U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Timing Intrusion Management Ensuring Resiliency (TIMER)

Managing Global Navigation Satellite System (GNSS) timing signals to avoid compromised situational awareness

Background

The deployment of synchrophasor systems to monitor grid operations, providing situational awareness of grid performance across wide geographic regions, for instance as input to Wide Area Monitoring, Protection and Control (WAMPAC) applications, has increased in recent years. In future years, synchrophasors may also be used for protection and control, in addition to the monitoring capability they are used for today. Currently, synchrophasors supplement energy management system (EMS) timing capabilities at the sites of many Independent Systems Operators (ISOs)/ Regional Transmission Organizations (RTOs), as well as many transmission owners, enhancing wide-area situational awareness of grid operations. PMUs use the timing clock derived from Global Navigation Satellite System (GNSS) receivers to sample and timestamp the voltage and current waveforms at PMU locations across the grid. Such measurements are sent to Phasor Data Concentrators (PDCs) for further time-aligned data stream synchronization.

Due to this reliance on GNSS, synchrophasors must be resilient against malicious compromise of the GNSS timing signal. This requires the development of new approaches to detect timing signal intrusions in the synchrophasor system.

Objectives

The objective of this project is to develop a timing intrusion management strategy that deploys attack detection modules. If an intentional timing intrusion takes place, this management strategy will use the intrusion detection capability built into the system to identify the location of the attack, allow a predictive understanding of the consequences, and inform the appropriate response.

Project Description

The timing intrusion detection modules are organized in layers, based on their operating frequency and their place in the system hierarchy. The intrusion detection process starts from the lowest level and works its way up layer by layer. To confirm and evaluate the performance expectations of the application under possible timing intrusions requires simulation of the actual power network events and prevailing conditions of interest in the network. This power network simulation then feeds the PMU with the corresponding waveforms (application tests) required to verify and determine that when a detection module senses an attack the applications are still within bounds of acceptable application accuracy and time response. Such bounds are determined through a sensitivity study for various intrusions.

Benefits

- Software and hardware solutions to detect timing intrusions in critical energy infrastructure that could compromise situational awareness of power grid operations
- Commercially deployable synchrophasor timing intrusion protection solutions
- Statistical methods for assessing the effectiveness and cost benefits of the proposed solutions

Partners

- Texas A&M Engineering Experiment Station (lead)
- Idaho Power Company
- Pacific Northwest National Laboratory (PNNL)

Period of Performance

October 2016 – March 2021

Project Cost

Total: $4,429,451

Federal: $2,999,501

Cost Share: $1,429,950

Content last updated: May 2017

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Mladen Kezunovic
Principal Investigator
Texas A&M University
979-845-7509
kezunov@ece.tamu.edu

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

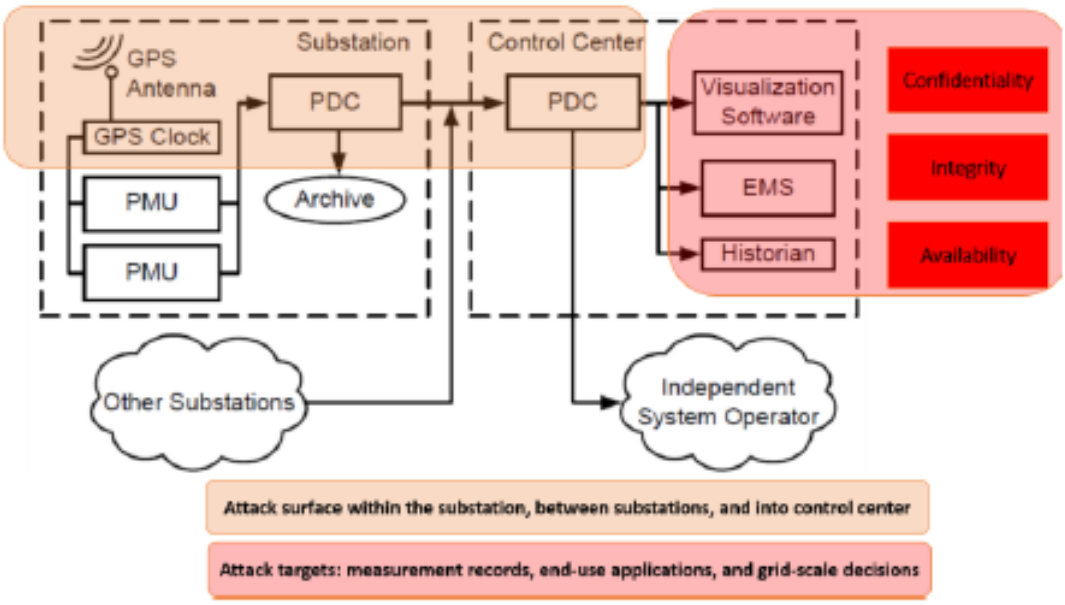

Figure 1: Timing intrusion attacks impact on applications

Tasks

The recipient has assembled a multidisciplinary team of experts from different disciplines, including power systems, computer science and communication, as well as experts in cybersecurity and synchrophasor applications, to solve the interdisciplinary problem of signal timing security.

Phase 1: R&D
Task 1: Specify requirements

The team will research requirements for cybersecurity measures that will be developed to strengthen cybersecurity for power grid synchrophasor systems.

Task 2: Develop timing intrusion detection modules

The modules will handle GNSS receivers, distribution of GNSS clock signals, PMUs, PDCs, networking and power system applications.

Task 3: Technology demonstration

The team will integrate the technology transfer from the R&D environment into the demonstration environment that closely reflects real-world conditions. The team will work with the electric utility and some selected industry vendor partners to gather key end-user feedback that supports commercialization and outreach efforts.

Phase 2: System Field Demonstration

Key components of the test approach are:

- Test architecture specification and software/hardware implementation
- Measurement and evaluation infrastructure set-up
- Deployment of detection modules
- Implementation of use cases for solution field evaluation and demonstration
- Solution evaluation and assessment reporting

Anticipated Results

Project results will include the following:

- Reference models for integrity checks of GNSS time distribution, PMU measurement accuracy, network protocol and message integrity, and application performance integrity
- Software and hardware solutions to detect timing intrusions of synchrophasor systems under adversary attacks
- Advanced testbed and field evaluations that will assure feasibility and eventual commercial deployment of proposed solutions
- Definition of attack surfaces, attack targets and attack vectors for the timing intrusion in the synchrophasor systems
- Risk-based evaluation methodology and metrics that will allow assessment of the effectiveness and cost benefits of the proposed solutions