U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

A Resilient Self-Healing Cyber Security Framework for Power Grid

Develop an attack-resilient Wide-Area Monitoring, Protection, and Control framework to help prevent and mitigate cyber-attacks

Background

The energy sector's *Roadmap to Achieve Energy Delivery Systems* envisions resilient energy delivery systems that are able to survive a cyber incident while sustaining critical functions. The research partnership described here is advancing methods to help detect and mitigate malicious cyber events which will further strengthen power grid cyber-resiliency.

Objectives

The objective of this research partnership is to develop an attack-resilient framework and associated algorithms to help secure the grid against cyber-attacks. This includes:

- Develop a self-healing Phasor Measurement Unit (PMU) network infrastructure
- Develop bad data detection and attack-resiliency methods for the State Estimation (SE) algorithm
- Develop anomaly detection and attack-resilient control methods for the Automatic Generation Control (AGC)
- Develop anomaly detection and resilience methods for wide-area protection schemes - Remedial Action Schemes (RAS)
- Develop model-based anomaly detection methods for the Optimal Power Flow (OPF) algorithm
- Implement and evaluate the effectiveness of the proposed anomaly detection and attack resiliency methods/algorithms on a realistic CPS Security Test bed

Project Description

The team will identify cyber-attack issues by researching and evaluating the attack model and attack vectors, perform an impact analysis, develop an attack mitigation framework and then evaluate the proposed solutions in the areas of monitoring and controls to formulate a workable protection solution.

For each of the Wide Area Monitoring Protection and Control (WAMPAC) applications (SE, AGC, RAS, OPF) the lessons learned from this research will be applied to the development of attack-resilient and self-healing attributes of the respective applications.

Benefits

- Will lay a scientific foundation for more secure and attack-resilient Wide-Area Monitoring, Protection, and Control (WAMPAC)
- In an evolving cyber threat landscape, the outcome of the project will have significant impacts on industrial practice now and in the future
- The PowerCyber testbed at ISU provides a realistic virtual infrastructure where experiments on distributed decision making in the smart grid environment can be performed

Partners

- Argonne National Laboratory (ANL) (lead)
- Pacific Northwest National Laboratory
- Iowa State University (ISU)
- Illinois Institute of Technology
- RTDS Technologies
- OPAL_RT Technologies

Period of Performance

March 2015 – February 2017

Total Project Cost

$2,000,000

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) 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 energy disruptions due to cyber-attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Jianhui Wang
Principal Investigator
Argonne National Laboratory
630-252-1474
jianhui.wang@anl.gov

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net

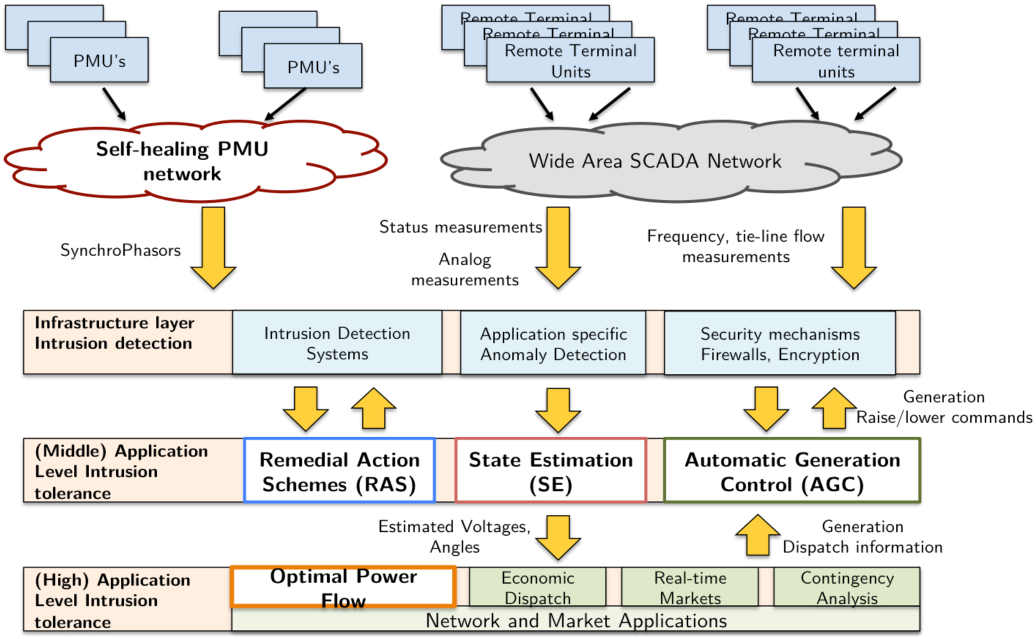
PMU's
PMU's
Remote Terminal
Remote Terminal
Remote Terminal Units
Remote Terminal
Remote Terminal
Remote terminal units
Self-healing PMU network
Wide Area SCADA Network
SynchroPhasors
Status measurements
Analog measurements
Frequency, tie-line flow measurements
Infrastructure layer Intrusion detection
Intrusion Detection Systems
Application specific Anomaly Detection
Security mechanisms Firewalls, Encryption
Generation Raise/lower commands
(Middle) Application Level Intrusion tolerance
Remedial Action Schemes (RAS)
State Estimation (SE)
Automatic Generation Control (AGC)
Estimated Voltages, Angles
Generation Dispatch information
(High) Application Level Intrusion tolerance
Optimal Power Flow
Economic Dispatch
Real-time Markets
Contingency Analysis
Network and Market Applications

Figure 1: Proposed resilient self-healing CPS security framework for WAMPAC

Technical Approach

This project will design a multi-layered defense architecture (defense-in-depth) with representative applications in wide-area monitoring, protection and control. At the application level, design will include increasingly attack-resilient algorithms. Elements will be tested on a PowerCyber testbed. Layered defense components include:

Infrastructure Layer Resilience

Identify (1) critical and non-critical systems and network connections; (2) systems with redundant communications and devices; and (3) trust reduction models to mask attack impacts.

Application Layer Resilience

Design increasingly attack-resilient algorithms to minimize the occurrence of undesirable incidents, minimize the impact so that the system returns to normal within a short time.

Phasor Measurement unit (PMU) Resilience

Minimize the risk by disabling known compromised PMUs and PMUs that are likely to become compromised due to propagation of the cyber-attacks, while keeping the power system observable.

State Estimation (SE) Resilience

Strategy is based on the concept of adding more redundancy in measurements. Propose the deployment of PMUs at strategic locations as a potential solution to the problem of data injections and topology manipulations.

Automatic Generation Control (AGC) Resilience

Anomaly detection algorithms compare real-time operation to a model that characterizes normal behavior in order to identify anomalies with the Area Control Error (ACE) forecast including an attacker manipulating frequency and tie-line measurements.

Optimal Power Flow (OPF) Resilience

Develop an algorithm that uses Principal Component Analysis (PCA) to determine whether input data passed to the OPF software module has been contaminated by cyber-attacks.

End Results

Project results will include the following:

- The impact of the proposed research will lay a scientific foundation for attack resilient WAMPAC through the development of innovative models, algorithms, and tools for attack/anomaly detection, attack mitigation, and attack resilience for the electric power grid that incorporates both cyber and physical system properties
- The outcome of the project will have significant impacts in industrial practice through suitable adoption of the proposed attack-resilient WAMPAC framework that articulates application-level security to complement cyber infrastructure security to realize a defense-in-depth approach for the future grid
- The transformative nature of the research will have profound impacts in developing a scientific foundation and operational algorithms/strategies to transform the “fault-resilient grid” (N-1 contingency) of today to an “attack-resilient grid” of the future