Supporting Security with Advanced Multimodal Grid Data Analytics

Website: http://cred-c.org/researchactivity/analytics

Researchers (ASU): Anna Scaglione, Teklemariam Tesfay

Industry Collaboration: This research benefits from the close collaboration of the industry partners and utilities. The main collaborators are:

- Power Standards Lab (PSL)
- Riverside Public Utilities (RPU)
- Electric Power Research Institute (EPRI)
- EnerNex LLC Engineering Consultant
- OSIsoft

The work in thread 1 overlaps with the DOE-Lawrence Berkeley Laboratory grant DE-AC02-05CH11231 (2015-2017) ($200,000) "LBNL/CEDS - Supporting Cyber Security of Power Distribution Systems by Detecting Difference between Real-Time Micro-Synchrophasor Measurements and Cyber-Reported SCADA." The work in thread 2 complements this and other activities in CREDC that make use of PMU readings, particularly for distribution grids.

Description of research activity:

Cyber-Physical Intrusion Detection Incorporating µPMU Measurements in Automated Distribution Systems: Assuring the Automated Distribution System (ADS) communication security is of utmost importance, especially for those applications that are time- and function-critical, and usually relate to expensive infrastructures. Considering the fact that the protocols used in this network are not secure, our idea is to introduce a Grid Security System (GSS) that extends the established cyber security notion of Network Intrusion Detection Systems (NIDSs) to comprise physical reliability metrics and leverage new sensing modalities.

An important feature of our GSS architecture is that it leverages emerging low-cost, Micro-Synchrophasor (µPMU) technology. µPMUs are synchronized, fast-sampling devices, developed to do real-time measurements in the distribution grid. Our GSS architecture is hierarchical, and the NIDS processing correlates different data sources including the µPMU data, and the monitored Distribution SCADA communication packets, which contain the physical and cyber data that are used in the control of the ADS.

The security policies are translated into mechanisms using the BRO framework, and implemented hierarchically as shown in Fig. 1. This would be the first time that BRO rules comprehend full knowledge of the physics of the physical infrastructure. The stage-1 servers are placed next to each µPMU and network tap, and are responsible for finding the anomalies in the functions of voltage and current phasor. The higher stages correlate an increasing amount of sensor information and prior information about the system and inspect for the anomaly and source of the anomaly.

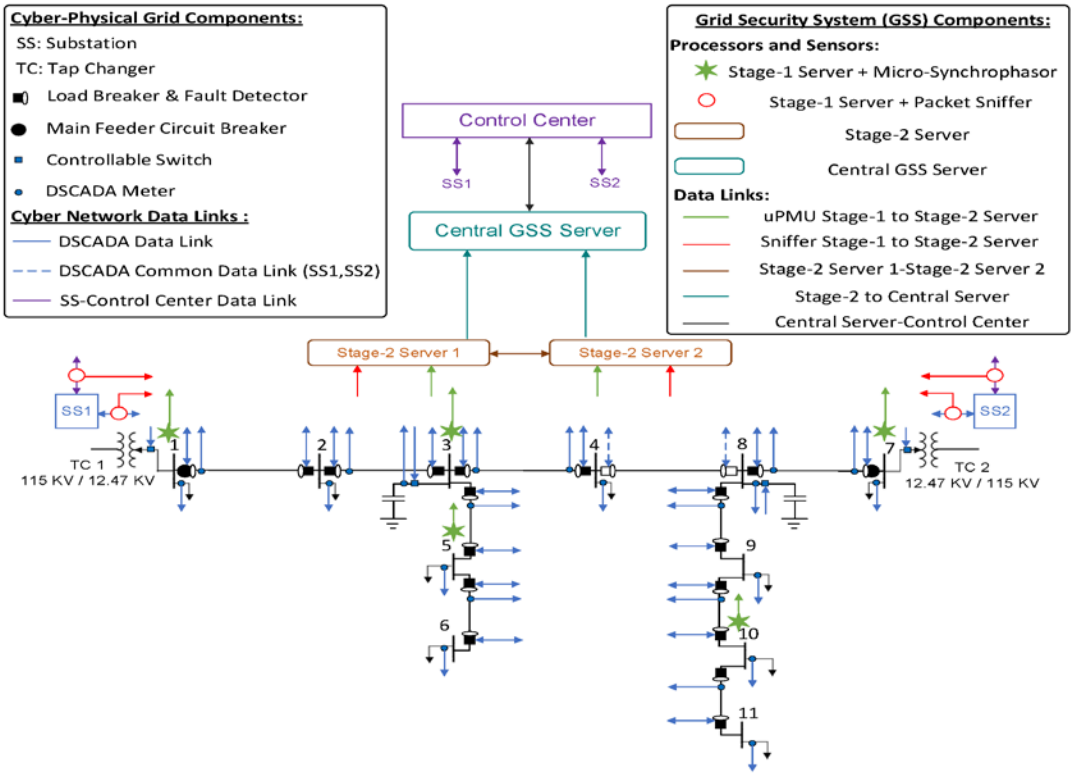

Fig. 1 Envisioned Automated Distribution System Equipped with Grid Security System

Addressing Data Quality Challenges and Forensic Analysis of Power Grid Measurements to Support Cyber-Physical Security: Having µPMU devices as a critical component in our other thread, we have observed that data quality issues arising due to noise or erroneous current and voltage transformers can lead to incorrect readings. We therefore decided to pursue a thread in this activity that deals with the data quality issues affecting the analytics that are developed to monitor the security status of the grid. However, this thread is not just limited to this issue. We also wish to extend the notion of "non-intrusive load monitoring (NILM)" algorithms for the forensic analysis of µPMU signals. The NILM algorithm disaggregates the signals in individual components that are traced back to the specific load activities in the grid. The objective of this analysis from a defender perspective, is to discriminate between normal and abnormal activities at the feeder by classifying the unique local features of the AC power signal associated to specific events and uses. We will test this idea using the current and voltage phasor measurements that are feeding into a computer server.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity directly aims to create automated mechanisms to "assess and monitor risk" at the level of electric power distribution networks, by using high resolution sensors, knowledge of the interactions of the cyber and physical realms, and a data management architecture designed to respond in real time and, thus help "manage cyber-incidents" promptly.

Summary of EDS gap analysis: We have identified gaps in lack of visibility to critical events in distribution automation systems, as well as data quality challenges to the use of grid measurements to support cyber security. This activity integrates high-resolution physical sensors, such as PMUs, into the reconnaissance of cyber-attacks into EDS, to enhance and complement the analysis of control area networks traffic. Rather than using model-free methods, our adaptive signal processing algorithms search for signatures by leveraging models based on system reliability principles and the law of physics so as to automate the detection, analysis and classification of the physical events and determine where and how cyber-assets may be compromised. Our sensor fusion architecture fully leverages distributed intelligence to be scalable to a large number of sensors and wide area collection deployment.

Full EDS gap analysis:

Cyber-Physical Intrusion Detection Incorporating µPMU Measurements in Automated Distribution Systems: In this thread, the main gap is the lack of visibility in distribution automation of events that could be caused by attacks and unreported failures of critical components, events that are difficult to detect by relying on a still evolving and not very advanced SCADA infrastructure. The common protocols that are being used (or under consideration for future use) in the monitoring and control network are not designed with security in mind [1]. In addition, the current security practices have proved to be insufficient, mainly because they are divorced from the physics of the grid [2]. In other words, there is a gap between security practices in the cyber world and the physical reliability that makes the current methods inadequate [3]. We desire to bridge the gap between the cyber and physical worlds by leveraging high-resolution measurements from micro-synchrophasor (µPMU) devices and defining cyber security mechanisms that analyze both cyber as well as physical signatures of attacks, enhancing the intrusion detection notion through these new sensing modalities.

The NESCOR scenarios [4, 5] are focused more on the intrusion methods for grid controllers and their potential consequences. Our analysis turns that around looking for a specific consequence that can be achieved by one or more cyber intrusion methods. They include the following from the NESCOR scenarios:

- DGM.1 Wireless Signals are Jammed to Disrupt Monitoring and Control
- DGM.2 Shared Communications Leveraged to Disrupt DMS Communications
- **DGM.3 Malicious Code Injected into Substation Equipment via Physical Access**
- **DGM.6 Spoofed Substation Field Devices Influence Automated Responses**
- **DGM.10 Switched Capacitor Banks are Manipulated to Degrade Power Quality**
- **DGM.12 Hijacked Substation Wireless Damages Substation Equipment**

We have started focusing on scenarios DGM.3, 6, 10, and 12, which appear to be more relevant when it comes to the use of physical measurement from µPMUs. DGM.6 prevents the DMS or operator seeing what is happening. DGM.3 allows for substation and feeder devices (scenario describes only substation – it should be augmented to include feeder pole-mounted controllers) to be reprogrammed for improper operation. DGM 10/12 describes the attacks necessary to operate load tap changer (LTC)'s and cap banks in a manner to cause physical damage.

Addressing Data Quality Challenges and Forensic Analysis of Power Grid Measurements to Support Cyber-Physical Security: DOE recognizes the importance of data analysis and forensics to be able to identify cyber-attacks [6]. Clearly, feeding bad quality measurements to the algorithms and analytics can have catastrophic consequences on the performance of the algorithms and analytics developed to support the cyber-physical security of the grid. However, by analyzing the quality of data being collected by µPMUs and performing forensic analysis on them, some of the NESCOR scenarios [4, 5] could have been detected and appropriate preventive actions could have been taken to protect the power system from damages.

In this thread, we aim to address this issue by identifying these consequences and propose some remedial actions to minimize the side effects of this issue on the analytics that are supposed to support the grid security. This thread however is not just limited to this issue. We would also consider extending the notion of "non-intrusive load monitoring (NILM)" for forensic analysis on the µPMU data to discriminate between the normal and abnormal regimes from an attacker and defender perspective.

Bibliography:

[1] J. Slay and M. Miller, Lessons learned from the maroochy water breach. Springer, 2008.

[2] A. A. Cardenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, “Attacks against process control systems: risk assessment, detection, and response,” in Proc. 6th ACM Symposium on Information, Computer and Communications Security, 2011, pp. 355–366.

[3] C. McParland, S. Peisert, and A. Scaglione, “Monitoring security of networked control systems: It’s the physics,” Security & Privacy, IEEE, vol. 12, no. 6, pp. 32–39, 2014.

[4] Lee, A. "Electric sector failure scenarios and impact analyses." National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute (EPRI), Palo Alto, California, Tech. Rep (2014).

[5] Jauhar, Sumeet, et al. "Model-based cybersecurity assessment with nescor smart grid failure scenarios." Dependable Computing (PRDC), 2015 IEEE 21st Pacific Rim International Symposium on. IEEE, 2015.

[6] D. Batz, et al. “Roadmap to achieve energy delivery systems cybersecurity”, Energy Sector Control Systems Working Group (ESCSWG), Washington, DC.