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

Distribution Grid Timing Spoofing Detection and Mitigation with Collaborative Autonomy

Lawrence Livermore National Laboratory (LLNL)

Colin Ponce

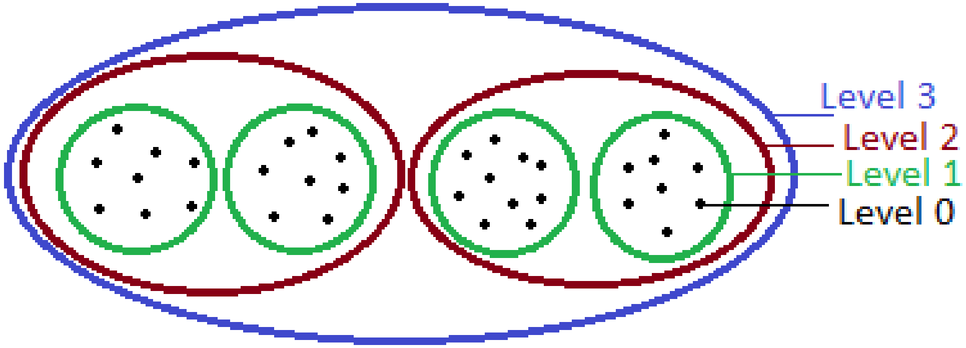
Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Distribution Grid Timing Spoofing Detection

Objective

- Develop collaborative autonomy-based hierarchical anomaly detection technology to detect timing spoofing attacks in the power distribution grid.



Schedule

- 5/2018 – 5/2021
- Key deliverables
  Hierarchical anomaly detection technology (May 2019); Mitigation strategy for an attack scenario (Oct 2019); 2 conference papers on detection and mitigation (Oct 2020); Live demonstration and facilitate tech transition (May 2021)
- Expected Capability
  Ability to detect timing spoofing attacks in distribution grid and to mitigate the effects for a given application

Total Value of Award:	**$ 2.4M (no cost share)**
Funds Expended to Date:	**9%**
Performer:	**LLNL**
Partners:	**Power Standards Lab**

Strategy for a resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection (MMATR)	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Strategy for a resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection (MMATR)	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Advancing the State of the Art (SOA)

Current State of the Art:

- GPS spoofing detection studied in academic literature
- Work is being done on secure GPS clocks that can detect and mitigate GPS spoofing attacks for the transmission grid.
- **However** these solutions typically too expensive for distribution grid equipment.

Our Approach:

- **Hierarchical anomaly detection** allows us to detect GPS (or other timing) spoofing attacks using data and equipment already available.
  - Data from distribution-level GPS clocks, microPMUs, smart meters, etc.
- Collaborative autonomy enables us to perform the analysis right at the sensing devices—more **secure** and **faster.**
- Will develop a mitigation for a chosen distribution-level application.
  - Allows utilities to **respond** during an attack.
- Utility and vendor interaction throughout facilitates commercialization of technology.

Challenges to Success

Challenge 1: Realistic testing

- Testing at multiple levels of fidelity.
  - in simulation, in laboratory, onsite with partner utility.

Challenge 2: Collecting data streams for prototyping

- Anomaly detection techniques can work with many types of data streams.
- Use simulation to demonstrate the effects of streams not attainable in prototyping.

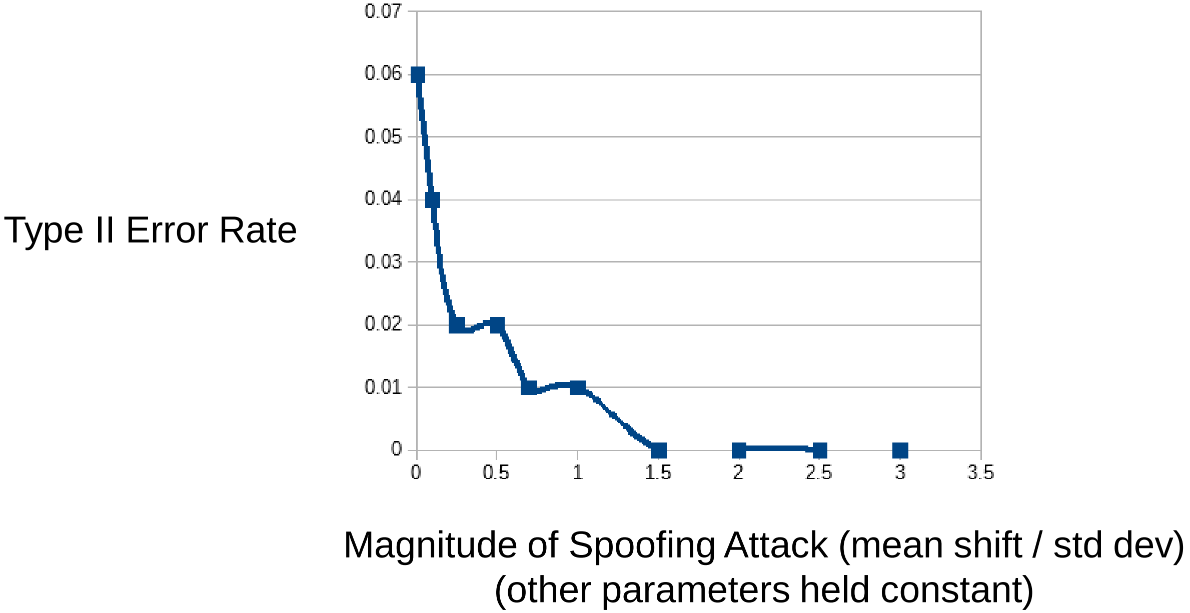
Challenge 3: Commercial expertise with developed software

- Regular interaction with utility and vendor
- Providing expertise and documentation to facilitate adoption

Progress to Date

Major Accomplishments

- Developed hierarchical anomaly detection approach to detecting timing spoofing attacks.
- Demonstrated validity of detection approach in simplified setting.



Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- **Targeted end users**
  - Utilities, vendors of distribution grid equipment.
- **Plans for industry acceptance**
  - o Partners include targeted end users
  - o Development of open-source software
  - o Publications in key conferences
  - o Working with partners to commercialize product

Next Steps for this Project

Approach for the next year

- Develop co-simulation platform for simulation and testing anomaly detection.
- Develop collaborative autonomy software on which to build anomaly detection technology.
- Implement hierarchical anomaly detection with collaborative autonomy.
- Full demonstration of hierarchical anomaly detection in simulation.

Collaborative Autonomy

Setting: Many low-powered, *unreliable* devices, spread out over a wide area, connected by some communications infrastructure.

An approach to computation and control that is

- Decentralized
- Real-time
- High reliability

Example algorithm:

Alternating direction method of multipliers (ADMM)

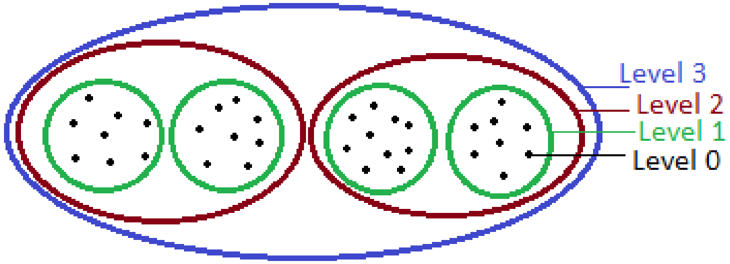
Hierarchical Anomaly Detection

Two phases:

I. Initialization Period

1. Collect data on all devices.
2. Compute expected behavior for data streams.
3. Compress data and send up to the next level.
4. Repeat 2-3 at each level of the hierarchy.

-Assume no spoofing is occurring.



Source: https://www.tutorialspoint.com/ims_db/images/hierarchies.png

II. Streaming anomaly detection

1. Collect data on all devices.
2. Single-level anomaly detection against initialized expectations.
3. Flag anomalies if found.
4. Compress data and send to the next level.
5. Repeat 2-4 at each level of the hierarchy.