Fault-Tolerant SDN Solution for Cybersecurity Applications

University of Western Macedonia (UOWM)

Kozani, Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Authors

Athanasios Liatifis, Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis
Department of Electrical and Computer Engineering
University of Western Macedonia, Kozani, Greece
{aliatifis, pradoglou, psarigiannidis}@uowm.gr

Christos Dalamagkas
Public Power Corporation, Athens, Greece
cdalamagkas@dei.gr

Thomas Lagkas
Department of Computer Science, International Hellenic University, Thessaloniki, Greece
tlagkas@cs.ihu.gr

Evangelos Markakis
Hellenic Mediterranean University, Greece
emarkakis@hmu.gr

Valeri Mladenov
Department of Theory of Electrical Engineering
Technical University of Sofia, Bulgaria
valerim@tu-sofia.bg

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Outline

- Introduction & Motivation
- Contribution
- Background
- Proposed System Architecture
- SDN-based Applications
- Conclusion

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Introduction & Motivation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Motivation

- Computer Networks have scaled up and are now entrusted to perform complex tasks successfully.
- Software Defined Networking (SDN) simplifies the management and control functions of networks
- SDN though introduces challenges as well.
  - High availability
  - Visual tools

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Contribution

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Contribution of our Work

- Design a high availability SDN solution suitable for a wide range of networks.
- Design and integrate a Synchronization Service to assist the master election process.
- Design and implement a web-based Dashboard and assist administrators in monitoring the network and enforce policies.

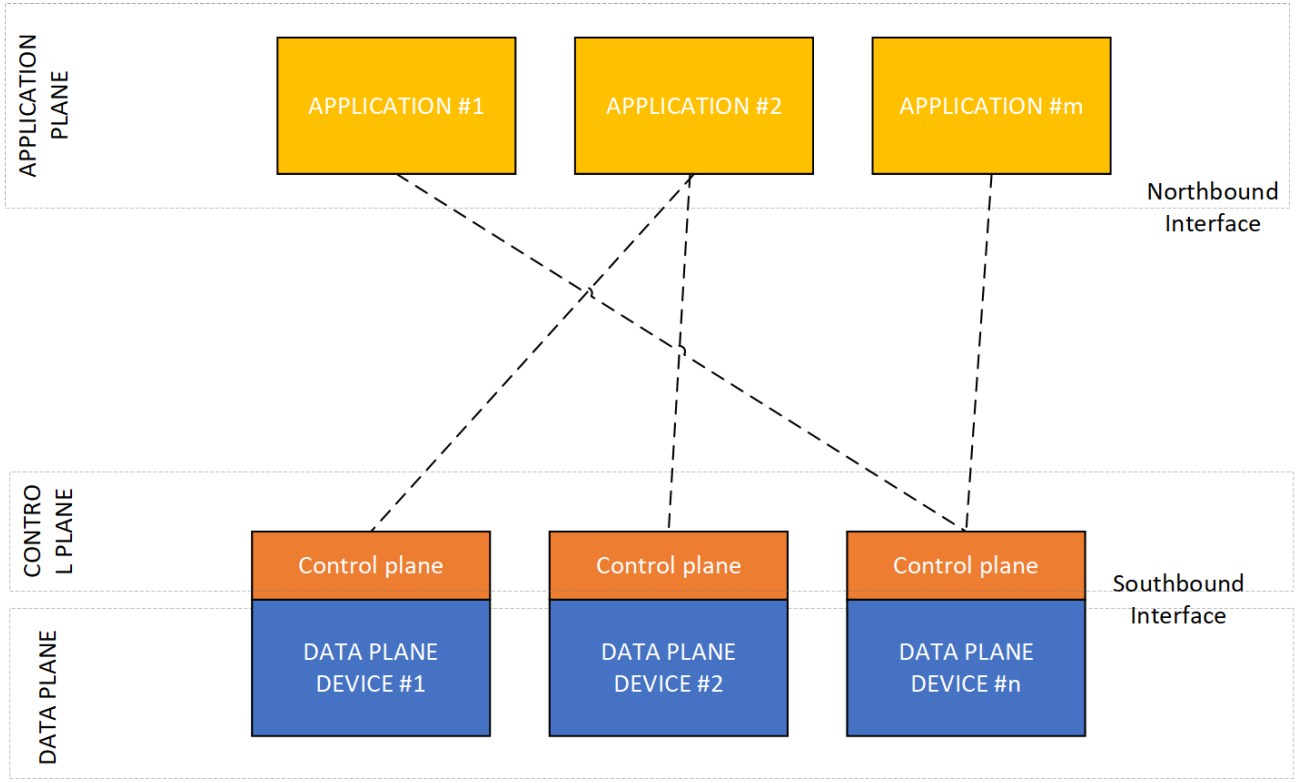
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Background

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Traditional Networking

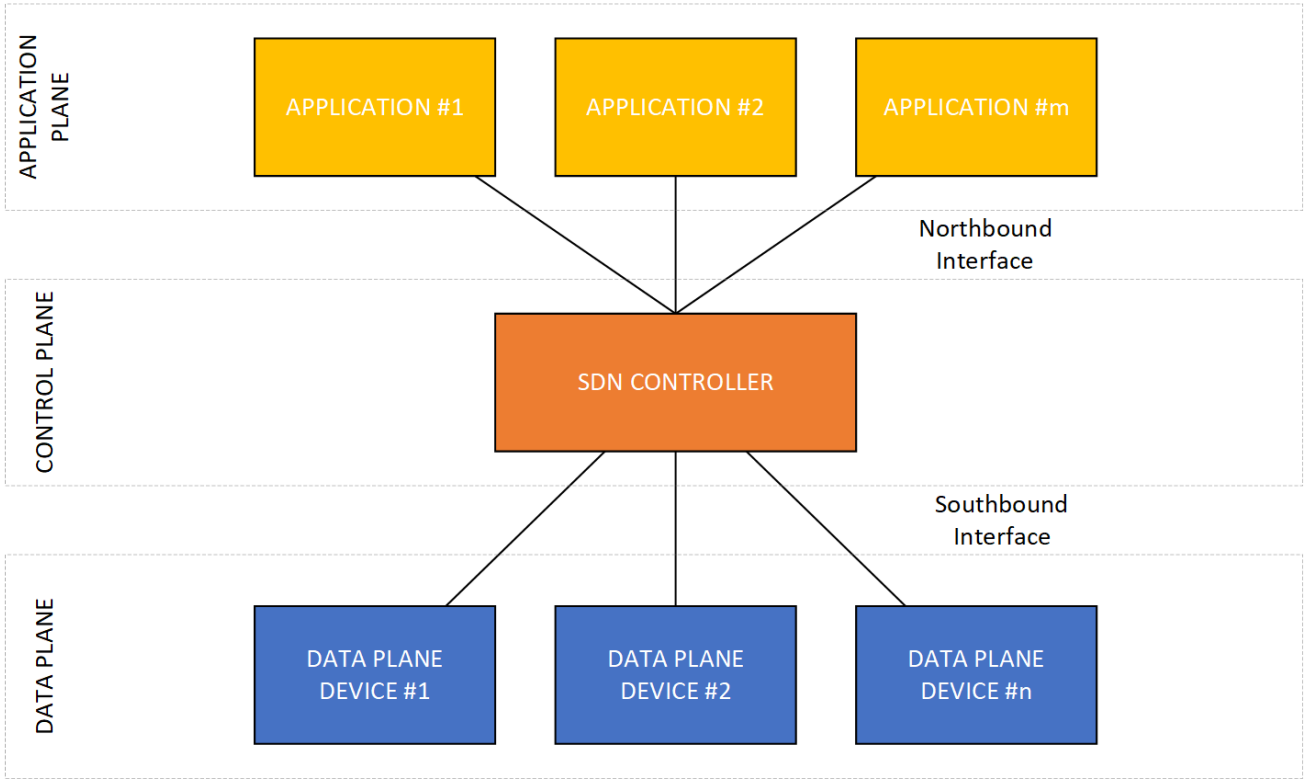
- Data plane and control planes are intertwined.
- Communication with data plane devices is not well-defined
- Data plane devices are task-specific and vendor locked
  - E.g., firewall, load-balancer, router



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Software Defined Networking

- SDN decouples data plane and control plane
- Offers a logically centralized control point (the SDN Controller)
- High-level policies are translated to low level device specific instructions
- Efficient Monitoring of network
- Well defined communication interfaces



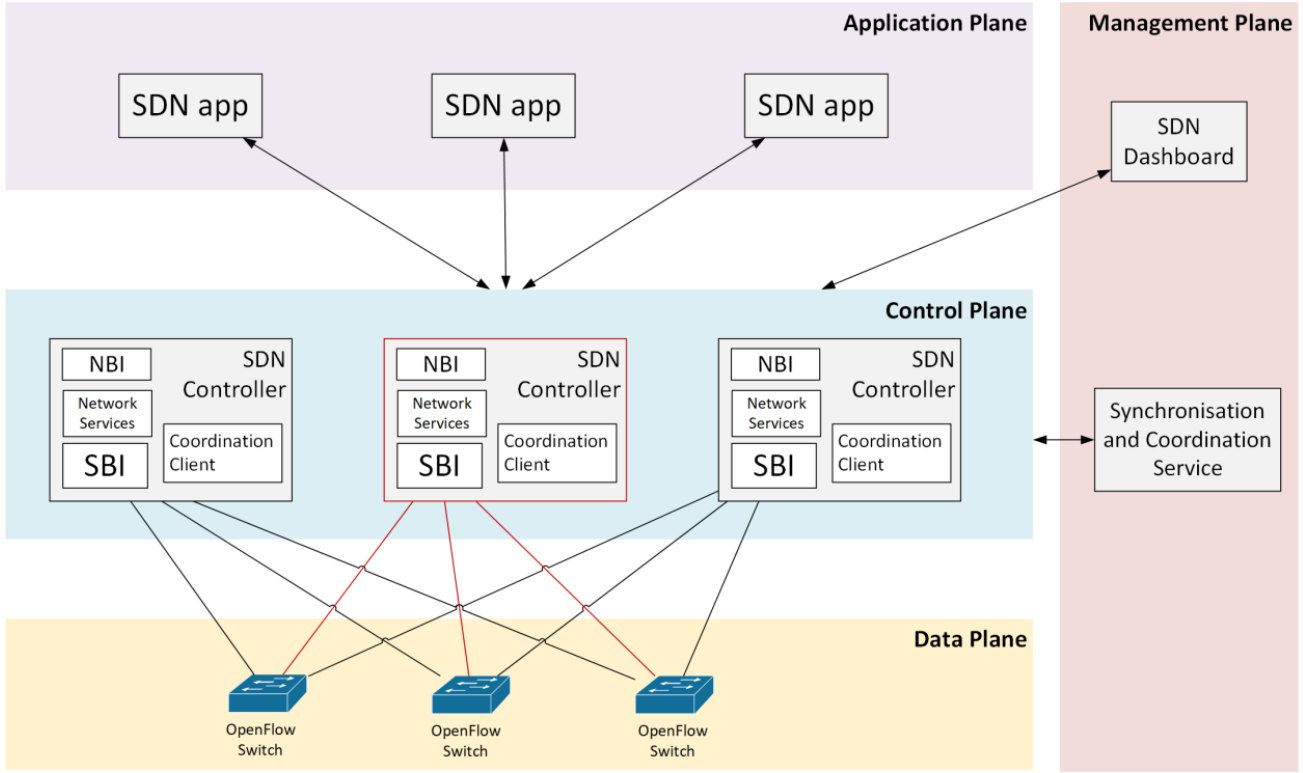
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Proposed System Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Proposed System Architecture: High level description

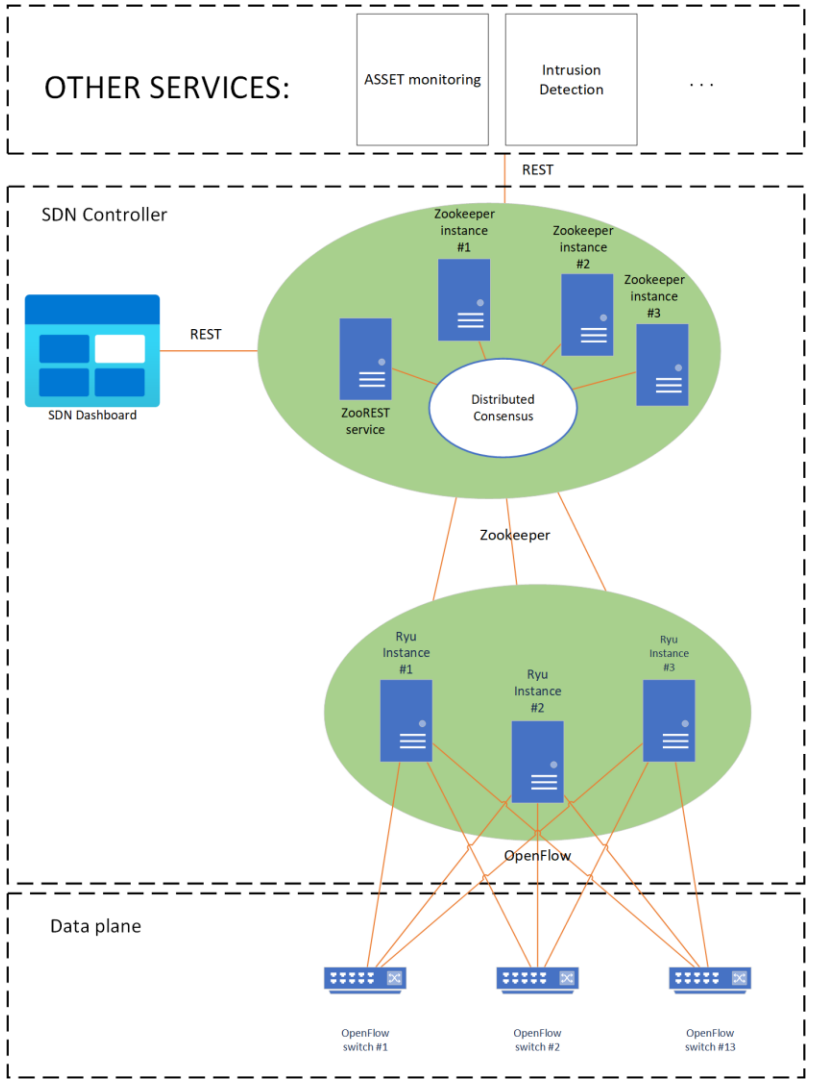
- Multiple SDN Controller instances
  - Ensure high availability
- Synchronization and Coordination Service (SCS)
  - Assists master controller election process
  - Ensures discovery of the master controller to SDN apps
- SDN Dashboard
  - Offers visual-based tools to the administrator



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Proposed System Architecture: Technical details

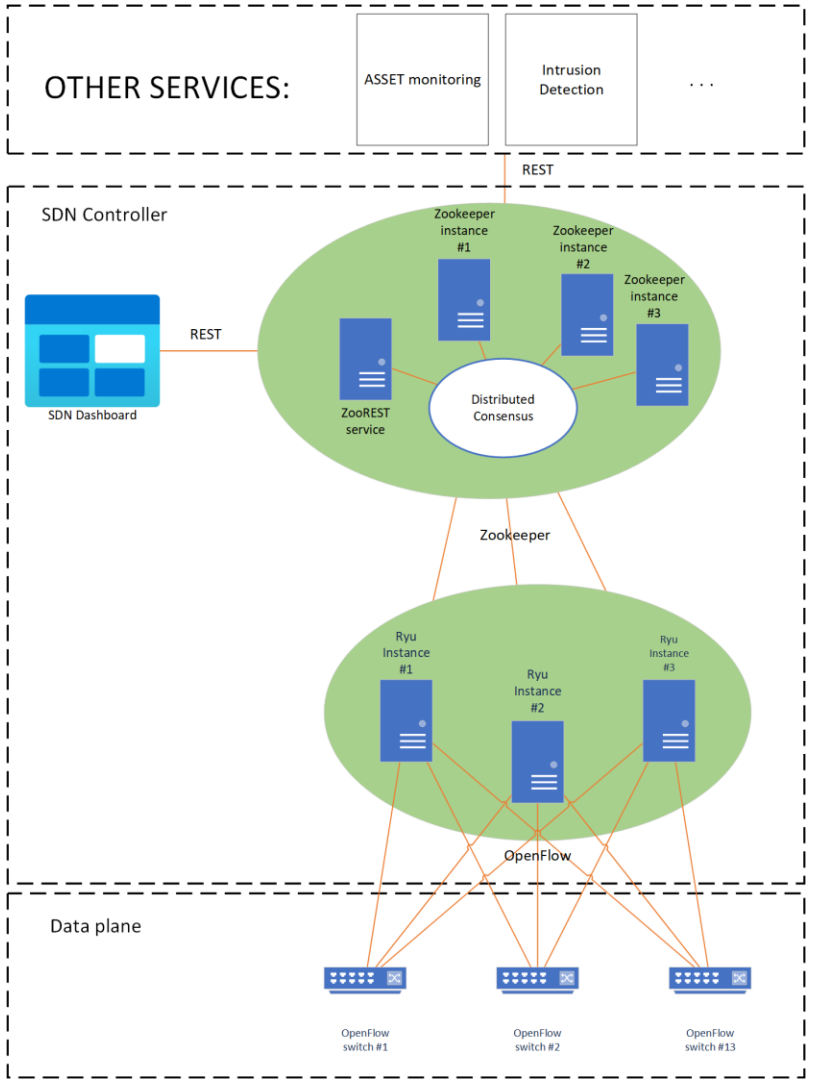
- Ryu SDN Controller framework
  - ✓ Python-based
  - ✓ easy to deploy
  - ✓ REST API as Northbound Interface
  - ✓ Multiple Southbound Interfaces (incl. OpenFlow)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Proposed System Architecture: Technical details

- Apache Zookeeper as the SCS
  - ✓ provides distributes service coordination
  - ✓ exposes a simple REST API for other services
  - ✓ offers a master election process

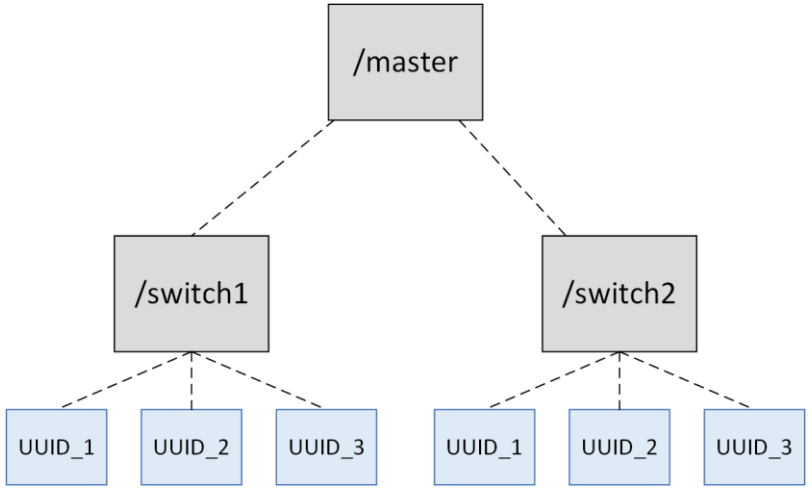


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Master controller election process

✓Based on Zookeeper Election Process.

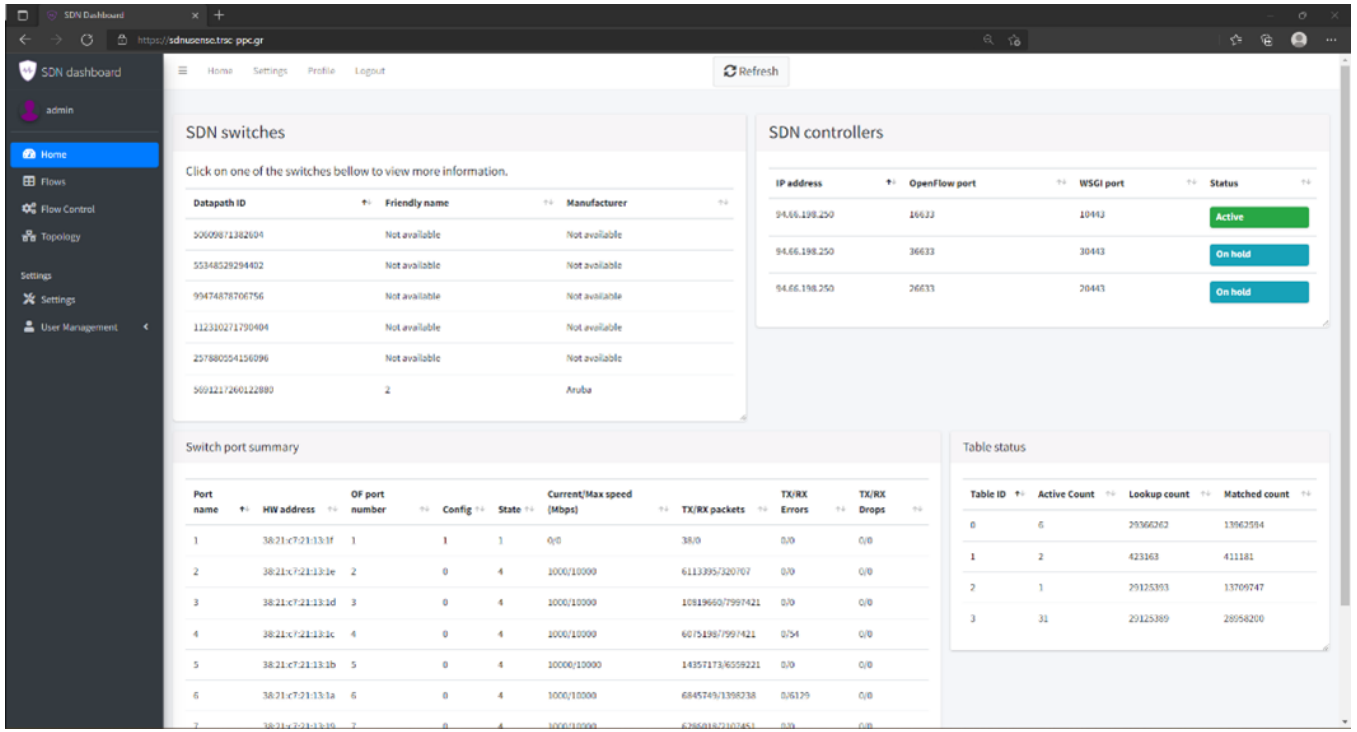
1. An SDNC registers a switch as a node (if not registered already)
2. The SDNC registers itself (UUID) as an ephemeral Zookeeper node (znode).
   1. The node obtains a unique ID
   2. The node is bound to the connection state
3. The znode with the lowest UUID value is elected as master

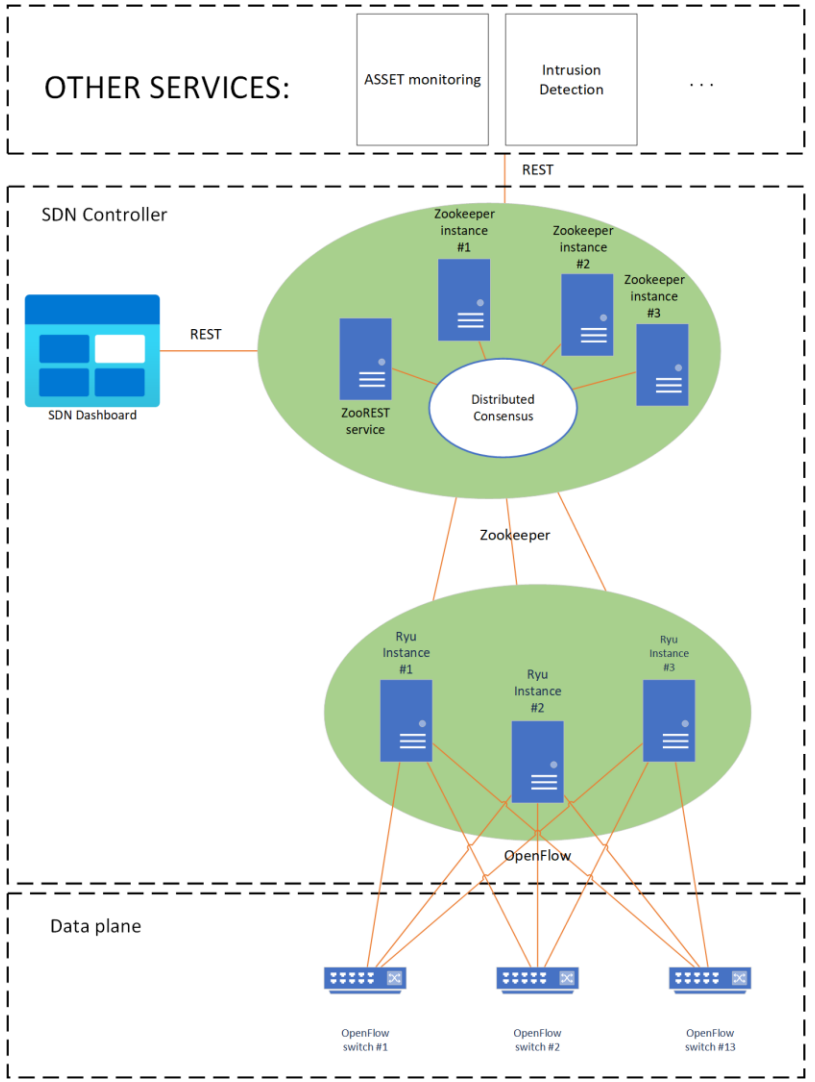


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Proposed System Architecture: Technical details

- SDN Dashboard
  - ✓Django-based application
  - ✓Offer the administrator a visual-based interface for monitoring/control





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications: SDN-enabled Devices

- Plethora of devices are hard to integrate
  - Security concerns
  - Peculiar behaviour regarding the network

- SDN-based infrastructure can:
  - ✓Assist the organization integrate these devices
  - ✓Enforce strict security policies
  - ✓Monitor the devices

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications: Risk Assessment

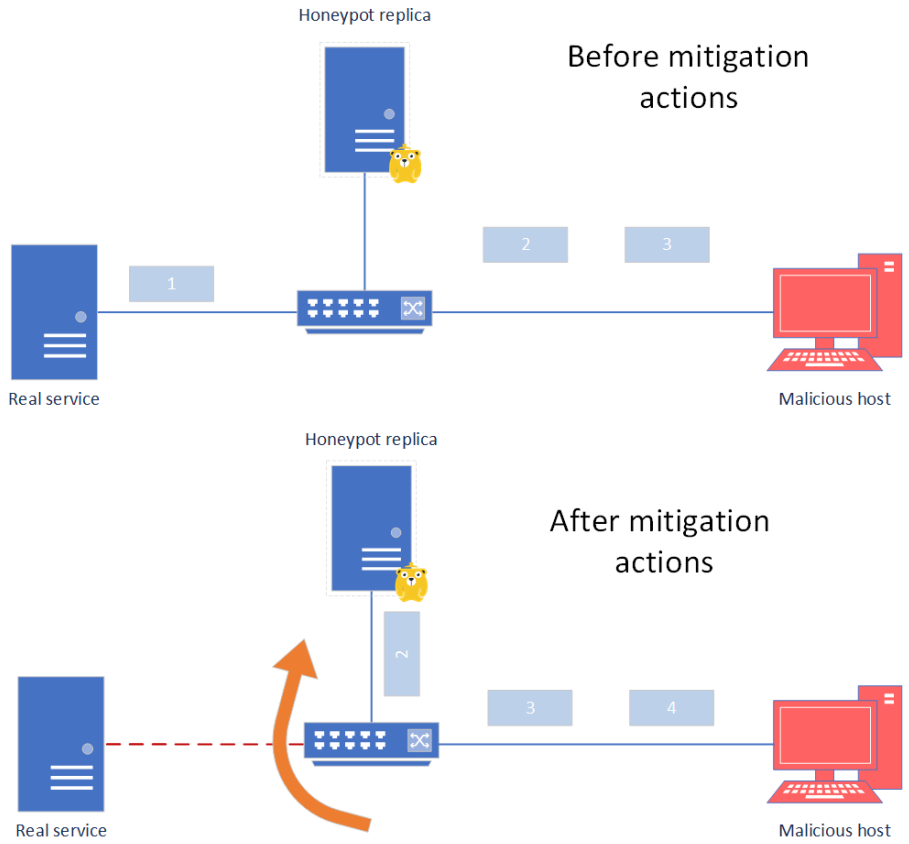
- Estimating the risk of a device can become a complex task
- Timely detection and mitigation of malicious actions is important for many use cases

- SDN technology can:
  - ✓Offer fine-grained statistics
  - ✓Provide details on communication behaviour of hosts
  - ✓Enrich risk evaluation processes with data plane measurements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications: SDN-based Honeypots

- What are Honeypots?
  - Software instances that emulate the behaviour of real assets/services
  - Based on their level of interaction: low, medium high
  - Based on their operation field: production, research
  - Based on their locations: server, client, hybrid



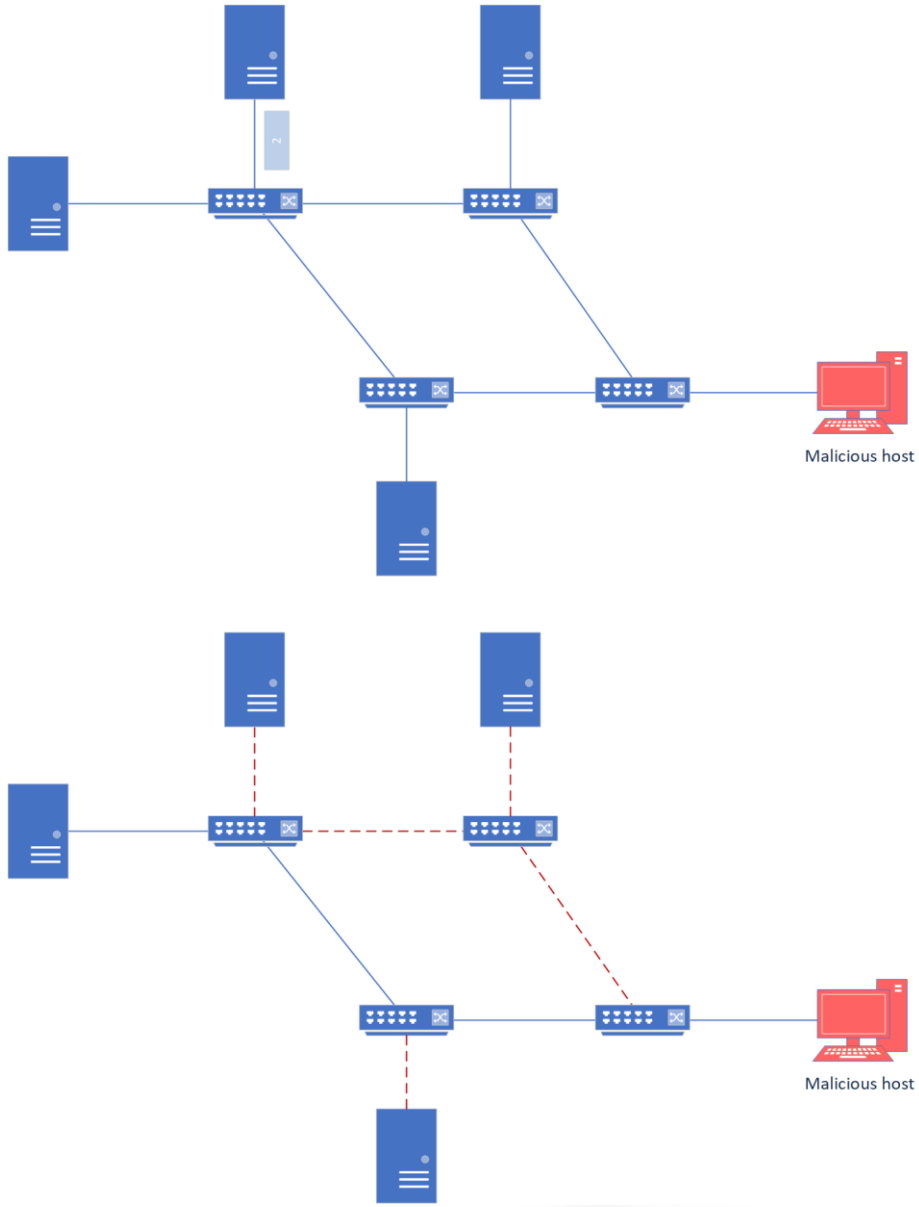
- Taking advantage of SDN honeypots can:
  - ✓Blend honeypot instances in production environments
  - ✓Redirect malicious actors to honeynets
  - ✓Ensure minimal network disruptions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications: Host isolation

- Malicious actions can lead to large disruptions
- Sensitive data leakage.

- Taking advantage of SDN an organization can:
  - ✓ deny communication access to specific hosts
  - ✓Isolate suspiciously behaving hosts
  - ✓Create levels of isolation



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

SDN-based Applications: High Precision QoS

- Many application enforce strict QoS
- Delivery of content must be ensured

- Leveraging SDN organisations can:
  - ✓Closely monitor network state
  - ✓Retrieve fine grained, real-time statistics
  - ✓Timely reroute traffic

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Conclusion

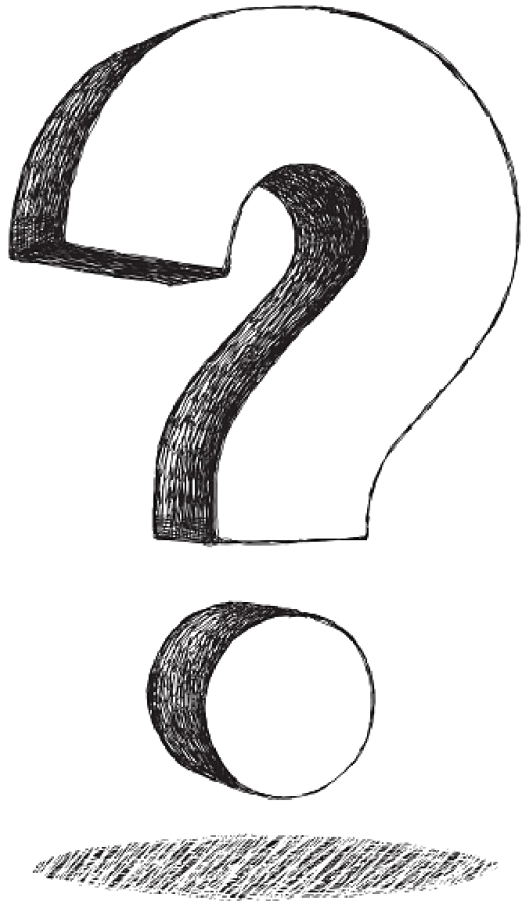
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Conlusion

- SDN technology can assist other decision-making processing
- Enforce policies in a flexible manner
- Better utilize the underlying networking infrastructure

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Thank you!



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936