The Institute for Cyber Security

Security Challenges in
Software Defined Networks (SDN)

Lecture 18

Outline

- Market and SDN
- Conventional Networks v.s SDN
- OpenFlow-enabled SDN devices
- SDN Security Applications
- SDN Security Challenges
- Community Debate regarding Security in SDN

Market and SDN

- In 2016, the market research firm IDC predicted that the market for SDN network applications would reach **US$3.5** billion by **2020**.
- Leading IT companies such as Nokia, Cisco, Dell, HP, Juniper, IBM, and VMware have developed their own SDN strategies.

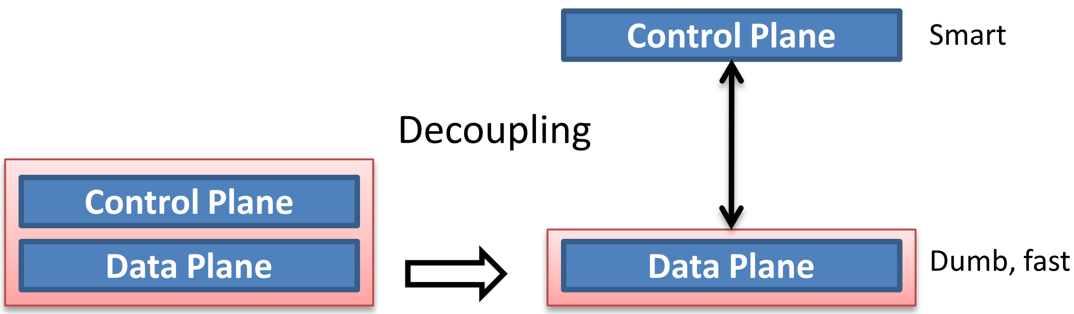
Marc C. Dacier, Hartmut Cwalinski , Frank Kargl , Sven Dietrich, Security Challenges and Opportunities of Software-Defined Networking, Apr 3, 2017

- In 2015, AT&T reduced provisioning cycle by 95% with SDN.

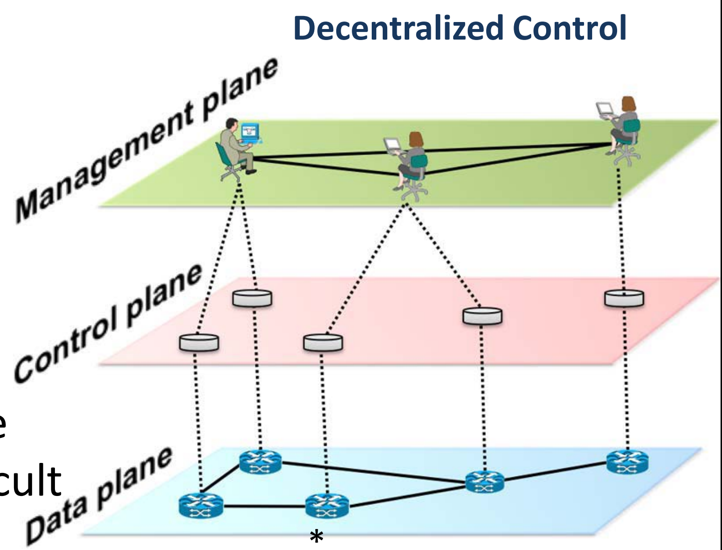
> *"We have taken a process from **low automation** and **weeks** to complete to **high automation** and **minutes** to complete. We're turning the industry on its head in an unprecedented way." John Donovan*

AT&T's analyst conference in August 2015, John Donovan

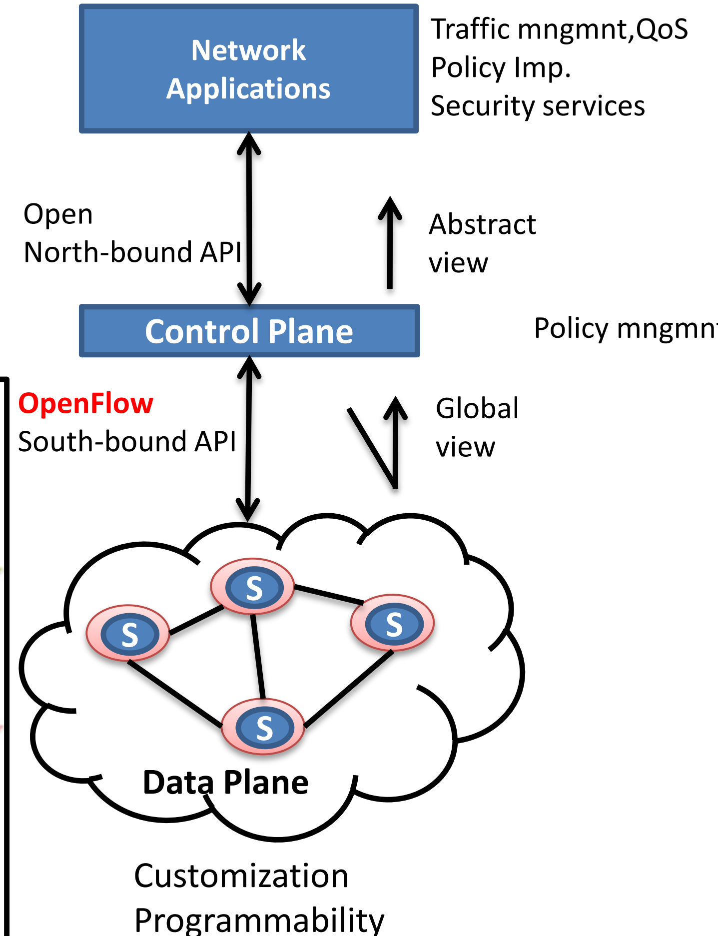
Conventional Networks vs. SDN



- Limited visibility
- Vendor-specfic
- Missconfiguration
- Poor responses
- Policy conflicts
- Security breaches
- Decentralized.
- Complex
- Static architecture
- Innovation is difficult
- Costly
- Yes costly



Conventional Networks



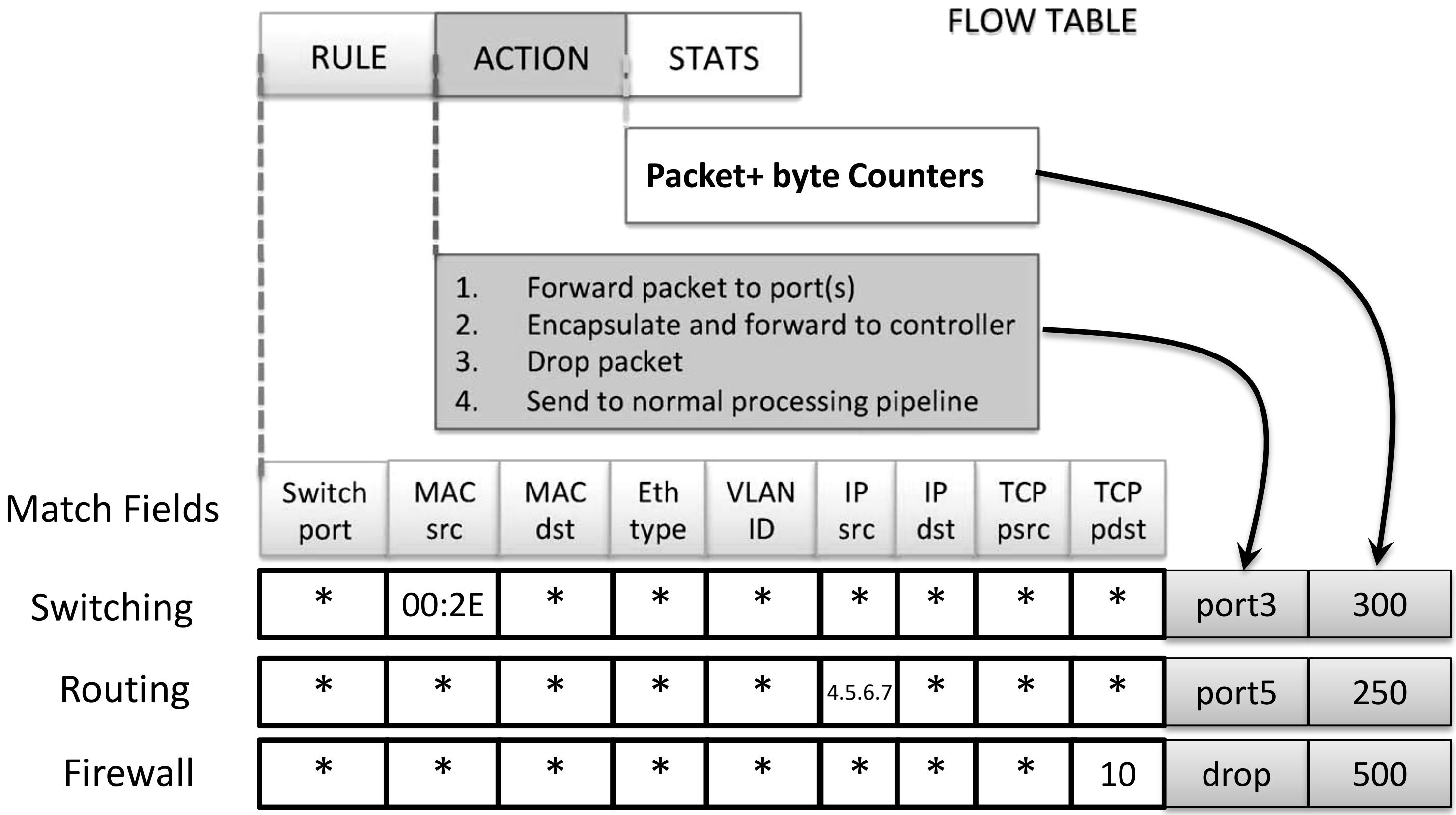
Software Defined Networks

*Figure: Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." *Proceedings of the IEEE* 103.1 (2015): 14-76.

OpenFlow-enabled SDN devices

OpenFlow is: Enabler of SDN

- Protocol between the control plan and data plane
- Describes how controller and a network forwarding device should communicate



I·C·S The Institute for Cyber Security

SDN security applications

UTSA

examples

- **Load Balancer**: send each HTTP request over lightly loaded path to lightly loaded server.
- **Firewall**: inform Central Controller about malware's packets, controller pushes new rules to drop packets.

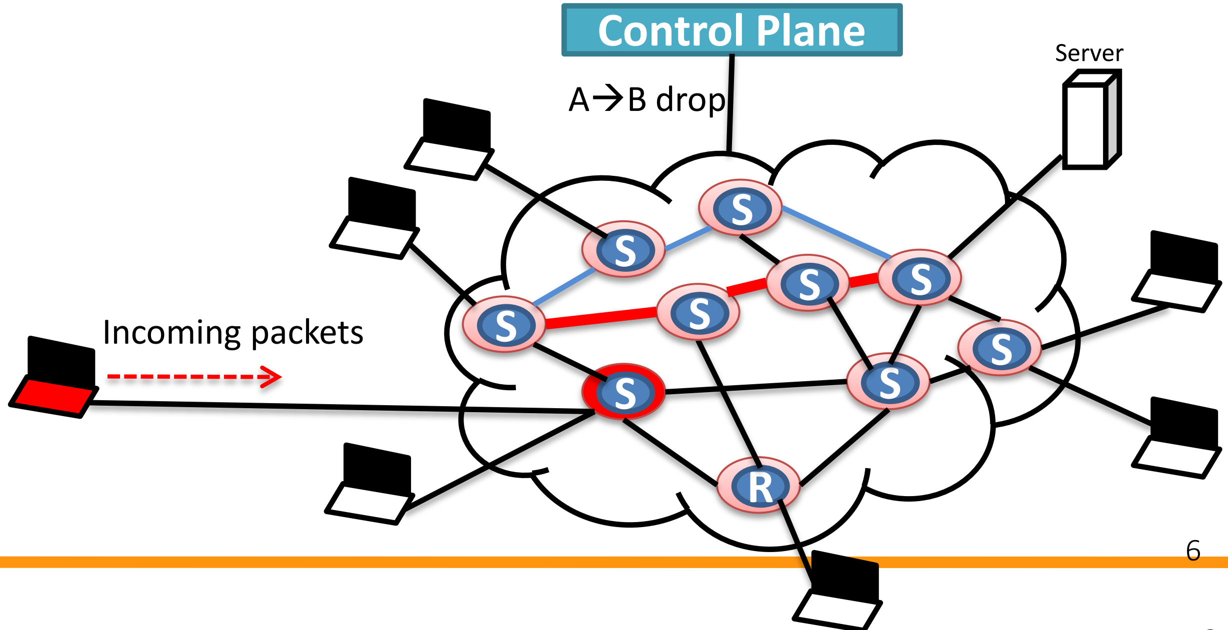
Routing, Load Balancer, Access Control, monitoring, firewall, DDoS Mitigation, IDS/IPS

Application plane

Abstract Network View

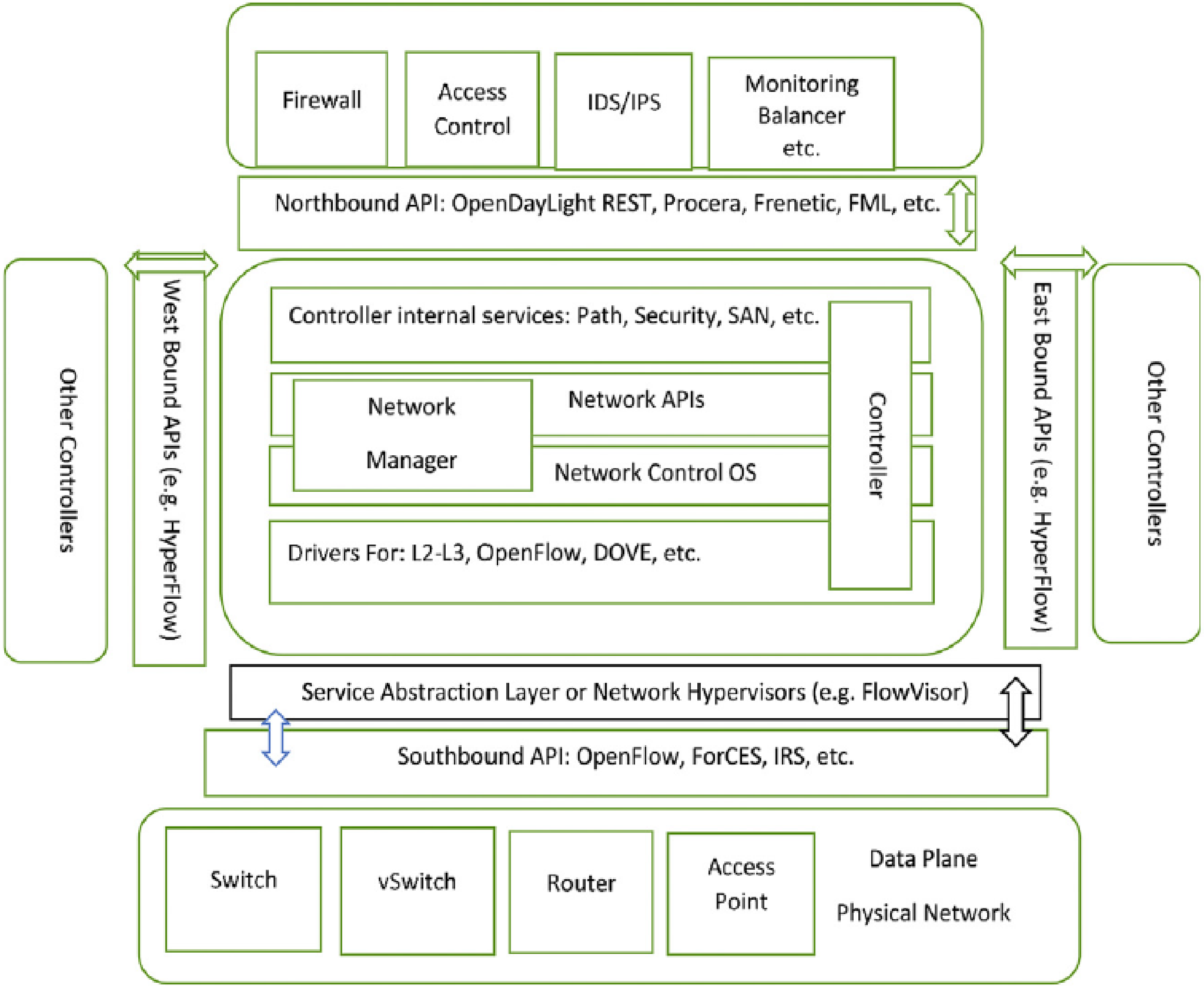
Network Virtualization

Up-to-date Global Network View



6

The big Picture
SDN Archetucture



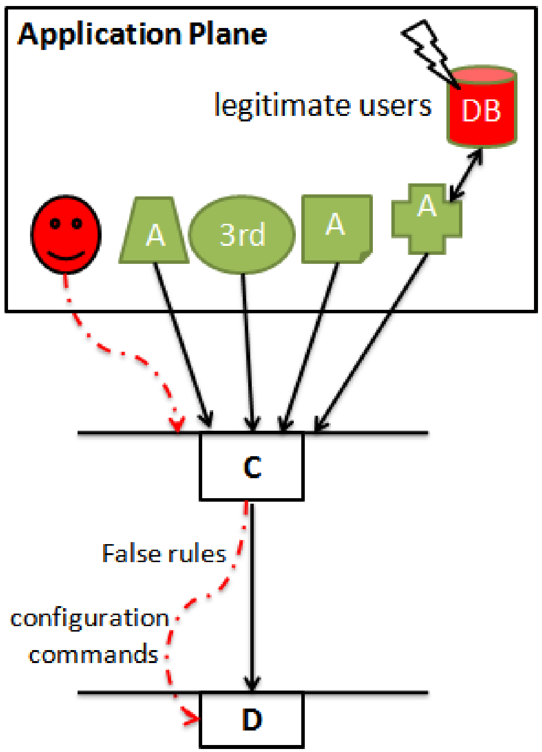
Alsmadi, Izzat, and Dianxiang Xu. "Security of software defined networks: A survey." *Computers & security* 53 (2015): 79-108.

SDN Security Challenges

Application Plane Security Challenges

- Lack of Authentication and Authorization
- Lack of Access Control and Accountability
- Fraudulent flow rule insertion

SDN aware & SDN unaware apps
Nested applications



Apps classes

- Service apps
- sensitive apps
  - Path characteristics
  - Access ports
  - Monitor traffic
  - Reject/Accept flows

Application Plane
Targeted Threat/Proposed Solution

Threats within/from apps

Framework for security apps development
(FRESCO Scripting language)

Security policy violation

Security policy verification framework

-Flover:
on controller
new/old rules conflict

-ndb: root cause

-OFRewind : trace anomalies

flow rules contradiction

Assertion-based language

-catch bugs before deployed
- forwarding loops
- black holes

Access control breach

Permission system (**PermOF**):
least privilege on apps

PermOF

The design is based on a Set of permissions & Isolation mechanisms

- Ensures controller superiority over applications
- Isolates control flow and data flow
- controller should be able to mediate all the apps' activity

Availability of sensitive info

real time

Category	Permissions
Read	read_topology read_all_flow read_statistics read_pkt_in_payload
Notification	pkt_in_event flow_removed_event error_event topology_event
Write	flow_mod_route flow_mod_drop flow_mod_modify_hdr modify_all_flows set_device_config set_flow_priority
System	network_access file_system_access process_runtime_access

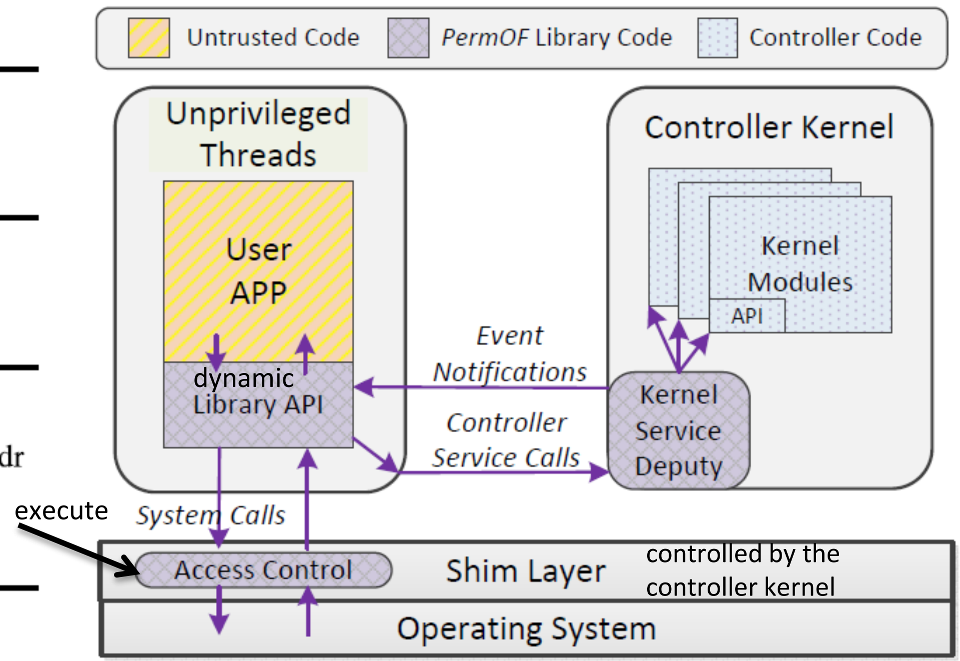


Figure 1: *PermOF* Isolation Framework

Wen, Xitao, et al. "Towards a secure controller platform for openflow applications." *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. ACM, 2013.

Control Plane Security Challenges

Threats due to Scalability

-Huge # flow rules

-saturation

DoS Attacks

-SDN response times

-IP packets with random headers

Challenges in Distributed Control Plane

Control Plane
Targeted Threat/Proposed Solution

Controller scalability

1. Wildcards mechanism
 -Load balancing: direct an aggregate of client requests to replicas
2. Increase the processing power **(McNettle controller)** parallelism
3. Hybrid reactively/Proactive controller

Switch port	MAC src	MAC dst	Eth type	VLAN ID	IP src	IP dst	TCP psrc	TCP pdst	Action
*	*	*	*	2	*	*	5	*	port9

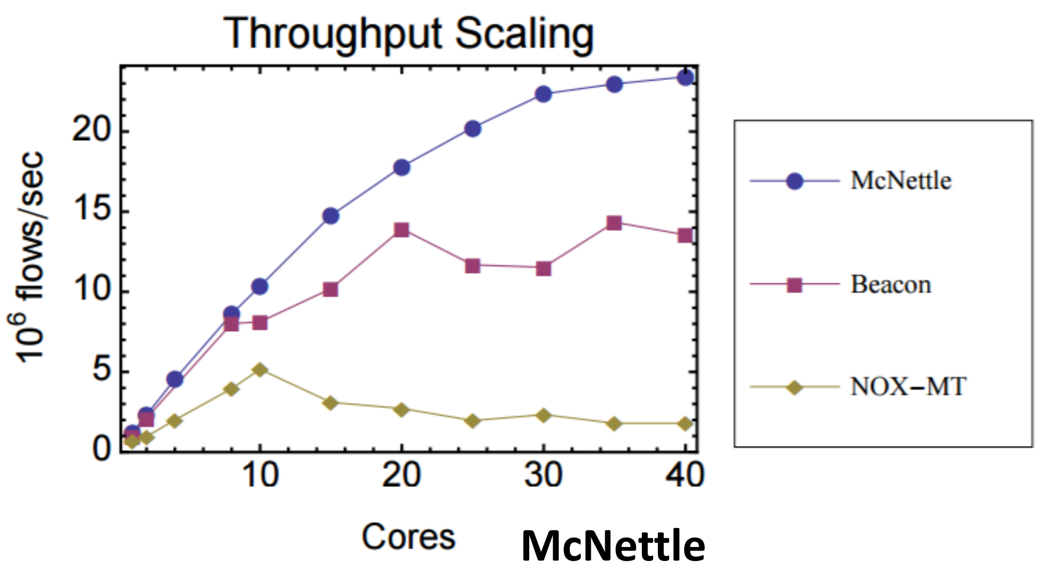
- NOX-MT scales to 5m f/s at 10 CPU cores
- Beacon → 13m f/s at 20 CPU cores
- McNettle →20m f/s at 46 CPU cores

DDoS Attack

Detection Framework
SDN DDoSDetection

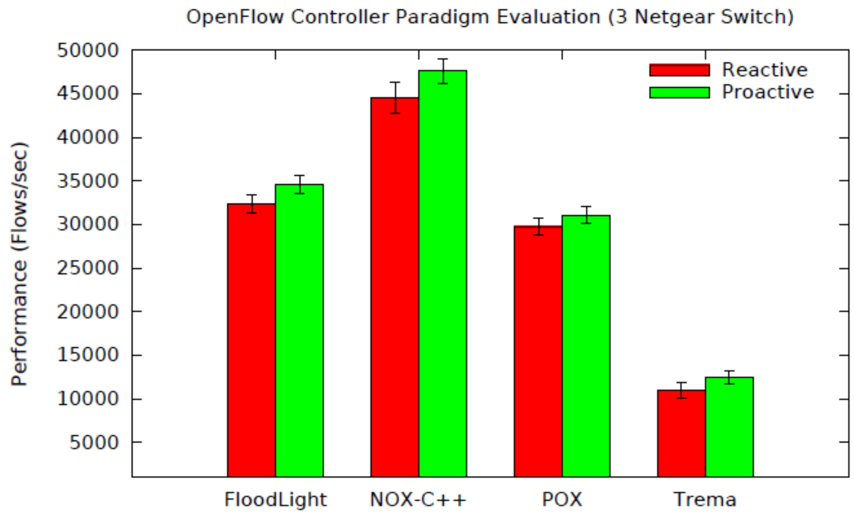
Challenges in distributed control plane

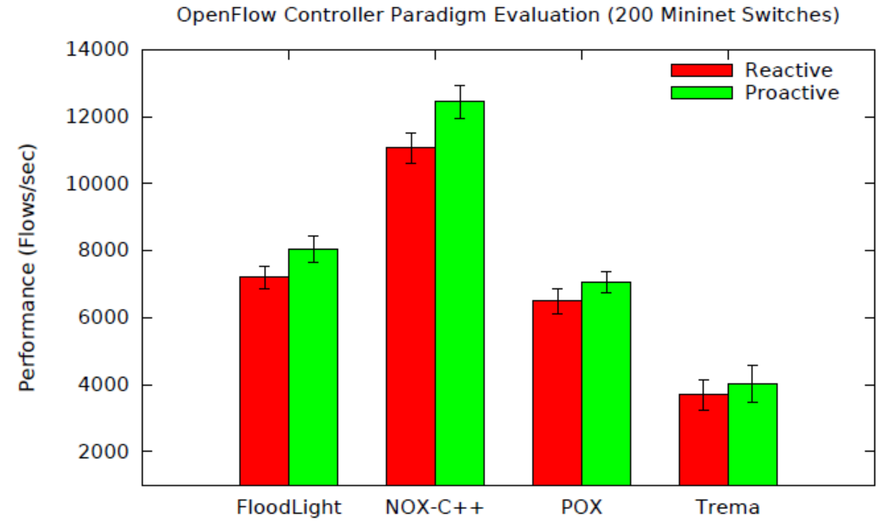
intra-domain & inter-domain **(DISO)**

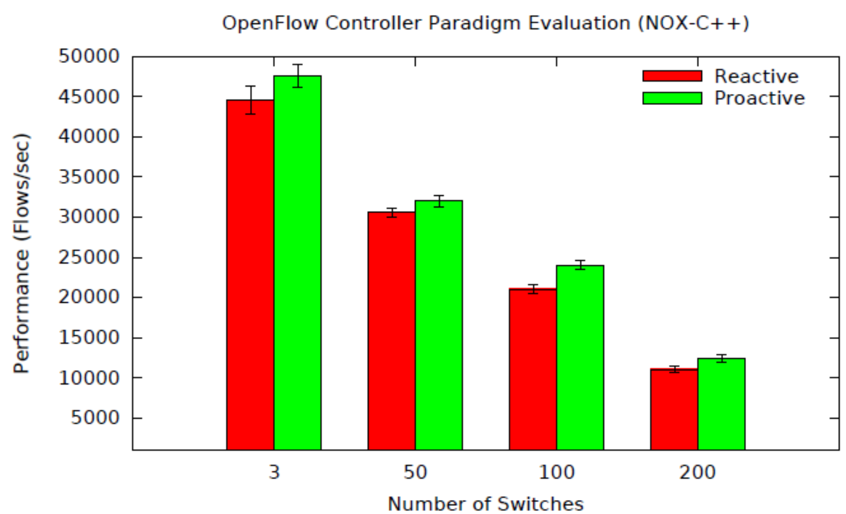


http://haskell.cs.yale.edu/wp-content/uploads/2013/04/thesis-singlespace.pdf

Reactively vs. Proactive Controller



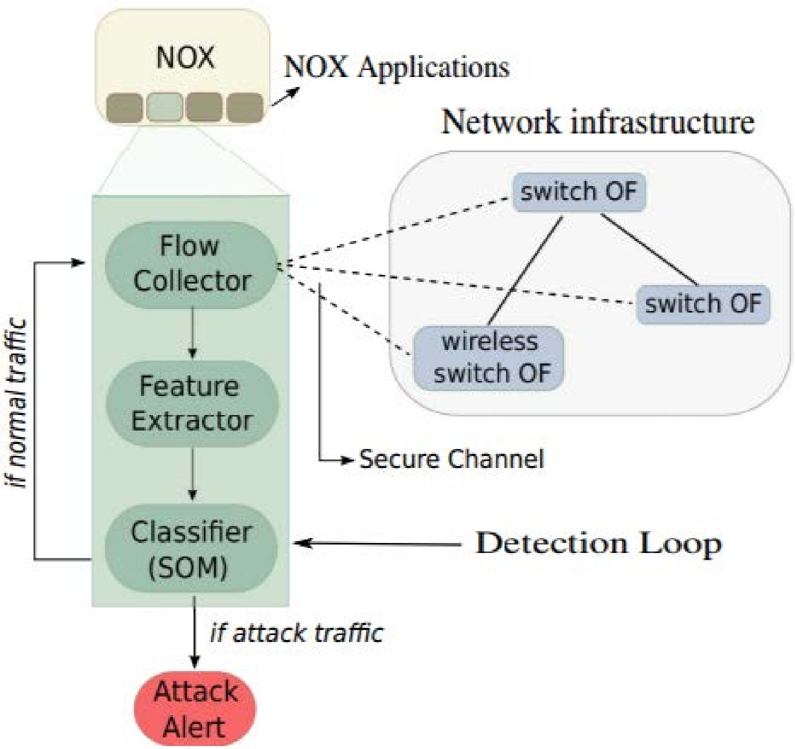


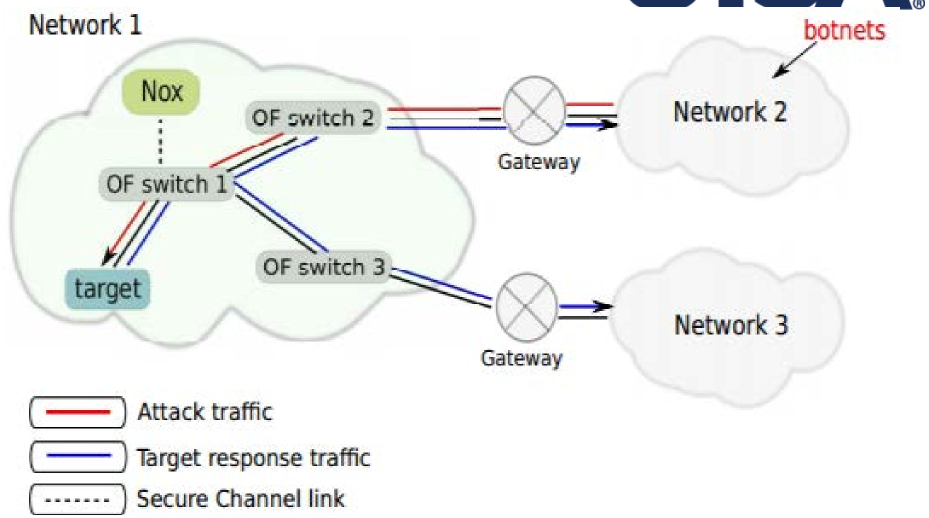


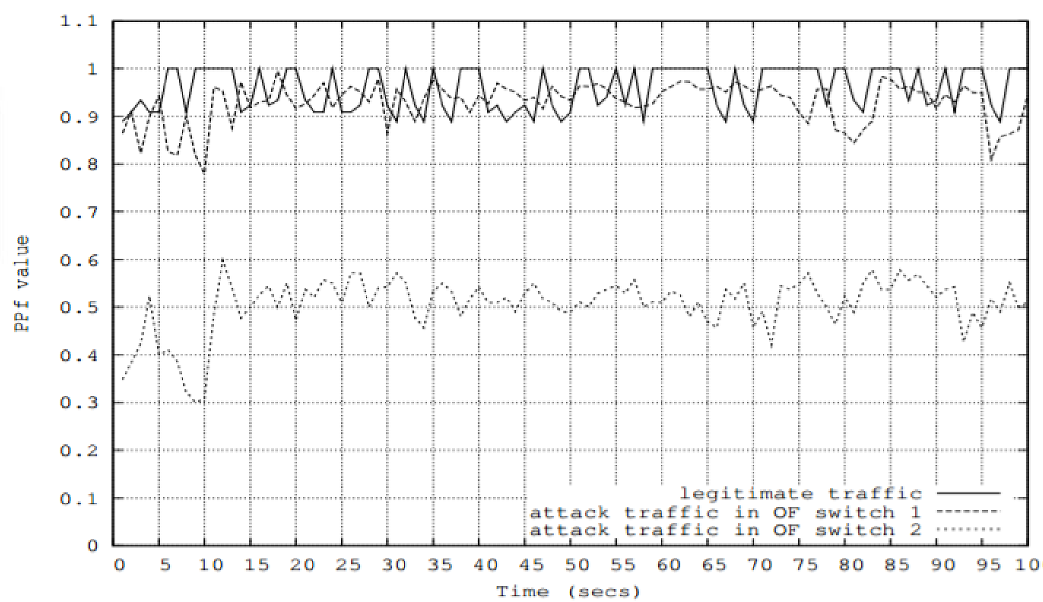
Marcial P. Fernandez, Evaluating OpenFlow Controller Paradigms, 2013

SDN DDoSDetection

1. **Flow collector module**: gathers flow entries within intervals.
2. **Feature extractor**: Avg. packets/f, Avg. Bytes /f, avg duration/f, growth of single-flows, and growth of different ports.
3. **Classifier**: Analyzes → Alarm?



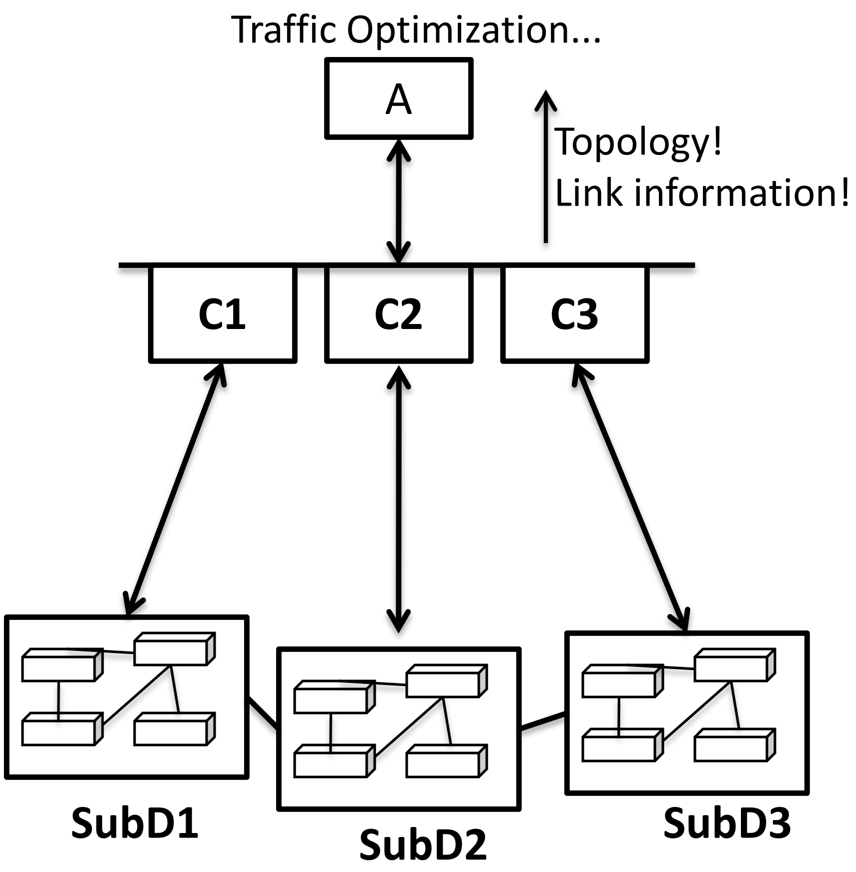




R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE 35th Conf. LCN,* Oct. 2010, pp. 408–415.

intra-domain & inter-domain
(DISO)

- **intra-domain :** manages its own network domain
  - compute the paths of flows
  - dynamically react to network issues (broken line, high latency, bandwidth cap exceeded)
  - redirecting and/or stopping traffic
- **inter-domain**:
  - discovers neighboring controllers and manages communication among controllers
  - exchange aggregated network-wide information with others



Data Plane
Security Challenges

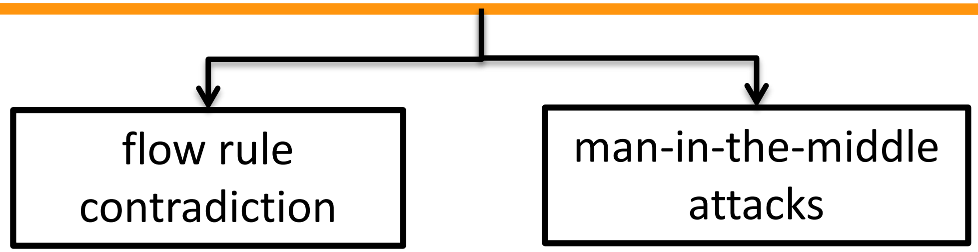
Flow rules installation

Genuine vs. malicious rules
Limited table entries
Limited switch buffer

Switch-Controller link

#switches per controller
path Length

Data Plane
Targeted Threat/Proposed Solution



Real-time contradiction check
FortNox

High level points

-- Debate

Centralization in SDN

The Good:

- Fast responsiveness
- Easy to removing policy inconsistencies
  - centralized routing algorithms
  - Firewalls
  - network-monitoring

The Bad:

- Single point of failure may be exploited by an **internal** or **external** attacker

Regarding DDoS

Bad: centralization added a new type of denial-of-service (DoS) vector.

Good: Effective management of existing DoS attack types

- Using Global view
- Traffic analysis

New security challenges but benefits appear to be predominant!!!

Marc C. Dacier, Hartmut Cwalinski , Frank Kargl , Sven Dietrich, Security Challenges and Opportunities of Software-Defined Networking, Apr 3, 2017

Attack Surface vs. Defense Opportunities

Good:

- In SDN defenders can create customized security solutions
- e.g Anomaly detection systems
  - Global view
  - Open hardware interfaces
  - Centralized control

Bad:

- Benefit the attackers (**zero day attacks**)
  - The centralized architecture
  - Lack of defender expertise
  - Still immature technology

Marc C. Dacier, Hartmut Cwalinski , Frank Kargl , Sven Dietrich, Security Challenges and Opportunities of Software-Defined Networking, Apr 3, 2017

Centralized vs. Distributed Approach

Good:

- Reduced complexity by splitting into planes.
  - Easier testable
  - E.g, routing algorithms simpler than the distributed approach in conventional networks.

Bad:

- Stressed by two aspects that strongly call for the use of a distributed approach.
  - The need for **scalability**
  - **Operational requirements (**fault tolerance)

Marc C. Dacier, Hartmut Cwalinski , Frank Kargl , Sven Dietrich, Security Challenges and Opportunities of Software-Defined Networking, Apr 3, 2017

Is SDN More Complex?, or Is It Simpler?

Implementing the control plane completely in software

Good :

- Programmability

Bad:

- Opposes simplicity : raises issues about algorithmic complexity.
  - **Why**: additional requirements that weren't imposed on classical networks but are now thinkable in SDN.
  - Simplicity is a key design principle in building secure systems.

SDN has the potential to be simple—but making it simple is quite complex.

Marc C. Dacier, Hartmut Cwalinski , Frank Kargl , Sven Dietrich, Security Challenges and Opportunities of Software-Defined Networking, Apr 3, 2017

Open problems & research directions

- How to implement **authentication and authorization** to certify SDN applications.
- How to implement **access control and accountability** in SDN.
- How to implement customized **security procedures** based on the **type or categories of applications.**
- How can we find **automated** derivation of Secure SDN **Configurations**.
- How can we secure the **controller-switches communication**?
- How can we perform efficient **intrusion detection** and **anomaly detection** in SDNs?
- How can we **operate SDN** in presence of **untrusted HW** components?
- How can we **protect the controller** itself?

Without security, SDN will not succeed!

Thank you