Securing Networked Industrial Control Systems with Software-defined Networking

Jiaqi Yan
Illinois Institute of Technology
10 West 31 Street
Chicago, Illinois
jyan31@hawk.iit.edu

Christopher Hannon
Illinois Institute of Technology
10 West 31 Street
Chicago, Illinois
channon@hawk.iit.edu

Xin Liu
Illinois Institute of Technology
10 West 31 Street
Chicago, Illinois
xliu125@hawk.iit.edu

Dong Jin
Illinois Institute of Technology
10 West 31 Street
Chicago, Illinois
dong.jin@iit.edu

ABSTRACT

A wide variety of ICSes connected to the physical world rely on the underlying network to monitor and control critical physical processes. Compromising communication network in ICSes will cause damaging impact on the healthy operation of critical national infrastructures related to power, water, gas and so on. In this work, we tackle various challenges to the protection of ICSes by applying SDN technologies and developing innovative security applications and tools. In particular, we install *ConVenus* between the control plane and data plane to enforce the congestion-free property in the network layer; on the data plane layer, we enhance the resilience of PMU networks against cyber attacks with *SelfHealer*[open to suggestions]; we build a hybrid testing platform *DSSnet* to support high-fidelity analysis of cyber attacks on SDN powered ICSes networks. To be more specific:

- **ConVenus**: With SDN-enabled global visibility, ConVenus adopts the dynamic data-driven paradigm to preserve congestion-free property throughout the lifetime of the delay-critical part of the ICSes network. When each time there is a network flow to be inserted, updated or removed, ConVenus performs the following steps: (1) identifies the minimum subnetwork that is affected by the incoming flow update (2) models the extracted subnetwork with a undirected graph as the network topology and a set of directed path as the network flows (3) runs a fast simulation algorithm to quickly compute the throughput of every flow in the network model and report congestion if it exists. By incrementally updating the model and rejecting the updates that causes congestion, ConVenus can guarantee that at any time the network is congestion-free.

- **SelfHealer** utilizes the feature of direct programmability offered by SDN to achieve resilience against cyber attacks in power grid. To firstly prevent further propagation of the attack, SelfHealer directly programs the SDN-enabled network switches so that compromised Phasor Measurement Units and Phasor Data Concentrators are isolated. Meanwhile, the disconnected yet uncompromised PMUs will be automatically reconnect to the network and thus self-heal the observability of the power system. The self-healing process is formulated as integer linear program model to minimize the overhead of the self-healing process, while considering the constraints of power system observability, hardware resources, and network topology.

- **DSSnet**[1] address the challenge that it is infeasible to create a physical testbed for modern ICSes given its large scope. We combines a power distribution system simulator with an SDN network emulator so that high performance and temporal fidelity are preserved without sacrificing the supported scalability. The combination is built on the foundation of a virtual time system: on one hand, virtual time system tightly controls (pauses and resumes) the execution of the emulation system whenever synchronization between two sub-system is required; on the other hand, by accurately dilating the clock of emulated network ends, DSSnet is able to emulate high bandwidth and low latency networks that exceeds resource capability available on the test machines.

1. REFERENCES

[1] C. Hannon, J. Yan, and D. Jin. DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation. In *2016 ACM SIGSIM Conference on Principle of Advanced Discrete Simulation (PADS)*, pages 1–11, May 2016.