Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

Lecture 11

SAPIENZA
UNIVERSITÀ DI ROMA

Outline for today

- Recap last lecture
- Software defined networking
- Report guidelines - points to consider

Outline for today

- Recap last lecture
- Software defined networking
- Report guidelines - points to consider

GDPR - What?

GDPR is a European law which went into effect on May 25, 2018. The GDPR lays down rules relating to the protection of fundamental rights and freedoms of persons, and in particular their right to the protection of personal data.

- Governs the type of notice that must be provided to people regarding how their identifiable data is used.
- Governs how companies are allowed to use and process identifiable data.
- Has strict requirements for using sensitive data.

GDPR - Controllers/Processors

- Controllers specify the means and purpose of the data processing.
  - The data controller gives instructions for processing to the data processor.
  - The controller is responsible for implementing measures to ensure that processing occurs pursuant to GDPR.

- Processors conduct the processing under the direction of the controller. The processor cannot process personal data except upon the instructions of the controller. The processor is tasked by the text of the privacy law with helping the controller with certain tasks, including information necessary to demonstrate compliance.

GDPR - Right to access data - Article 15

- Article 15 of the law establishes one of the most fundamental rights in the Internet:
  - The users have the right to request to web sites a copy of all the personal data that they have about them. The goal of this right is to return control and awareness to the users of the personal data they share, consciously or not.

What will we see today?

- The results of a broad world-scale investigation on the actual deployment of the GDPR.
  - Step by step analysis of all the phases to a subject access request
  - Over 300 of the most popular websites according to Alexa ranking

GDPR - Right to access data

- First step: create and utilize real accounts on these services
- Second step: ask for your data and evaluate

GDPR - Asking the data - focus

- While asking the data information about the relevant phases needs to be collected such as:
  - Privacy policy compliance
  - Request methodology
  - Identification
  - Response format
  - Response time
  - Information obtained

Sharing data via email and no email encryption

- Sending sensitive data as plain email or plain attachment can be risky:
    - The email can be sent to an incorrect recipient.

      The email and the attached file are saved on the email server (an attacker gains unauthorized access to it)

Over ⅓ of the responses

Outline for today

- Recap last lecture
- Software defined networking
- Report guidelines - points to consider

Software defined networking

SDN is an approach to networking that uses software controllers that can be driven by application programming interfaces (APIs) to communicate with hardware infrastructure to direct network traffic.

Software defined networking

Approach to networking that aims:

- to make networks more flexible, scalable, and programmable.
- Make the topology independent of physical one

Traditional networking vs. SDN

- In traditional networking, both the control plane (which determines how data packets are forwarded) and the data plane (which handles the actual forwarding of packets) are tightly integrated within network devices.

- SDN is the separation of control and data planes. This separation allows for programmability and automation of network configurations and policies. This enables network administrators to dynamically control and manage network traffic flows according to application requirements and business needs.

Traditional networking challenges/issues

- Lacking abstraction
- Unpredictable outcome from distributed algorithms
- Cross protocol interactions can be challenging
- A device needs to be properly configured
- Unable to have a clear intent

SDN

- Centralizing the control plane enables more powerful abstractions
- Express intent network-wide (for example better security)
- Distributed systems techniques to make central control scalable and fault tolerant
- Networks provisioned by software

SDN - some benefits

- Ease of network control
- Agility
- Flexibility
- Greater control over network security
- Simplified network design and operation
- Modernized telecommunications

SDN - ease of network control

Separating the packet forwarding functions from the data plane enables direct programming and simpler network control.

This could include configuring network services in real time, such as:

- Ethernet or firewalls, or quickly allocating virtual network resources to change the network infrastructure through one centralized location.

SDN - agility

SDN enables dynamic load balancing to manage the traffic flow as need and usage fluctuates, it reduces latency, increasing the efficiency of the network.

SDN - flexibility

Network operators have more flexibility to control the network, change configuration settings, provision resources, and increase network capacity due to the software-based control layer.

SDN - network security

SDN allows set policies from one central location to determine access control and security measures across the network by workload type or by network segments.

SDN - simplified design and operation

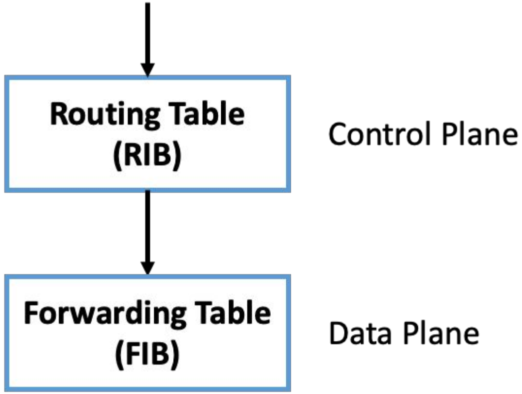
You can use a single protocol to communicate with a wide range of hardware devices through a central controller.

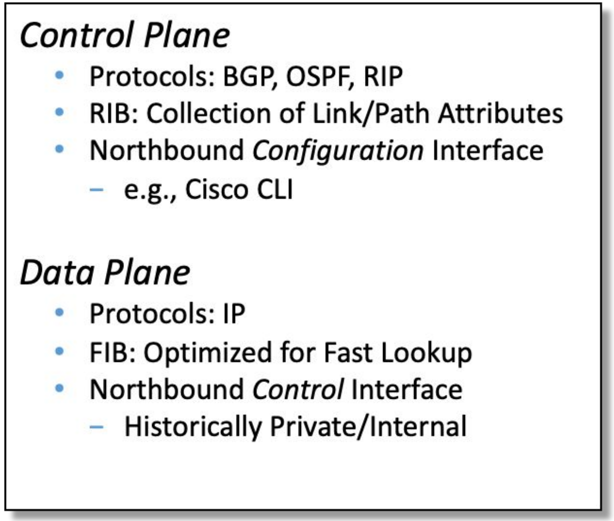
SDN - modernized telecommunications

Through the use of SDN service providers can provide distinct network separation and control to customers.

This helps service providers improve their scalability and provide bandwidth on demand to customers.

Traditional - control & data plane





Control Plane

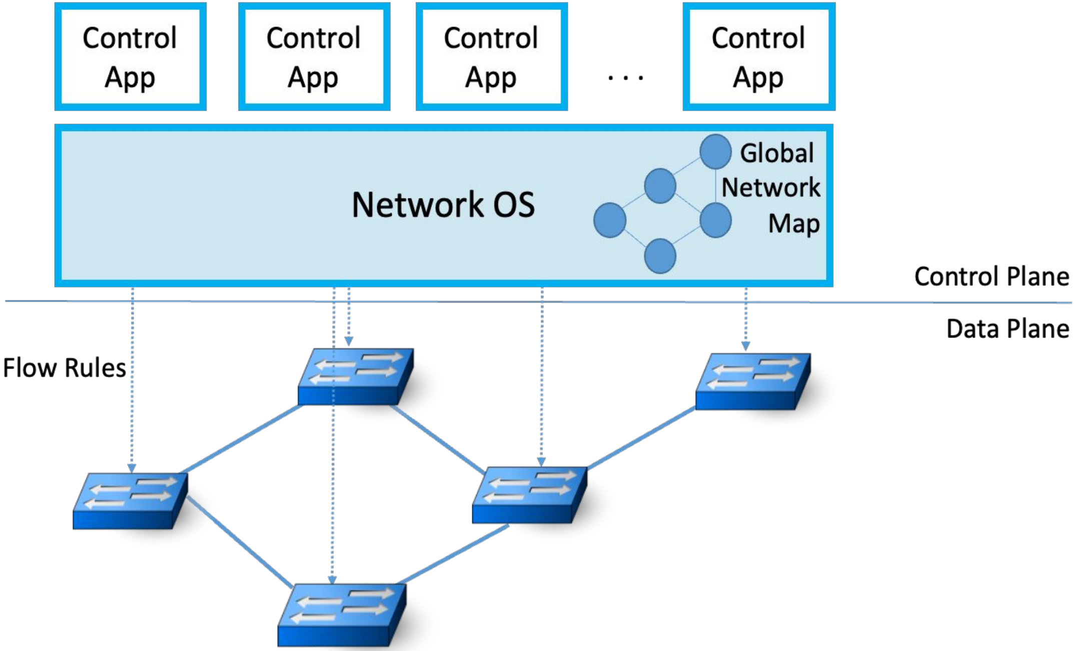
- Protocols: BGP, OSPF, RIP
- RIB: Collection of Link/Path Attributes
- Northbound *Configuration* Interface
  - e.g., Cisco CLI

Data Plane

- Protocols: IP
- FIB: Optimized for Fast Lookup
- Northbound *Control* Interface
  - Historically Private/Internal

The **control plane** (how data is forwarded) and the **data plane** (which handles the actual forwarding of data packets) are **tightly integrated** within network devices such as routers and switches.

SDN



The control plane is centralized in an SDN controller, while the data plane remains distributed across network devices.

Network OS

- Network OS: distributed system that creates a consistent, up-to-date network view
  - Runs on servers (controllers) in the network

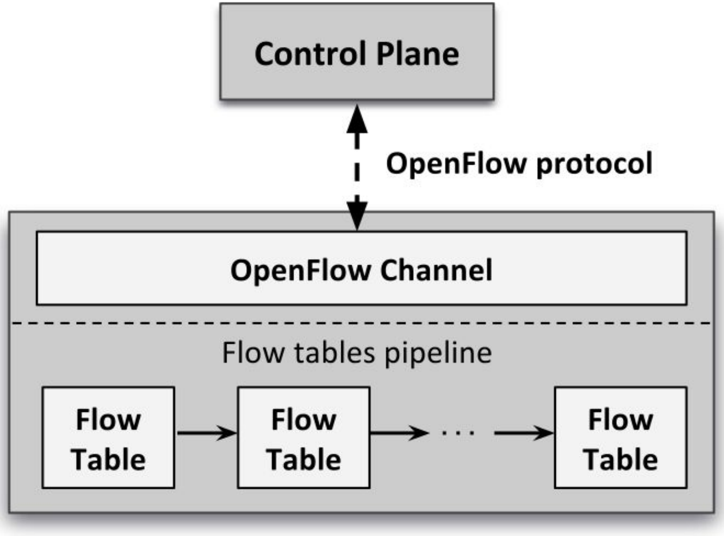
- Uses forwarding abstraction to:
  - Get state information from forwarding elements
  - Give control directives to forwarding elements

Control programs

- Control program operates on a view of network
  - Input: global network view (graph/database)
  - Output: configuration of each network device

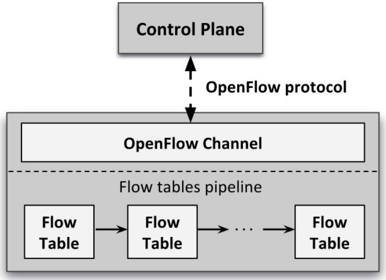
HowTo-SDN - OpenFlow

- Most widely adopted
- Provides a standard communication interface between the data plane and control plane.



OpenFlow Switch

OpenFlow



The control plane can program the network devices in a reactive manner.

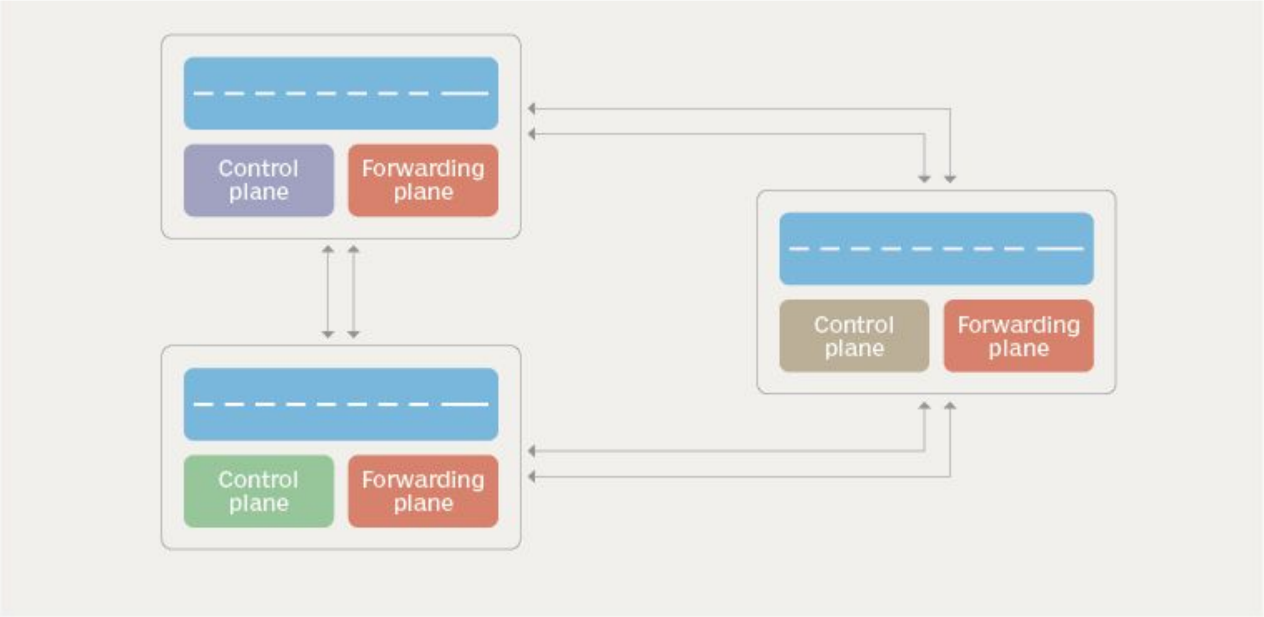
Whenever an OpenFlow switch receives a new inbound network flow, it sends a request to its controller in the control plane, which in turn creates and installs on the switch a new rule indicating how to manage the flow.

OpenFlow

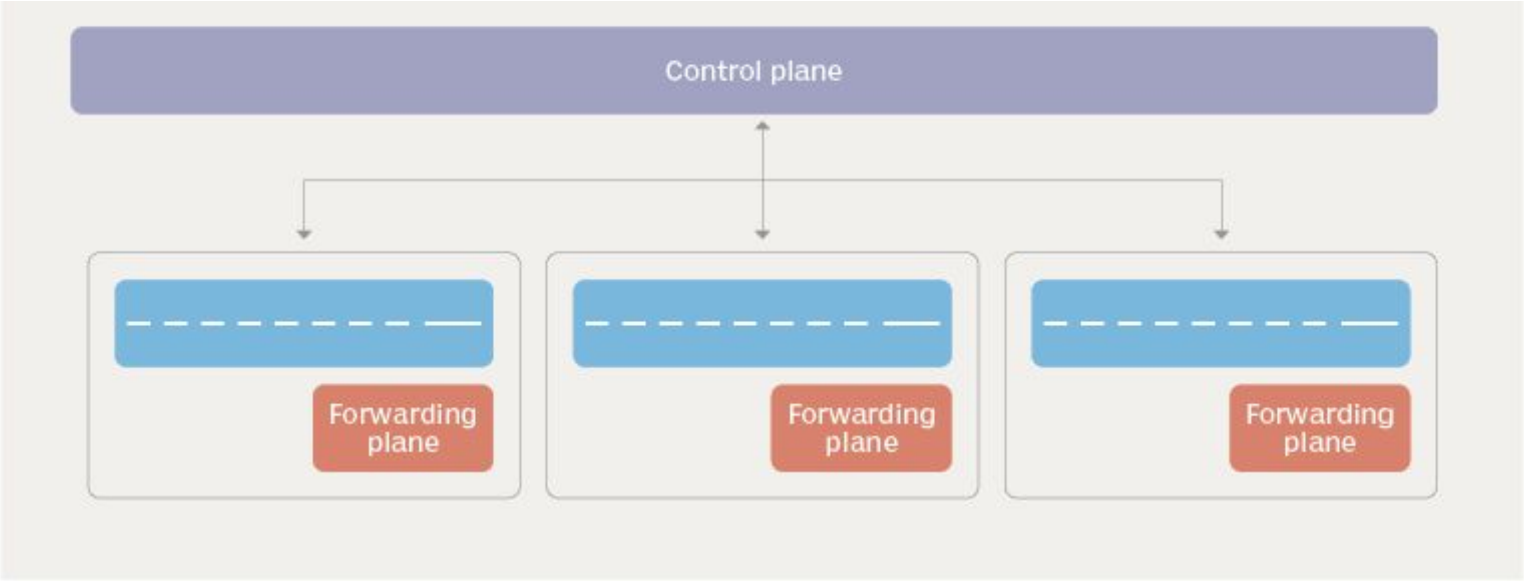
In traditional network design, each switch would contain a routing table that it used to decide how to route each packet. This routing table is largely static and it would be updated by the administrator individually on each router.

In OpenFlow, an SDN controller is the control plane. The SDN controller contains the logic and does the decision-making for how the network traffic should flow between the switches.

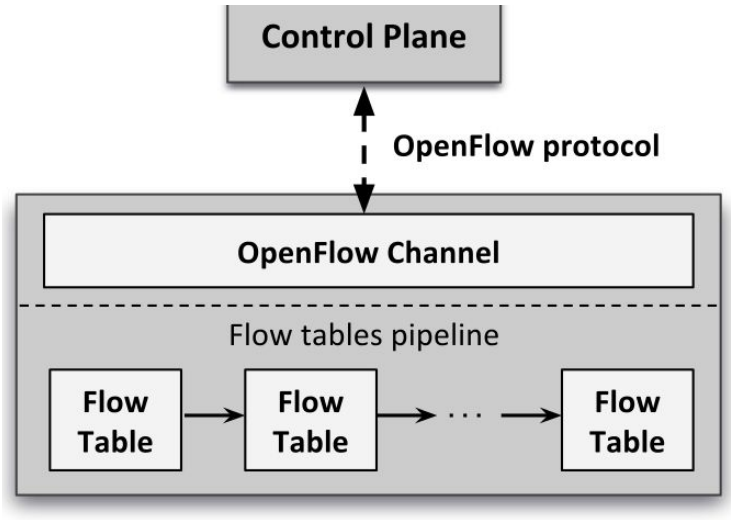
Traditional Network



SDN


Control plane
Forwarding plane
Forwarding plane
Forwarding plane

OpenFlow



OpenFlow Switch

- Switch maintains a set of Flow Tables
  - Organised in a pipeline
- Each flow table hosts a set of Flow Rules
  - Flow rules define what actions to perform on a given network flow
- Control plane installs flow rules
  - Either statically or dynamically

Where is the catch?

- Allowing for a flexible network management, this on-demand management of network flows also introduces some security threats.

Issue

- Allowing for a flexible network management, this on-demand management of network flows also introduces some security threats.

- Extensive communication between the data and control plane can potentially result in a bottleneck for the whole system.

Control plane saturation attack

Installation of rules on the switches is driven by the traffic generated from network users.

- an attacker can exploit this behavior to attack the control plane, by flooding an OpenFlow switch with a large number of **unique** flows.
- for each network flow, the switch will forward a request to the controller, overwhelming it if the rate of new inbound network flows is high enough.

Control plane saturation - the attack

- High number of unique flows:
    - OpenFlow switch will contact the controller to ask for a new flow rule
    - The controller then processes the request, crafts a response containing a series of flow rules, and forwards it to the OpenFlow switch.

Control plane saturation - the attack

- High number of unique flows:
  - OpenFlow switch will contact the controller to ask for a new flow rule
  - The controller then processes the request, crafts a response containing a series of flow rules, and forwards it to the OpenFlow switch. (performed for each new inbound network flow)

Control plane saturation - the attack

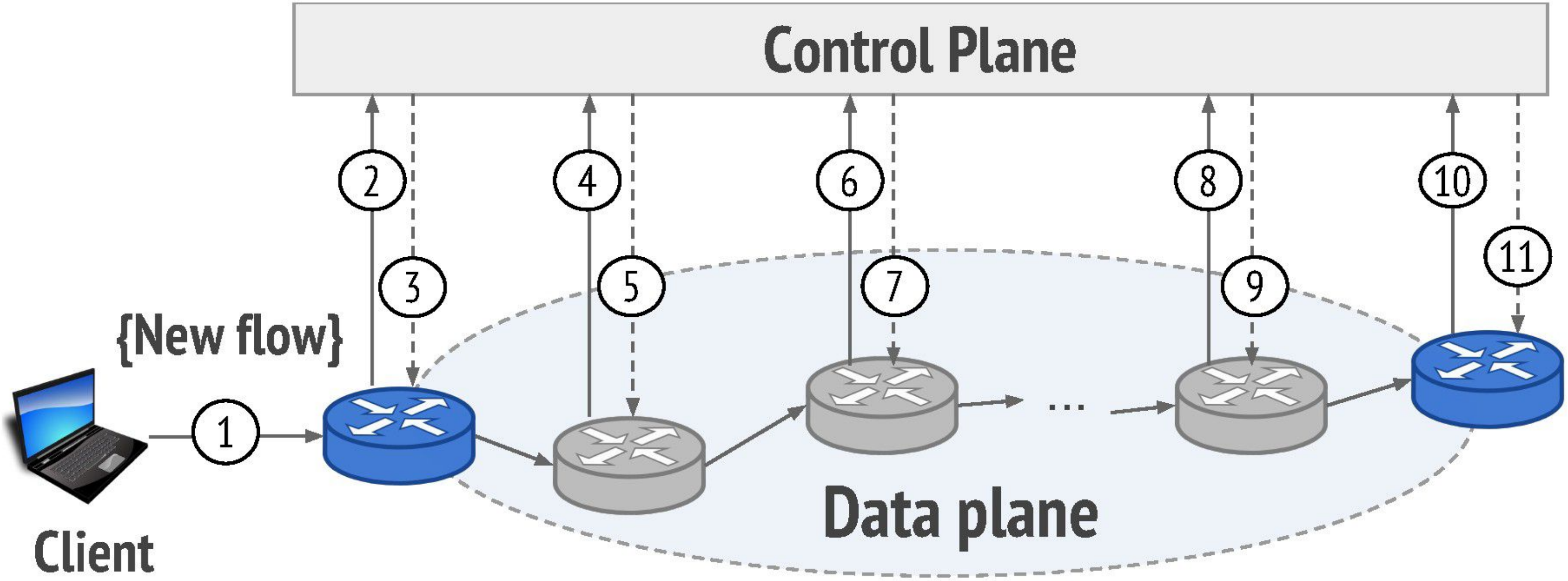
- High number of unique flows:
    - OpenFlow switch will contact the controller to ask for a new flow rule
    - The controller then processes the request, crafts a response containing a series of flow rules, and forwards it to the OpenFlow switch. (performed for each new inbound network flow)
    - Attack Rationale: generate new network flows quickly enough, such that the controller will not be able to keep up with the incoming requests and will be incapacitated from serving other legitimate connections.

Control plane saturation - long paths

Given a new flow -> the controller installs a flow rule only on the OpenFlow switch that performed the flow request.

Control plane saturation - long paths

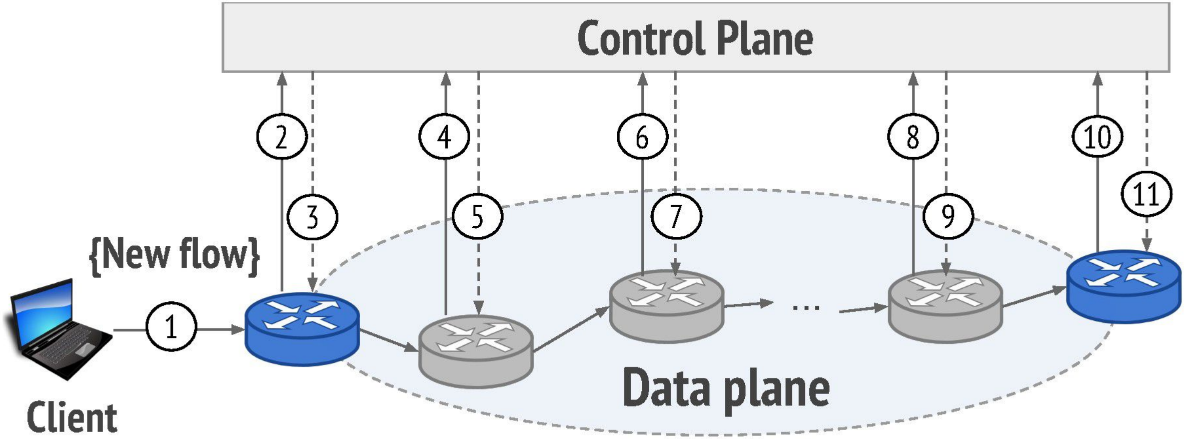
If the SDN subnetwork is big enough, the packet will be routed through other switches of the subnetwork, each of which will send a flow rule request to the controller



Control plane saturation - long paths

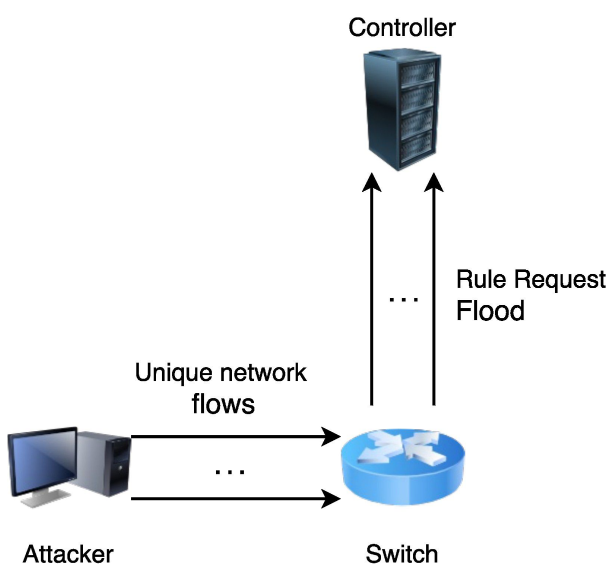
If the SDN subnetwork is big enough, the packet will be routed through other switches of the subnetwork, each of which will send a flow rule request to the controller.

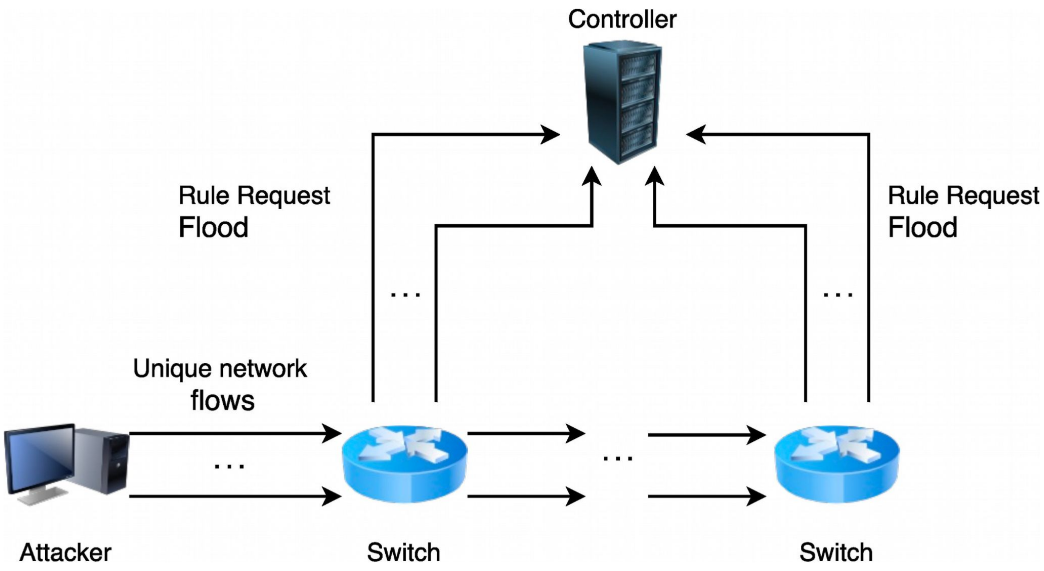
Long paths - amplification of the effect on the control plane



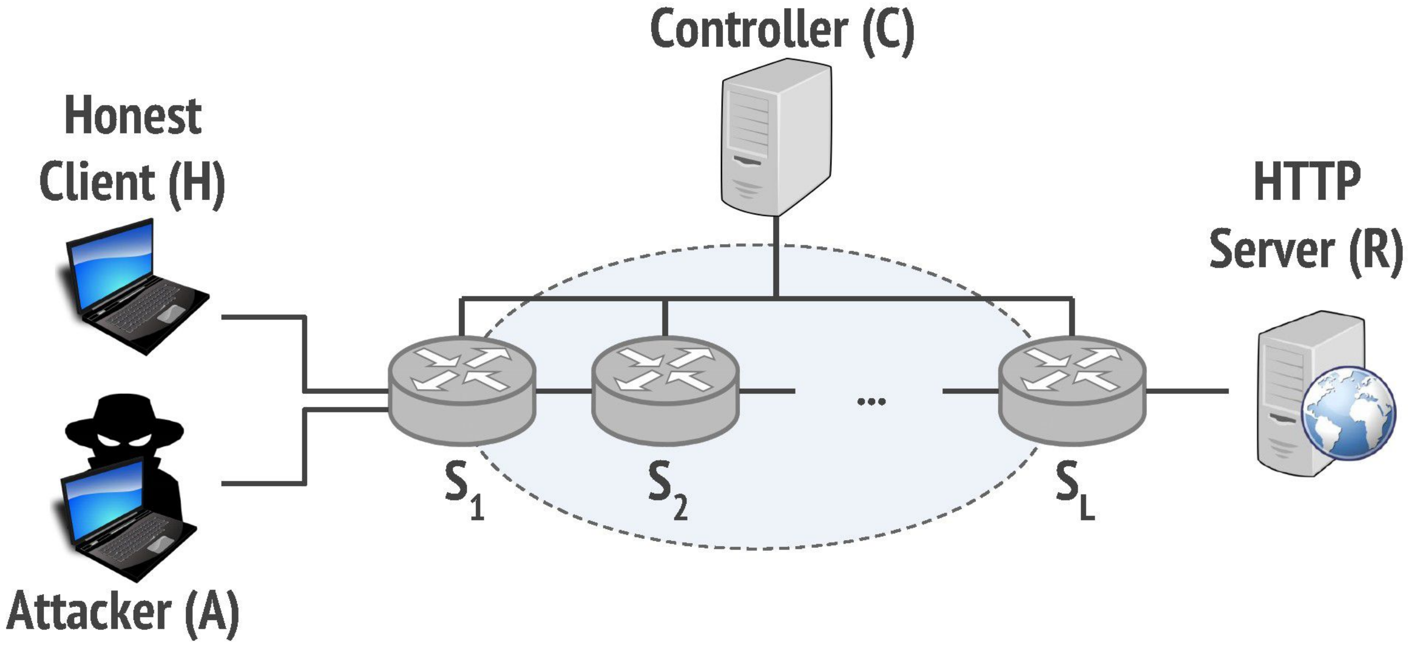
Control plane saturation - long paths

Long paths - amplification of the effect on the control plane

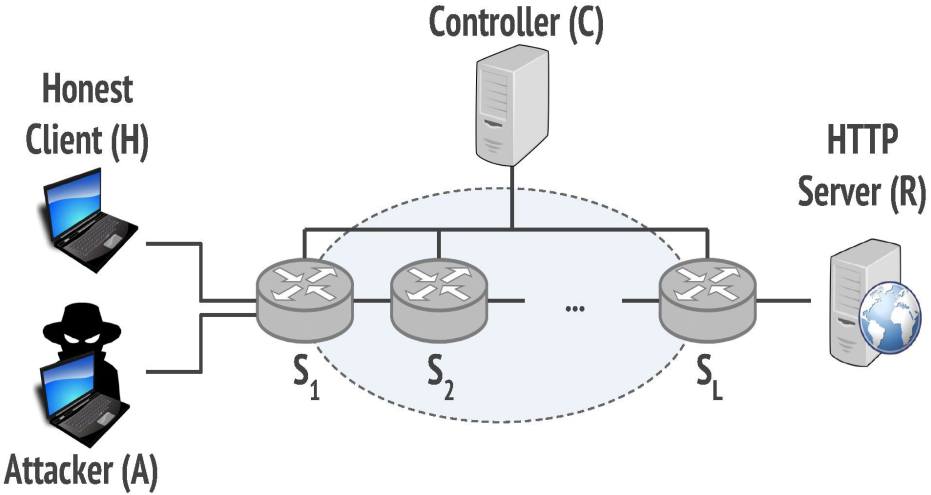




An attack scenario



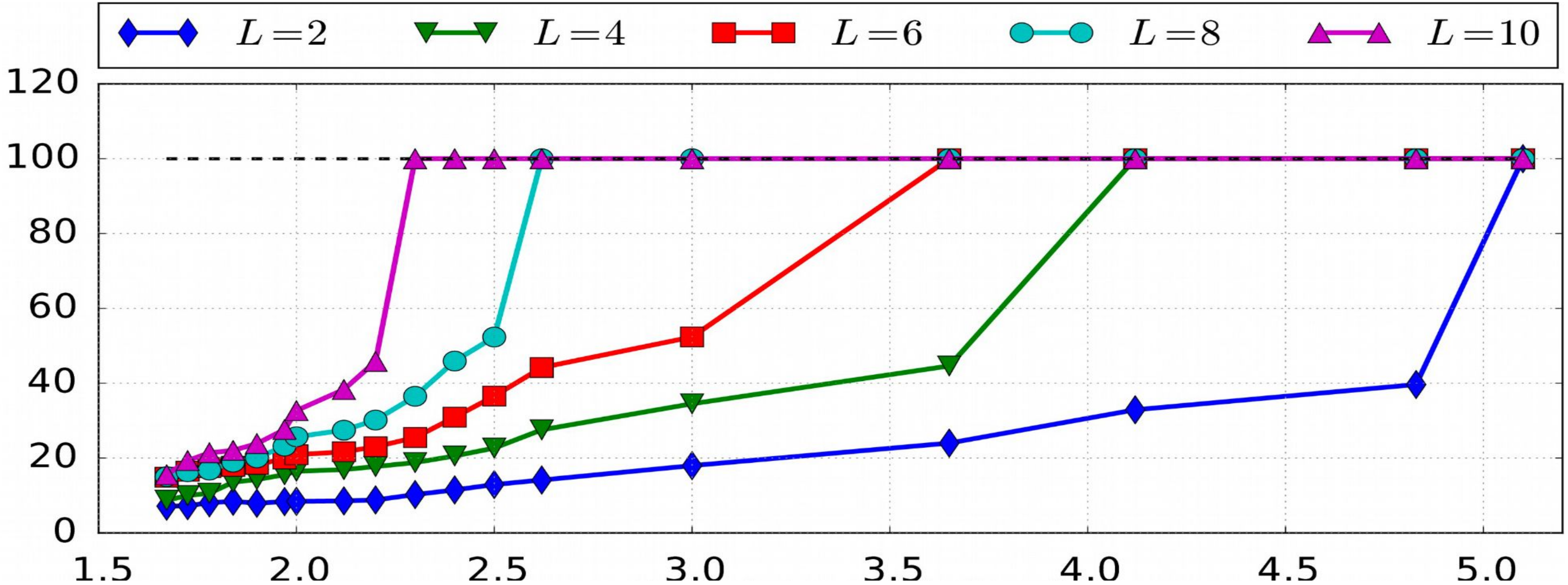
Evaluation



- Varying path length
- Impact on client
  - avg. page retrieval time
- Impact on controller
  - inbound traffic
  - serviced requests ratio
- Impact on switch
  - requests loss in the path

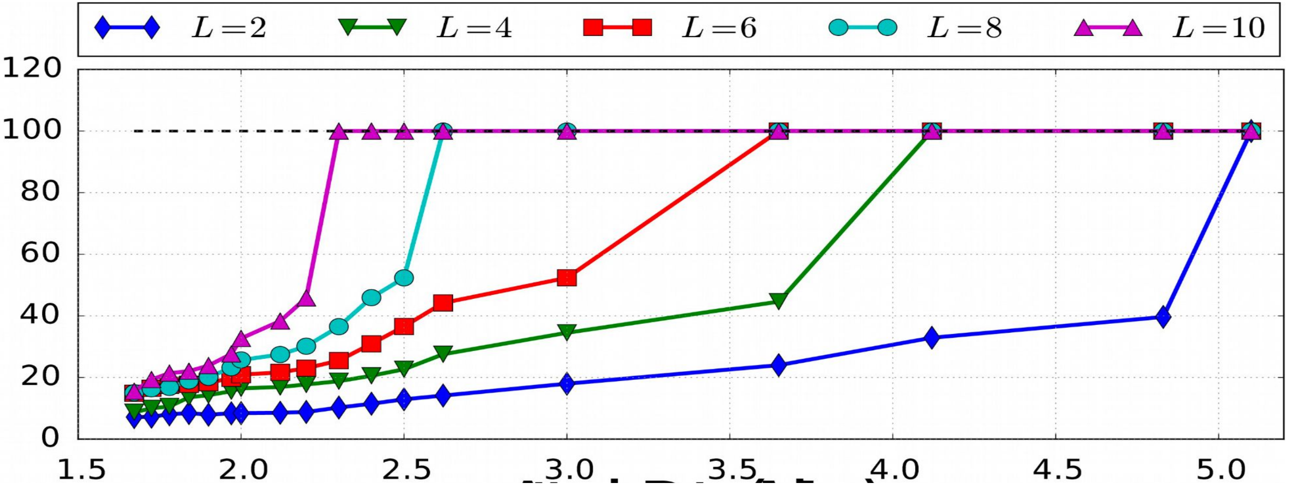
Impact on the client

Measure the time overhead introduced by the attack when a client retrieves a web page from server



Impact on the client

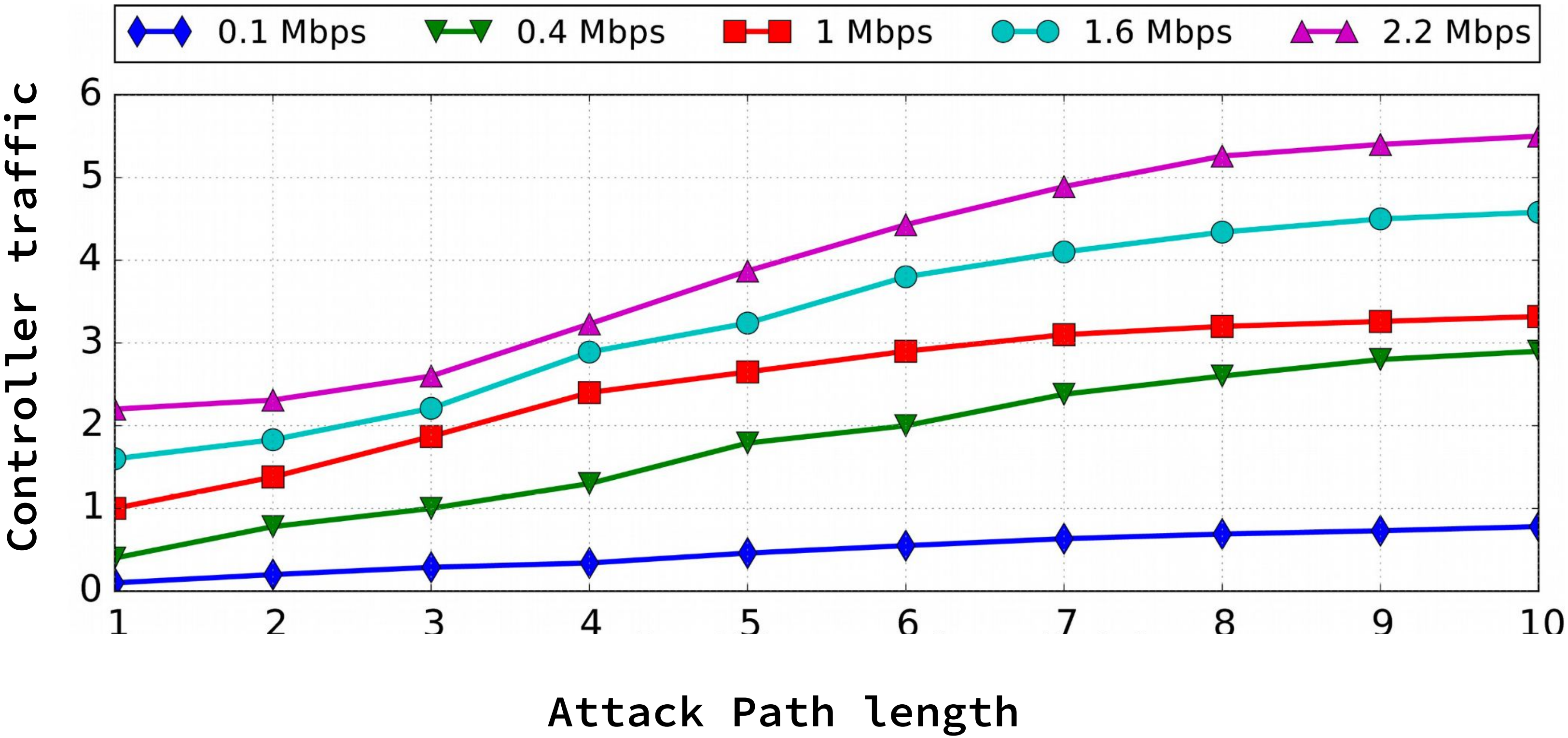
- Leveraging a path of length L = 4, need around 4 Mbps attack rate to perform a saturation attack
- Using a path of length L = 2 an attacker will only increase the webpage retrieval time to 30 sec.
  - (100 second as controller incapacitated)



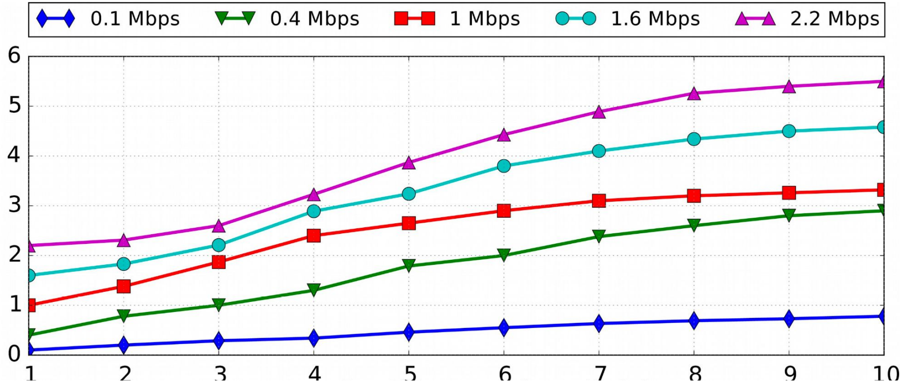
Impact on the controller

1. Measure the amount of PacketIn packets at the controller when under attack
2. Measure Ratio between PacketIn and the corresponding FlowAdd sent by the controller in response
3. CPU utilization of the controller

Impact on the controller - amount of PacketIn at controller



Impact on the controller



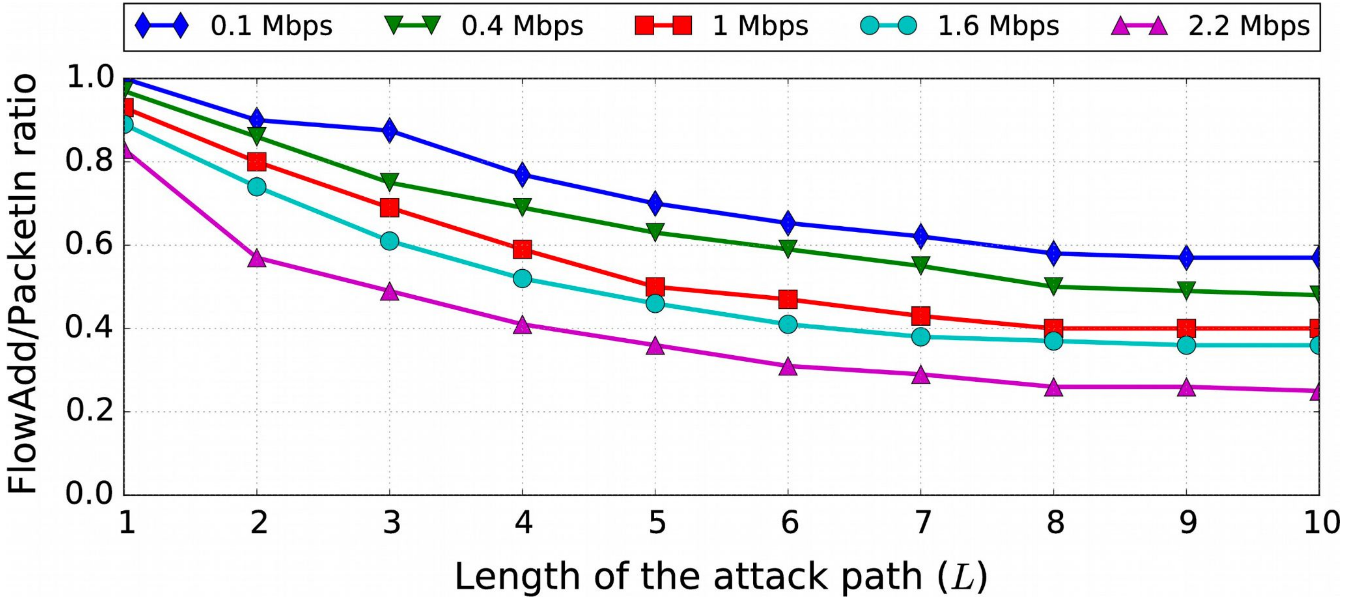
There is a loss of FlowAdd packets attributed to controller capacity saturation and to flow table saturation at each switch.

As the controller approaches the point of saturation, it is not able to keep up with the rate of incoming PacketIn requests anymore.

Large portion of the attack packets are not forwarded to the next hop in the attack path, thus causing a reduced amplification effect on the attack.

Impact on the controller - FlowAdd/PacketIn

Large portion of the attack packets are not forwarded to the next hop in the attack path, thus causing a reduced amplification effect on the attack.



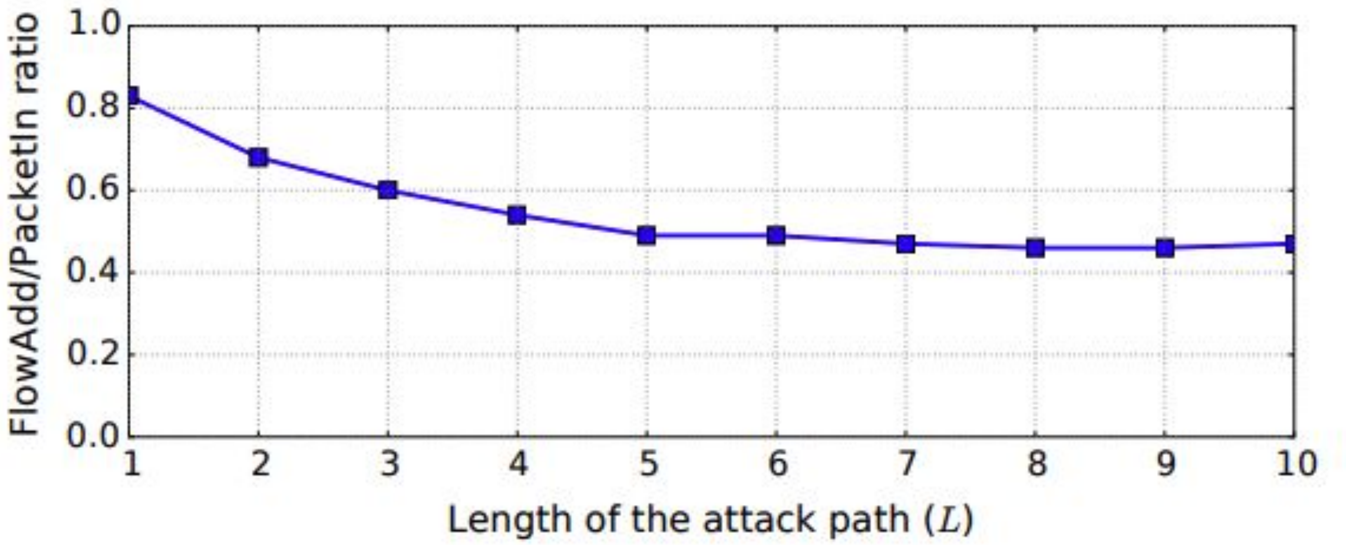
Impact on the controller - CPU utlization

Non-attack setting: utilization 5-15%

Attack setting: from 55 to 100% utilization.

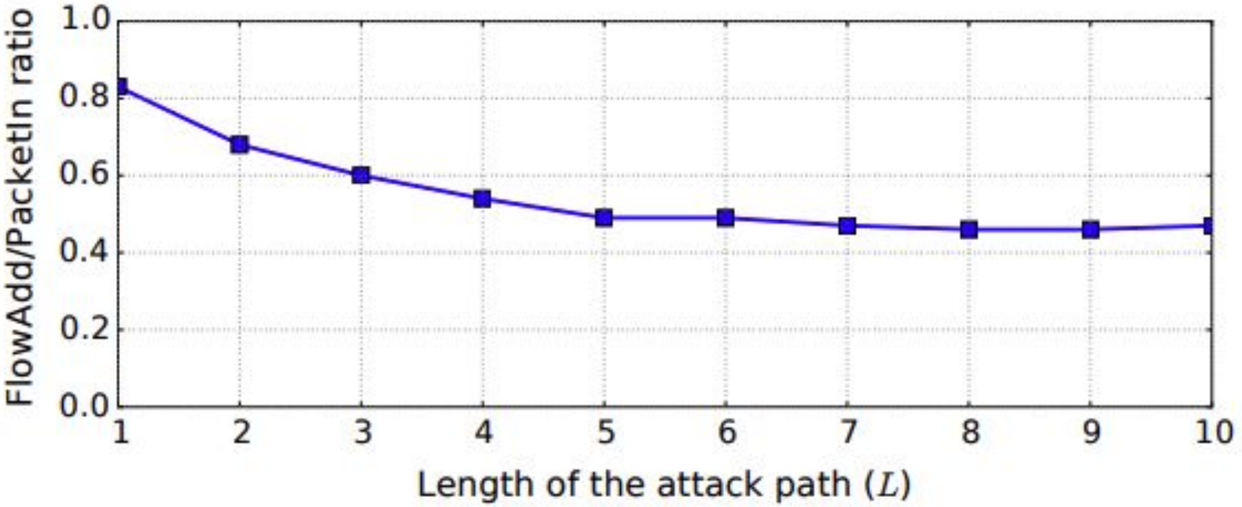
Switch level analysis

Measure the responsiveness of the controller at each switch in the attack path.



Switch level analysis

As the length of the attack path grows, there is a considerable decrease in the responsiveness of the controller, which at some point stabilizes. This stabilization is mainly due to packet loss, as the controller reached its saturation point.

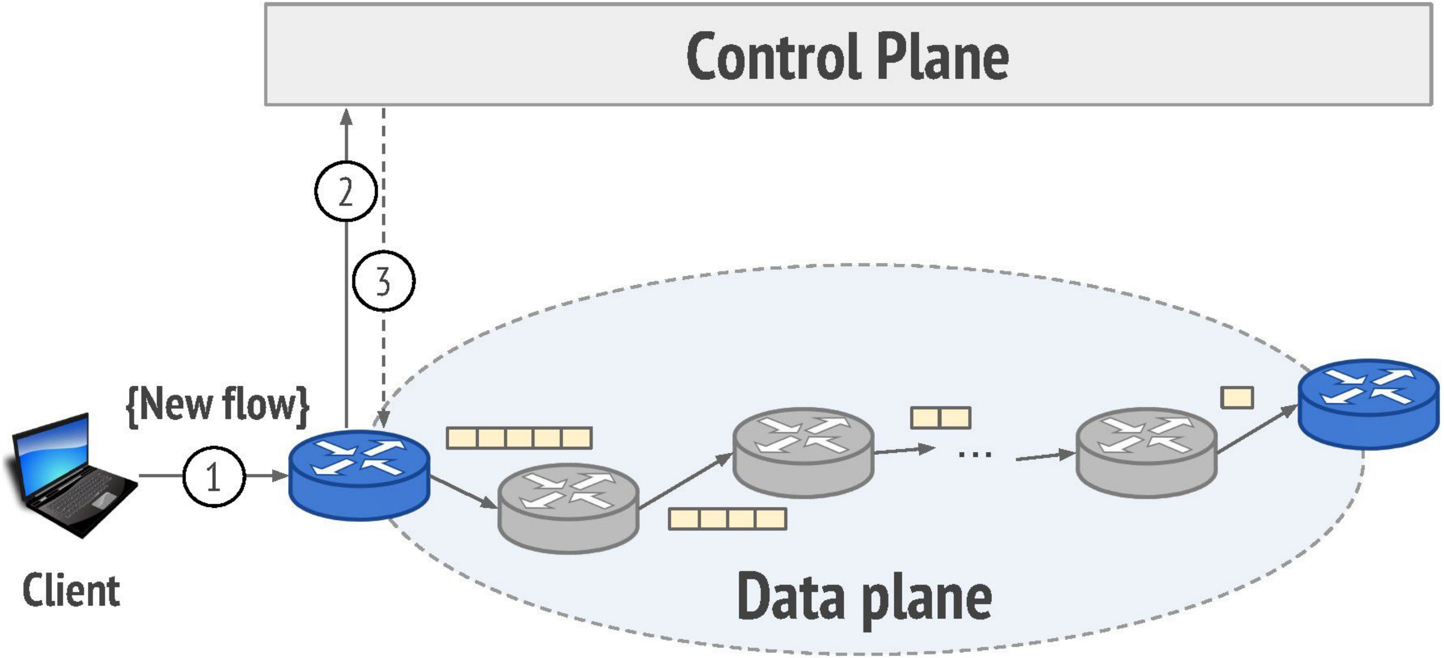


Fixed attack rate of 2.2Mbps

Possible mitigation strategies

Flow rule piggybacking

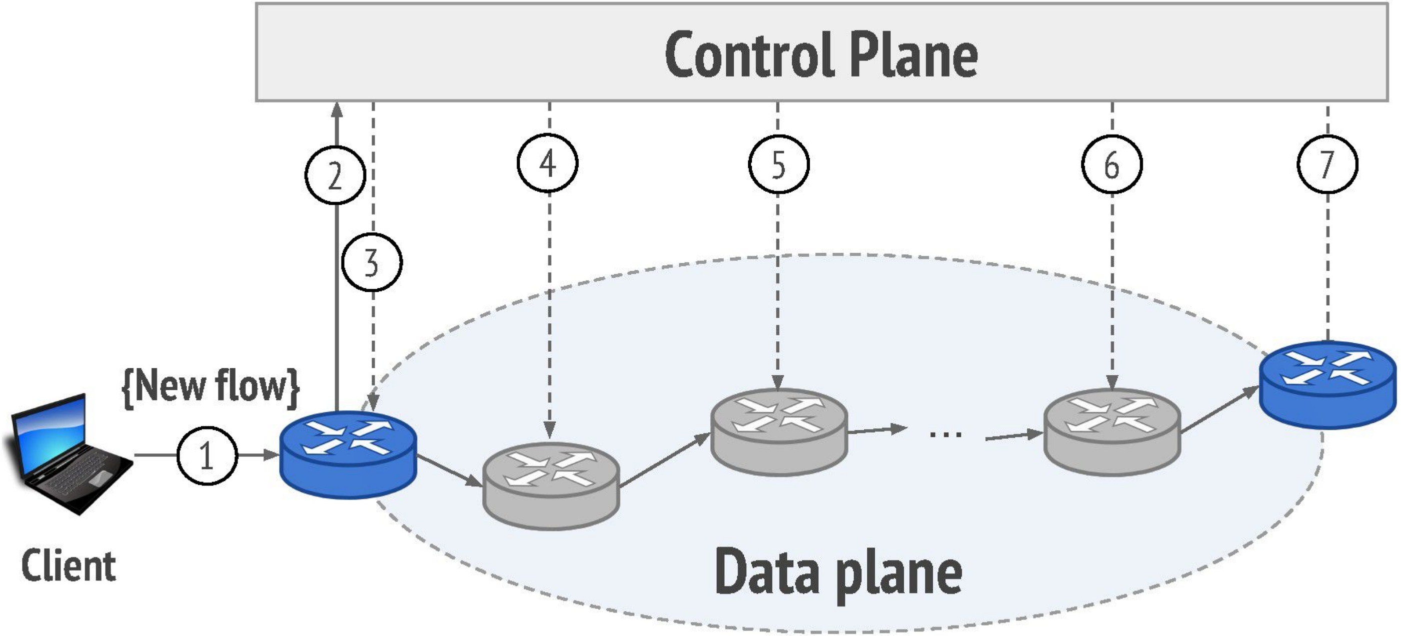
- control plane pushes all rules in one response
- switch install first rule and forwards remaining



Possible mitigation strategies

Flow rule push

- Controller pushes rules on all switches on path after the first request



Outline for today

- Recap last lecture
- Software defined networking
- **Report guidelines - points to consider**

Points to consider on the written report

The following general points need to be considered:

- What problem are you addressing?
- Is the project academic or industrially oriented?
- What has been tried before? What is in the marketplace or academic literature?
- How can this project be done?
- Select approaches to form the basis of the solution, ensure you can justify it.

More specific...

- Identify the problem clearly. (You need to put some thought into it)
- (optional) Conduct a SWOT analysis, if you find it useful.
  - As part of the process for giving credibility to your research project you might conduct a SWOT analysis. This will rigorously establish the ‘position’ of your idea versus an existing idea.
  - Your SWOT analysis should be done in some detail. As an example of a SWOT analysis of an IT product, see the Apple-SWOT-Analysis: https://research-methodology.net/apple-swot-analysis/

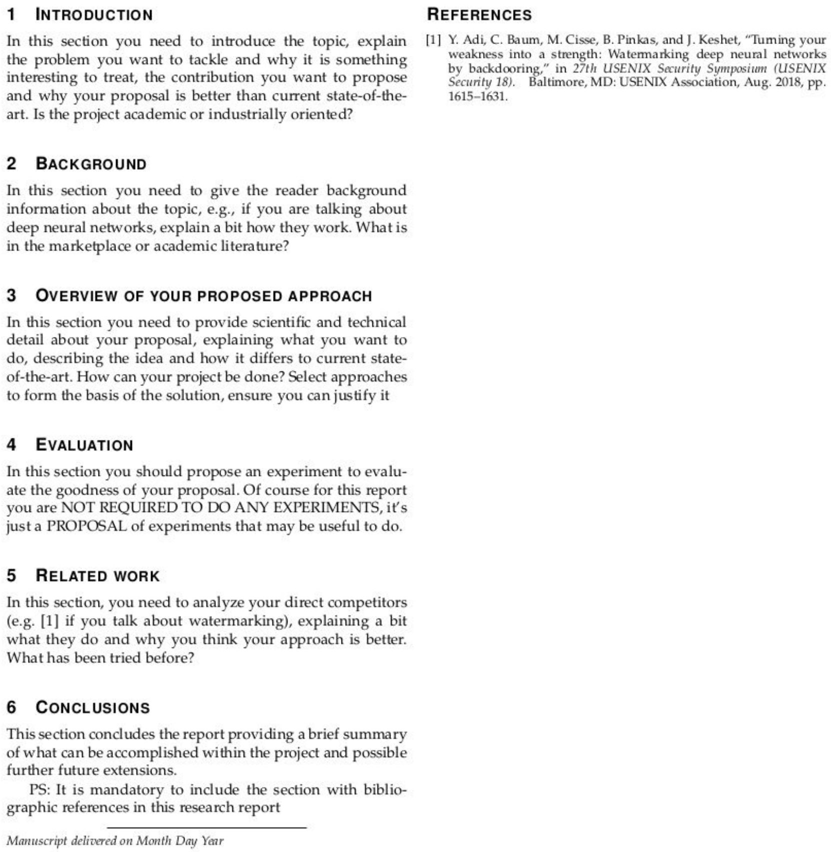
More specific...

- (optional) Provide an appendix with the project Work Breakdown Structure, if you find it useful. As an example, see https://en.wikipedia.org/wiki/Work_breakdown_structure

More specific...

- Scientific and technical detail.
  - Then, include the scientific and technical components of the idea.
  - This needs to be detailed enough to convince someone that it will work.
  - It does not need to be a fully fledged proposal of the project. You will find at this stage that while you have many good ideas, some of them might not work. This is absolutely fine, because at this stage you should just collect enough thoughts to support your idea convincingly and logically.

Report organization - template



1 Introduction

In this section you need to introduce the topic, explain the problem you want to tackle and why it is something interesting to treat, the contribution you want to propose and why your proposal is better than current state-of-the-art. Is the project academic or industrially oriented?

2 Background

In this section you need to give the reader background information about the topic, e.g., if you are talking about deep neural networks, explain a bit how they work. What is in the marketplace or academic literature?

3 Overview of your proposed approach

In this section you need to provide scientific and technical detail about your proposal, explaining what you want to do, describing the idea and how it differs to current state-of-the-art. How can your project be done? Select approaches to form the basis of the solution, ensure you can justify it

4 Evaluation

In this section you should propose an experiment to evaluate the goodness of your proposal. Of course for this report you are NOT REQUIRED TO DO ANY EXPERIMENTS, it's just a PROPOSAL of experiments that may be useful to do.

5 Related work

In this section, you need to analyze your direct competitors (e.g. [1] if you talk about watermarking), explaining a bit what they do and why you think your approach is better. What has been tried before?

6 Conclusions

This section concludes the report providing a brief summary of what can be accomplished within the project and possible further future extensions.

PS: It is mandatory to include the section with bibliographic references in this research report

Manuscript delivered on Month Day Year

References

[1] Y. Adi, C. Baum, M. Cisse, B. Pinkas, and J. Keshet, "Turning your weakness into a strength: Watermarking deep neural networks by backdooring," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1615–1631.

Reading Material

1. Software defined networking: Link-1, Link-2