Towards a Secure and Resilient Industrial Control System with Software-Defined Networking

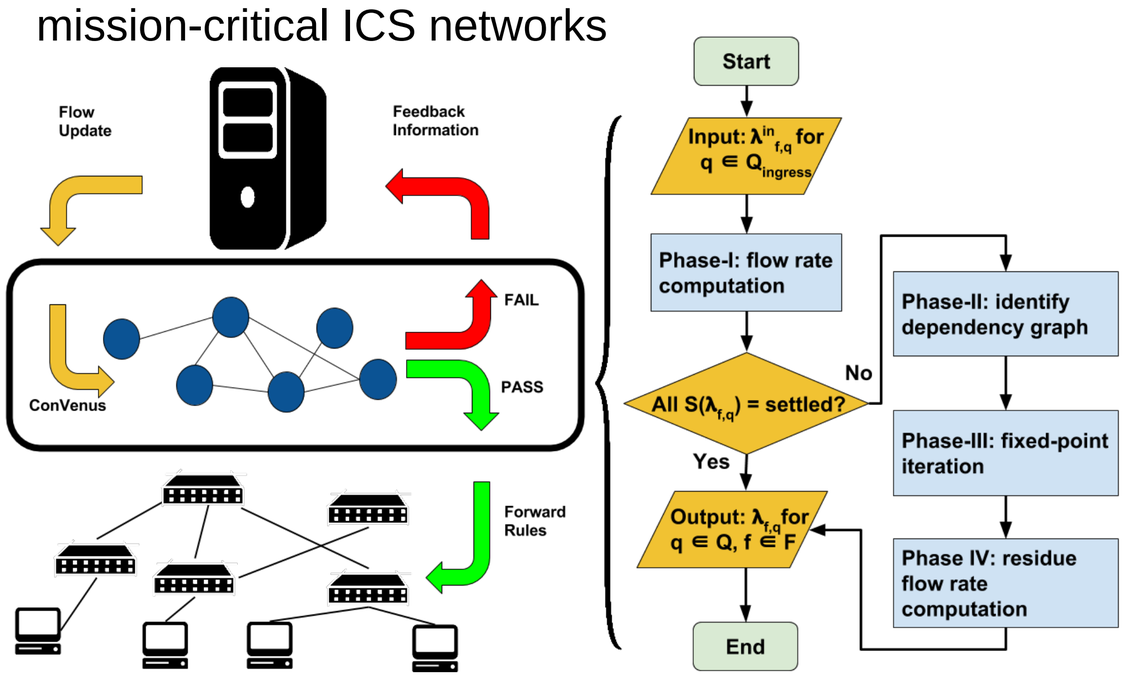
Dong (Kevin) Jin, Jiaqi Yan, Xin Liu, Christopher Hannon (Illinois Institute of Technology)
Hui Lin, Zbigniew Kalbarczyk, Ravishankar Iyer (University of Illinois Urbana-Champaign)
Chen Chen, Jianhui Wang (Argonne National Laboratory)
Cheol Won Lee (National Security Research Institute, South Korea)

Motivation

Modern Industrial Control Systems (**ICS**) increasingly rely on the computer and communication networks to efficiently monitor and control the critical physical processes. Compromising those networks can impact the successful operations of the critical infrastructures, including power grids, oil and gas distribution systems, weapon systems, etc. In this work, we apply the emerging **SDN** technology to secure ICSes in the context of Smart Grid, and investigate several innovative **SDN-aware cyber-security applications**.

ConVenus

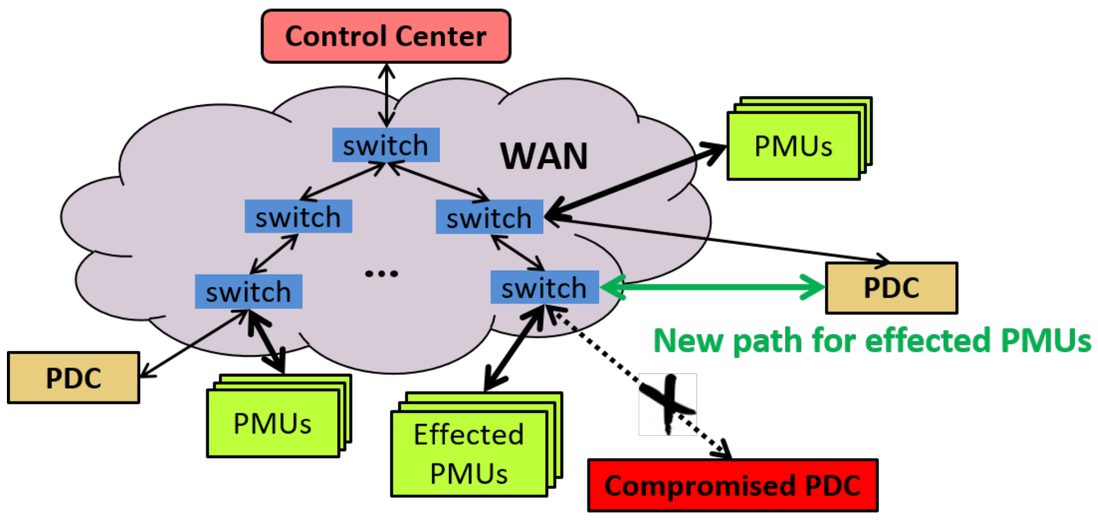
- Verify every incoming flow update rules from the control plane to the forwarding plane in **real time**
- Preserve the **congestion-freedom** in time-critical and mission-critical ICS networks



SelfHealer

Directly program SDN switches upon attack detection so that

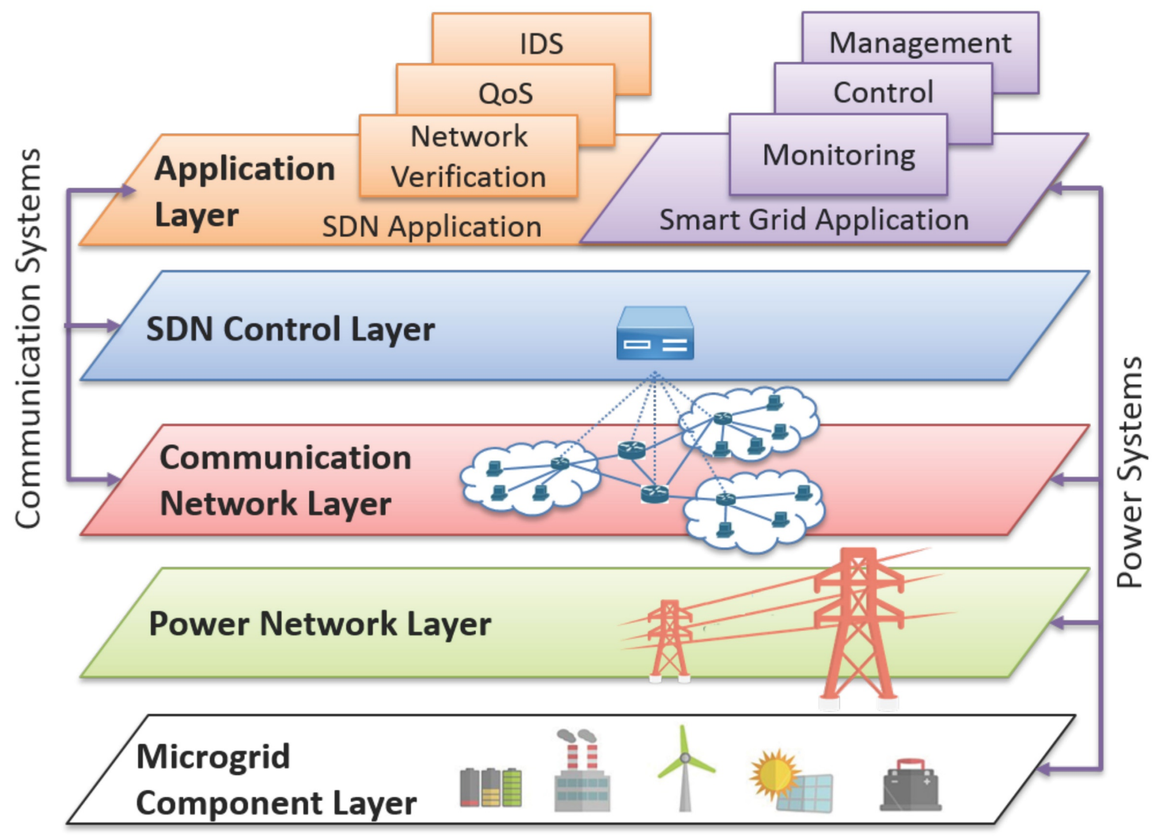
- PMUs are isolated from the compromised PDCs;
- Disconnected yet uncompromised PMUs are **automatically** reconnect to the network;
- Power system observability is restored with **minimal** overhead during the self-healing process



SDN-based Approach

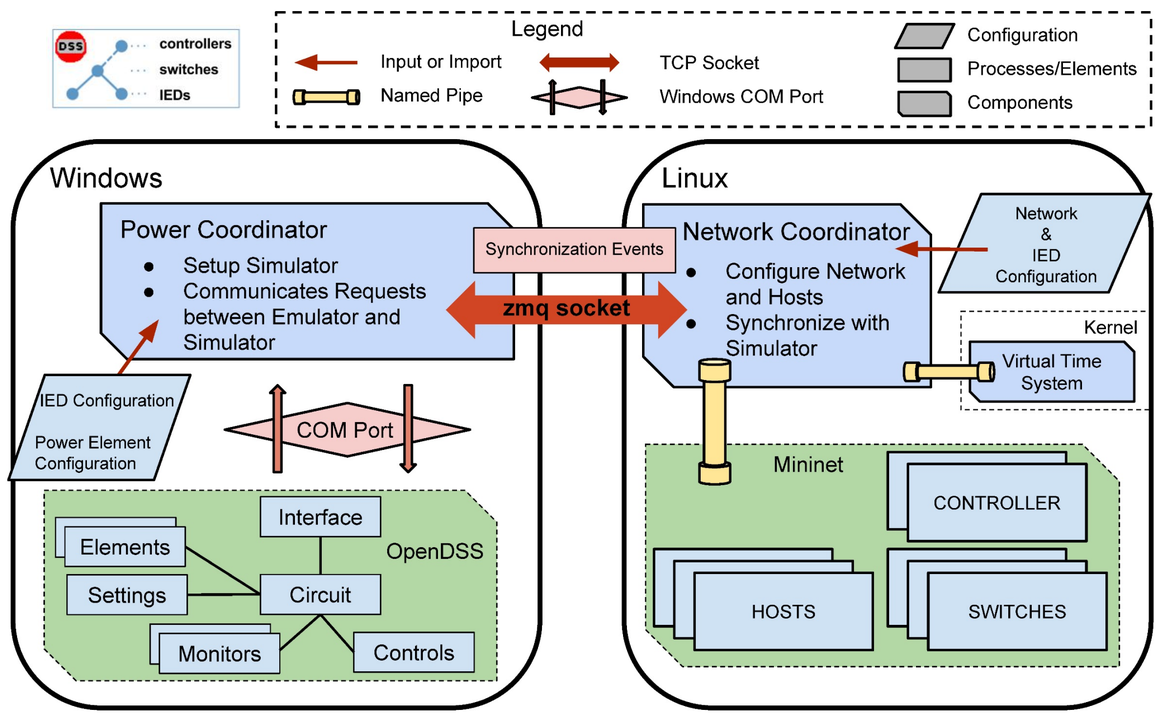
Within the SDN-enabled smart grid

- We install **ConVenus** between the control plane and the data plane to enforce the correct network-layer invariants (e.g., congestion-freedom).
- On the data plane layer, we enhance the resilience of PMU networks against cyber attacks with **SelfHealer**.
- We build a simulation/emulation testbed **DSSnet** to support high-fidelity analysis of cyber-attacks on SDN-enabled ICSes.



DSSnet

- Integrate electric **power distribution system simulation** (OpenDSS) with **SDN network emulation** (Mininet)
- Test and evaluate SDN-aware applications for ICS resilience and security
- Based on **virtual-time-system**-based synchronization



INFORMATION TRUST INSTITUTE

ILLINOIS

SCIENCE OF SECURITY VIRTUAL ORGANIZATION