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

Tempus Project

A time synchronization platform to protect energy delivery systems from GPS-based attacks

Background

The energy sector utilizes Global Positioning System (GPS) based clock devices to provide a common time reference to Intelligent Electronic Devices (IEDs) that monitor, control, and protect power systems. For example, synchrophasors that are used for wide area monitoring, providing unprecedented visibility into grid operations across wide geographical regions, require time synchronization to be within 1µs. In future years, synchrophasors could inform the IED to be used for control and protection, in addition to their use today for situational awareness.

GPS-based receivers may be susceptible to signal loss, jamming, and signal spoofing. GPS jamming and spoofing are deliberate denial-of-service and counterfeit signal generation attacks that adversely impact the end applications using this technology. A GPS spoofing attack generates signals that closely mimic the authentic GPS signals and transmits them at a slightly higher power. The GPS receiver inside the GPS clock locks to the counterfeit signal and continues to operate without any alerts to the user.

Objectives

As part of the Tempus project, SEL plans to develop and demonstrate a comprehensive solution for detecting spoofing attacks and defending GPS-based systems. The project will include the development of innovative algorithms and electronics that detect GPS signal manipulation for critical applications that use timing signals in the energy sector.

Project Description

SEL will research, develop and demonstrate the capabilities of a secure, modular, and customizable time synchronization platform that provides layers of protection from GPS spoofing attacks. The secure GPS clock product will have the configurability and flexibility to receive multiple time and frequency input signals from diverse sources. These time sources will be satellite, time, and frequency signals from local and wide area networks. Multi-constellation receiver technology will be developed as part of this project along with slow signal spoof detection algorithms. By applying advanced signal processing algorithms and voting schemes, the manipulation or counterfeit attacks on the time signals will be detected and mitigated. Once the GPS spoofing attack is detected, the secure GPS clock will fall back to a trusted, reliable time source, thereby protecting the end devices from the spoofing attack.

Visualization tools for the time synchronization platform will be developed to provide for configuration and management, including role-based access control, user authentication, and password management. Additionally, these tools will provide the health and status of satellite, time, and frequency inputs and outputs, so that users can maintain continuous, real-time situational awareness of the cybersecurity state, and perform pre- and post-event analysis.

Benefits

- GPS spoof resilience will allow critical energy delivery infrastructure to operate efficiently under adversarial conditions like GPS signal loss and manipulation.
- Auto failover to a trusted time source under GPS spoofing attack

Partners

- Schweitzer Engineering Laboratories (lead)
- Bonneville Power Administration (BPA)

Period of Performance

November 2016 – November 2019

Total Project Cost

Total: $4,334,557

Federal: $3,424,056

Cost Share: $910,501

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

Dan Rippon
Principal Investigator
Schweitzer Engineering Laboratories
509-338-4399
dan_rippon@selinc.com

Current Contact as of Aug. 2020

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

Figure 1. SEL EMC, Environmental, and Mechanical Design Verification Test Facility

GPS Clock Platform Features

- Identification and logging of the GPS spoofing event and other signal anomalies for post event analysis
- Auto failover to a trusted time source under GPS spoofing attack
- Configurability to select sensitivity thresholds and the response times for GPS spoofing attacks based on critical application need, such as PMUs and protective relays
- Flexibility to configure and support diverse time code and frequency inputs/outputs from local and wide area networks
- Multi-constellation timing receiver technology
- Multiple holdover oscillator options like Temperature Compensated Crystal Oscillator (TCXO), oven-controlled crystal oscillator (OCXO), and Cesium to provide accurate time signals to end devices during GPS spoofing attack or signal loss
- Centralized Logging, Password Management, and User Authentication

Demonstration Approach

The Tempus project team will perform all the functional testing at SEL. The team will work with project partner Bonneville Power Administration (BPA) to perform laboratory testing with devices utilizing GPS-based timing signals for specific applications to validate the product. Then, the team will perform field testing at a selected BPA site. The project team will monitor the performance of the secure GPS clock and the end devices under a variety of test conditions to ensure the product will operate as expected when deployed at a wide scale in the energy sector.

Anticipated Results

Project results will include the following:

- Cyber-secure time synchronization platform for critical substation applications, with automatic fail-over to a trusted time source in the event of GPS spoofing
- Identification and logging of the GPS spoofing event and other signal anomalies for post event analysis
- Multi-constellation timing receiver technology