Practical Labs for Teaching SDN Security

Souvik Das, Kamil Sarac

Department of Computer Science,
The University of Texas at Dallas,
Dallas TX USA

26th Colloquium on Information Systems Security Education (CISSE)

Introduction

Traditional Networking vs SDN

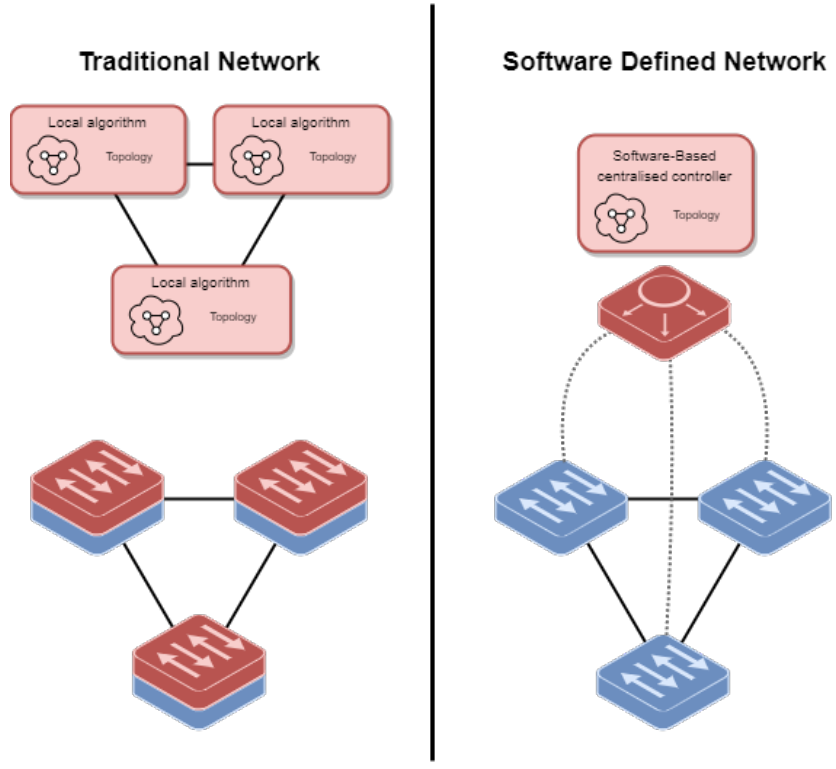
- Survivability vs Flexibility
- Division of Control and Data Plane

Related Security Issues

- Denial-of-Service
- Unauthorized Access
- Configuration Issues
- Network Sniffing
- Man-in-the-Middle
- Side-channel Vulnerabilities

Advanced Solution Methodologies

- Moving Target Defense
- Closed Loop Automation
- Machine Learning



Source: Reddit

Figure: Traditional Networking vs SDN

Lab Framework and Methodology

- Activity Guidelines
- Technical Hints
- Reference Materials
- Comprehensive Tutorials
- Testing Guidelines
- Instructor Manuals
- Hackathon
- Warm-up Activities
- Lab Workspace (VM)
  - Mininet
  - Docker
  - IDE
  - OpenvSwitch
  - ONOS
  - Linux Command Line Utilities:
    - hping, iperf, ssh, tc, ip, arp, ethtool, etc.

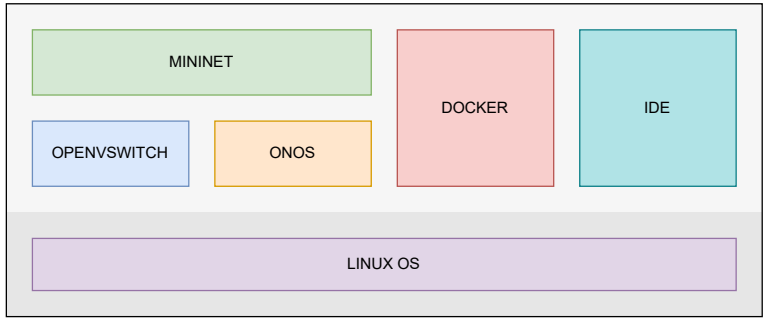


Figure: VM Composition

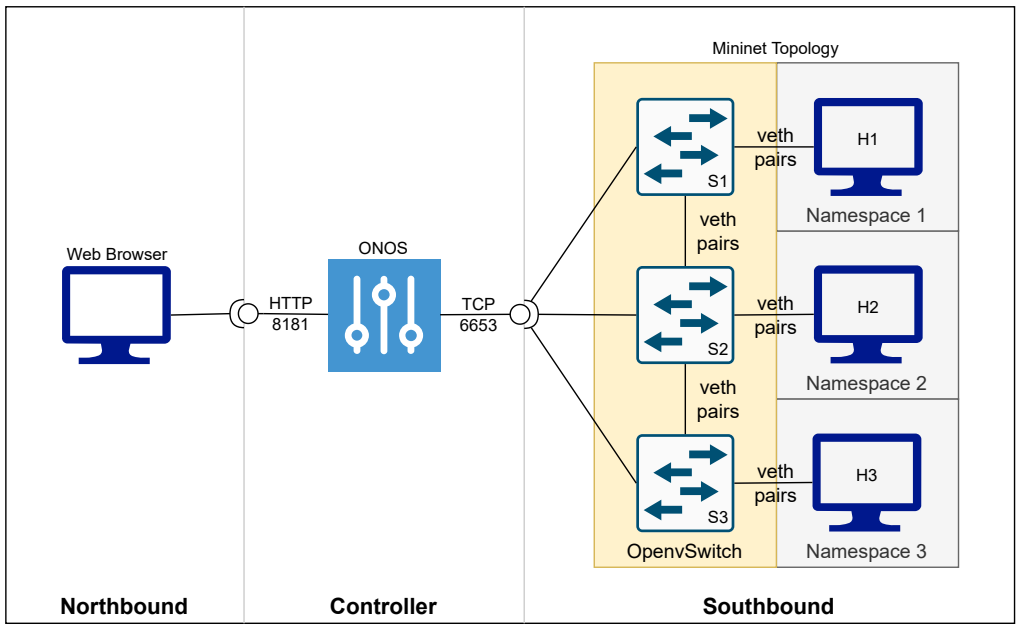


Figure: A Simulated SDN Deployment on Lab Workspace

Lab 1: Unauthorized Access by Compromised Controllers

- Multiple SDN Controllers
  - Scalability
  - Resiliency
- Distributed Network Control
- Shared Network Config
- Security Issues
  - Unauthorized Access
  - Man-in-the-Middle
- No Trusted Party
  - Byzantine Generals Problem
- Solution Methodology
  - Voting Heuristic

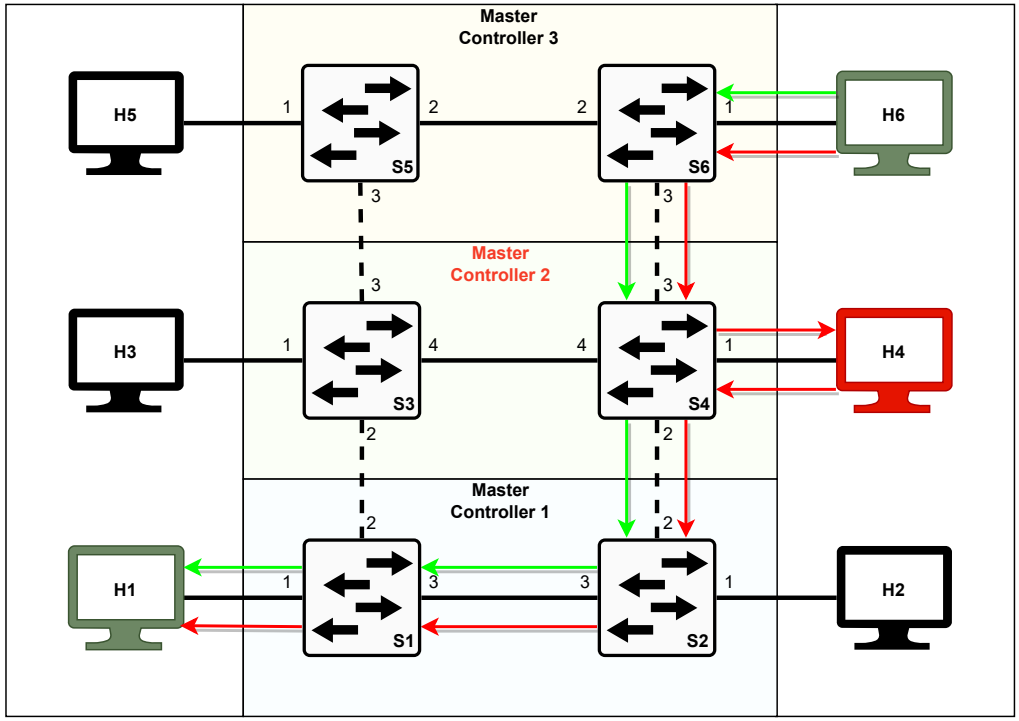


Figure: Multi-controller SDN setup with (red) and without (green) MITM attack

Lab 2: Unauthorized Access by Unauthorized Applications

- Multiple Tenants
  - Controller Application Module
    - Trusted Entity
  - Operates Network Flows
  - Conflicting Workflows
    - Foo: DROP Packet if Rate $>$ 10 PPS
    - Bar: FORWARD Packet if Rate $<$ 15 PPS
- Security Issues
  - Unauthorized Operations
    - Conflicting Objectives
    - Integrity Violation
- Solution Methodology
  - Brokered Access Control

	Priority(Foo) > Priority(Bar)	**Priority(Foo) < Priority(Bar)**
Rate < 10	Bar App is allowed to add its flow rule.	Bar App is allowed to add its flow rule.
10 < Rate < 15	Bar App's flow rule is deleted and Foo App is allowed to add its flow rule.	Foo App is denied to add its flow rule and Bar App's flow rule persists.
15 < Rate	(Never Reached)	Bar App's flow rule persists.

Figure: Expected workflow events for tenants Foo & Bar

Lab 3: DoS Attack Detection and Mitigation

- Denial-of-Service (DoS)
  - Security Issue
  - Service Disruption
  - Overwhelmed Network
- Detection Methodologies
  - Volume-based
  - Entropy-based
  - Resource-based
- Mitigation Strategies
  - Obtained Heuristics
  - Adaptive Bubble Burst

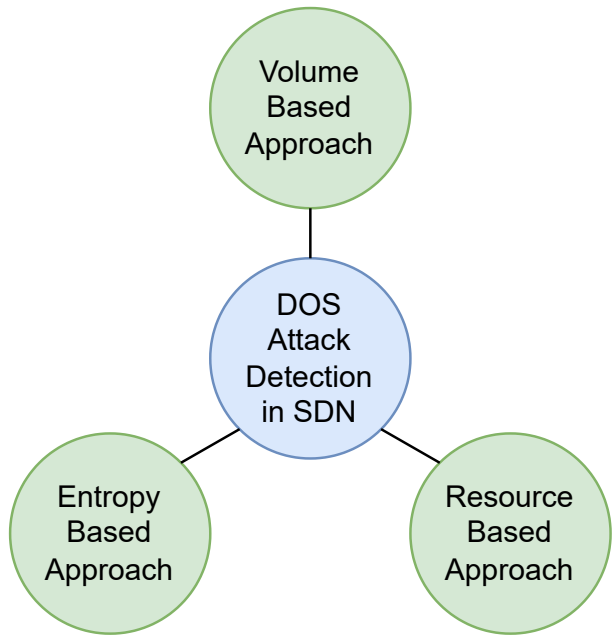


Figure: DoS attack detection mechanisms

Lab 4: Network Configuration Issues

- Northbound SDN Applications
  - Controller REST API
  - Open-ended Interface
  - Installs network policies
    - Set of flows
- Security Issues
  - Inconsistent Network Config
    - Policy Conflicts
    - Network Cycles
- Solution Methodology
  - Northbound Application Manager
    - Proactive Resolution
    - Reactive Resolution

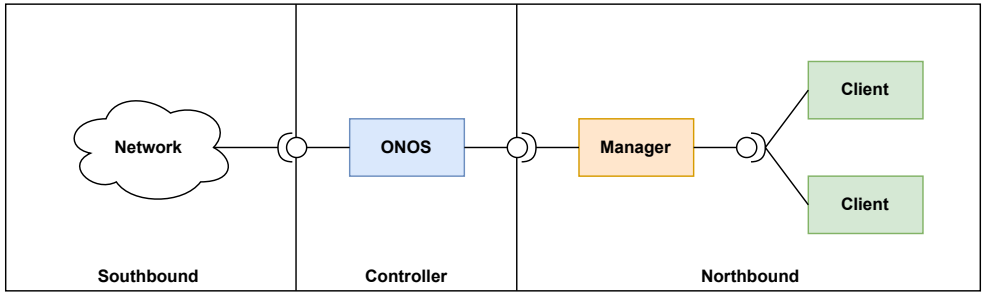


Figure: Lab Overview

Field	Description
id	ID of the client (e.g. "App 1", "App 2")
type	Type of policy - "forwarding", "forbidden" or "unmanaged"
src-ip	IP address of the source host in the policy
dst-ip	IP address of the destination host in the policy
priority	Priority of flows in the policy
flows	Comma separated list of flows in the policy. Format: "<switch-dpid, in-port, [out-port(s)]>, ..." Example: "<of:0000000000000002,1,[3]>, <of:0000000000000001,3,[2]>"

Figure: Example of a policy schema

Lab 4: Network Configuration Issues

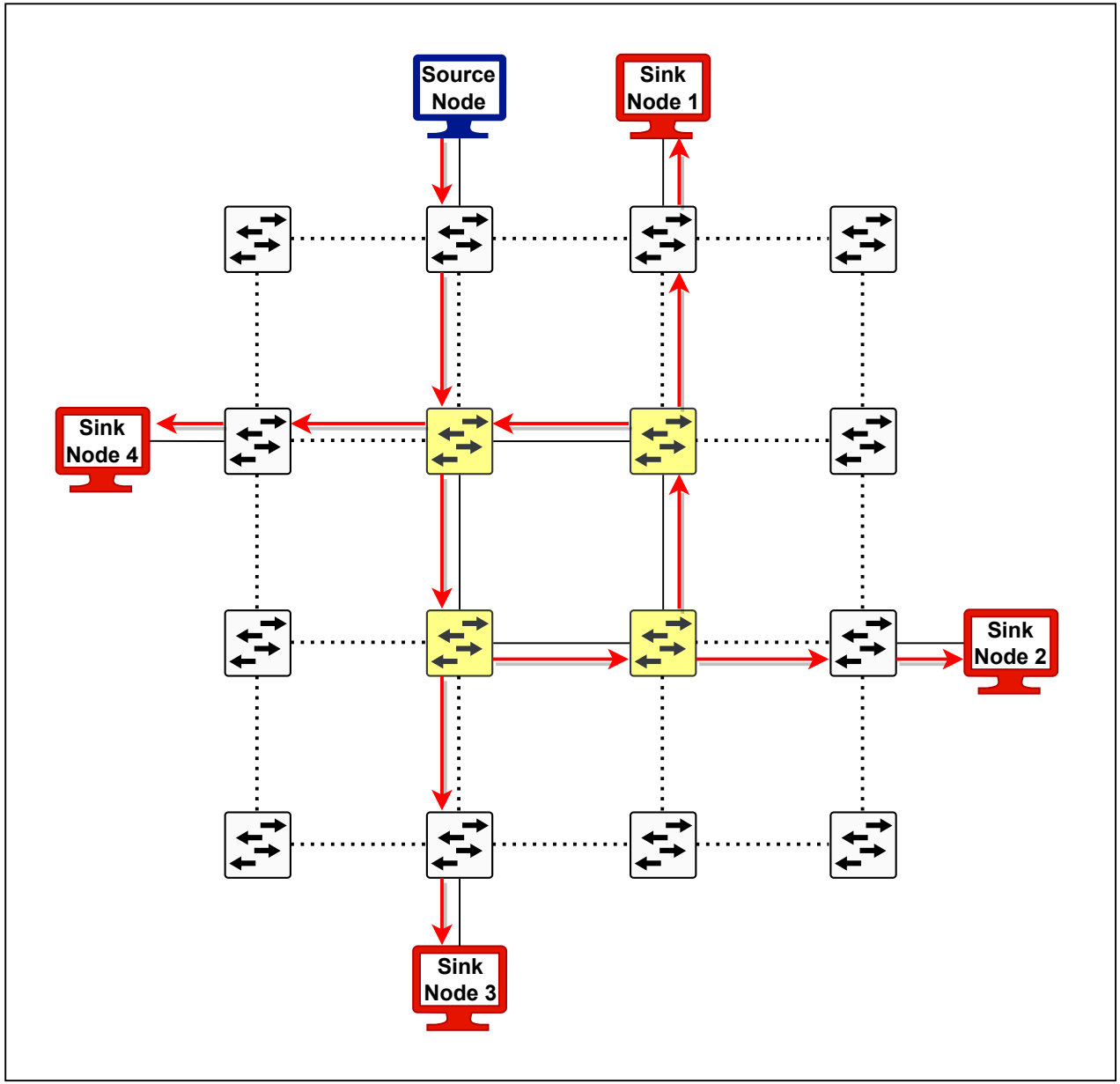


Figure: Example of network cycle due to poor network policies

Lab 5: ARP Spoofing Attack Mitigation

- Address Resolution Protocol (ARP)
  - Maps IP to MAC Address
  - Network Switching
- Security Issues
  - Spoofing Attacks
    - Impersonation attack
    - Man-in-the-Middle (MITM)
    - Denial-of-Service
    - Unsolicited ARP
- Mitigation Strategies
  - MITM based Attack Prevention
  - Host Tracking and Filtering
  - Stateful ARP Inspection
- Host Mobility
  - Identity vs Location
  - Entropy Heuristics

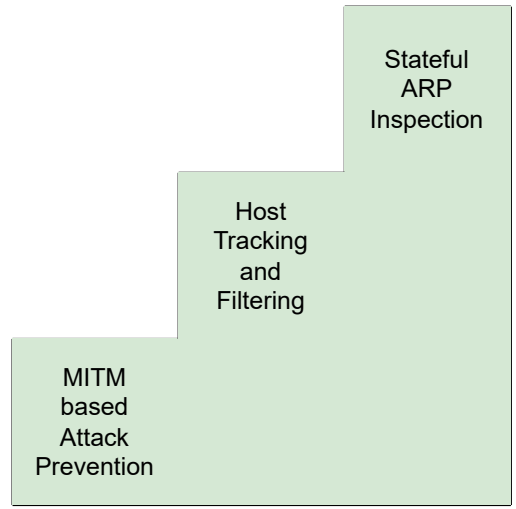


Figure: ARP spoofing attack mitigation strategies

Lab 6: Moving Target Defense

- Network Communication
  - Identifying Hosts
  - Identifying Paths
- Security Issue
  - Network Sniffing
  - Attack Staging
- Moving Target Defense
  - Defense Strategy
  - Introduces Unpredictability
- Solution Methodologies
  - Random Host Mutation (RHM)
  - Random Route Mutation (RRM)

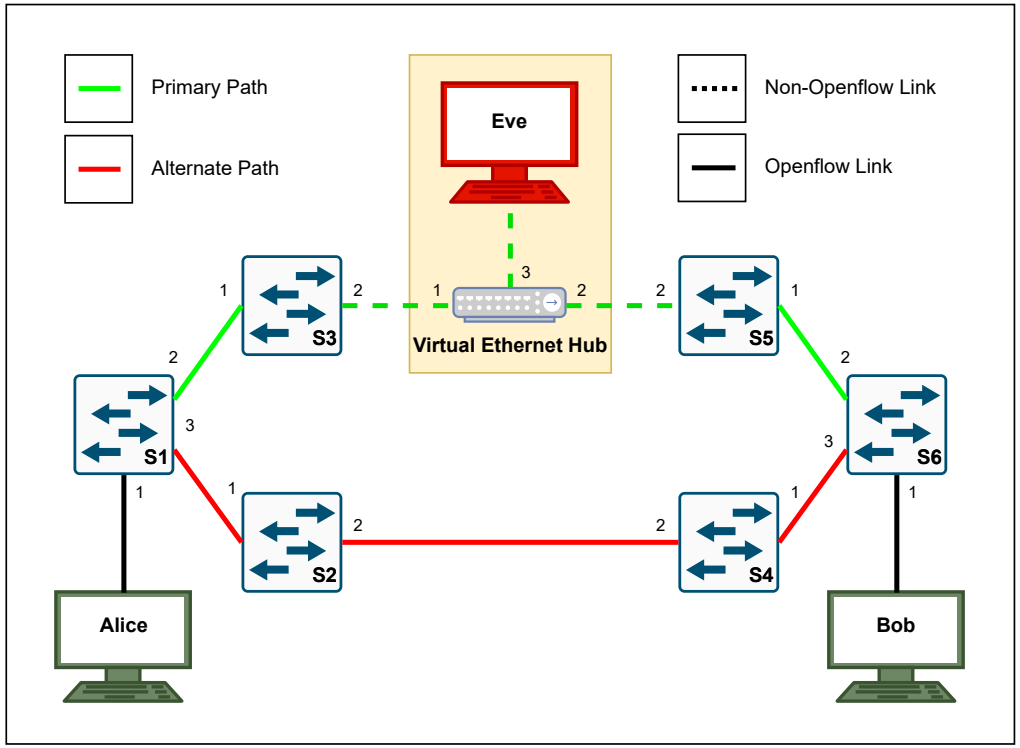


Figure: Example of RRM with an adversary (Eve)

Lab 7: ML-based Network Intrusion Detection System

- Detect Malicious Traffic
  - Depends on scenario
  - Ineffective heuristics
- Lab Scenario
  - TCP SYN Flooding Attack
- Solution: ML-based NIDS
  1. Identify Flows
     - Argus
  2. Collect Flows
     - Filebeat
     - Elasticsearch
  3. Learn & Classify Flows
     - Training Dataset
     - Scikit-learn
  4. Mitigate Attack
     - ONOS REST API

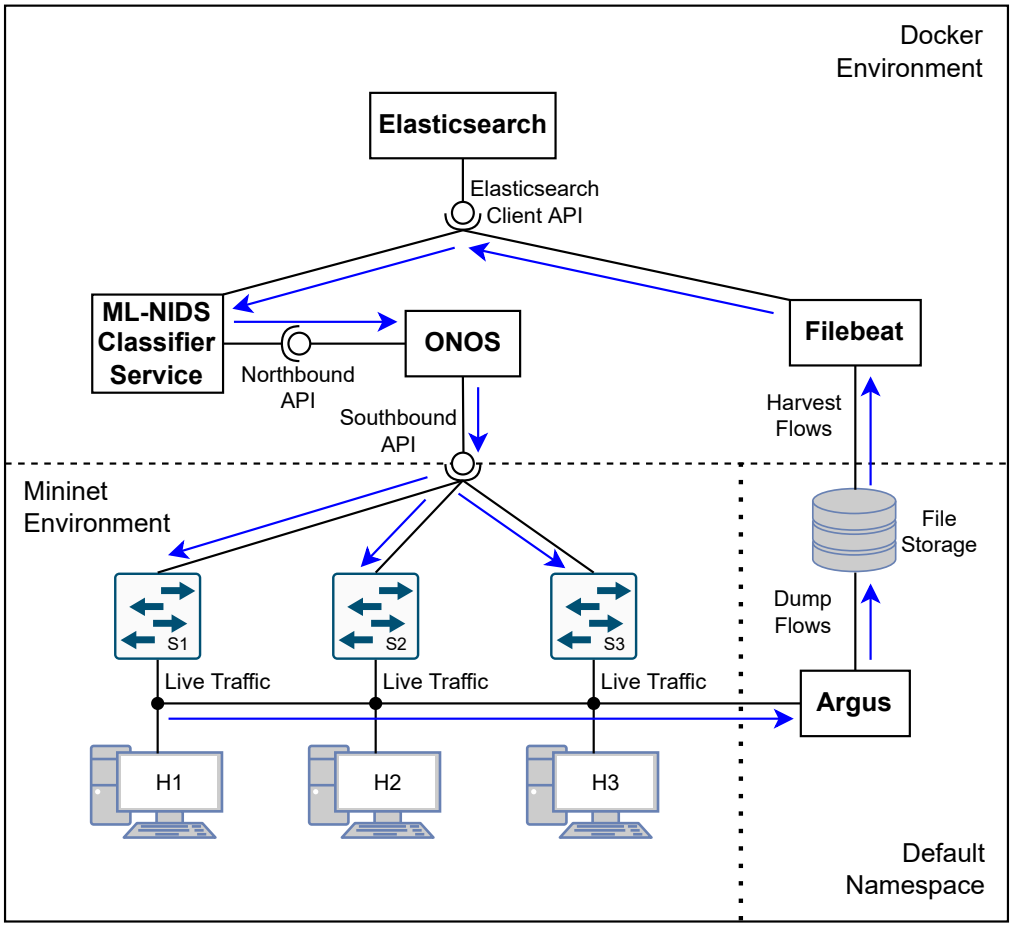
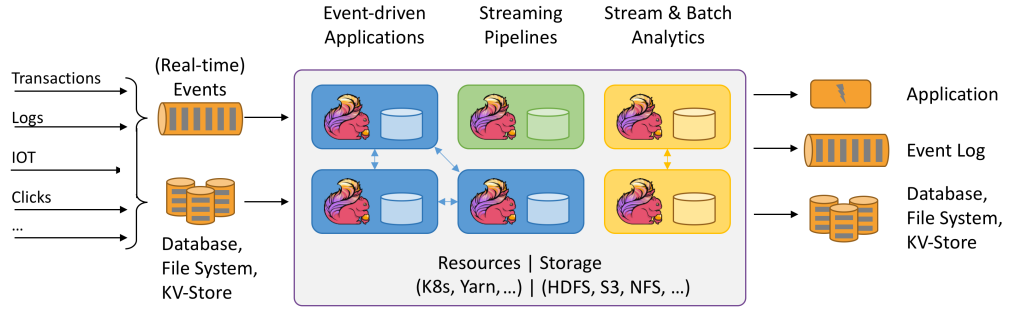


Figure: ML-based NIDS setup overview

Lab 8: Closed Loop Automation

- SDN Feedback Sources
  - Network
  - Applications
- Closed Loop Automation
  - Feedback Mechanisms
  - Automate Control
- Apache Flink
  - Distributed Data-stream Processing
- Lab Scenarios
  1. Streaming Application Bottleneck
     - Packet vs Record processing
  2. SDN Overlay
     - Overlay path capacity bottleneck
- Solution Methodologies
  1. Streaming Application-aware Quality-of-Service
  2. Responsible Overlay Traffic Migration



Source: flink.apache.org

Figure: Apache Flink Pipeline

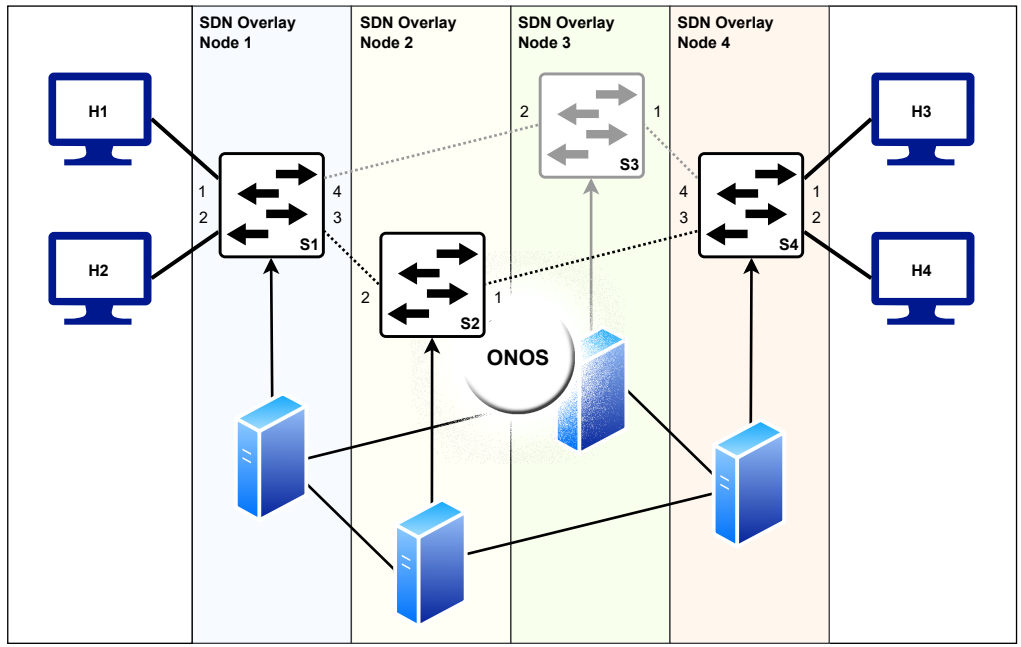


Figure: SDN Overlay Setup

Conclusion

- In practice, different deployment scenarios require different solutions to address the network and application security issues related to SDN.
- We have developed a number of security lab activities inspired from those realistic and practical SDN deployment scenarios.
- Our lab provides students with a structured framework to try out new solutions that they may come up with either by themselves or in consultation with relevant academic papers.