Specification-Based Process Control Attack Detection in Substation Automation

Muhammad Nouman Nafees, Neetesh Saxena, and Pete Burnap
Computer Science and Informatics, Cardiff University, Cardiff, United Kingdom

Introduction

The Substation Automation is a critical entity of the smart grid, consist of many physical control processes.

- High capability attackers can target process control attacks to disrupt the power operations by stealthily compromising multiple components of the system.
- Existing attack detection strategies lack the appropriate trust model and implicitly assume two or more components in process control loop are trusted.

Contributions

- Employ specification-based data-driven approach to detect process control attacks.
- Semi-automate the specification mining process by utilizing the Substation Configuration Language (SCL) files.
- Store additional information describing process control logic for various scenarios.
- Perform the attack on IEEE 12-bus system using PowerWorld simulator to study the impact of the attack and implement our detection approach on power system case.

Threat Model and Approach

Attack Scenario

- Adversaries gain remote access to distance relay and PLC.
- They modify the relay logic and replay the normal relay logic to the PLC's internal logic tables.

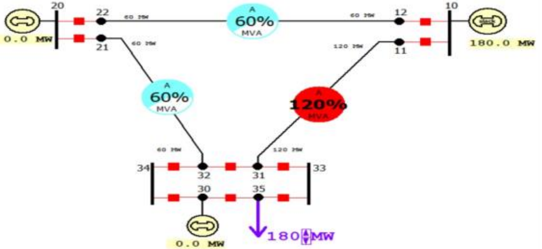

Fig. 1. IEEE 12-bus system.

Approach

- Leverage the SCL documentation for our IDS to store additional information describing process control logic.
- Create a temporal state-based model, where we correlate and map the predefined control rules in the PLC.
- To detect malicious command attacks in the process control loop, we utilize power system security metric System Aggregate Megawatt Contingency Overload (SysAMWCO).

Validation

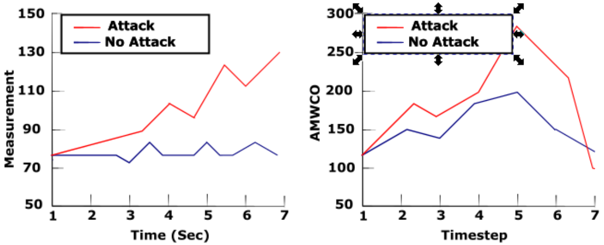

Fig. 2. Process control attack detection with control invariant measurement and AMWCO metric.

Future Work

- Further explore the efficacy of our approach on physical testbed.
- Formalize other process control attack scenarios.
- More control logics will be utilized in mapping the correlation tables for our detection approach.

Reference

J. Nivethan and M. Papa, "A scada intrusion detection framework that incorporates process semantics," in Proceedings of the 11th Annual Cyber and Information Security Research Conference, pp. 1–5, 2016.