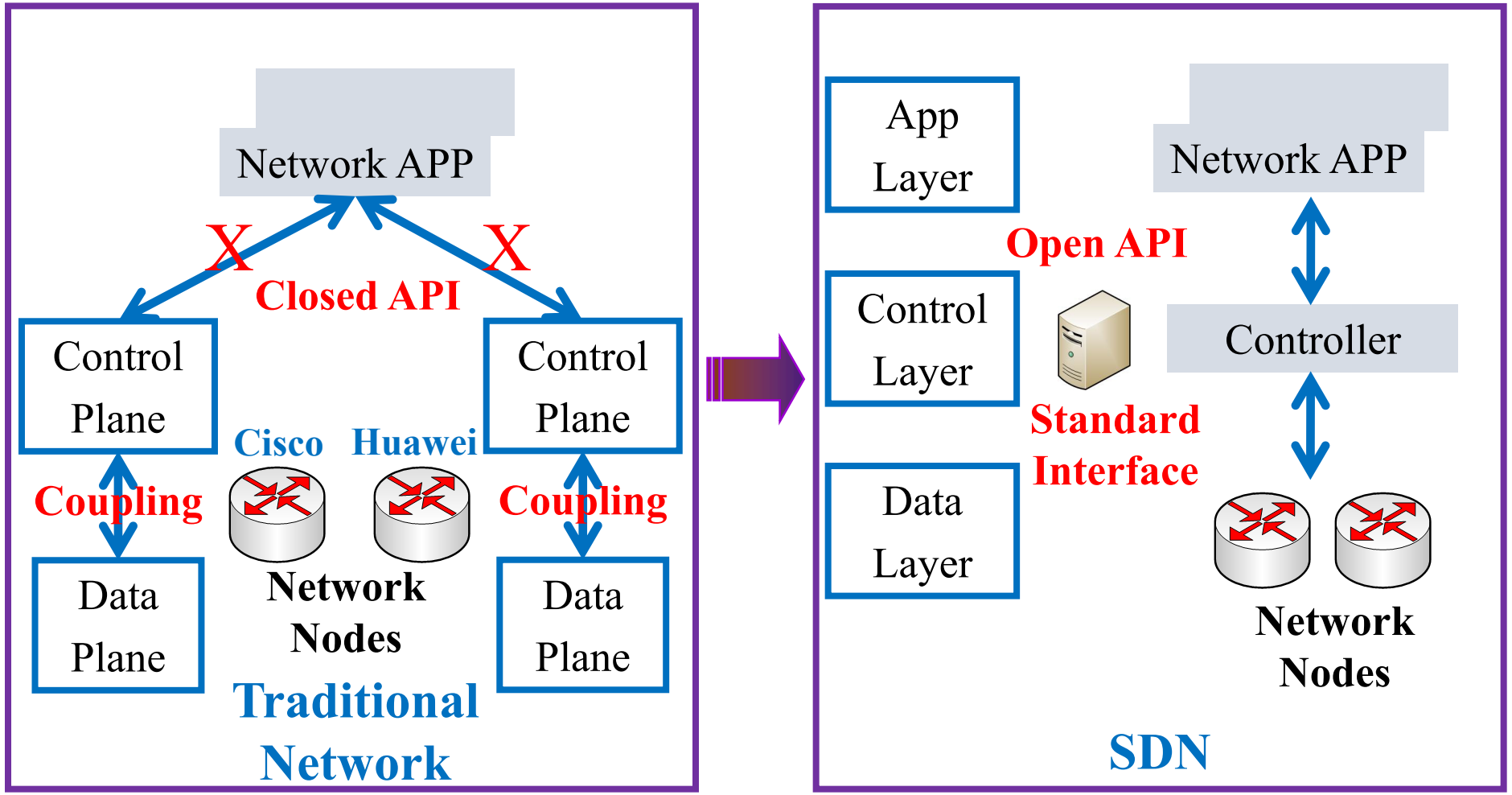

# FloodShield: Securing the SDN Infrastructure Against Denial-of-Service Attacks

**Menghao Zhang** Jun Bi Jiasong Bai Guanyu Li

Tsinghua University

# Software Defined Networking

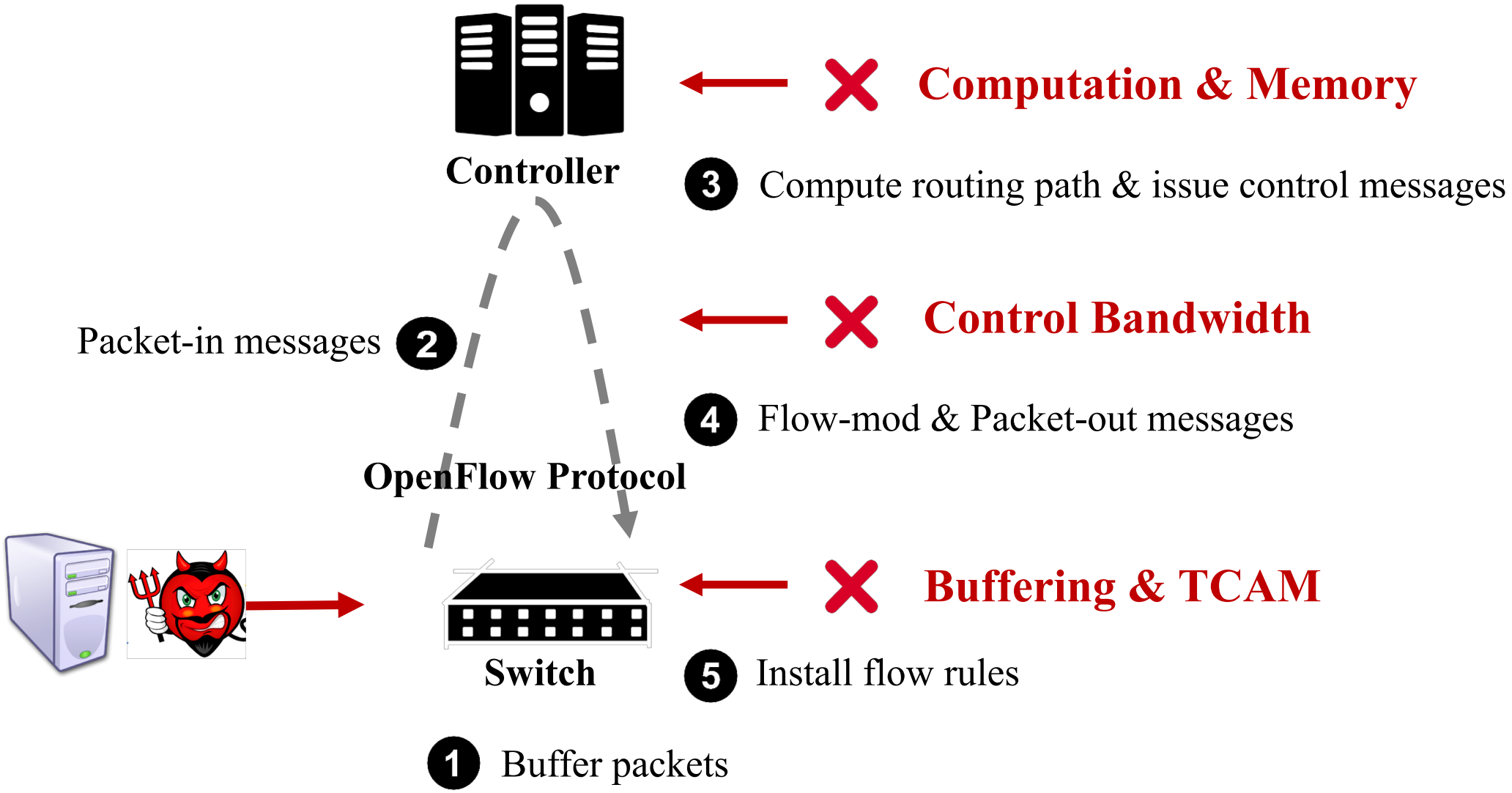



Fine-grained and Centralized network control

Decoupling of control plane and data plane

Unprecedented programmability

# Data-to-control-plane Saturation Attack



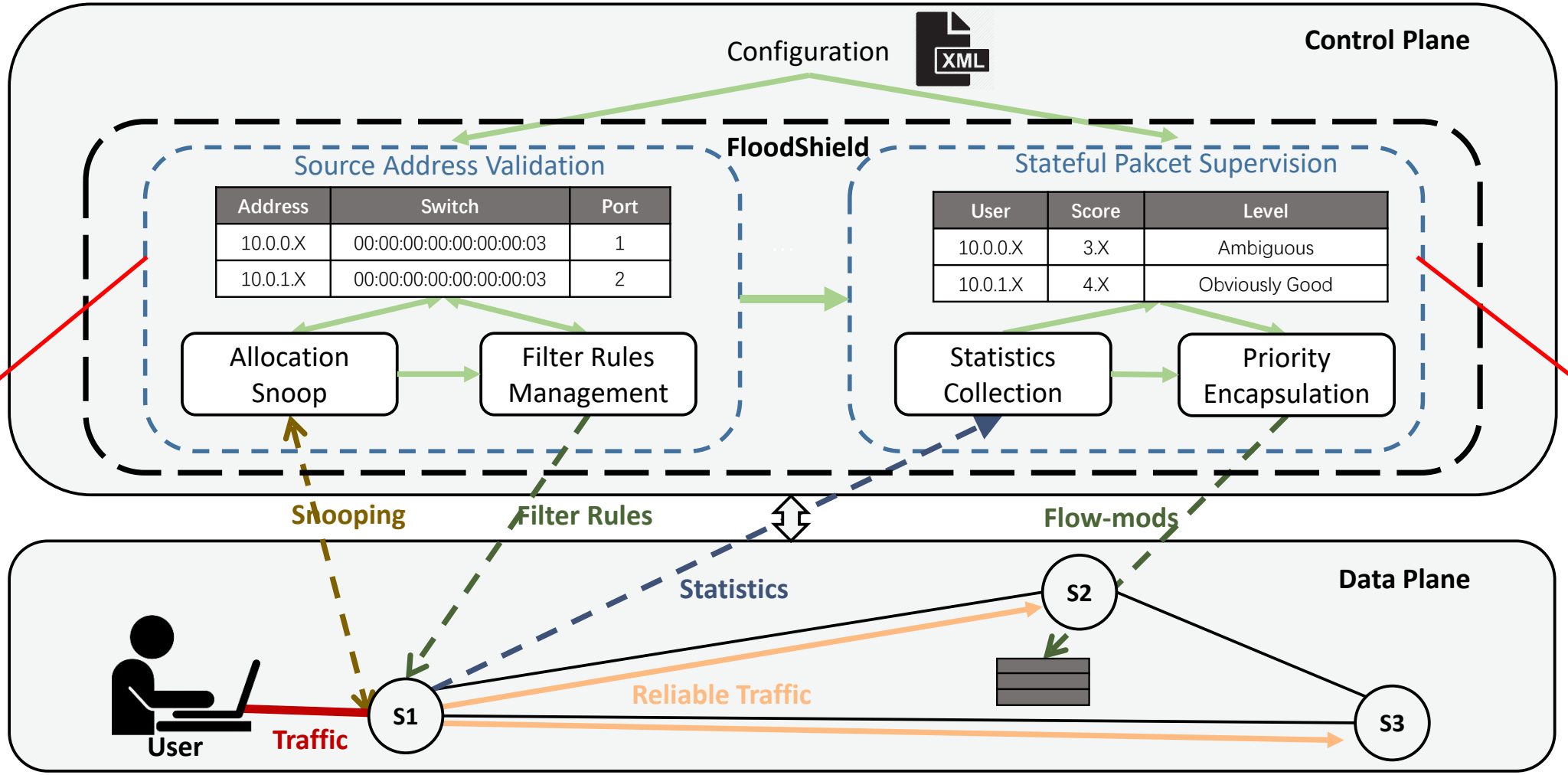
# Previous Studies

- AVANT-GUARD（CCS'13）
  - Modify switches: add *connection migration* module and *actuating trigger* module to enhance the scalability and responsiveness
- FloodGuard（DSN'15）
  - Adopt *proactive flow rule analyzer* in the controller
  - Introduce *data plane cache* to the data plane
- FloodDefender（INFOCOM’17）
  - Introduce *table-miss engineering*, *packet filtering* and *flow table management* to the controller

# Limitation Summary

| | Provide overall protection | Easy for deployment | Lightweight for controller |
|---|---|---|---|
| AVANT-GUARD（CCS'13） | ✗ | ✗ | ✓ |
| FloodGuard（DSN'15） | ✗ | ✗ | ✓ |
| FloodDefender（INFOCOM'17） | ✓ | ✓ | ✗ |
| FloodShield | ✓ | ✓ | ✓ |

# FloodShield Architecture



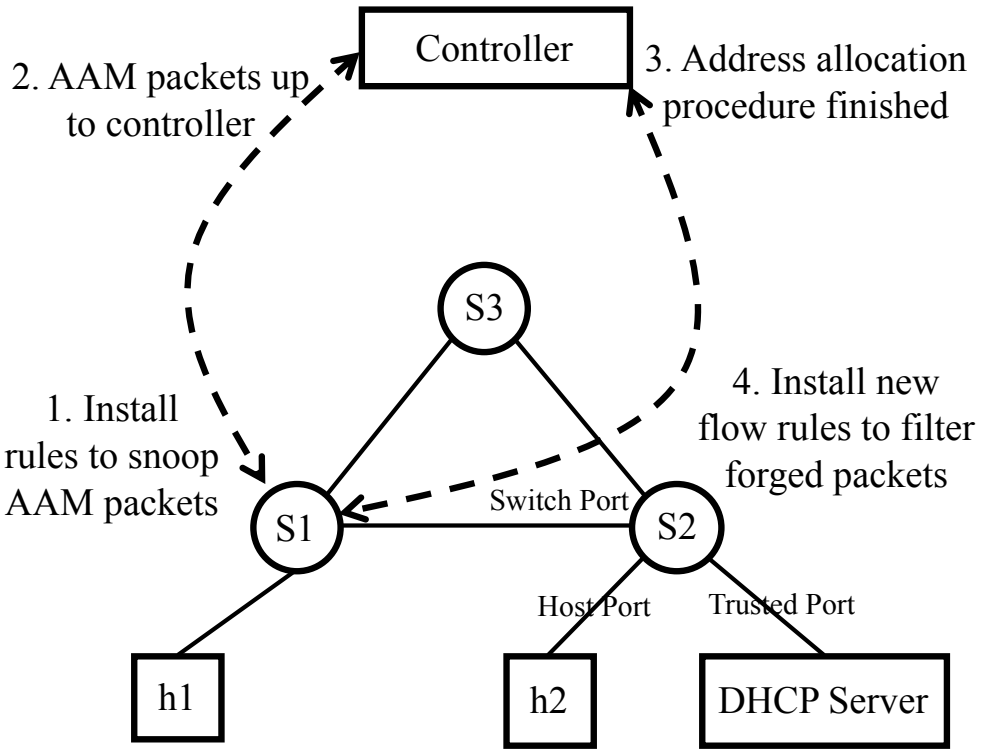

Filters the forged packets directly in the data plane

monitors the packet states of each real address to make further service different iation

# Source Address Validation Module

- Source Address Validation Enforcement Position
  - Switch port classification
    - Switch Port, Host Port, Trusted Port
    - As long as source address validation is performed on the Host Ports, the traffic in the data plane is validated and trustworthy.
- Source Address Validation Enforcement Approach
  - **Monitoring**: Controller monitors the procedures of address allocation protocols (e.g., DHCP) to establish the *Binding Table*, where each binding entry is in the format of ⟨*Address, Switch, Port*⟩.
  - **Binding**: Controller *explicitly* installs *Filter Flow Rules* in the data plane switches to filter the unbound source addresses.

# Examples of Source Address Validation Module

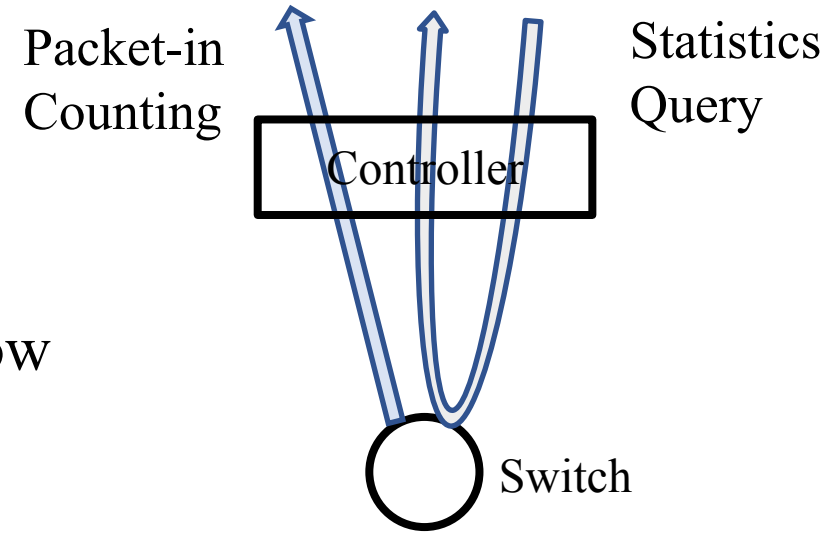



**Monitoring** Example

| The Structure of Filter flow Table in switches | | | |
|---|---|---|---|
| **Group Name** | Match Fields | Priority | Instruction |
| **Host Ports** | in port=hport, mac src=given mac src, ipv4, ip src=given ip src | 2 | jump to table 1 |
| **Host Ports** | in port=hport, mac src=given mac src, arp | 2 | jump to table 1 |
| **Host Ports's filter** | in port=hport, ipv4 | 1 | drop |
| **Host Ports's filter** | in port=hport, arp | 1 | drop |
| **Switch Ports** | in port=sport | 1 | jump to table 1 |
| **Trusted Ports** | in port=tport | 1 | jump to table 1 |

**Binding** Example

# Stateful Packet Supervision Module

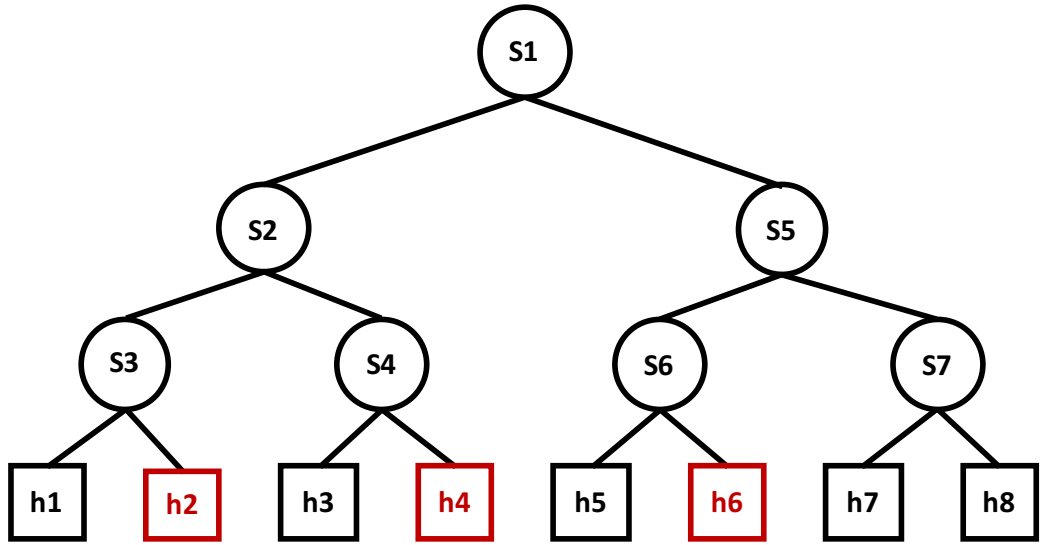



- Precise Behavior Evaluation
  - Traffic feature collection
    - Frequency of New Flows + Packet Number Per Flow
  - Behavior evaluation quantization
    - Linear Mapping
    - Exponential Weighted Moving Average (EMWA) $w_i = (1-\alpha)w_i + \alpha w_{in}$
- Dynamic Service Differentiation

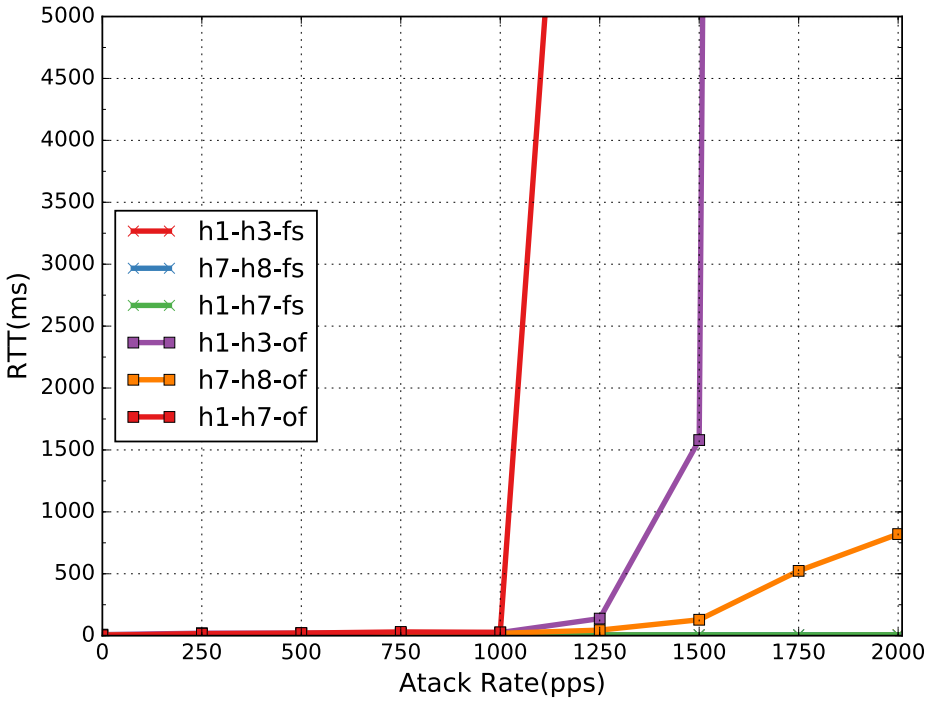
| Behavior-based Network Service Differentiation | | |
|---|---|---|
| **Evaluation Level** | Countermeasure | Importance |
| **Obviously Malicious** | drop/rate-limit in the ingress switch for a period | none/low |
| **Ambiguous** | probability acceptance | low |
| **Obviously Good** | deal all | high |

# Implementation and Evaluation

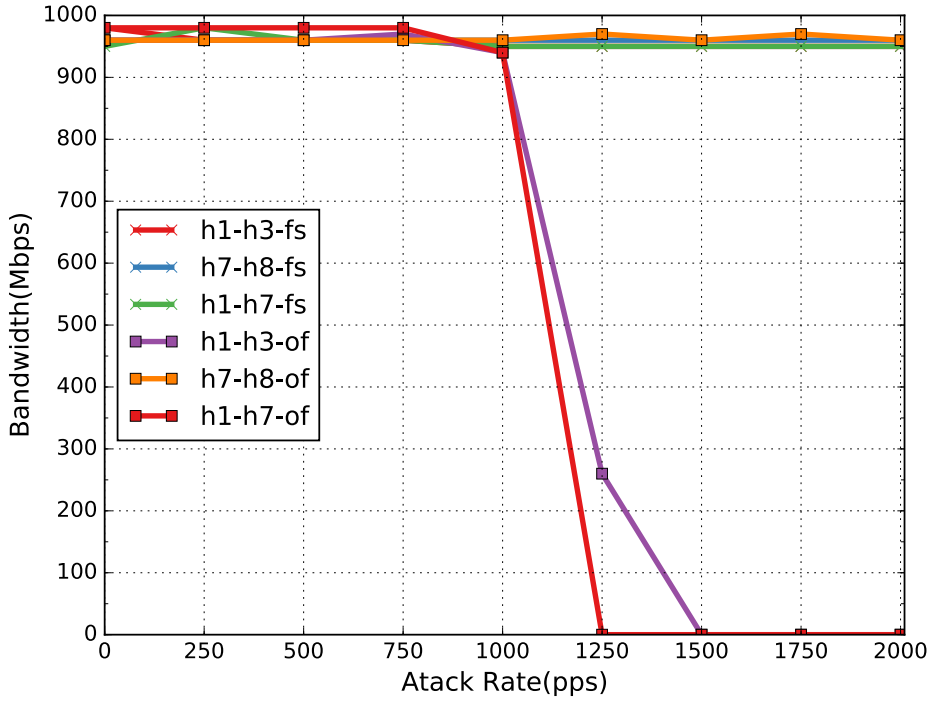
- Implementation
  - Floodlight 1.2 open source controller
  - Mininet to emulate network environment
  - Compared targes： origin OpenFlow (of)， FloodGuard (fg)， FloodDefender (fd)
- Experiment
  - Two Dell R730 servers
  - 1 Controller, 1 Mininet



# End-to-end Effect



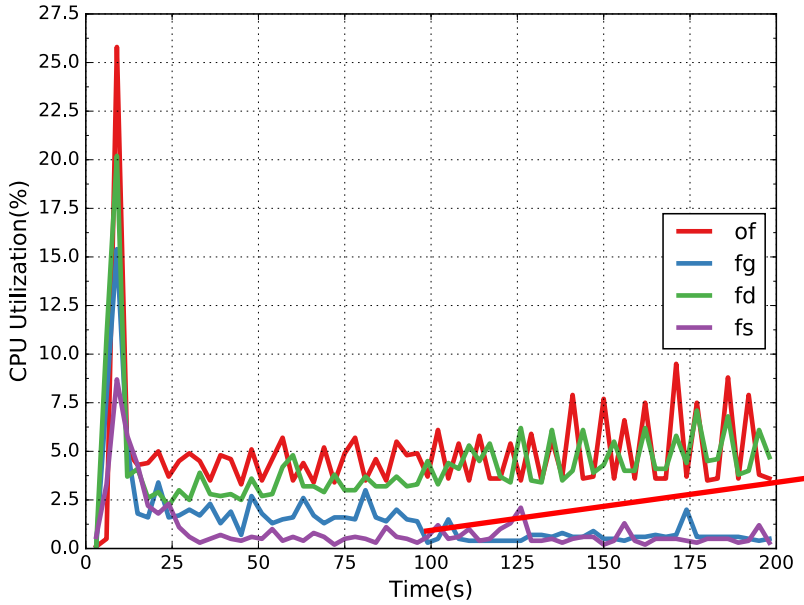

Round Trip Time




Available Bandwidth

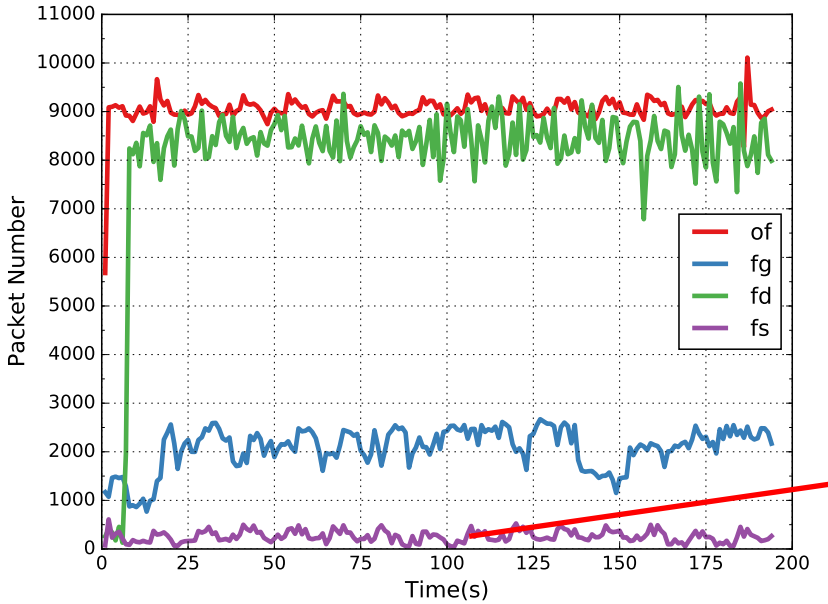
- FloodShield provides effective end-to-end protection for the SDN infrastructure.

# Resource Utilization




CPU Utilization of Controller

Mininum CPU Utilization




Control Channel Utilization

Minimum Control Messages

| Average Flow Rule Number | | | | |
|---|---|---|---|---|
| | Normal Users | Attackers | Overheads | All |
| **OpenFlow** | 535.30(27%) | 1423.14(71%) | 0(0%) | 1959.21(98%) |
| **FloodGuard** | 389.77(19%) | 508.38(25%) | 2.75(0.3%) | 900.77(45%) |
| **FloodDefender** | 492.09(25%) | 250.37(13%) | 571.2(28%) | 1313.11(66%) |
| **FloodShield** | 679.17(34%) | 97.70(5%) | 5.32(0.6%) | 799.87(39%) |

Minimum Flow Table Occupation

# Discussion

- Traffic feature imitation problem
  - The evaluation criterion and the selected features are unknowable to the attacker under normal circumstances. Even if he could obtain these information, the cost for this saturation attack is multiplied, for he has to send multiple packets for each flow and reduce the new flow frequency to get a higher evaluation score.
- Intention hiding problem
  - Attacker may behave correctly firstly, get classified as benign user, and then change his behavior.→EMWA resolves this problems perfectly. (The convergence speed depends on the α in EWMA. The bigger α is, the faster the evaluation score converges.)

# Summary

- Conclusion
  - Problem Identification
    - The drawbacks of state-of-the-art approaches.
  - FloodShield Framework: comprehensive, deployable and lightweight
    - Source Address Validation
    - Stateful Packet Supervision
  - Prototype Implementation and Evaluation
    - Effective protection for the SDN infrastructure with less resource consumption and negligible overheads.
- Future work
  - Source address validation at the gateway scenario

# Thanks!
# Q&A

*netarchlab.tsinghua.edu.cn*

*zhangmh16@mails.tsinghua.edu.cn*