Project: Incorporating Blockchain/P2P Technology into an SDN-Enabled Cybersecurity System to Safeguard Fossil Fuel Power Generation Systems

Project Number: DE-FE0031742

University of North Dakota
College of Engineering and Mines

Annual Technical Review (Spring 2021)
May 19th, 2021

Project Description and Objectives

Overview

- **This project aims to strengthen the security protection of software defined networking (SDN) for facilitating its deployment in fossil fuel power generating systems.**
  - The security protection solution makes use of the blockchain and the peer-to-peer (P2P) technologies.
  - This project is in response to Area of Interest 2 of DE-FOA-0001991.
  - AOI 2: "*investigate how cutting-edge network technologies such as blockchain may be leveraged and integrated into industrial monitoring and process control systems for optimized, cybersecure operation of electricity generating units.*"
- **This project aims to produce two deliverables:**
  - A cloud-based networking platform for prototyping and experimenting various designs of safeguarding the software-defined networks deployed in electric power systems.
  - A blockchain/P2P-based technology for detecting the compromised controllers in a software defined network.
    - The application will operate in the cloud-based networking platform.
- **The outcomes of this project will serve in**
  - Meeting the general security requirements of the electric power generating systems.
  - Mitigating the security risks targeting the vulnerabilities of SDN-enabled operational networks.

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Strategic Alignment of Project to Fossil Energy Objectives (1)

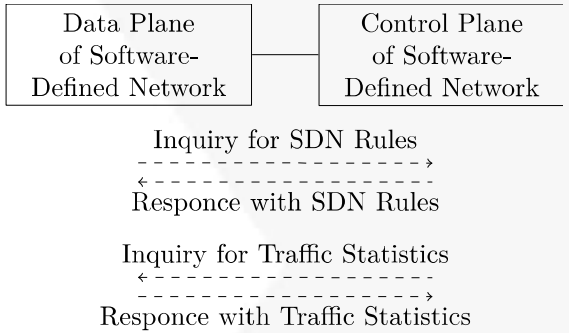
- **Serving for Meeting the General Security Requirements of Electric Power Systems**
  - Safe operations of power systems rely on the fundamental security mechanisms
    - Authentication, Authorization, and Anti-spoofing.
- **Serving for Facilitating the Deployment of SDN-Enabled Operational Networks**
  - Software Defined Network (SDN) technologies will be increasingly adopted to support data communications in electric power systems.
  - The Department of Energy had sponsored research projects on
    - Applying SDN technology to support the device-to-device communications;
    - Prototyping a dashboard application for providing the operators with a global view of the SDN-enabled operational networks.
- **Serving for Addressing the Threats Targeting the SDN-Enabled Operational Networks**
  - SDN paradigm faces new security threats and attacks.
  - Our project addresses the security risks targeting SDN technology and the protection solutions.

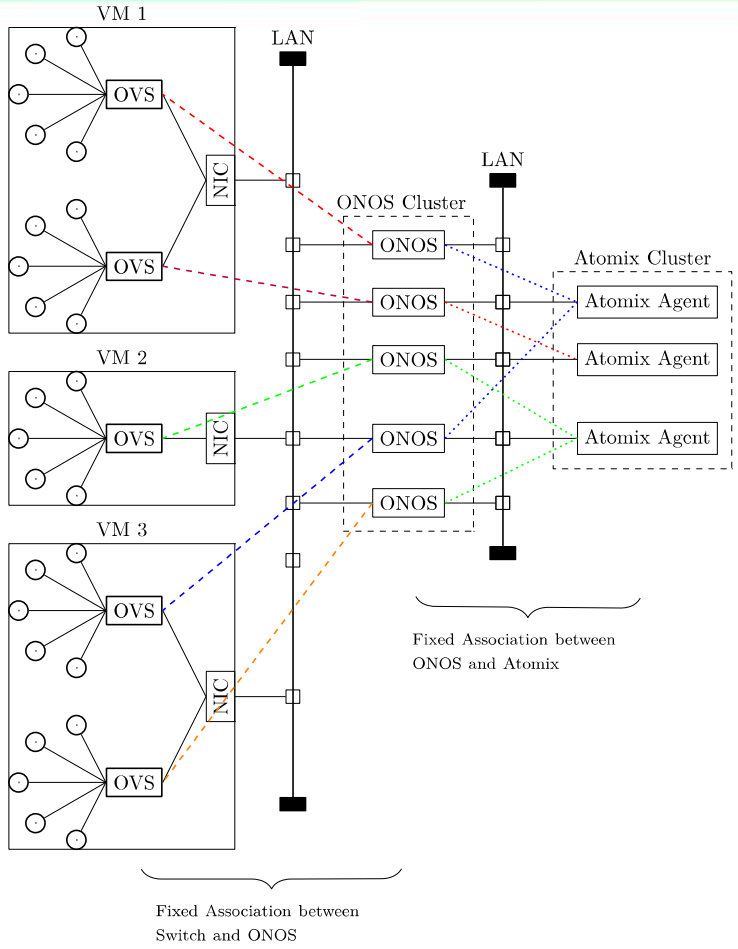
UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Strategic Alignment of Project to Fossil Energy Objectives (2)

System Diagrams of traditional Software-Defined Network





- Key vulnerabilities
  - Lack of detection on security breaching.
  - Lack of effective mechanism for excluding compromised SDN controllers from a SDN.

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Technology Benchmarking (1)

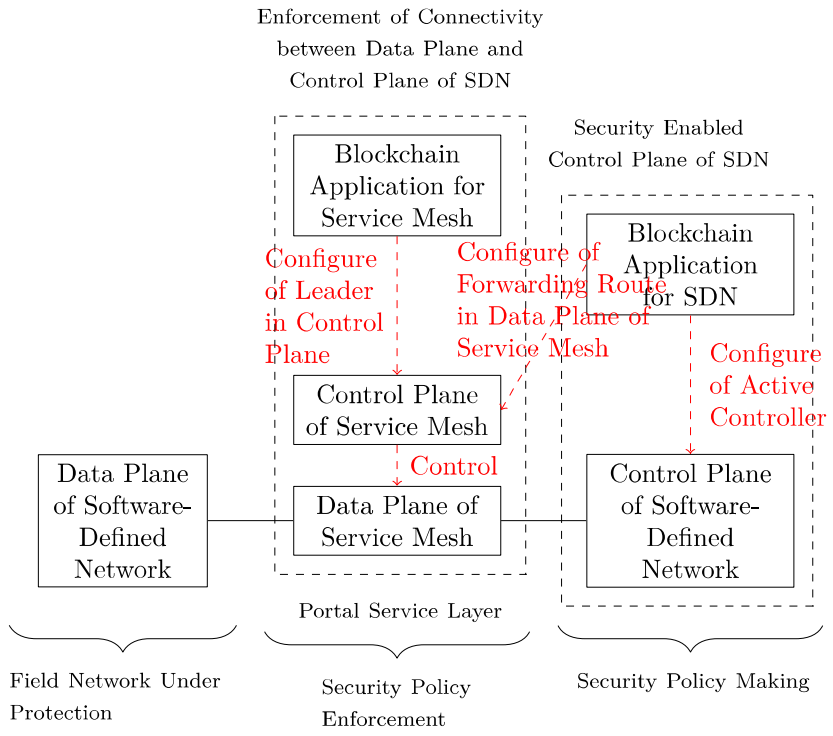
- This project aims to construct
  - A cloud-based networking platform which can be used for
    - Studying the threats targeting SDN-enabled operational networks deployed in electric power systems, and
    - Prototyping security protection solutions thwarting the attacks targeting the control plane, the forwarding plane, and the communications between the control plane and the forwarding plane.
  - A blockchain/P2P-based technology for detecting the compromised controllers in software defined networks.
- Industry/input or validation
  - This project is in collaboration with *Minnkota Power Cooperative.*
  - *Minnkota Power Cooperative* helps to facilitate decision-makings on the scientific and technical direction of the project and will be a user of the cloud-based networking platform.

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Technology Benchmarking (2)

- This project aims to enable security protection for SDN.
  - Enabling detection of compromised SDN controllers by constructing blockchain applications.
  - Enabling exclusion of compromised SDN controllers by decoupling the direct and fixed connectivity between the data plane and control plane in SDN.
    - A portal service layer is used to decouple the two planes.



UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

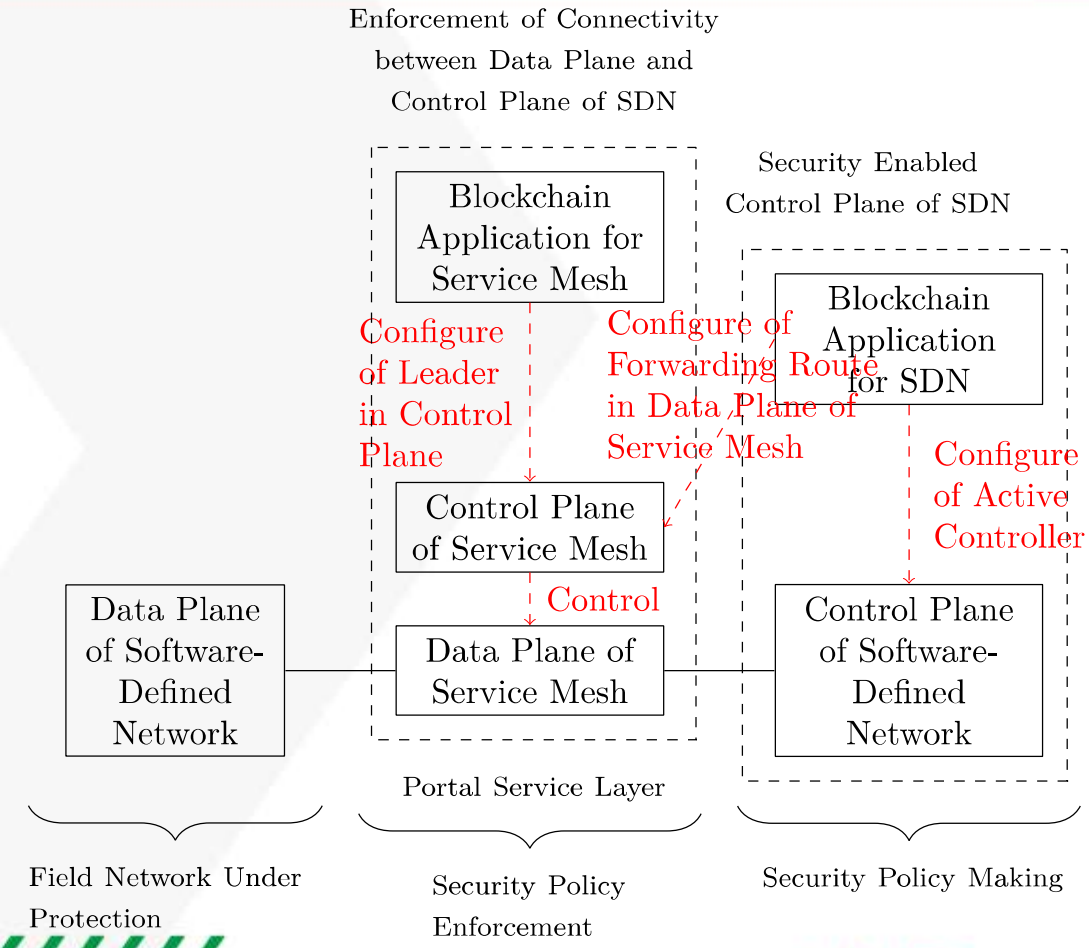
Overview of Major Efforts

- We have conducted 4 efforts in this project.
  - Determined the overall structure of the security-enabled SDN system.
  - Constructed a private cloud platform over 3 Dell servers.
    - The testbed operates in the private cloud.
    - The testbed supports simultaneous run of multiple SDN simulations.
  - Constructed the SDN with a controller cluster.
    - Mininet is used for simulating the data plane of the SDN (DP-SDN).
    - A cluster of ONOS controllers is used for the control plane of the SDN (CP-SDN).
  - Constructed the portal service layer to bridge the data plane and the control plane of an SDN.
    - The portal service layer is materialized in the form of a service mesh which consists of
      - A data plane (DP-SM): a set of *Envoy* proxies.
        - Forwarding traffic between DP-SDN and CP-SDN.
        - The forwarding paths are determined by CP-SM.
      - A control plane (CP-SM): a set of *Consul* agents.
        - Determine the forwarding paths in DP-SM.

UND UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

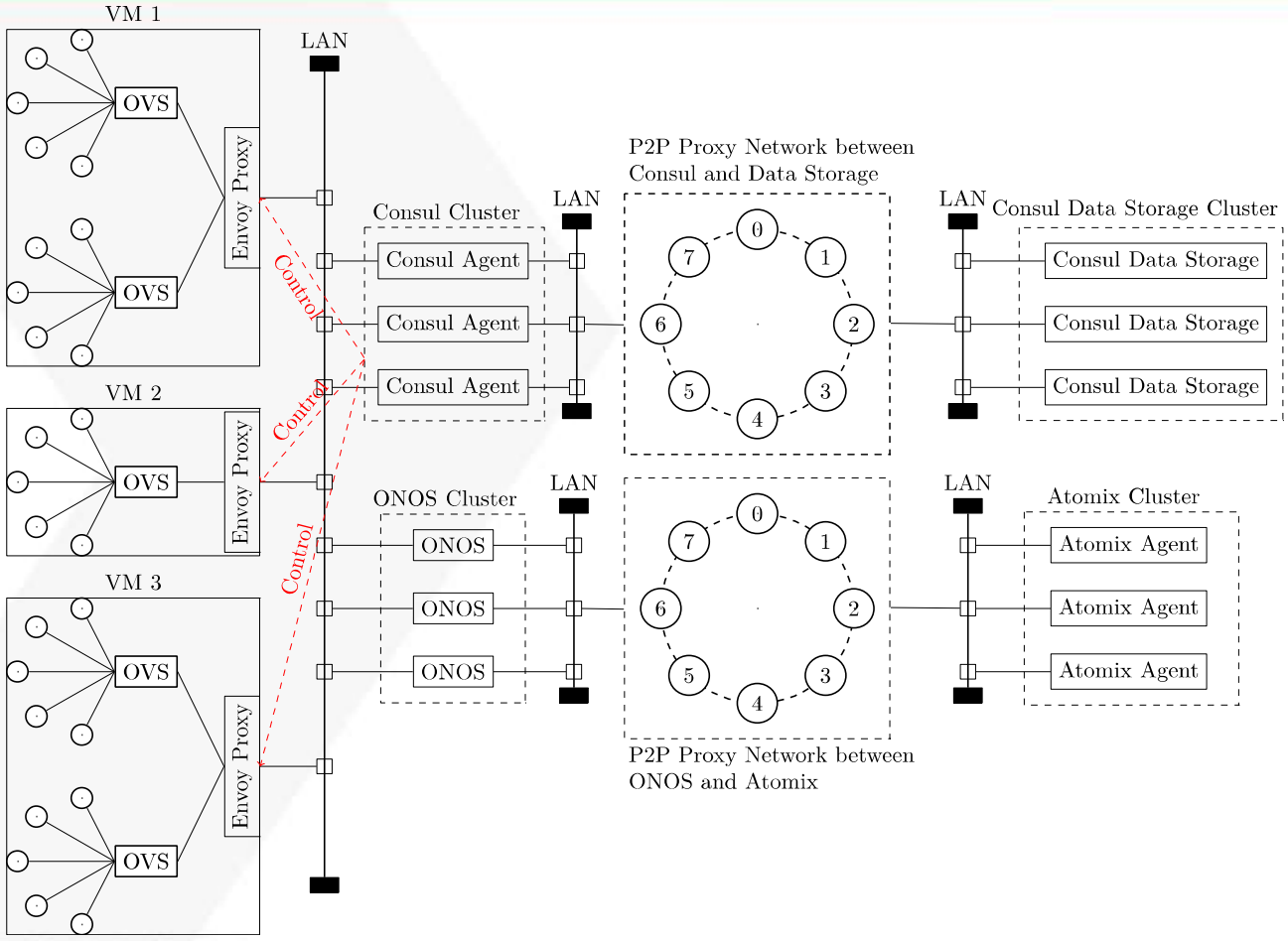
Overall Structure of Security-Enabled SDN System (1)



UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

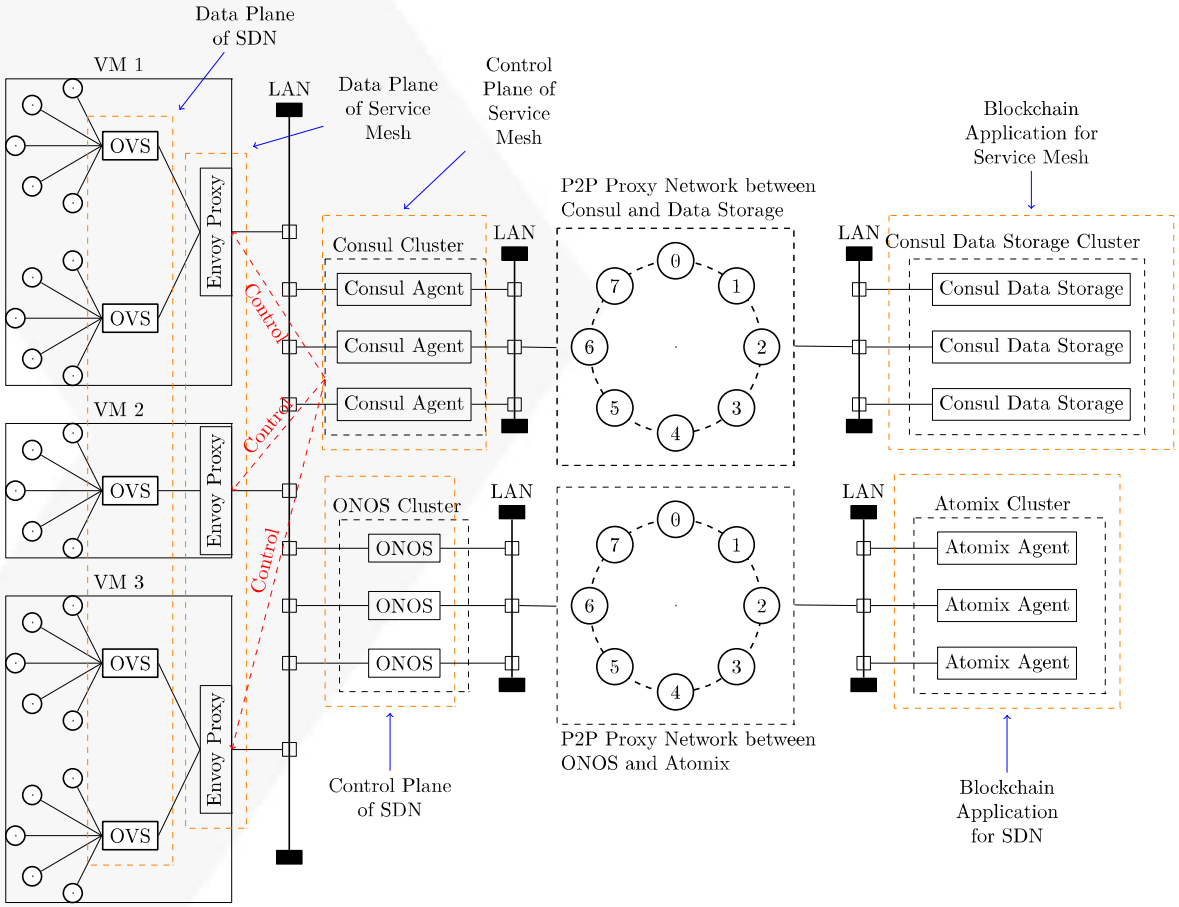
Overall Structure of Security-Enabled SDN System (2)



UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Overall Structure of Security-Enabled SDN System (3)



UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Current Status of Project

- This project started on September 1st, 2019 for a 3 years duration.
- This project , and there is no available comparison with known benchmark.
- There is no major change in the project goals/objectives.
- We have made some changes in the actual implementation of the tasks.
  - We have decided to construct the originally proposed testbed in the form of a cloud-based networking platform.
  - We have decided to adopt the proof-of-reputation consensus model for detecting the compromised network controllers in SDN networks.

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Current Status of Project

- This project started on September 1st, 2019 for a 3 years duration.
- Timeline of major tasks and milestones:

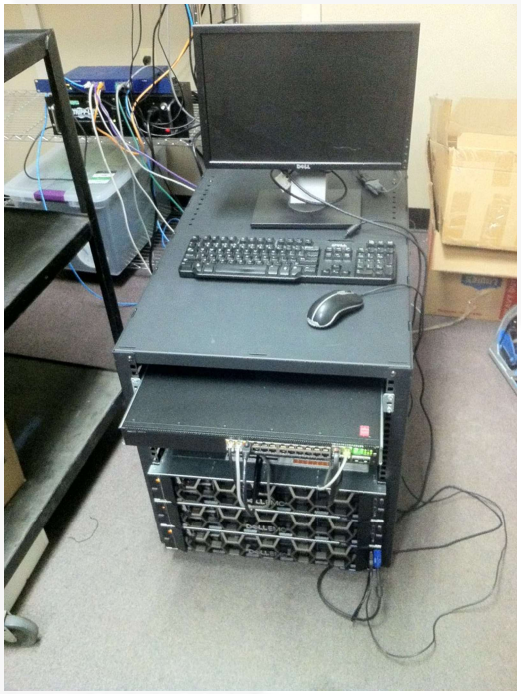
Task Description	Planned		Achieved	
	Start Date	End Date	Start Date	End Date
Task 1.0 -- Update project management plan	9/1/19	9/30/19	9/1/19	9/30/19
Task 2.0 -- Demonstration of Sample Runs of an SDN System	10/1/19	4/30/20	10/1/19	5/30/20
Subtask 2.1 -- Demonstration of Installation of Software on Controllers and Switches	10/1/19	11/30/19	10/1/19	12/31/19
Subtask 2.2 -- Demonstration of Traffic Flows Between SDN Switches	12/1/19	1/30/20	12/1/19	2/28/20
Subtask 2.3 -- Demonstration of Query for Rules	2/1/20	2/28/20	2/1/20	3/31/20
Subtask 2.4 -- Demonstration of Traffic Flow Handling Based on Rule Specifications	3/1/20	4/30/20	3/1/20	5/30/20
Task 3.0 -- Demonstration of a P2P Inquiry Platform in the SDN System	5/1/20	4/30/21	5/1/20	4/20/21
Subtask 3.1 -- A Justification Report of the Choice of a P2P Open-Source Package	5/1/20	5/30/20	5/1/20	6/15/20
Subtask 3.2 -- Demonstration of Querying Rules from the P2P System	6/1/20	11/30/20	6/1/20	4/20/21
Subtask 3.3 -- Making SDN Forwarding Switches to Query Rules from the Inquiry Platform	12/1/20	4/30/21	12/1/20	4/20/21
Task 4.0 -- Demonstration of Use Case of Identifying a Compromised Controller	5/1/21	8/31/22	2/1/21	
Subtask 4.1 -- Demonstration of a Blockchain System Running on Top of a P2P System	5/1/21	10/1/21	2/1/21	
Subtask 4.2 -- Demonstration of Replicated Rules in Blockchain System	11/1/21	1/30/22		
Subtask 4.3 -- Demonstration of Storing Replicated Data Chunks in Blockchain System	2/1/22	6/1/22		
Subtask 4.4 -- Demonstration of Identifying a Compromised Controller	7/1/22	8/30/22		

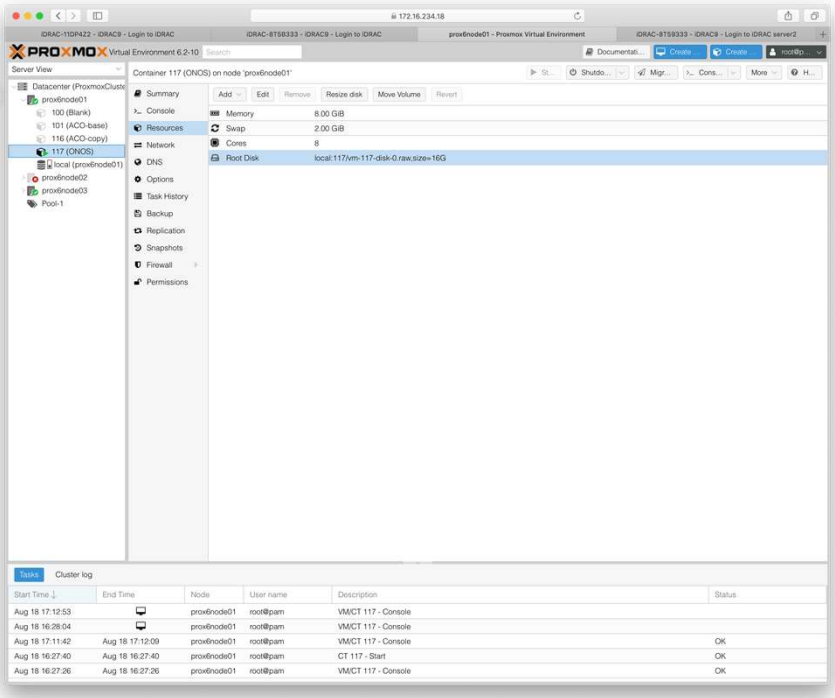
UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Before 2020 Review Meeting (1)

- Deployment of a cloud infrastructure running across 3 servers
  - Hardware: 3 high-end Dell servers (Model PowerEdge R540).
  - Software: Proxmox Virtual Environment (PVE) and OpenStack.



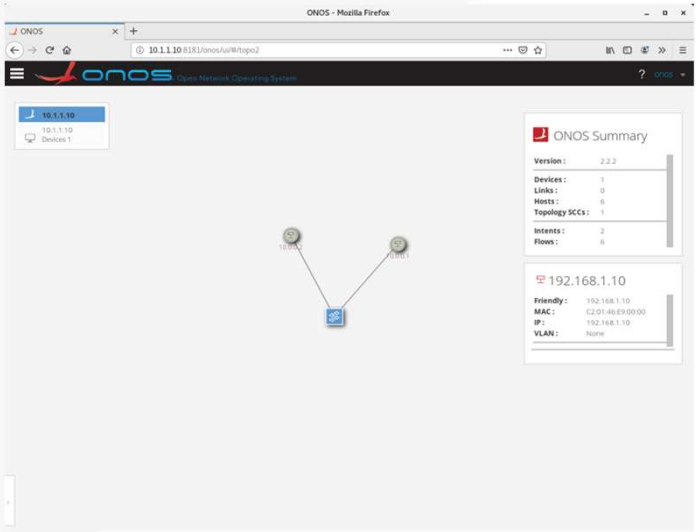


UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Before 2020 Review Meeting (2)

- Deployment of an Openflow-based SDN environment
  - Data plane: *mininet* is used to emulate OpenvSwitch (OVS) switches
  - Control plane: *Open Network Operating System (ONOS)* is used to emulate an OVS controller.
  - Running Openflow networks in the cloud environment.

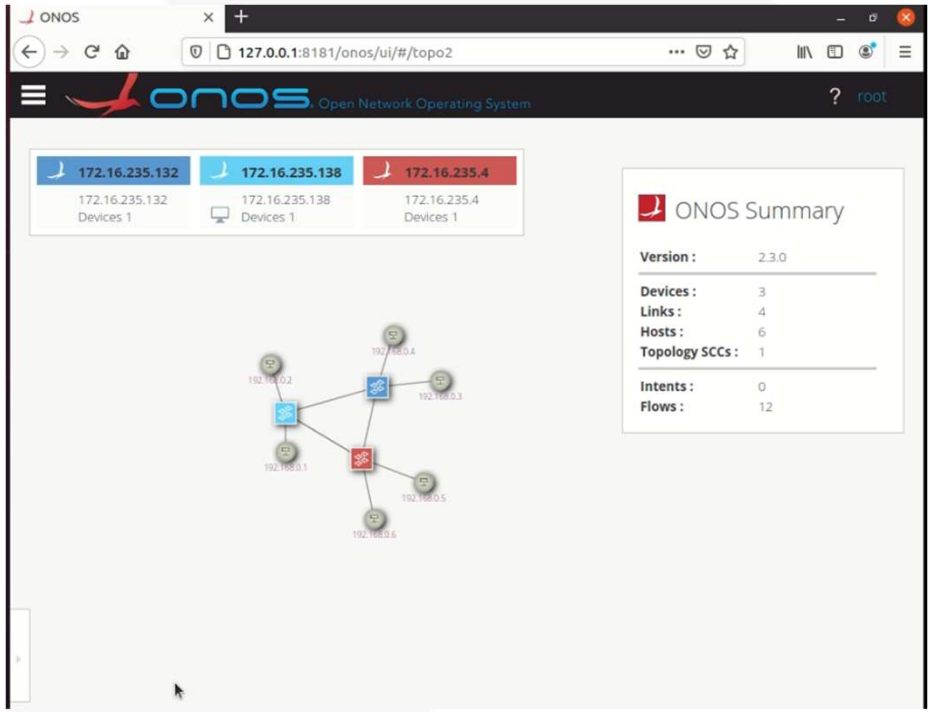


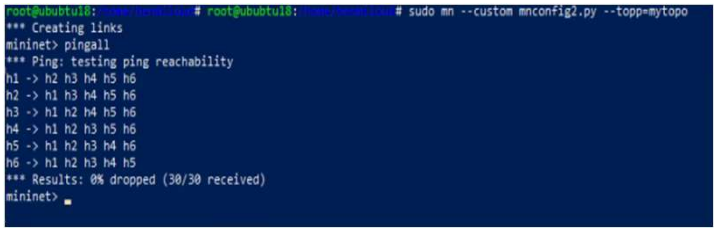
UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Since 2020 Review Meeting (1)

- Constructed the SDN with a controller cluster.
  - Mininet is used for simulating the data plane of the SDN (DP-SDN).
  - A cluster of ONOS controllers is used as the control plane of the SDN (CP-SDN).
  - A cluster of Atomix agents is needed for forming a cluster of ONOS controllers.



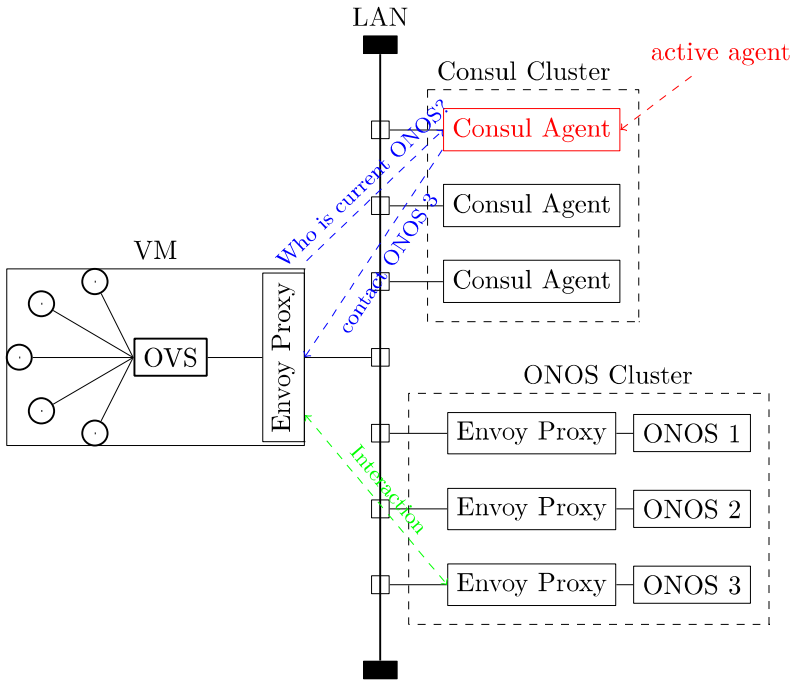


UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Since 2020 Review Meeting (2)

- Constructed the portal service layer to bridge the data plane and the control plane of an SDN.
  - The portal service layer is materialized in the form of a service mesh which consists of
    - A data plane (DP-SM): a set of *Envoy* proxies.
      - Forwarding traffic between DP-SDN and CP-SDN.
      - The forwarding paths are determined by CP-SM.
    - A control plane (CP-SM): a set of *Consul* agents.
      - Determine the forwarding paths in DP-SM.
  - In the demo of a SDN with a cluster of ONOS controllers shown on the previous slide, OVS switches interact with ONOS cluster through the portal service layer.
    - Manual configuration of the portal service layer as of now.
    - We will continue to enable automatic configuration by enabling the xDS service in Consul cluster.

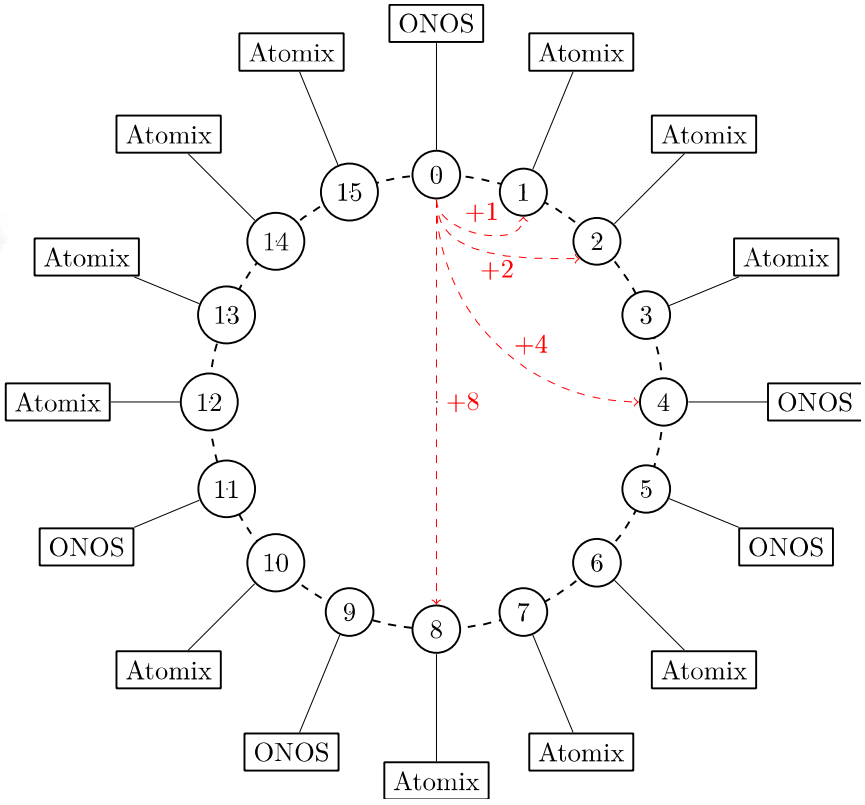


UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Since 2020 Review Meeting (3)

- Constructed the peer-to-peer (P2P) network to bridge between .
  - A cluster of ONOS controllers is used as the control plane of the SDN (CP-SDN).
  - A cluster of Atomix agents is needed for forming a highly available (HA) cluster of ONOS controllers because the formation of a HA cluster requires a Raft protocol to be run in the Atomix cluster.
  - A P2P network is used to bridge between a cluster of ONOS controllers and a cluster of Atomix agents.
    - An ONOS controller acts as an inquirer.
    - An Atomix agent acts as a data storage.

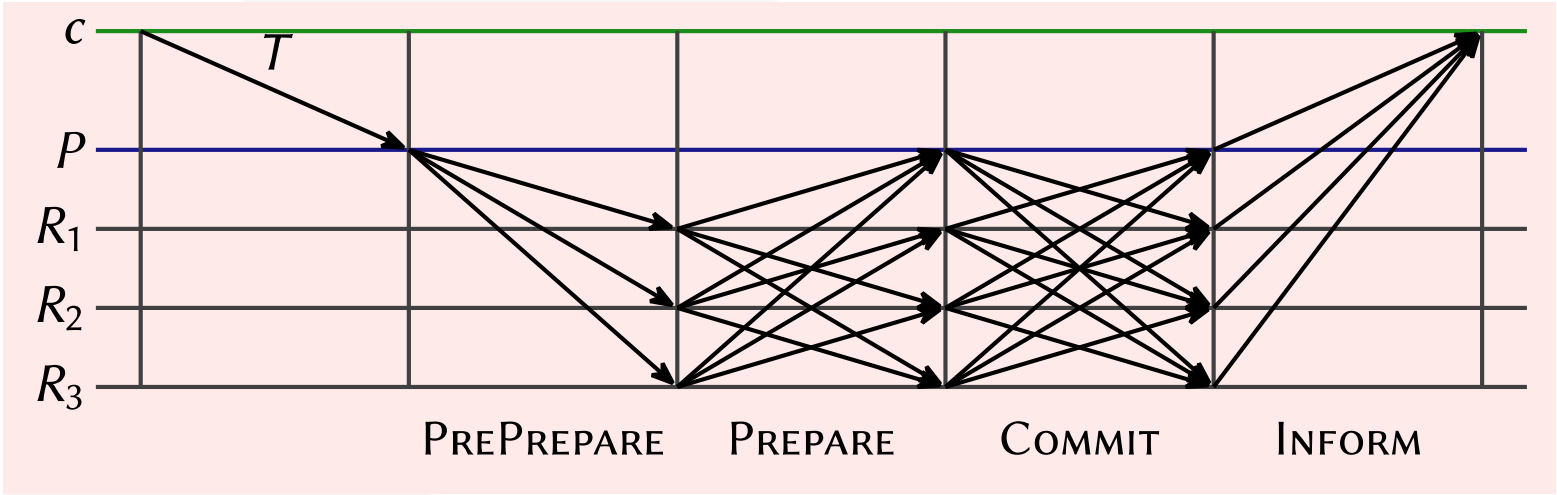


UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Accomplishments Since 2020 Review Meeting (4)

- Started to construct a BFT data storage with reduced communication overhead.
  - Raft protocol runs in Atomix data storage to support high availability of replicated data stores.
  - Raft protocol only tolerates fail-stop or fail-recover failures, but it does not tolerate Byzantine failures.
  - Practical BFT consensus can tolerate Byzantine failures and requires to transmit $3*n+2*n^2$ messages.
- Our goal: a BFT consensus algorithm in which a 3PC only produces a linear communication overhead.



(Figure is from a lecture note on practical BFT.)

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Next Steps (1)

- Develop a BFT consensus algorithm with linear communication overhead.
  - We are close to finish developing a 2-rounds group key agreement protocol which allows a group of participants to agree upon a common secret value.
  - The communication overhead of this group key agreement protocol is linear in the number of participants.
  - We plan to convert this group key agreement protocol into a BFT consensus algorithm.
- Prototyping the BFT consensus algorithm by modifying the Raft code in Atomix.
- Risk:
  - Prototyping the BFT consensus algorithm may be risky and time consuming.
- Risk mitigation:
  - We will also find open-source implementation of practical BFT (pBFT) algorithm and integrate the open-source pBFT implementation with Atomix, while we will attempt to prototype our low-overhead BFT consensus algorithm.
  - Bottom line: we will ensure pBFT with quadratic communication overhead to be used to provide BFT consensus in Atomix data storage.

UNIVERSITY OF NORTH DAKOTA

Project Description and Objectives

Next Steps (2)

- To develop a blockchain application (called blockchain-1) for detecting and excluding a compromised ONOS controller.
  - The blockchain application runs on top of Atomix data storage which provides BFT consensus.
  - Detection: A compromised ONOS controller is the one which had issued inconsistent rule to OVS switches.
  - Exclusion: The blockchain application configures the xDS in the Consul cluster to exclude a compromised ONOS controller after the detection.
- To develop a blockchain application (called blockchain-2) for detecting and excluding a compromised Consul agent.
  - It is also important to detect and exclude a compromised Consul agent since the Consul agent enforces the decision made by blockchain-1 application.

Project Description and Objectives

Next Steps (3)

- To continue the work on the P2P networks
  - The current work on P2P networks is highly simplified for demonstrating that an ONOS cluster can also be formed after a P2P network is used to bridge between a cluster of ONOS controllers and a cluster of Atomix agents.
  - We will continue to work on configuring the partitions in the P2P network by adding more peers.
- To construct the coordinated executions of multiple subsystems adopted in the testbed.
  - Currently, different subsystems have to be run piece-by-piece manually without being able to make a coordinated execution through running a single launching instruction.
- Many auxiliary tools have to be implemented for collecting experiment data in the simulation of an SDN.

UNIVERSITY OF NORTH DAKOTA

Acknowledgment

This material is based upon work supported by the Department of Energy Award Number DE-FE0031742.

Disclaimer:

"This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."

UNIVERSITY OF NORTH DAKOTA