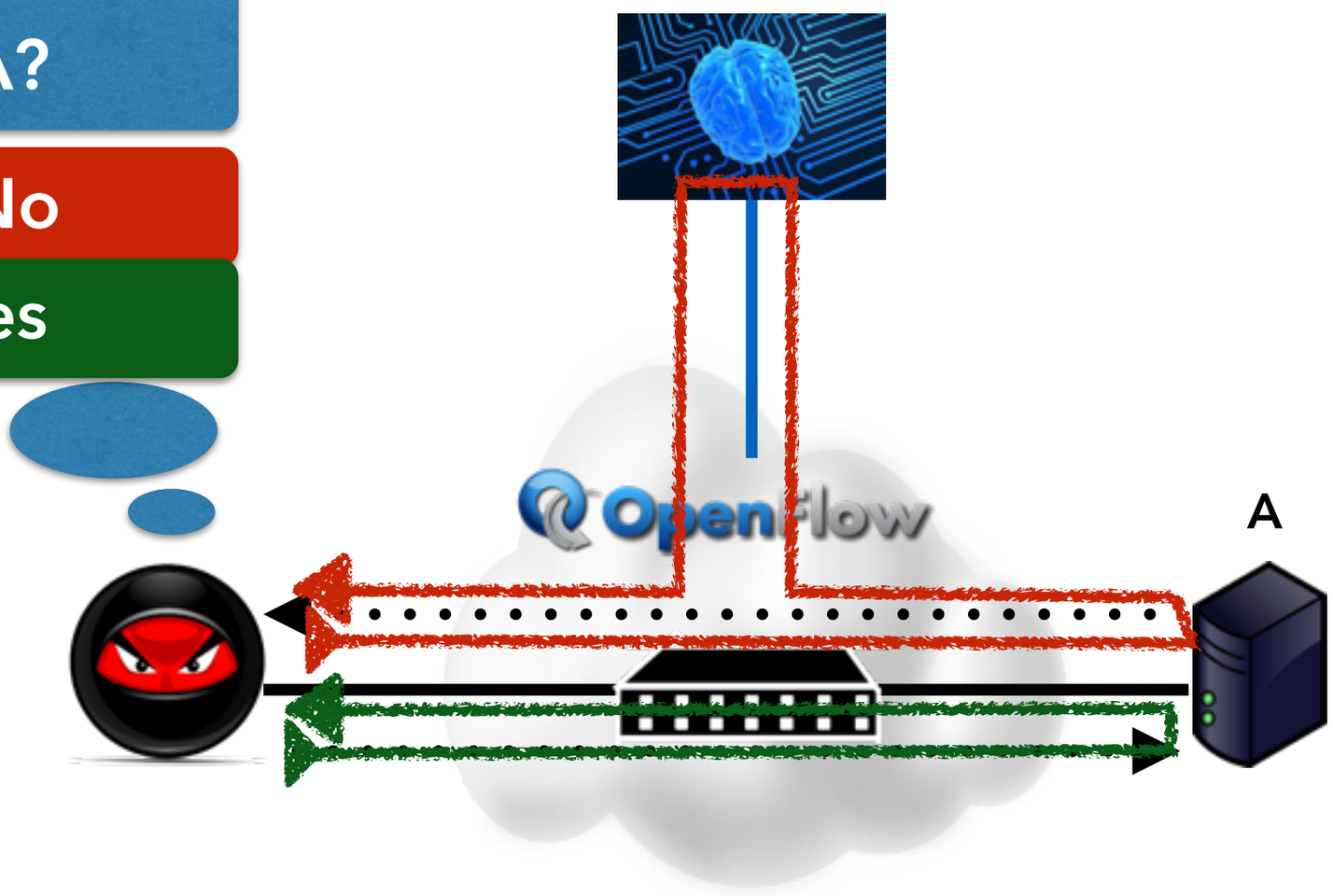

```
PING 1.1.1.2 (1.1.1.2) 56(84) bytes of data.
64 bytes from 1.1.1.2: icmp_seq=1 ttl=64 time=2.56 ms
64 bytes from 1.1.1.2: icmp_seq=2 ttl=64 time=0.345 ms
64 bytes from 1.1.1.2: icmp_seq=3 ttl=64 time=0.044 ms
```

A Simple OpenFlow Timing Attack

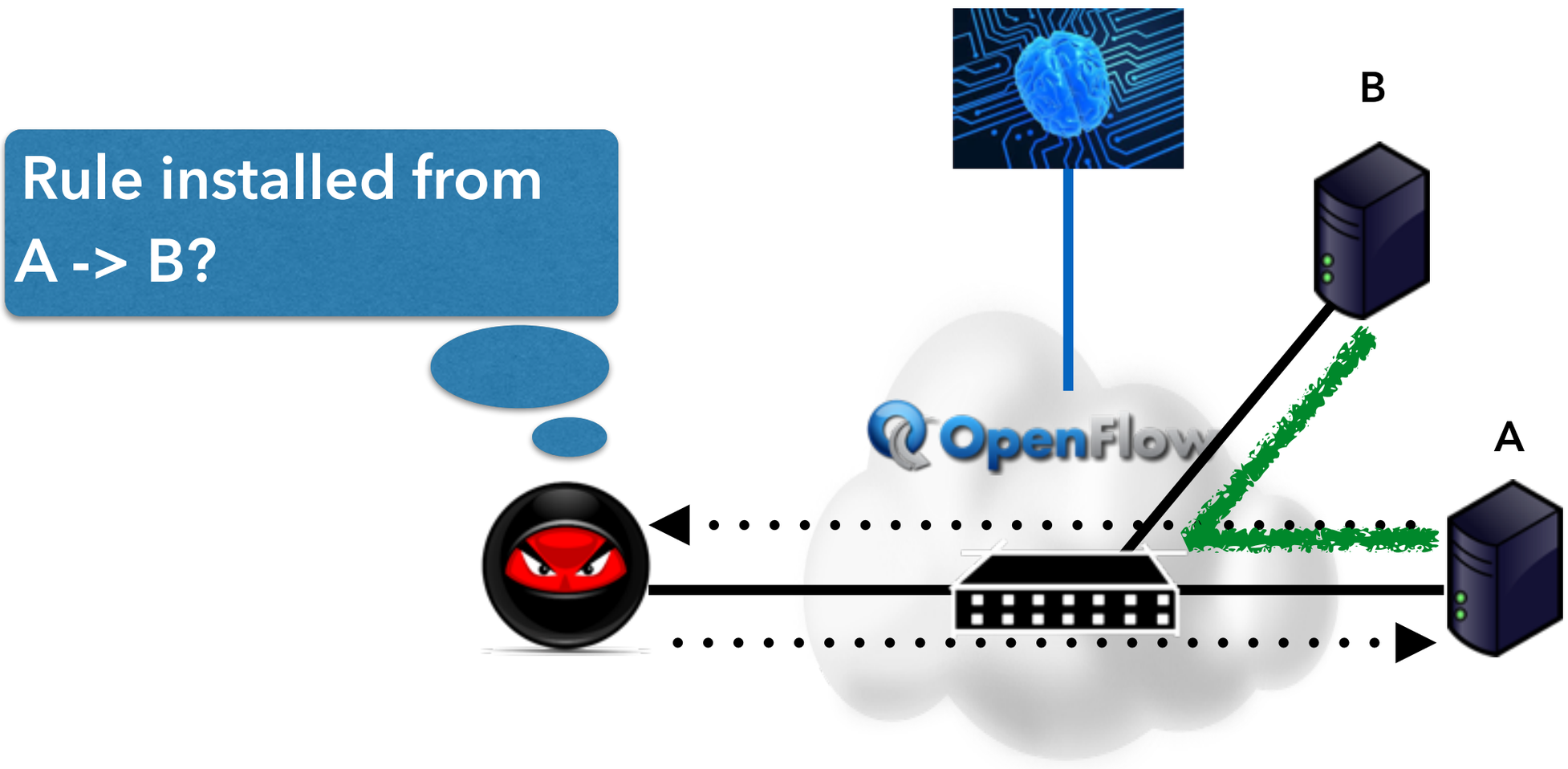
Rule installed from My host <–> A?

High RTT –> No

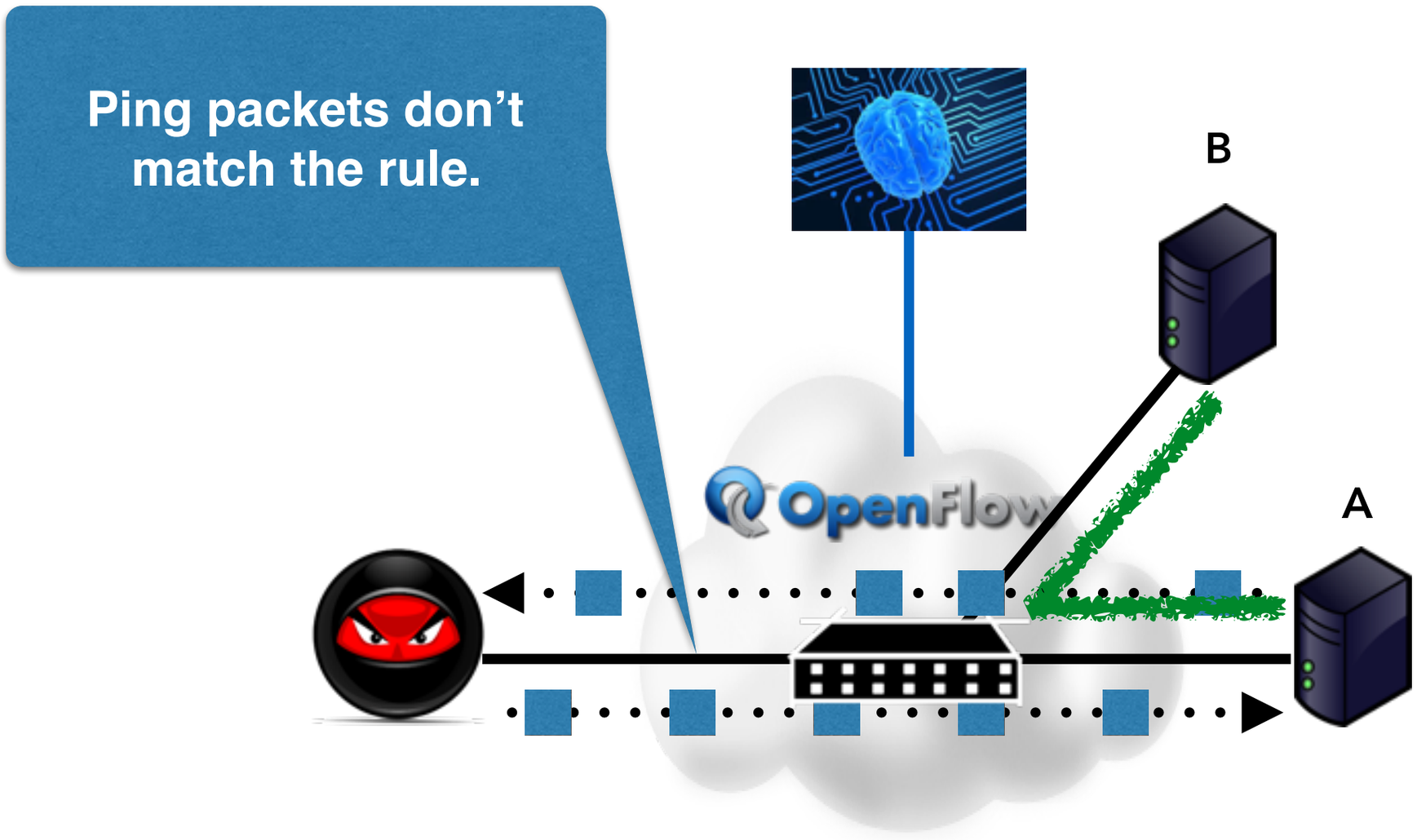
Low RTT –> Yes



A Simple OpenFlow Timing Attack: Limitations

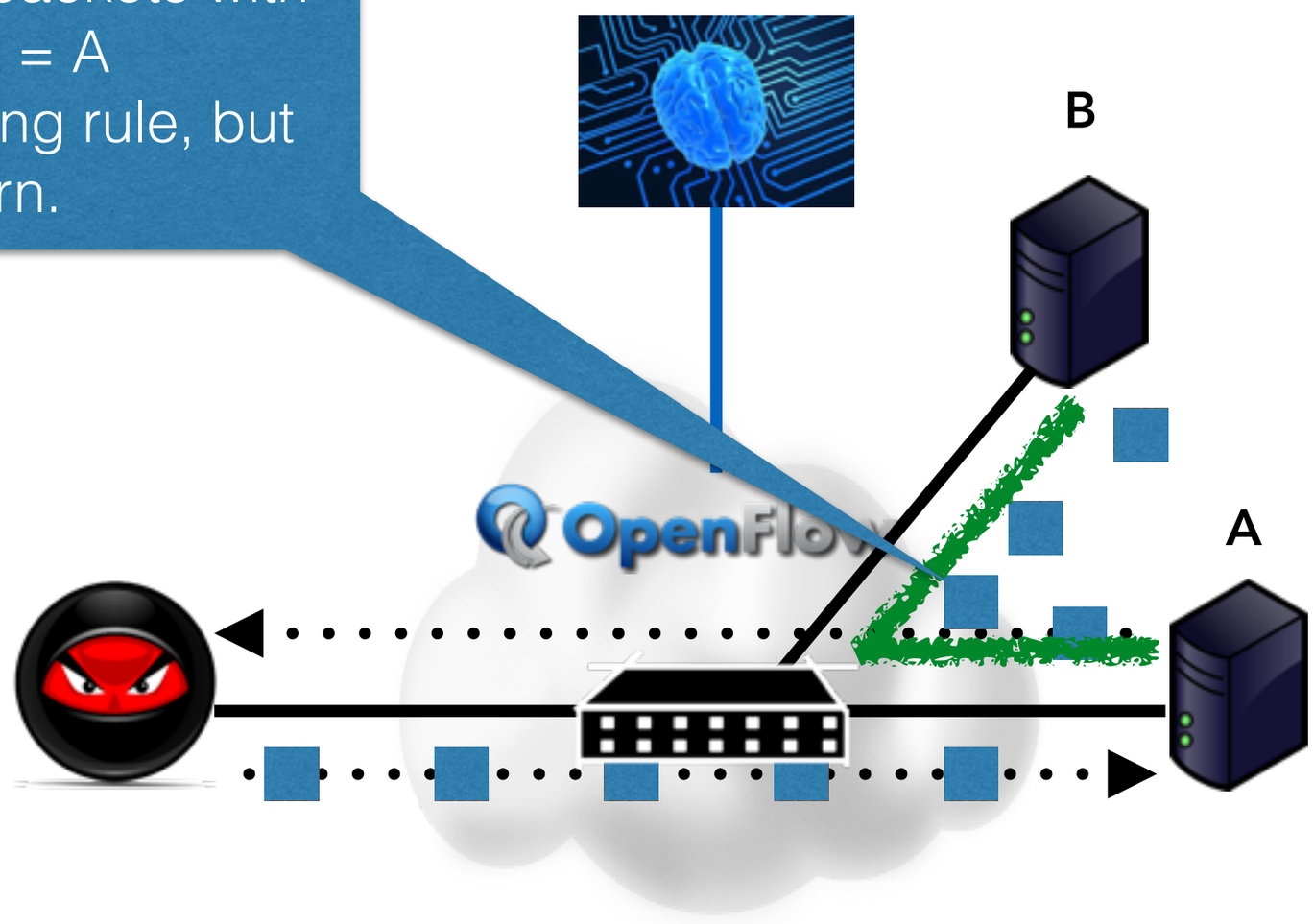


A Simple OpenFlow Timing Attack: Limitations



A Simple OpenFlow Timing Attack: Limitations

replies to spoofed packets with
src = B, dst = A
match the forwarding rule, but
don't return.



Previous OpenFlow Timing Attacks Based on this Property

Do switches have aggregate rules installed? [1]
How large are switch flow tables?[2]

Can we design a more general attack to learn which forwarding rules are installed on switches, and when they get installed?

[1] ... *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–6. IEEE, 2013.

[2] J. Leng, Y. Zhou, J. Zhang, ... *preprint arXiv:1504.03095*, 2015.

Outline

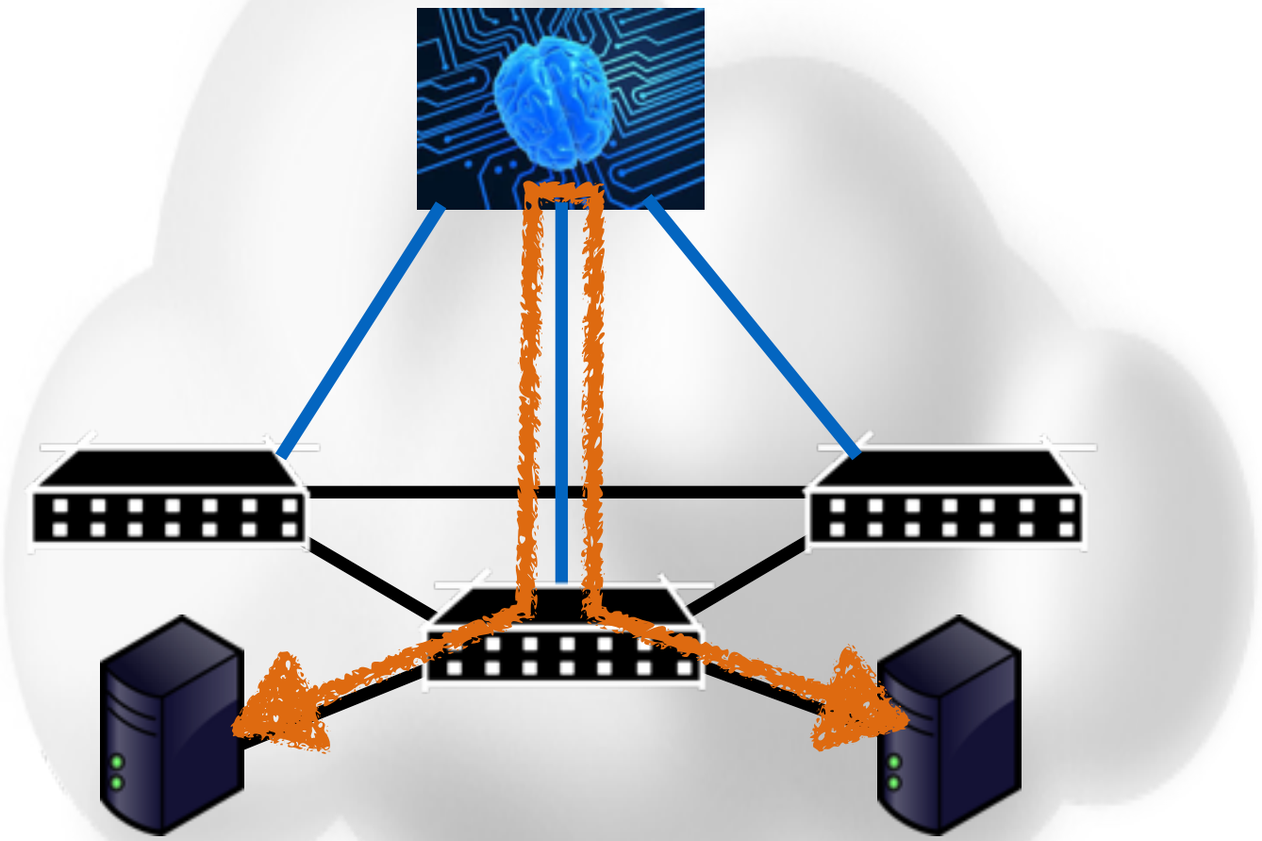
Introduction

OpenFlow Timing Attacks

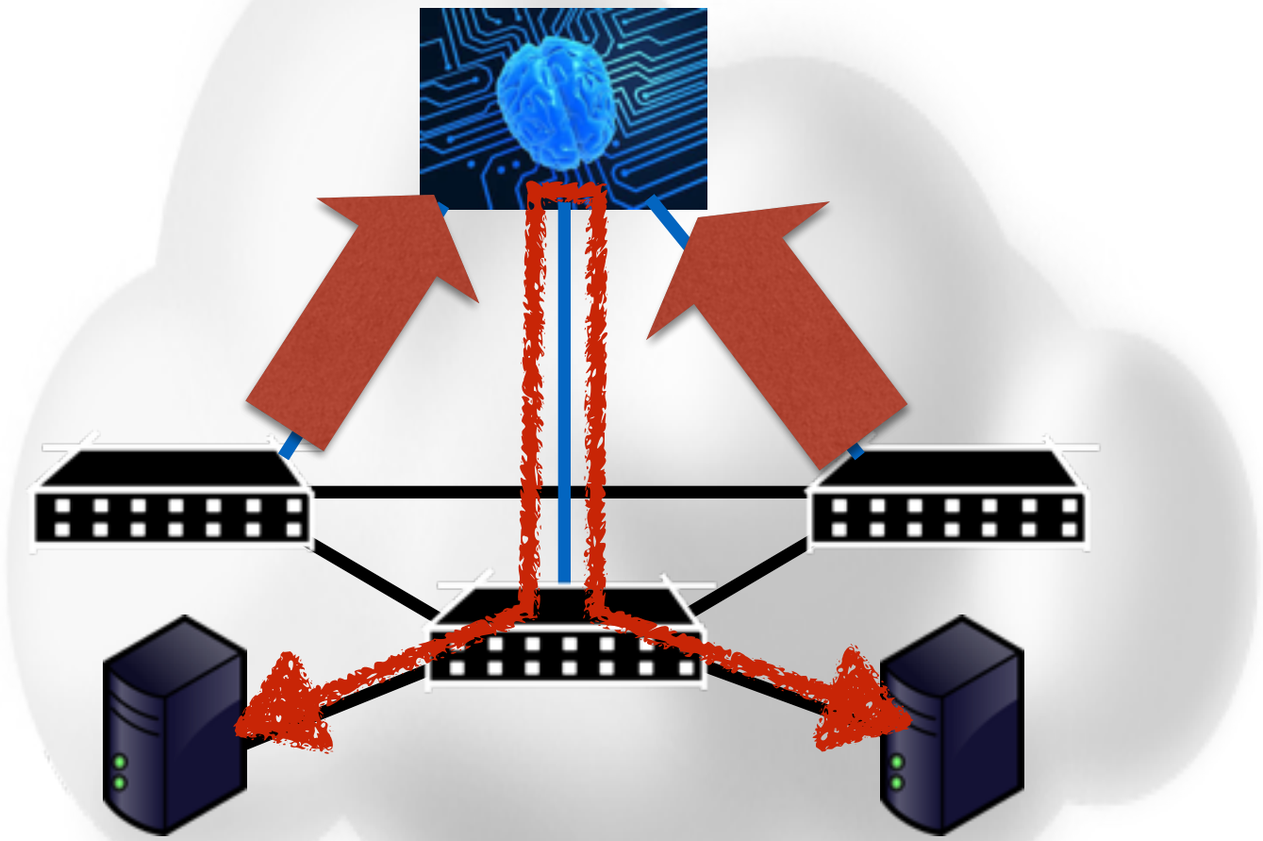
A More General OpenFlow Timing Attack

Preliminary Results

OpenFlow Timing Property: Control Planes Response Time Depends on Load



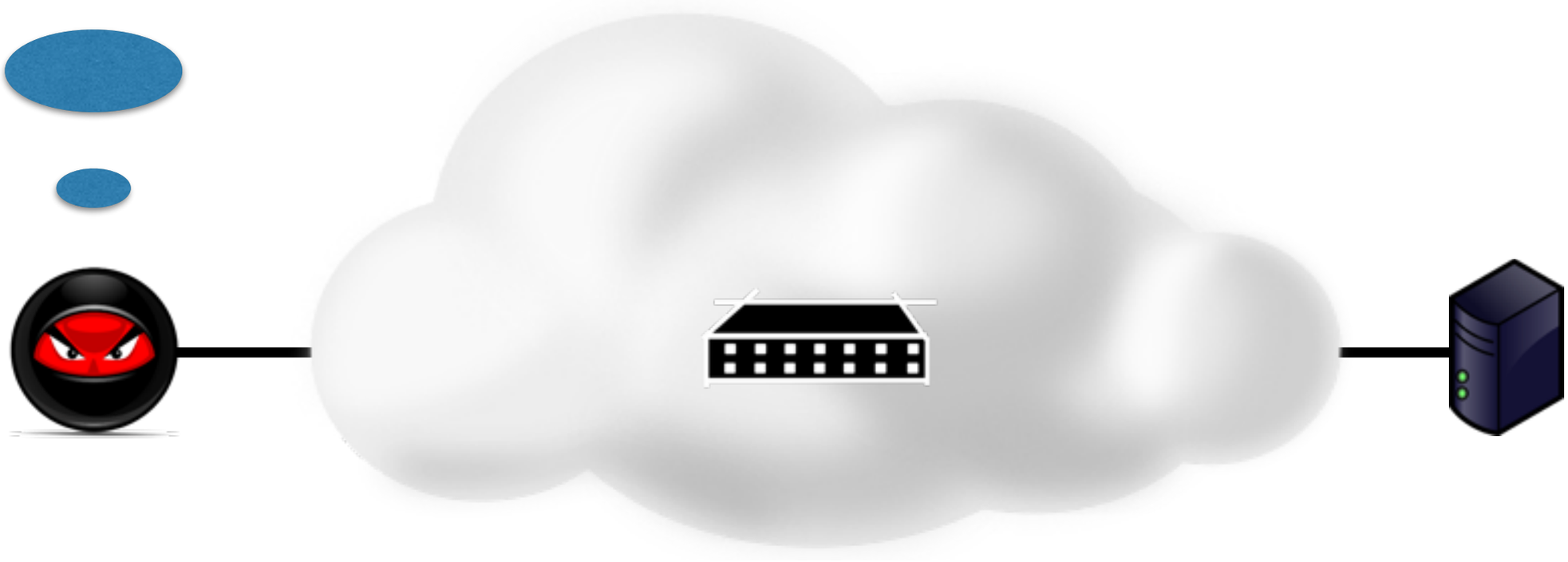
```
PING 1.1.1.2
64 bytes from 1.1.1.2: time=2.56 ms
64 bytes from 1.1.1.2: time=0.345 ms
64 bytes from 1.1.1.2: time=0.044 ms
```



```
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
```

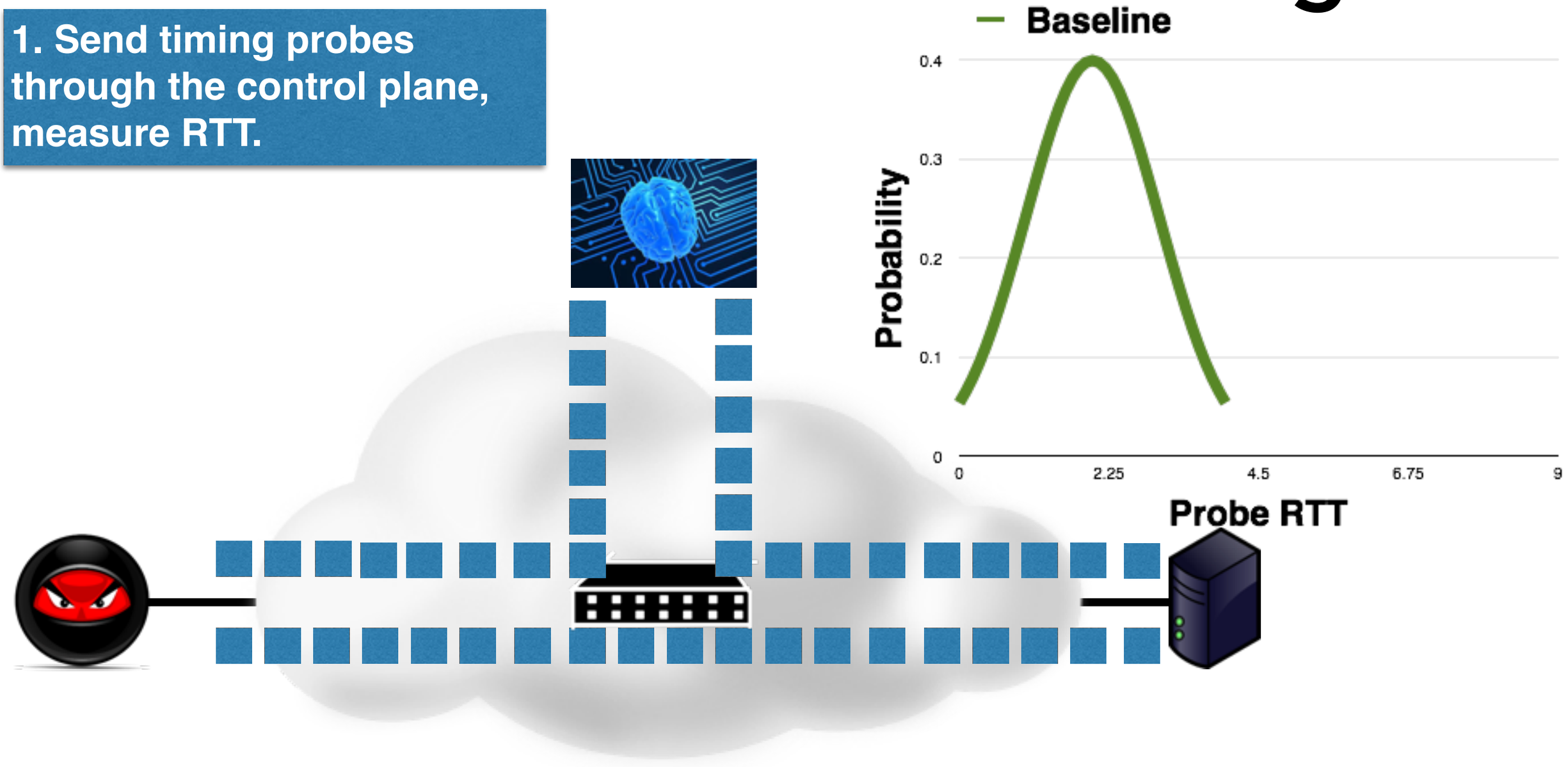
The Basic Approach: Estimating Control Plane Load Change

Will these packets match a rule?



The Basic Approach: Estimating Control Plane Load Change

1. Send timing probes through the control plane, measure RTT.

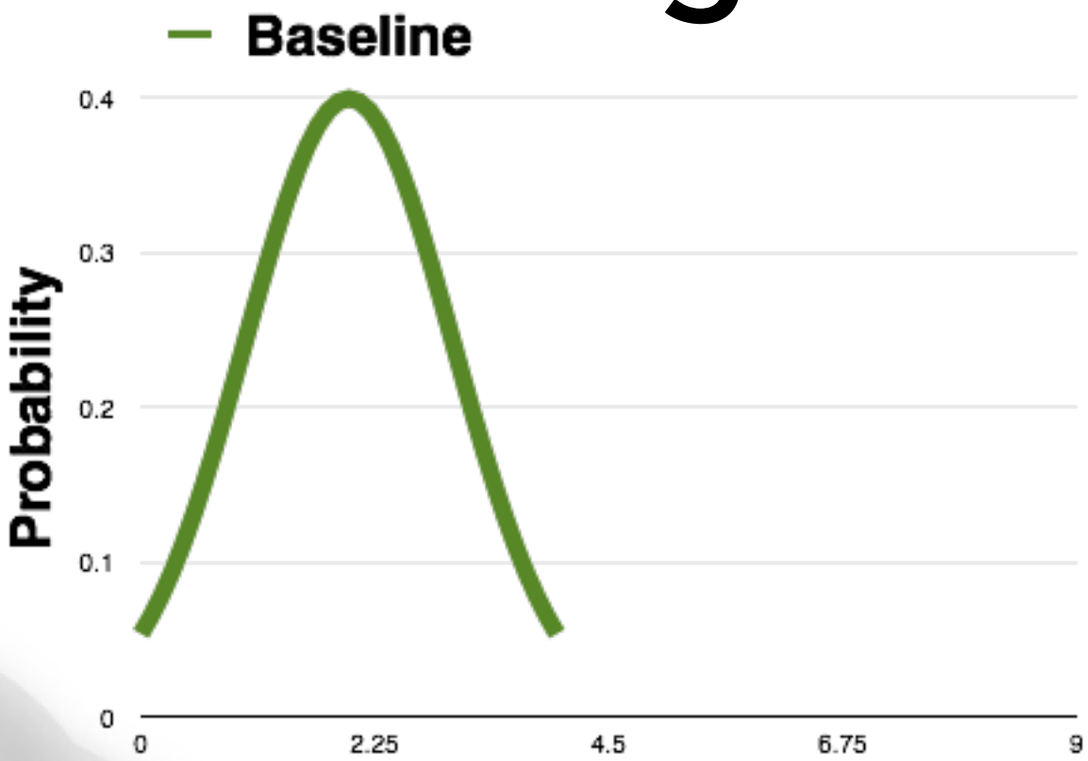


The Basic Approach: Estimating Control Plane Load Change

1. Send timing probes through the control plane, measure RTT.

2. Send test packets into the network.

Test Packets



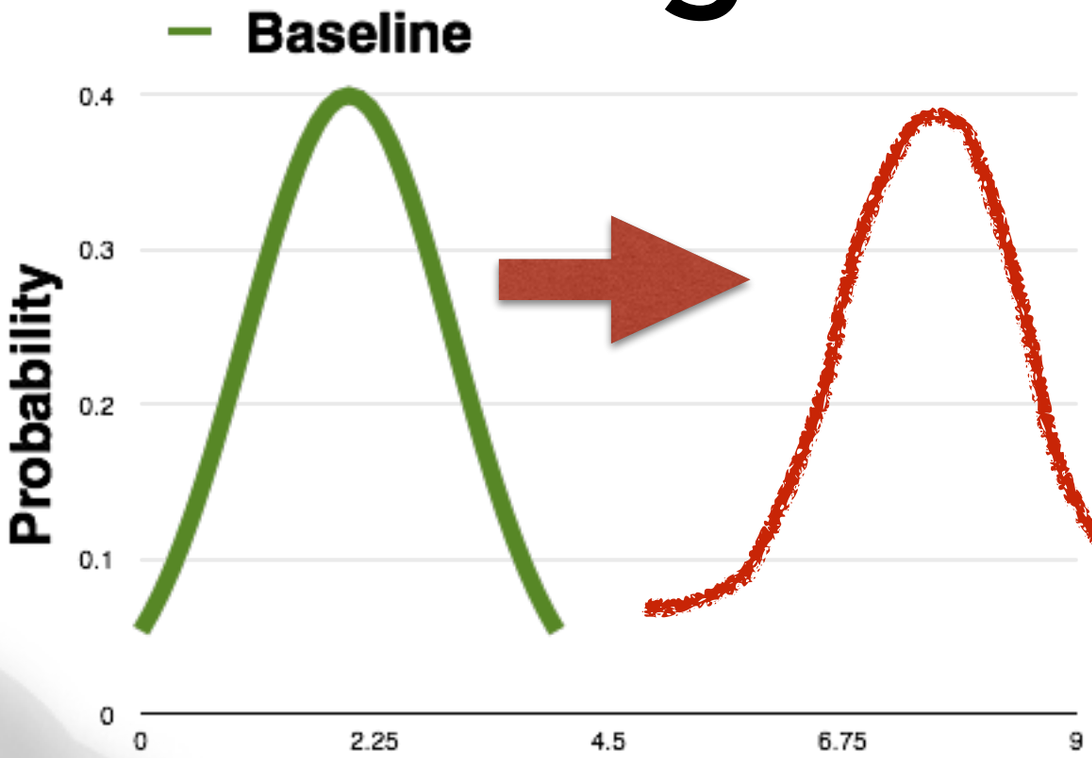
The Basic Approach: Estimating Control Plane Load Change

1. Send timing probes through the control plane, measure RTT.

2. Send test packets into the network.

3. If the packets reach the controller, its load will increase, delaying the probes.

Test Packets



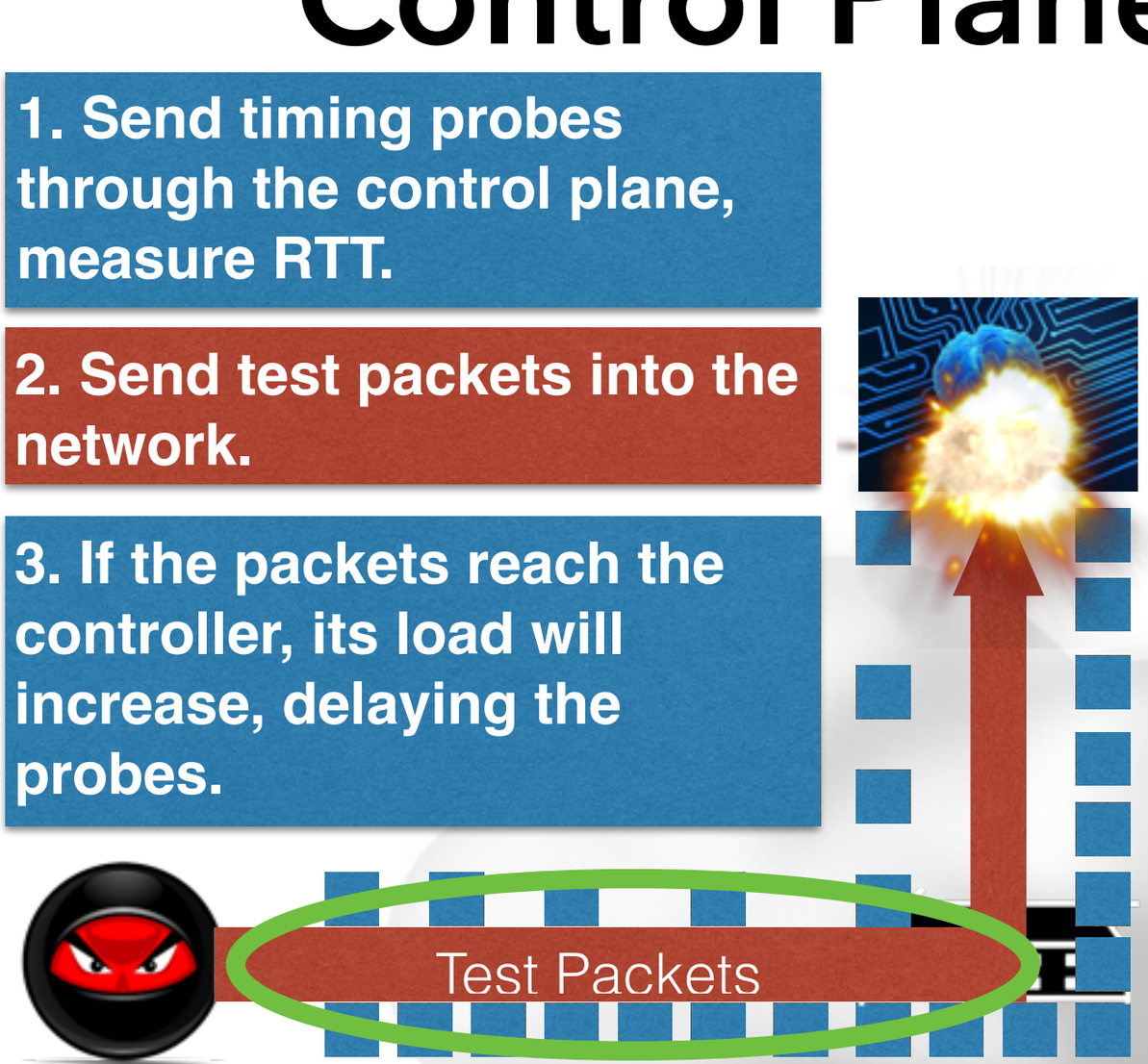
Probe RTT

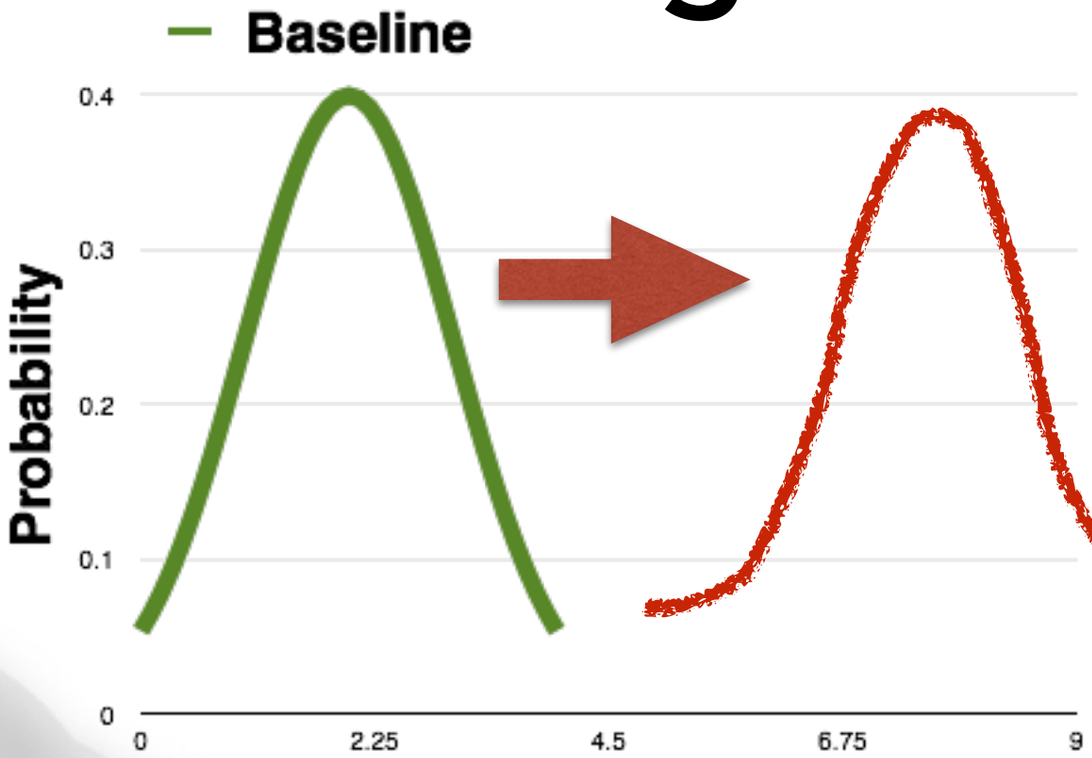
The Basic Approach: Estimating Control Plane Load Change

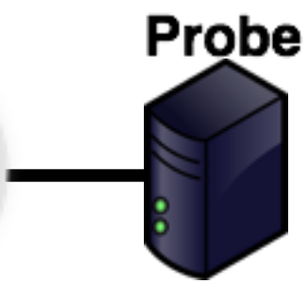
1. Send timing probes through the control plane, measure RTT.

2. Send test packets into the network.

3. If the packets reach the controller, its load will increase, delaying the probes.







Learning Higher Level Configuration Details

Which forwarding rules are installed in the switches?

Which fields are wildcarded?

What kind of application is the controller running?

Which packets reach the controller?

Which sequences of packets cause the controller to install flows?

Outline

Introduction

OpenFlow Timing Attacks

A More General OpenFlow Timing Attack

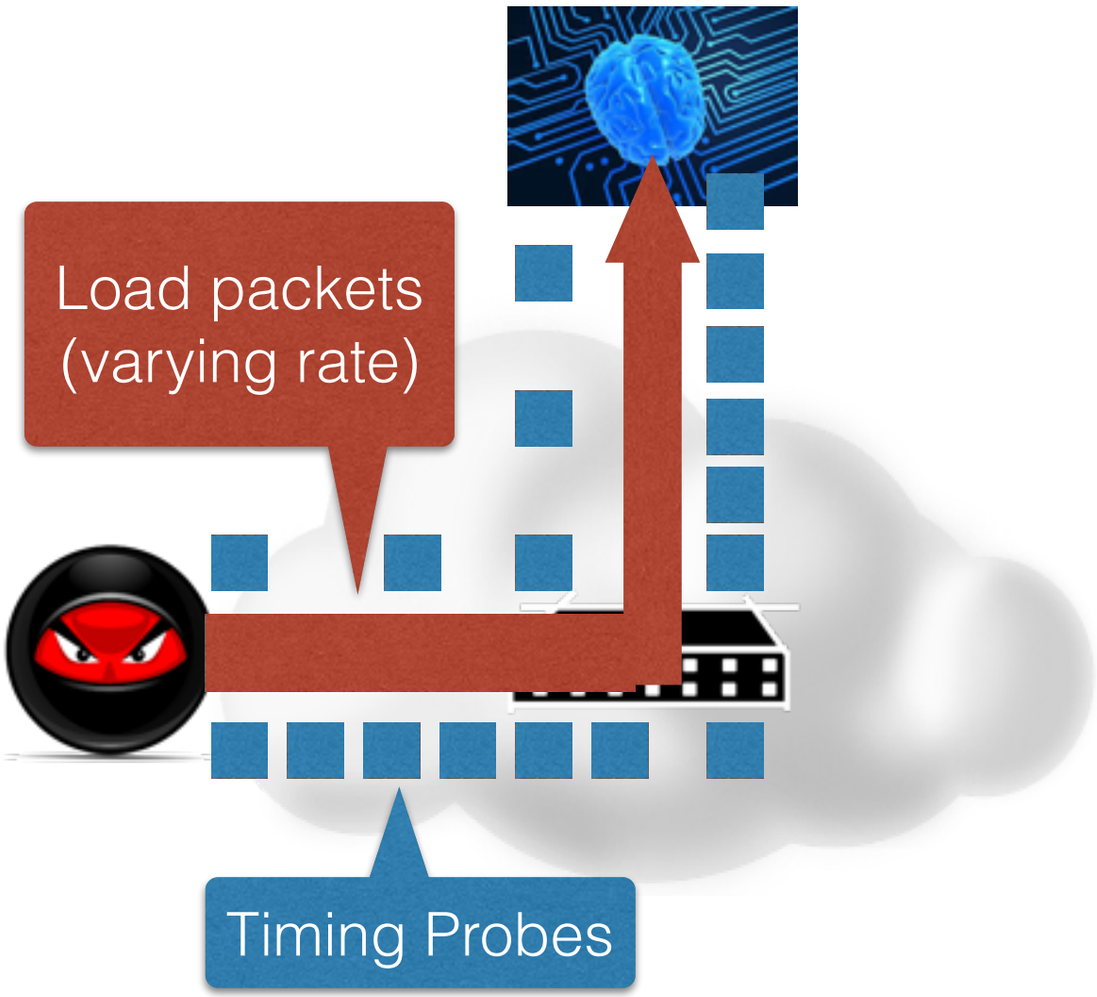
Preliminary Results

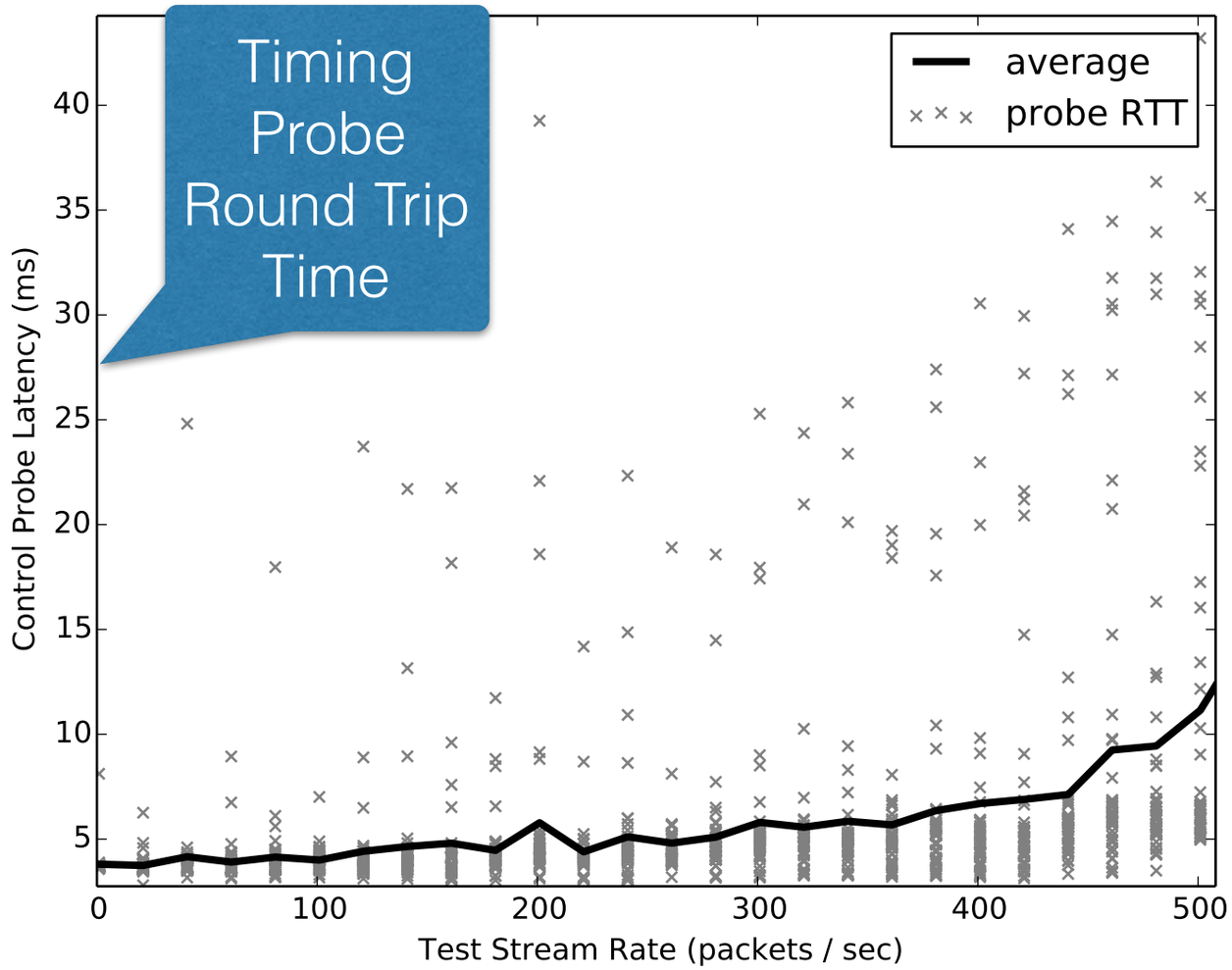
Preliminary Results

Does probe RTT estimate controller load?

Can an adversary learn if a forwarding rule is installed?

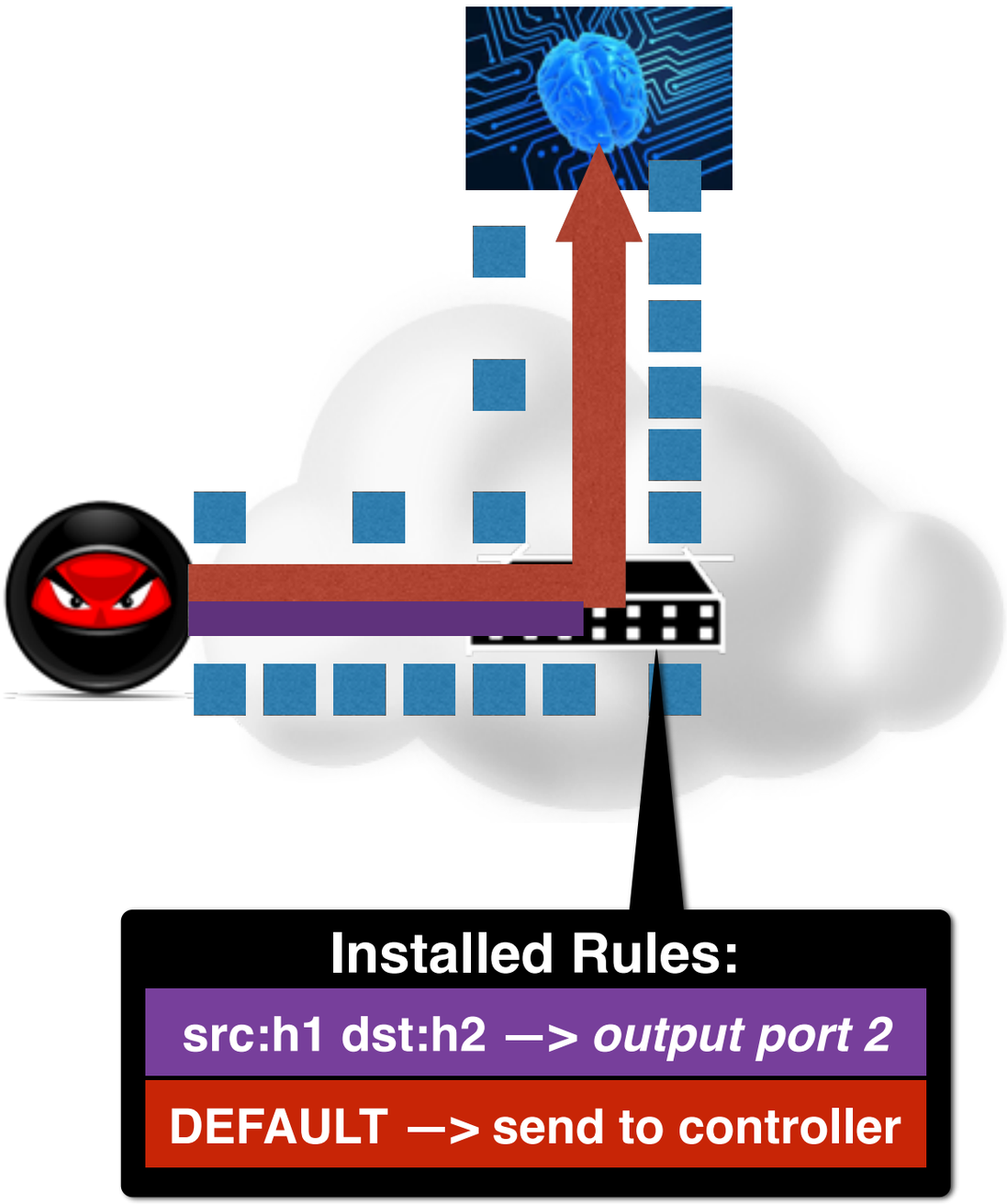
Estimating Controller Load





Packets per second sent to controller

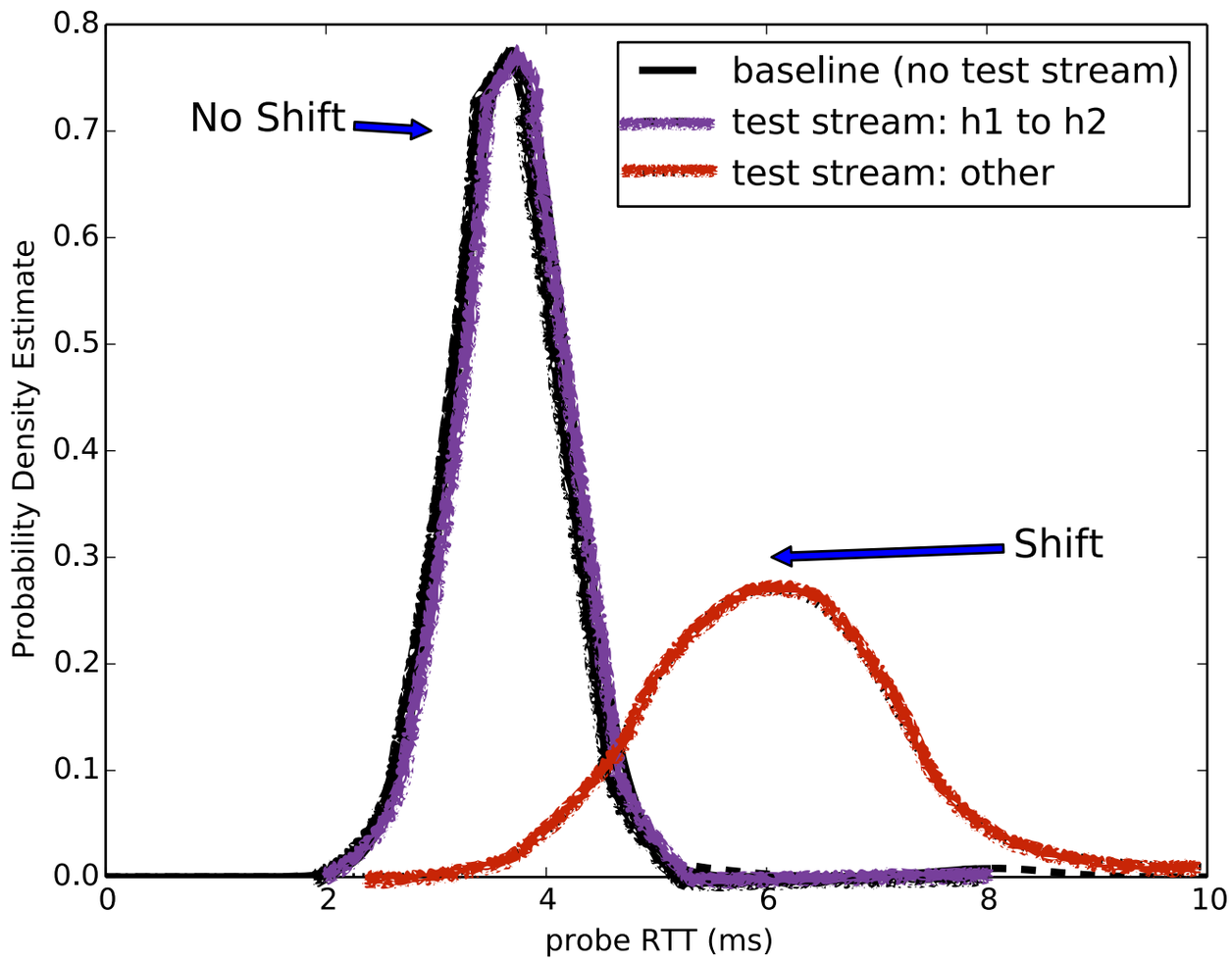
Learning if a Rule is Installed



Installed Rules:

src:h1 dst:h2 —> *output port 2*

DEFAULT —> send to controller



Timing Probe Round Trip Time

More in the Paper

Timing SDN Control Planes to Infer Network Configurations

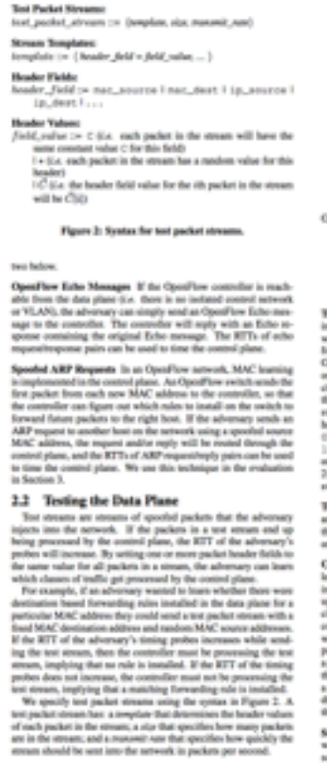
ABSTRACT

1. INTRODUCTION

2. INFERENCE ATTACK OVERVIEW

2.1 Timing the Control Plane

3. EVALUATION



Test Packet Streams:

Stream Templates:

Header Fields:

Header Values:

Figure 2: Syntax for test packet streams.

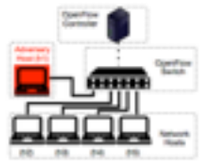


Figure 3: A diagram of our testbed network.

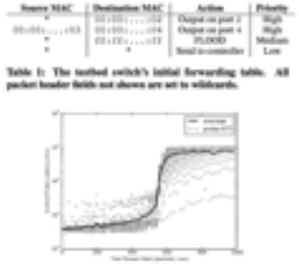


Table 1: The testbed switch's initial forwarding table. All packet header fields not shown are set to wildcards.

Figure 6: Timing probe RTT as test stream packet rate varies, for test streams that are processed by the control plane.

3.1 Are packets reaching the controller?

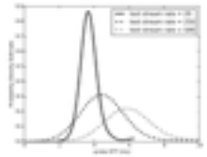


Figure 5: Probe RTT distribution estimates with test streams of different rates that get processed by the control plane.

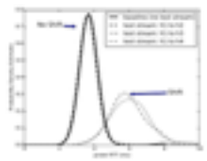


Figure 4: Probe RTT distribution shifts when the adversary sends test streams with no matching forwarding rules.

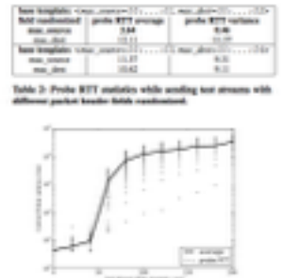


Table 2: Probe RTT statistics while sending test streams with different packet header fields randomized.

Table 3: Probe RTT statistics during two trials to determine the sequence of packets that causes a rule to be installed. High RTT followed by low RTT indicates that rules are installed.

Figure 7: Probe RTT as test stream packet rate varies, for a test stream where each packet invokes a rule installation.

3.2 Is the controller installing forwarding rules?

4. CONCLUSION

5. REFERENCES

Thank You!

Timing SDN Control Planes to Infer Network Configurations

- OpenFlow networks have timing side channels
- Adversaries can potentially learn fine grained information about OpenFlow networks, and their configurations, **without compromising equipment**
- There are many implications and (hopefully) defenses

Penn
University of Pennsylvania

University of Colorado Boulder

Potential Defenses

Real time controllers?

Middlebox detectors and filters?

Programmable switches? (OFX, P4)