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

Timing Authentication Secured by Quantum Correlations (TASQC)

Developing terrestrial, wireless, authenticated, precise timing distribution system to energy grid devices

Background

Phasor measurement units and data concentrators have brought unprecedented visibility into real-time grid operations. Data collected from across the grid must be time-synchronized to facilitate combining data from separate sources to perform analysis like state estimation. GPS offers widely broadcast, highly accurate timing signals, but GPS signals can be easily spoofed in part because they lack authentication for the source of the signals.

A ground-based alternative that delivers accurate timing signals with authentication could be used for a variety of increasingly sophisticated protocols. Quantum Key Distribution (QKD) systems have been developed that can ensure secure basis for encryption between two or more communicators, but an integrated system is needed to make use of the quantum keys for authentication and communication tasks for grid devices that lack dedicated optical fiber connections.

Objectives

- Without relying on GPS signals, utilities will be able to establish complete end-to-end control of security for time-sensitive data
- Offer the improved security afforded by the techniques of quantum communication through a relatively modest infrastructure
- Support a suite of increasingly secure timing protocols and a wide range of authenticated communication tasks

Project Description

The TASQC project is developing a system of ground-based timing and communication beacons featuring security that is enhanced by geographically distributed quantum correlations and that takes full advantage of the direction of information flow for power systems management. Unlike GPS-based timing schemes, this new system will feature transmitted timing signals that are *a priori* unknown, making them appear truly random to an eavesdropper and very difficult to spoof. In addition, the signals will include quantum correlations that will provide several avenues for authenticating not only the timing signals, but also power systems data (e.g., sent from a PMU to a substation) and other communications tasks.

Benefits

- Brings security of quantum key distribution to broadcast topology
- Gives utility control and ownership of the time distribution capability that their PMUs and other SCADA systems depend on
- Supports authentication of crucial grid data making data more trustworthy and allowing decisions to be made with confidence
- Provides flexible infrastructure that could apply to multiple types of communication and messaging protocols
- Industry Advisory Board ensures technical relevance and smooth transition from research concept to proof-of-principle system

Partners

- Oak Ridge National Laboratory (lead)
- Pacific Northwest National Laboratory
- Sandia National Laboratory
- University of Texas at Austin
- Qubitekk

Period of Performance

October 2014 – September 2020

Total Project Cost

$2,998,061

Content last updated: May 2016

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

Phil Evans
Principal Investigator
Oak Ridge National Laboratory
865-576-9447
evanspg@ornl.gov

Current Contact as of Aug. 2020

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

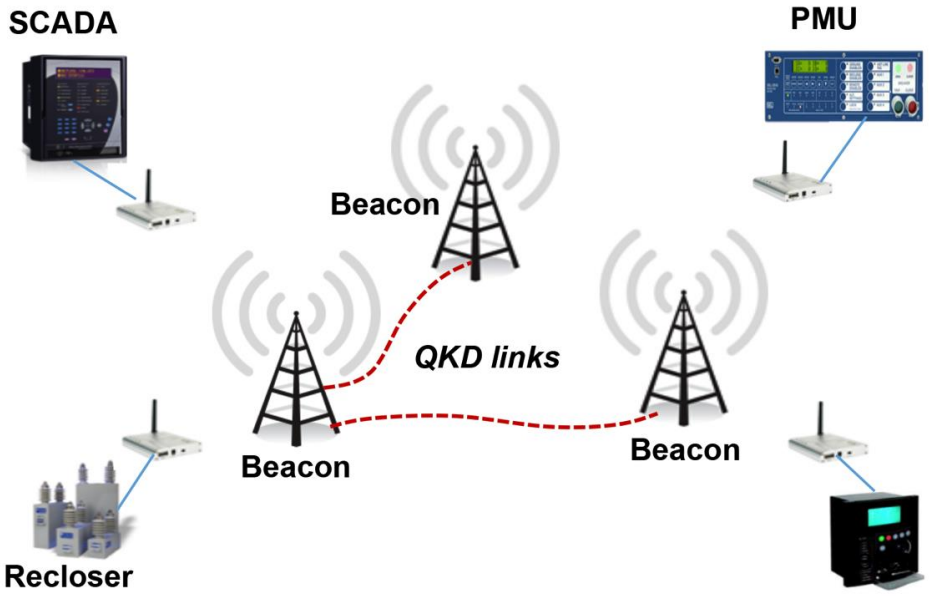

Figure 1: Model timing signal distribution network, facilitated by quantum key distribution among the signal beacons.

Technical Approach

The TASQC project will develop a quantum-agnostic system, integrated with wireless technologies, to securely distribute time to grid devices. The project is developing the quantum backbone link, the wireless transmitters and receivers, and the security algorithms and protocols that compose this system in three tasks.

Phase 1: Develop Prototype System

- Develop a prototype system consisting of two wireless transmitting beacons and a quantum link between them as well as a wireless receiver and test-bed
- Implement Quantum Key Distribution system and base protocol to disseminate timing signals
- Communicate with utilities and power systems community to solicit feedback on industry needs

Phase 2: Develop and Test Protocols

- Develop and test a suite of protocols to address security vulnerabilities. The suite extends beyond the base protocol implemented in Phase 1 and is guided by industry.
- Refine system performance metrics and characterize the ease of implementation for each protocol
- Demonstrate integration of other QKD systems within the TASQC platform.

Phase 3: Refine and Enhance Hardware

- Improve the performance and extend the capabilities of the prototype system built in Phase 1.
- Communicate with the power systems community to ascertain cybersecurity needs and assess industry impact for trusted-node or multi-beacon systems.

Project Results

Project results will include the following:

- TASQC base system for broadcasting quantum-correlated and authenticated timing signals from multiple discrete locations
- Suite of protocols tested and validated for secure execution on the TASQC system
- Demonstration of the TASQC system at an industry demonstration facility