Timing Intrusion Management Ensuring Resiliency (TIMER)

Funded by DOE through the Office of Electricity Delivery and Energy Reliability's Cybersecurity of Energy Delivery Systems (CEDS) Program

Topic Area 1: Detect Adversarial Manipulation of Energy Delivery Systems Components

Project Summary

The project director/principal investigator(s): Dr. Mladen Kezunovic, (Project Director and PI, ECE, TAMU); Dr. Steven Liu (CSE, TAMU) and Dr. Alex. Sprintson (ECE, TAMU), Michael Mylrea, Jeff Dagle, Paul Skare, Chris Bonebrake, Dr. Mark Rice (Pacific Northwest National Laboratory (PNNL)), Dr. Milorad Papic (Idaho Power Company (IPC)), Dr. Manu Parashar and Dr. Jay Giri (Alstom/General Electric (Alstom/GE))

Total cost of the project: $4,429,451

Project duration: 3 years starting in September 2016

The objectives of the project: Following the Northeastern power grid blackout of August 14, 2003 that affected over 50 million people and resulted in an economic loss of billions of dollars, government and industry were tasked to develop the next generation control infrastructure for the electricity grid for the 21st century. Over $4 billion was invested through the American Recovery and Reinvestment Act (ARRA) of 2009 alone to address this national challenge, along with additional investments from the private sector (investor owned utilities),by developing and deploying synchrophasor systems nationally. Currently there are close to 2000 phasor measurement units (PMUs) that feed the synchrophasor systems installed in the East, West and Texas grid interconnections. Such systems provide superior control capabilities over the legacy Energy Management Systems (EMS) with Supervisory Control and Data Acquisition (SCADA) front-end due to their high sampling rate and time-correlated measurements using timing signals from the Global Positioning System (GPS) of satellites. The vulnerability of such systems to an inaccuracy due to a compromised GPS timing signal or intentionally induced latency associated with the synchrophasor measurement transmission has been a major concern. To be able to deploy such solutions in industry, new approaches to detect timing signal intrusions in the synchrophasor system will need to be developed. The key research focus of this proposal is to develop detection methods and tools to manage timing signal intrusions to assure resiliency of the synchrophasor and legacy EMS solutions. The research and development component of this study requires expertise in the impact of timing intrusions on GPS and the resultant inaccuracies on synchrophasor applications, as well as on timing inaccuracies in the control and communication parts of the synchrophasor end-to-end solution. The proposed large-scale testbed and field demonstration evaluations are needed to enable assessment of the benefits and impacts of such sophisticated timing intrusion management methods.

The project ***objective*** is to assemble a multidisciplinary team of experts from TEES coming from different disciplines, including power systems (Kezunovic), computer science (Liu) and communication (Sprintson), as well as experts in cybersecurity and synchrophasor applications from PNNL, to collaborate and use the combined knowledge to solve this interdisciplinary problem in a synergistic way. A team of industry partners, IPC and Alstom/GE, will facilitate implementation of an end-to-end solution to the timing intrusion attacks to illustrate the benefits. This evaluation approach using large-scale deployment is needed to convince the industry that the proposed timing detection intrusion methods are assuring resiliency of trustworthiness in synchrophasor systems. A focused commercialization effort will be pursued by the Alstom/GE team to promote the results of this project and assure they are widely known and eventually used by the industry. The project will employ close to a dozen graduate students assuring the workforce development for future industry needs is also well supported.

Description of the project:

a) Methods to be employed. To detect timing intrusions, the project deploys powerful and distinctively innovative methods:

- The Injection of known waveforms enabling the end-to-end synchrophasor solution testing and calibration of the timing requirements by deploying Use Cases for type and application test,
- The computational methods for calculating GPS reference signals using the Order of Pseudorange (OOP) of Global Positioning System (GPS) signals, and
- The data mining and statistical methods for tracking communication traffic patterns that can reveal subtle timing intrusion attacks on computational nodes and communication links.

The newly developed timing intrusion modules (TIMs) will also be supported with advanced implementation of execution scheduling methods to insure scalable and interoperable deployment.

b) The potential impact of the project (i.e., benefits, outcomes). This project is expected to provide multiple outcomes and associated benefits:

- Software and hardware solutions to detect timing intrusions that will enhance resiliency of synchrophasor systems under adversary attacks,
- Advanced testbed and field evaluations that will assure feasibility and eventual commercial deployment of proposed solutions, and
- Risk-based evaluation methodology and metrics that will allow assessment of the effectiveness and cost benefits of the proposed solutions.

c) Major participants (for collaborative projects). The proposed multidisciplinary team is a collaborative effort between TEES, PNNL, IPC and Alstom/GE. The expertize provided by the individual organizations spans several important disciplines and individual contributions:

- *TEES team*: It will provide project leadership and expertize needed to develop hardware and software solutions for TIMs. The team PI (Project Director) has prior experience in leading large-scale projects for over 30 years. He has also demonstrated extensive industry experience through 25 years of private consulting practice serving the needs of over 50 companies world-wide. His R&D portfolio over the last 30 years totals over o $30 million, including a recent successfully completed $5.5 million ARPA-E project with over half a dozen participating organizations with 30 researchers. The rest of the TEES team are senior faulty with an extensive record of prior research funding from NSF, industry and government agencies. The team will be supplemented with close to a dozen senior graduate students trained with very advanced research and implementation skills.
- *PNNL team*: It consists of half a dozen individuals with very diverse backgrounds, ranging from synchrophasor systems, testbed implementations, cybersecurity solutions and practical industry applications. The team will be led and coordinated by a project manager with extensive experience in DOE projects. The PNNL's DOE R&D portfolio spans dozens of successful projects with practical impacts.
- *IPC team*: It will be led by a Senior Application Engineer with a strong background in reliability and resiliency and possessing both theoretical and practical skills. This engineer will be assisted by a technical and management team that has a strong, vested interest in the outcomes of the project.
- *Alstom/GE team*: It will consist of several senior engineers and two Lead Engineers, one with wide expertise in EMS and Synchrophasor deployments, and one with new product development expertise who will be responsible for the implementation and commercial efforts respectively.

The project success will be assured through various testing and evaluation stages made possible with an extensive large-scale testbed infrastructure available at TEES and PNNL, as well as real life field demonstrations to be hosted by IPC. A Formal metrics will be implemented to quantify the benefits.