GMLC Project Communications Summary

Date:10/31/2019
Project Title: Threat Detection and Response with Data Analytics
Project Number: 1.4.23
Principal Investigator: Jovana Helms
Person Completing this Document: Jovana Helms, Sean Peisert, Adrian Chavez, Sid Siddharth

1. What problem is the project solving or what opportunity is it addressing?
   This project is developing analytics for different data sources on the distribution grid to identify and detect complex cyber threats. The specific data considered within this project were smart meter data, inverter data, building to grid transaction data and ethernet gateway data.

2. Who collaborated on this project? (e.g. labs, universities, utilities, vendors, others)
   LLNL, LBNL, SNL, PNNL (initially ORNL and INL but the project was rescoped in it's second year and ORNL and INL were not part of the continuation), SEL, Austin Energy, Pecan Street, EPB, Johnson Controls
3. What is the solution or outcome that the project delivered?
   The project delivered various analytics specific to data source analyzed. For each dataset, a baseline operation profile has been developed that can be used to detect anomalous behavior, as well as potential impacts of cyber attacks that can result from an attack to the respective part of the system (i.e smart meters, inverters, building to grid transactions)
4. How does the solution/outcome break new ground or how is it differentiated from other R&D projects?
   To the best of our knowledge this is the first project that looked at 4 separate data sets on the distribution grid and developed analytics and tested them in simulation and lab setting to identify impacts and potential for detection of cyber attacks.
5. How is the deliverable or outcome of the project being used?

This project set the foundation for Digital Twin Reinforcement Learning proposed and funded through GMI in 2019. The project demonstrated how different component of the distribution system can be used to cause broader impacts via cyber means. Work performed by LBNL lays the groundwork for the development of controllers capable of re-dispatching inverter voltage regulation function settings to mitigate cyber attacks on DER systems. While the research performed in this project was low TRL to be transferred to industry partners at the end of the project, significant progress was made that can be leveraged in the future.

6. Impact metrics – has project impacted grid modernization in any quantifiable way? (E.g. reliability, resiliency, efficiency, DER integration, event response, etc.)
   This project was aimed at improving grid resiliency, security and enable event response in case of cyber attacks. Work performed at LBNL is aimed at enabling automated response by solar inverters in case a disruptive event, such as cyber attack, is detected.
7. What IP and/or industry recognition or adoption has the project resulted in?
   - James Obert, Adrian Chavez, Jay Johnson, “Distributed Renewable Energy Resource Trust Metrics and Secure Routing”, Computers & Security Journal 88 101620, Elsevier, 2019.
   - James Obert, Adrian Chavez, “Graph-based Event Classification in Grid Security Gateways”, IEEE Artificial Intelligence for Industries Conference, 2019.
   - James Obert, Adrian Chavez, Jay Johnson, “Behavioral Based Trust Metrics and the Smart Grid”, The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2018.
   - Daniel Arnold, Shammya Saha, Ciaran Roberts, Anna Scaglione, Nathan G. Johnson, and Sean Peisert, “Adaptive Control of Smart Inverters for Distribution Grid Cybersecurity”, submitted to IEEE Transactions on Power Systems
   - Sridhar S., A. Ashok, M.E. Mylrea, S. Pal, M.J. Rice, and S.G. Gourisetti. 2017. "A Testbed Environment for Buildings-to-Grid Cyber Resilience Research and Development." In Resilience Week (RWS 2017), September 18-22, 2017, Wilmington, Deleware, 12-17. Piscataway, New Jersey:IEEE. PNNL-SA-126405. doi:10.1109/RWEEK.2017.8088641
   - Pal S., S. Biswas, S. Sridhar, A. Ashok, J. Hansen, and V.C. Amatya. 2018. "Understanding Impacts of Data Integrity Attacks on Transactive Control Systems." In IEEE ISGT NA 2020. PNNL-SA-138041

- Nur N., S. Sridhar, S. Pal, A. Ashok, and V.C. Amatya. 2019. "A Clustering Approach for Consumer Baselining and Anomaly Detection in Transactive Control." In International Workshop on Applied Machine Learning for Intelligent Energy Systems (AMLIES). PNNL-SA-139353.
- Chellappan, K., Rivera-Soto, R. “Framework for Unsupervised Anomaly Detection on Smart Meter Data”, submitted for publication

8. If you look ahead 5-10 years, how do you see the work of this project impacting grid planning and operations in the U.S.?

   Analytics developed in this project can be a foundation for detection and response algorithms deployed across the distribution system. The baseline of normal behavior can be used by industry and operators to understand when their system is outside of normal parameters. Identified impacts of cyber attacks to the distribution system is providing valuable information to the operators on how their system might be affected and what is the severity of impacts they could expect to see in the event of cyber attack. Additional research is needed to account for the full complexity of the system and enable data fusion across the data from various components to enable detection of sophisticated cyber threats.