FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks

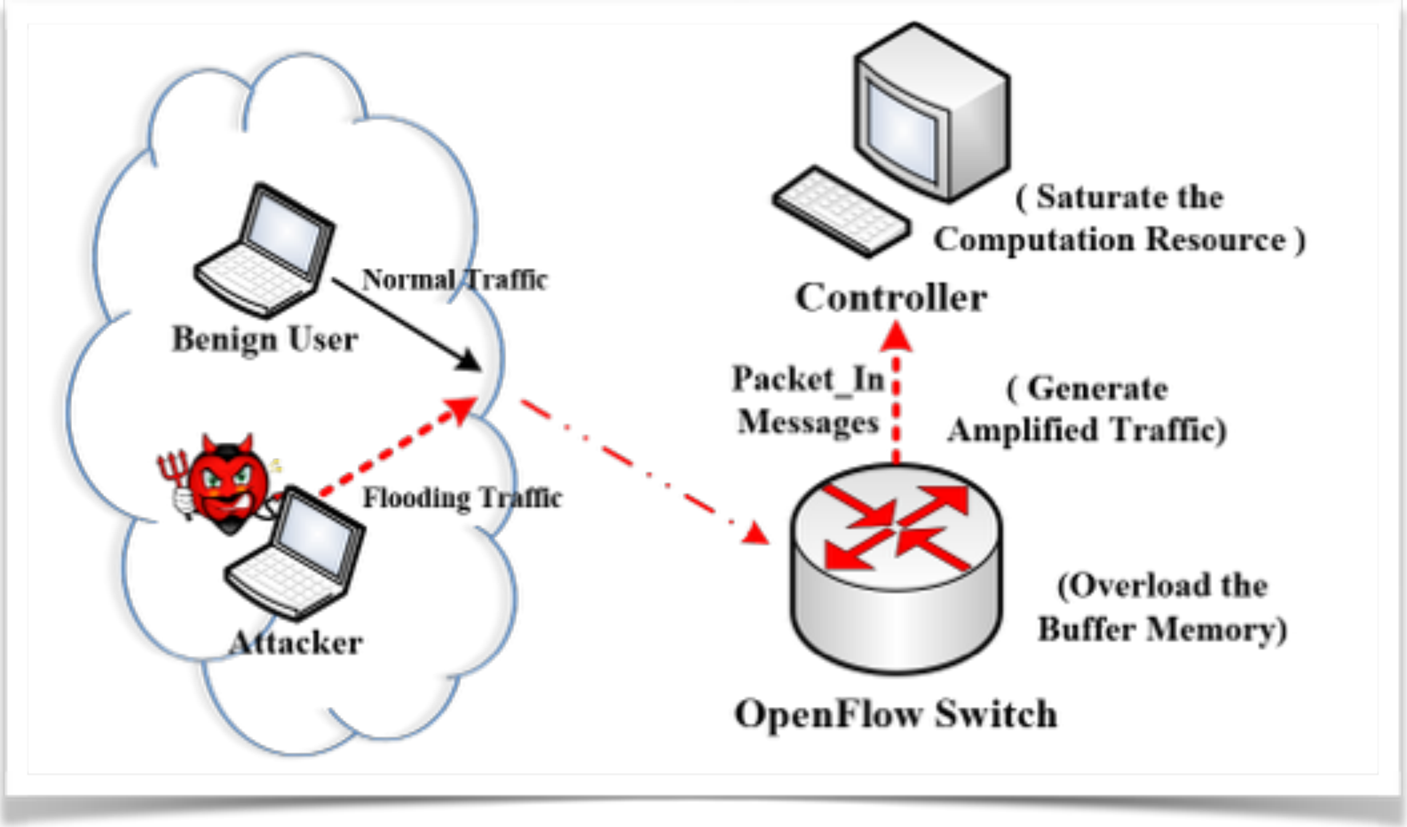
DSN 2015

Haopei Wang, Lei Xu, Guofei Gu

SUCCESS Lab Texas A&M University

- This paper address on *data-to-control plane saturation attack*, which overloads the infrastructure of SDN networks.
  - amount of *table-miss* packets
  - consume resources

- This paper address on *data-to-control plane saturation attack*, which overloads the infrastructure of SDN networks.
  - amount of *table-miss* packets
  - consume resources


(Saturate the Computation Resource)
Controller
Normal Traffic
Benign User
Packet_In Messages
(Generate Amplified Traffic)
Flooding Traffic
Attacker
(Overload the Buffer Memory)
OpenFlow Switch

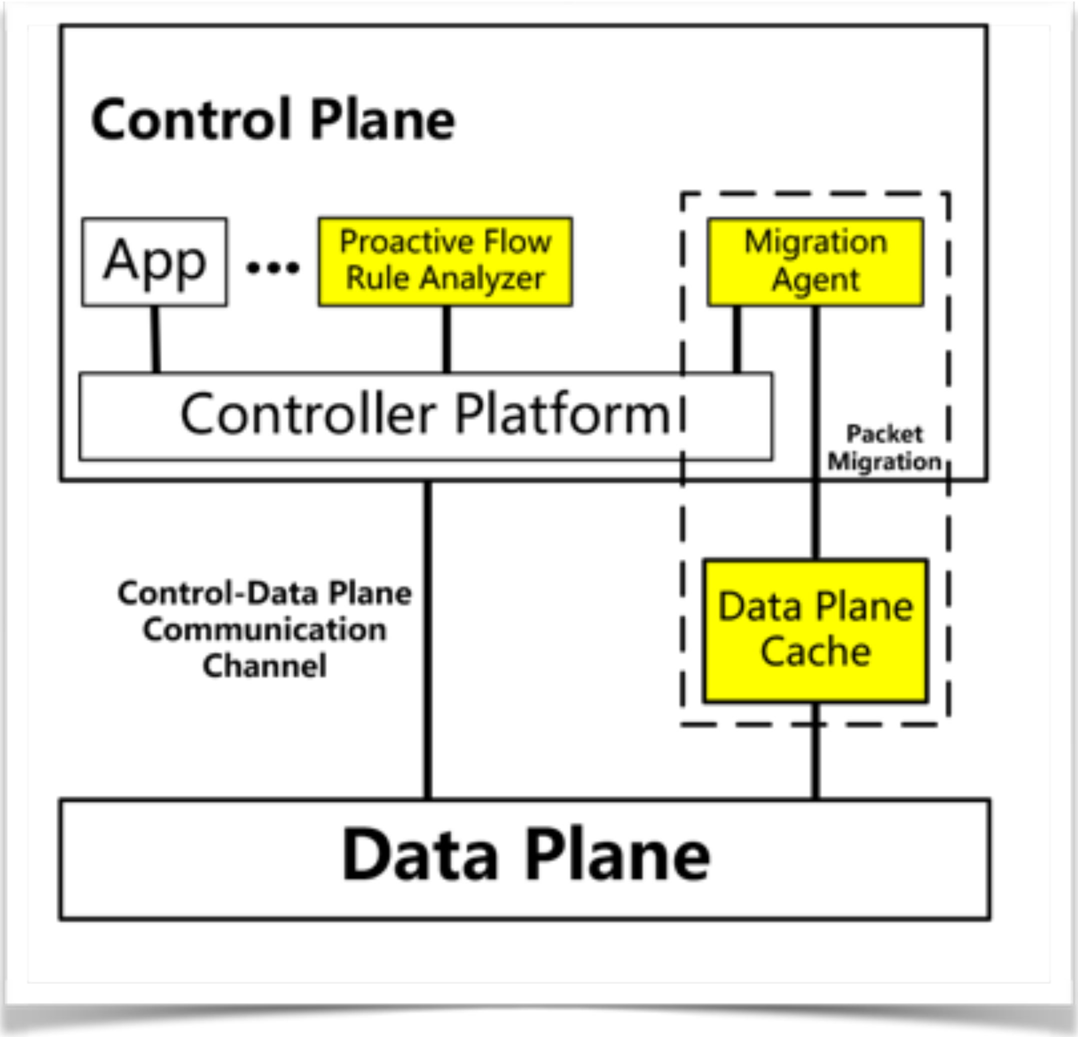
FLOODGUARD

FLOODGUARD

- Proactive Flow Rule Analyzer
- Packet Migration

FLOODGUARD

- Proactive Flow Rule Analyzer
- Packet Migration



Proactive Flow Rule Analyzer

Proactive Flow Rule Analyzer

- If we can pre-install all flow rules into the data plane that the problem can be solved.

Proactive Flow Rule Analyzer

- If we can pre-install all flow rules into the data plane that the problem can be solved.

HOW CAN WE ADDRESS THIS CHALLENGE??

Proactive Flow Rule Analyzer

Proactive Flow Rule Analyzer

- Proactive flow rule analyzer dynamically derives proactive flow rules.

Proactive Flow Rule Analyzer

- Proactive flow rule analyzer dynamically derives proactive flow rules.

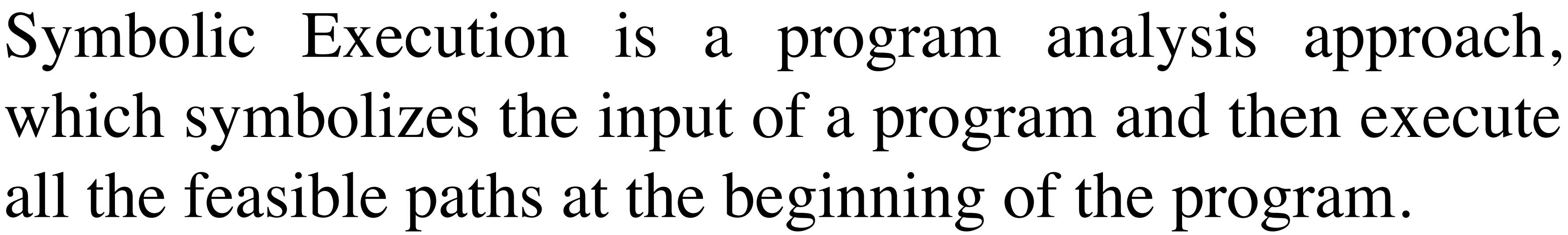
  Proactive flow rule analyzer which covers all the possible rules.

Proactive Flow Rule Analyzer

- Proactive flow rule analyzer dynamically derives proactive flow rules.

Proactive flow rule analyzer which covers all the possible rules.

Symbolic Execution



Symbolic Execution is a program analysis approach, which symbolizes the input of a program and then execute all the feasible paths at the beginning of the program.

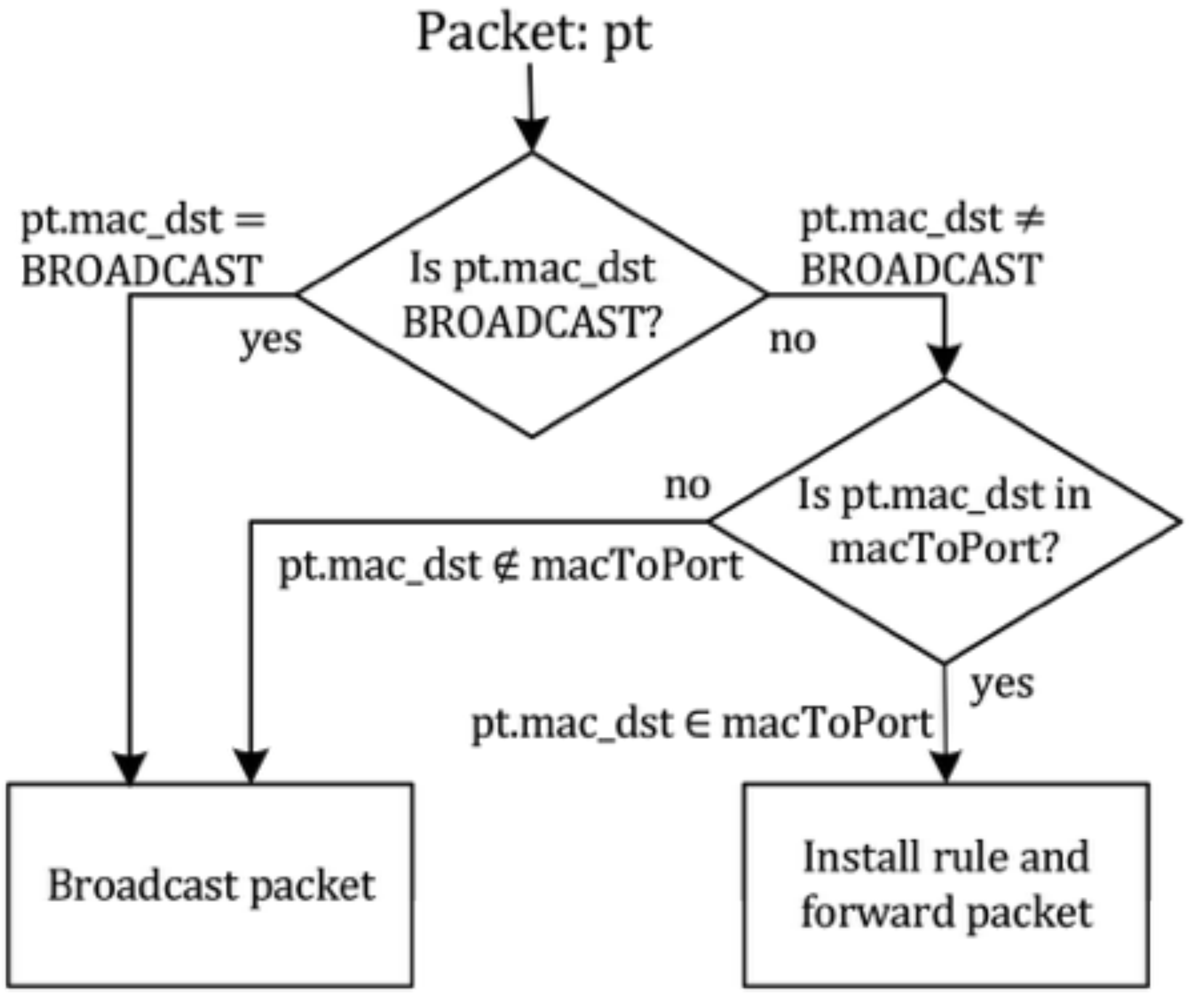
Proactive Flow Rule Analyzer

Proactive Flow Rule Analyzer

A sample symbolic execution

Proactive Flow Rule Analyzer

A sample symbolic execution



Proactive Flow Rule Analyzer

Symbolic Execution

Proactive Flow Rule Analyzer

Symbolic Execution

OFFLINE

Proactive Flow Rule Analyzer

Symbolic Execution

- OFFLINE
  - For the sake of reducing runtime overhead.

Proactive Flow Rule Analyzer

Symbolic Execution

OFFLINE

For the sake of reducing runtime overhead.

RUNTIME

Proactive Flow Rule Analyzer

Symbolic Execution

OFFLINE

For the sake of reducing runtime overhead.

RUNTIME

For the sake of solving the dynamical change.

Packet Migration

Packet Migration

Installing proactive flow rules during the attack will preserve major functionality of SDN.

Packet Migration

Installing proactive flow rules during the attack will preserve major functionality of SDN.

However, there are some *table-miss* packets.

Packet Migration

Installing proactive flow rules during the attack will preserve major functionality of SDN.

However, there are some *table-miss* packets.

It is unacceptable that drop the table-miss packets.

Packet Migration

Installing proactive flow rules during the attack will preserve major functionality of SDN.

However, there are some *table-miss* packets.

It is unacceptable that drop the table-miss packets.

1. Some events are not processed.
2. The new packets cannot be learned by analyzer.

Packet Migration

Packet Migration

Migration Agent

Packet Migration

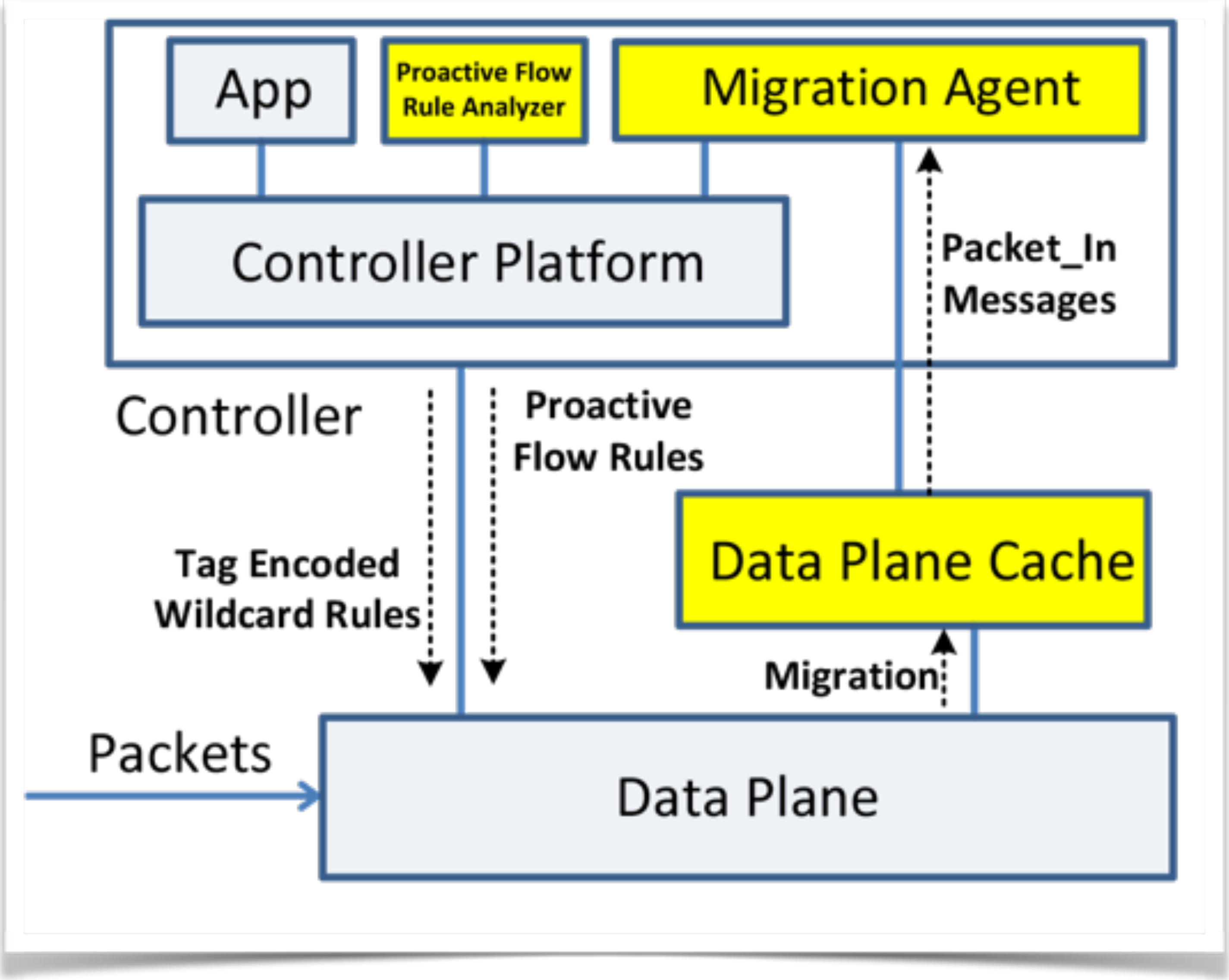
Migration Agent

1. Detect the saturation attack
2. Migrate table-miss packets
3. Rate limit

Packet Migration

Migration Agent

1. Detect the saturation attack
2. Migrate table-miss packets
3. Rate limit



Packet Migration

Packet Migration

Data plane cache

Packet Migration

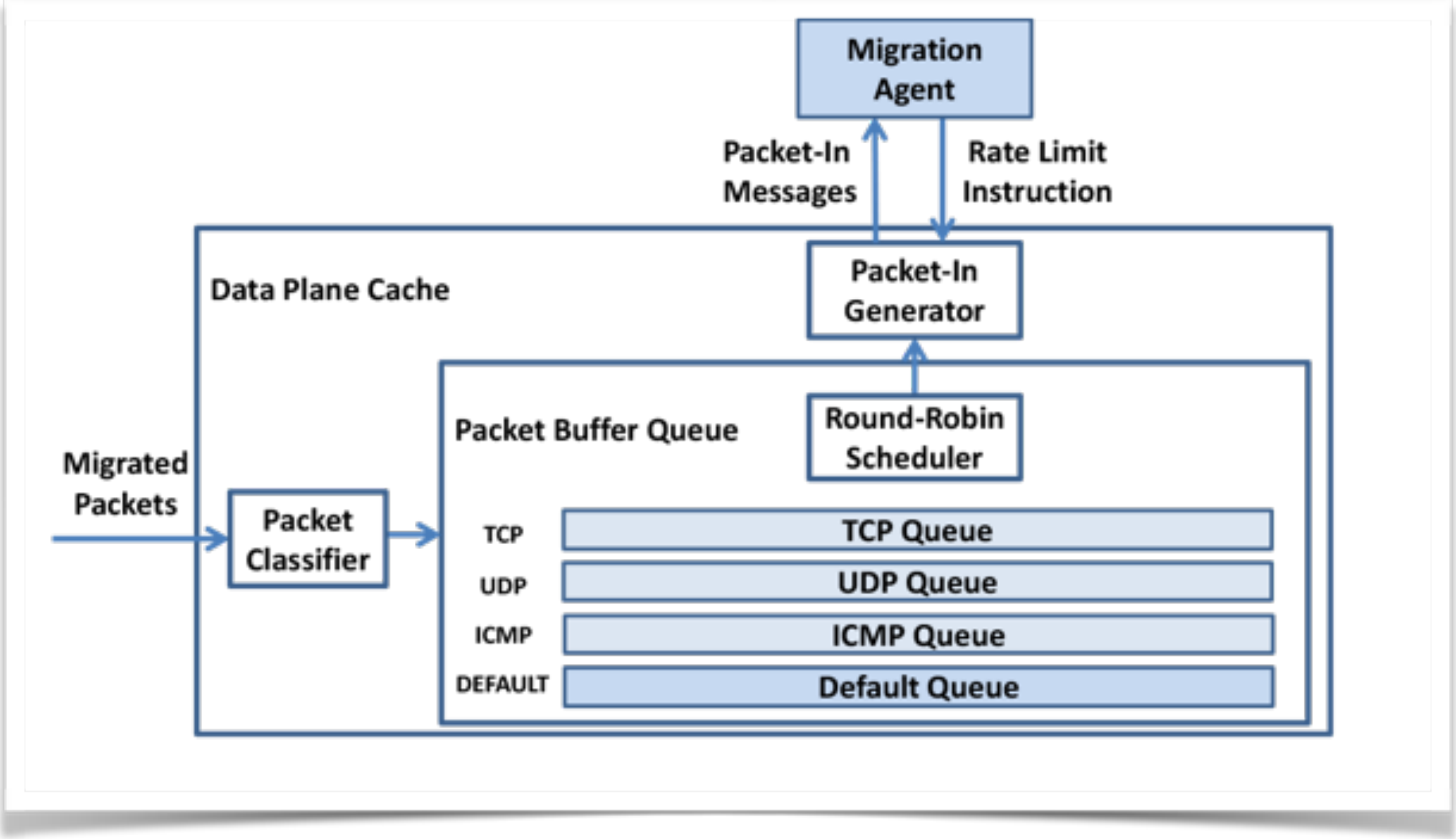
Data plane cache

1. Packet classifier
2. Buffer queue
3. Packet-in generator

Packet Migration

Data plane cache

1. Packet classifier
2. Buffer queue
3. Packet-in generator



Evaluation

Evaluation

1. Software

   -MININET

2. Hardware

   -OpenFlow-enabled commercial LinkSys WRT54GL switch

Evaluation

1. Software

   -MININET

2. Hardware

   -OpenFlow-enabled commercial LinkSys WRT54GL switch

Controller: POX

Evaluation

1. Software

   -MININET

2. Hardware

   -OpenFlow-enabled commercial LinkSys WRT54GL switch

Controller: POX

Topology:

Evaluation

1. Software

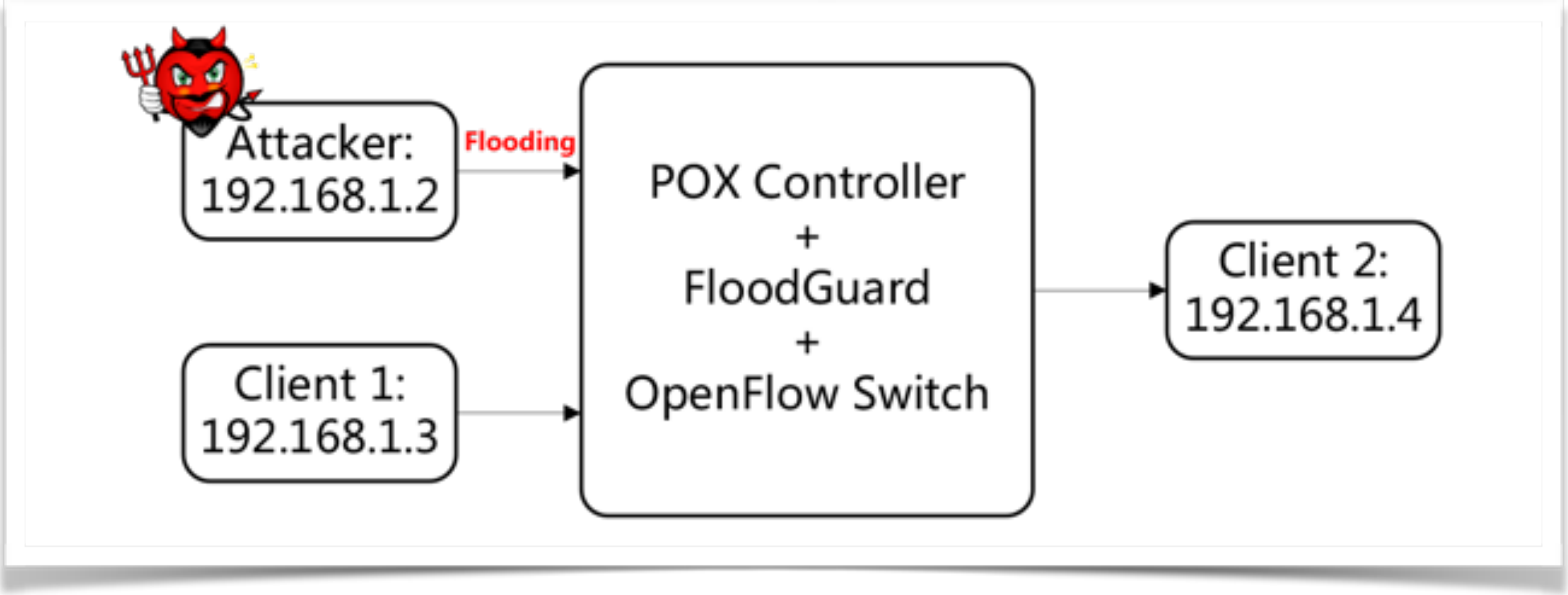
   -MININET

2. Hardware

   -OpenFlow-enabled commercial LinkSys WRT54GL switch

Controller: POX

Topology:



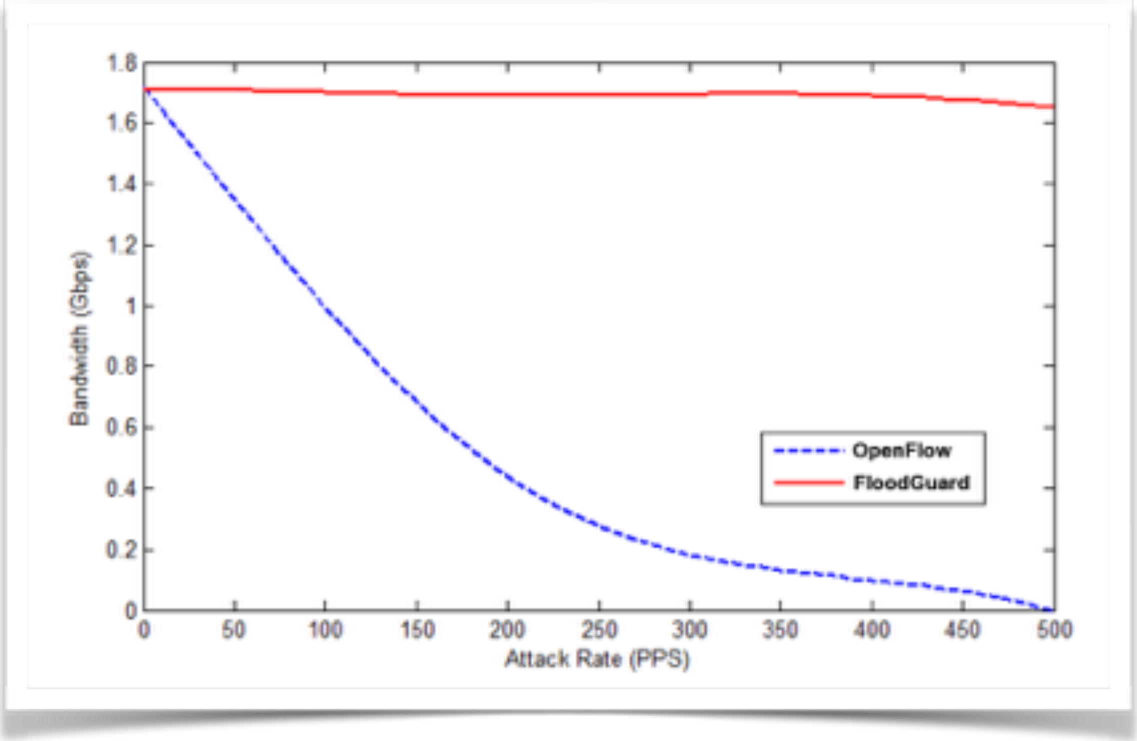
Evaluation

Evaluation

Defense Effects

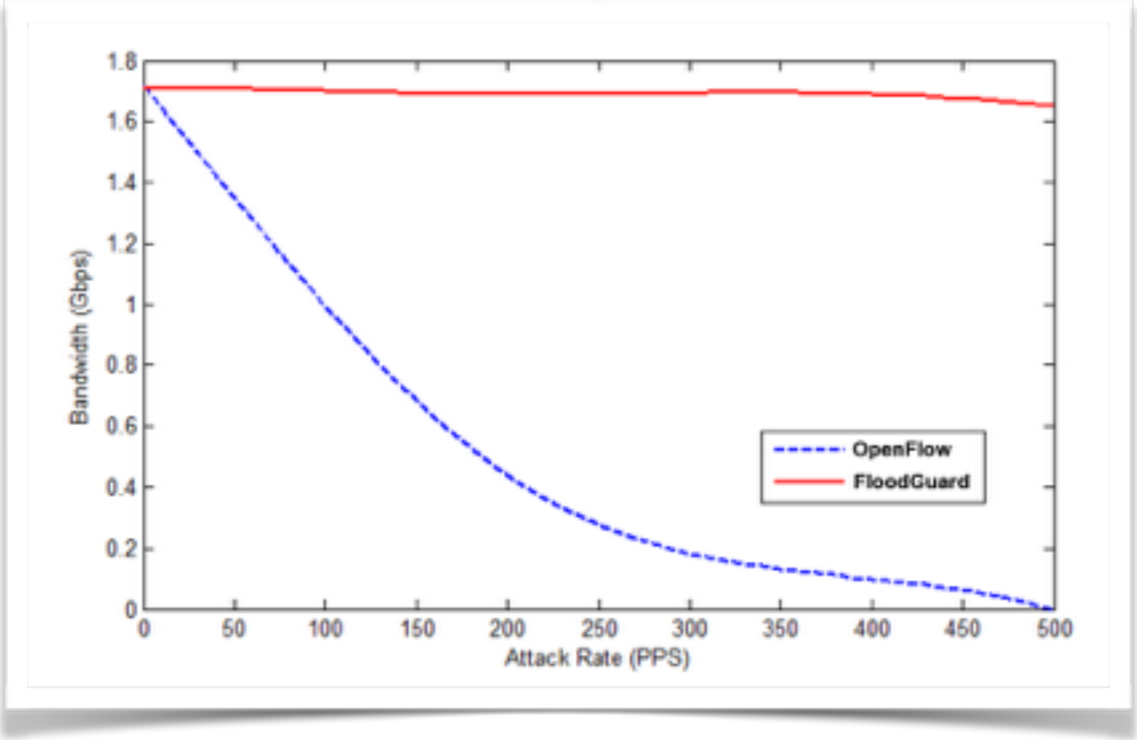
Evaluation

Defense Effects



Evaluation

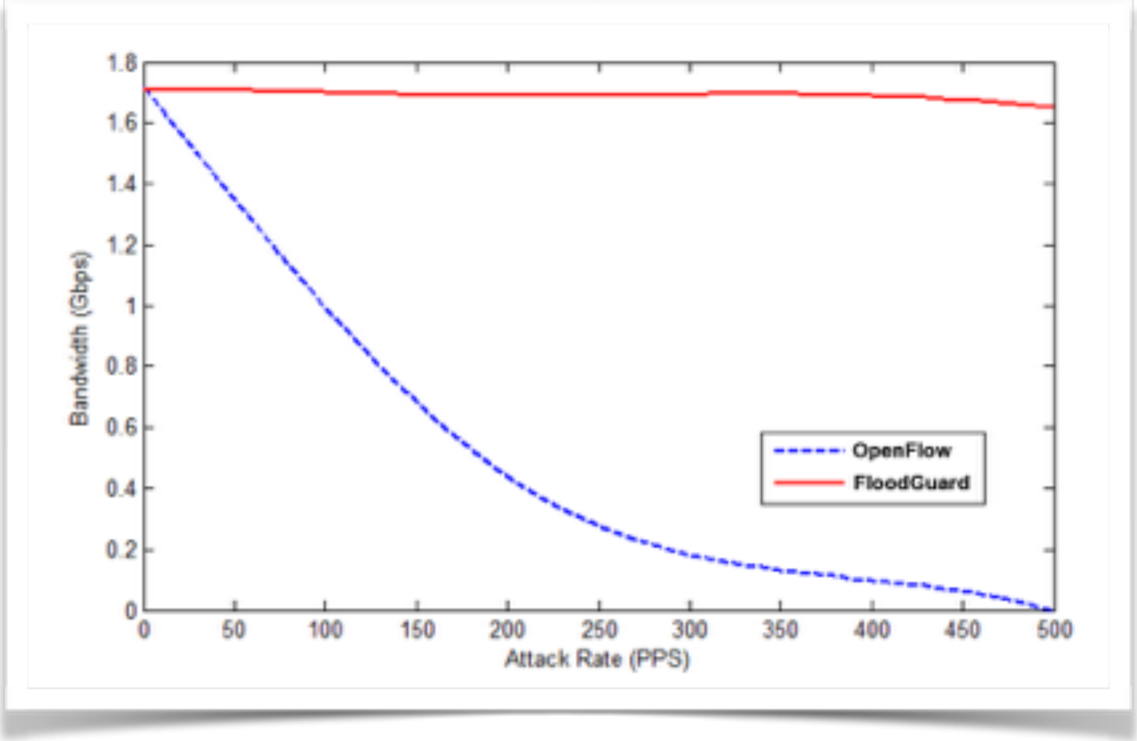
Defense Effects

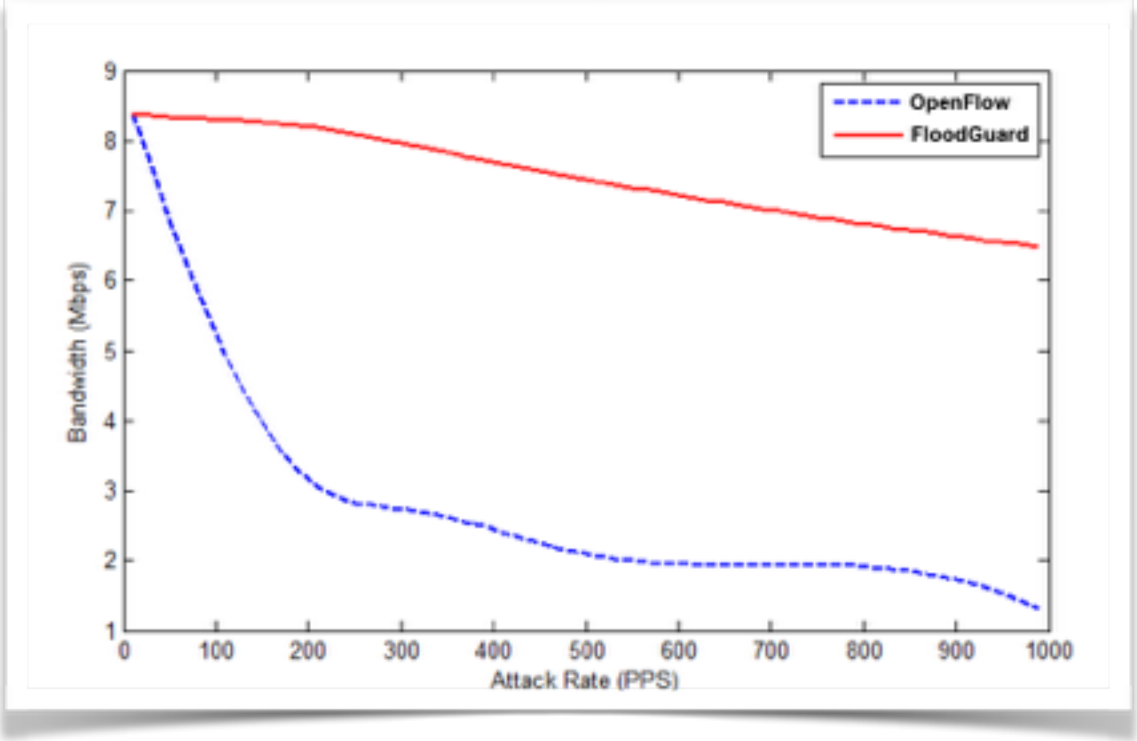


Software

Evaluation

Defense Effects

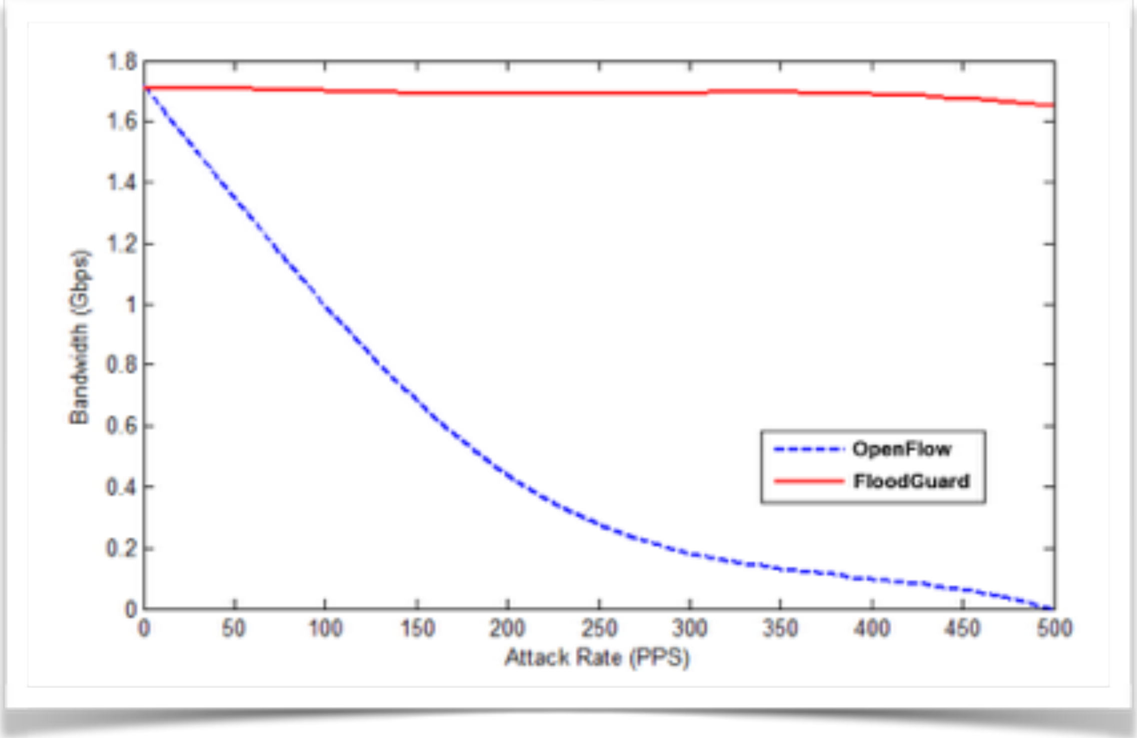


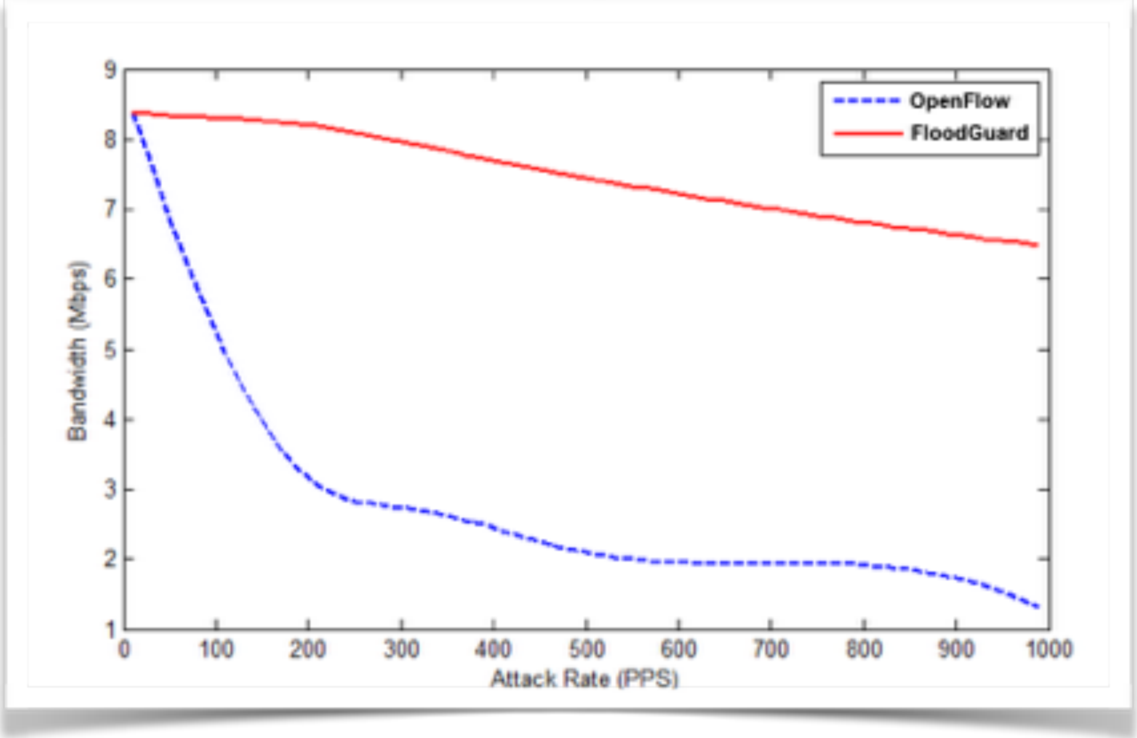


Software

Evaluation

Defense Effects





Software

Hardware

Evaluation

Evaluation

Defense Effects

Evaluation

Defense Effects

Saturation attack: 100PPS

Evaluation

Defense Effects

Saturation attack: 100PPS

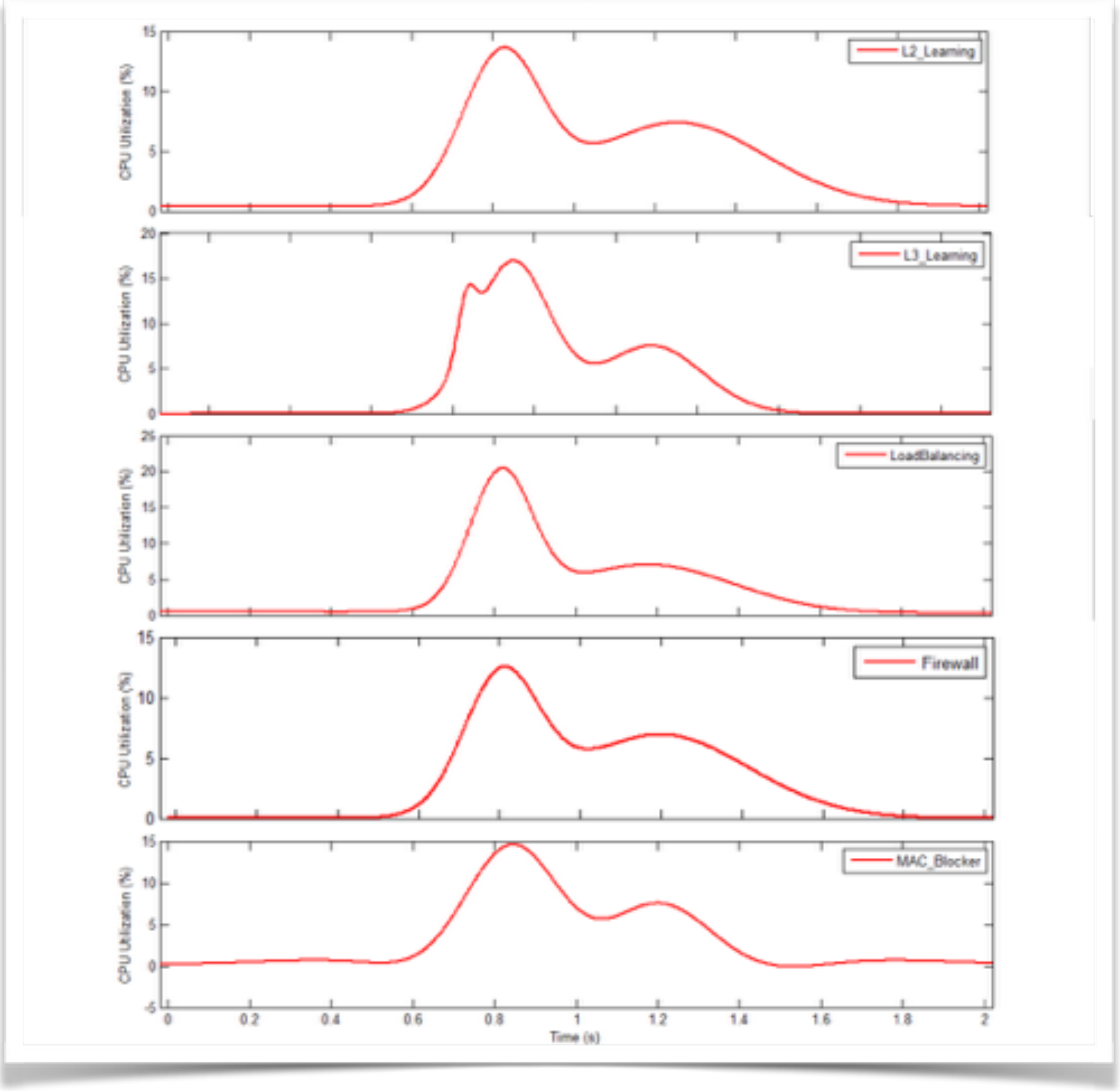
1. L2_learning
2. L3_learning
3. LoadBalancing
4. Firewall
5. MAC_blocker

Evaluation

Defense Effects

Saturation attack: 100PPS

1. L2_learning
2. L3_learning
3. LoadBalancing
4. Firewall
5. MAC_blocker

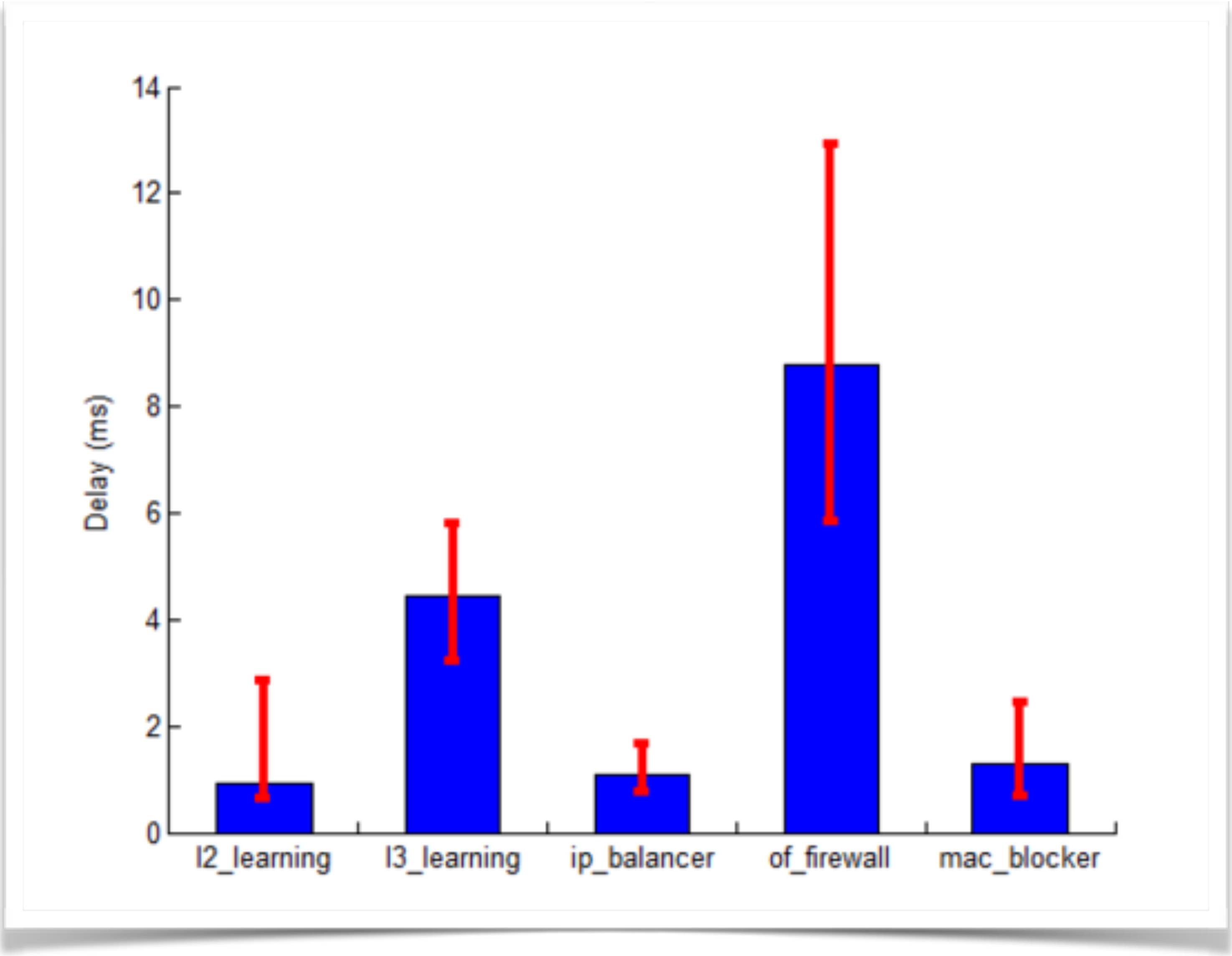


Evaluation

Overhead

Evaluation

Overhead



Evaluation

Evaluation

Overhead

Evaluation

Overhead

AVERAGE DELAY OF THE FIRST PACKET IN EACH NEW FLOW

Evaluation

Overhead

AVERAGE DELAY OF THE FIRST PACKET IN EACH NEW FLOW

OpenFlow	OpenFlow+FLOODGUARD		
Total	Total	Data Plane Cache	Packet Migration
130ms	157ms	30ms	127ms