Towards Attack Resilient Data Analytics for Power Grid Operations

Website: http://cred-c.org/researchactivity/analytics4gridops

Researchers (OSU): Eduardo Cotilla-Sanchez, Jinsub Kim, Shashini De Silva, Travis Hagan

Industry Collaboration:

- Pacific Power
- Schweitzer Engineering Laboratories
- We are currently seeking additional collaborators from industry, power utilities, or national labs. Through collaboration, we hope to extend our robust learning framework to other interesting applications beyond microgrid control. Further, we would like an opportunity to test our idea with a testbed or real-life system. Contact Eduardo Cotilla-Sanchez to discuss how you can engage or collaborate with our research team.

Description of research activity: In order to make a power grid resilient to cyber attacks, it is necessary to assure that power system control and protection schemes can function properly to isolate faults, mitigate damage, and recover lost components, in the presence of an on-going attack. However, critical power system control and protection decisions such as microgrid islanding, relay tripping, and load shedding are inherently data-dependent, and they can be exploited by an adversary through data integrity attacks to produce malicious control decisions. The aforementioned applications are representative examples where compromised data may directly lead to malicious control actions, but countermeasures have not yet been developed. In this activity, we will fill this gap by developing novel data analytics for microgrid islanding, relay operation, and load shedding that are resilient to data integrity attacks. First, we will consider the problem of identifying stable islanding/reconnection timings for microgrids. Islanding or reconnection of a microgrid, if not done properly and under right conditions, can harm the stability of the grid. Existing techniques for determining stable islanding/reconnection timings rely on local measurements of the status of the points of common connections, but such techniques are prone to producing wrong results if the integrity of status measurements is compromised. An adversary might be able to exploit this vulnerability in his or her attempt to destabilize the grid by leveraging data integrity attacks. In this activity, we will develop a technique resilient to data integrity attack so as to predict stable islanding/ reconnection timings based on real-time PMU data. Second, we will develop resilient analytics that can advise reliable load shedding and relay operating schemes based on real-time PMU data, in the presence of a data integrity attack. Such a technique is essential for mitigating damages from contingencies induced by a cyber attack that may involve a data integrity attack. We envision that the developed techniques can be integrated into existing microgrid management and power system protection toolsets to enhance resiliency of grid operation to data integrity attacks. The outcome of the activity will help to achieve the 2011 DOE roadmap vision of resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
The activity is mainly concerned with developing data analytics for power system protection (*e.g.*, load shedding, relay tripping, microgrid islanding) that are resilient to data integrity attacks. Data integrity attacks can be carried out as part of a larger adversarial effort, and attack-resilient analytics for power system protection are needed to mitigate damage to the power grid in the event of cyber attacks, thereby reducing the associated risk. The outcome of the activity will help to achieve the 2011 DOE roadmap vision of resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Summary of EDS gap analysis: In the era of smart grid, the adoption of advanced data analytics is expected to aid decision making at a variety of operations in the power grid such as power system protection. Nevertheless, the potential impact of compromised data on grid operations has not yet been studied. In this activity, we aim to fill this gap

by investigating vulnerability of existing data analytics for power system protection and control and developing a resilient analytics that can advise operators with reliable decisions even in the presence of data integrity attack.

Full EDS gap analysis: In the era of smart grid, the adoption of advanced data analytics is expected to aid decision making at a variety of operations in the power grid, *e.g.*, power system protection. However, under a cyber attack on the power grid, data integrity can be compromised and such data analytics might be exploited by the adversary to disrupt grid operations. Nevertheless, the resiliency of power system analytics against data integrity attacks is not considered in practice for grid operations. In this activity, we aim to fill this gap by developing resilient data analytics to detect and mitigate the impact of compromised data on EDS operations.
The use of data analytics relying on real-time measurements such as data from phasor measurement units (PMUs) has been proposed more than a decade ago for power system control and protection, *e.g.,* protective relay control, load shedding, and subnetwork islanding [1-5]. The main motivation is to exploit real-time feedback information to improve performance of control strategies. Nevertheless, such approaches can lead to disastrous events under several cybersecurity failure scenarios of Wide Area Monitoring, Protection, and Control (WAMPAC) described in the NESCOR report [6]. For instance, PMU data can be compromised under the WAMPAC 2, 4, and 12 scenarios. In those failure scenarios, controllers advised by the analytics based on the compromised data can send out undesirable control commands. Most proposed security measures are focused on securing the integrity of PMU data [7, 8]. However, considering a variety of potential attacks on PMUs, including a simple GPS signal spoofing attack, it is risky to assume that PMU data integrity will never be compromised. To our knowledge, approaches to make the analytics for power system protection and control resilient to compromised data have not yet been considered.

Therefore, in the proposed activity, we aim to fill this gap by developing analytics resilient to compromised data such that the resilient analytics can advise operators with reliable protection and control options even under a failure of WAMPAC (WAMPAC 2, 4, or 12 scenarios.)

Bibliography:

[1] C. W. Taylor, D. C. Erickson, K. E. Martin, R. E. Wilson and V. Venkatasubramanian, “WACS-Wide-Area Stability and Voltage Control System: R&D and Online Demonstration,” in *Proceedings of the IEEE*, vol. 93, no. 5, pp. 892-906, May 2005.

[2] E. O. Schweitzer, D. Whitehead, G. Zweigle and K. G. Ravikumar, “Synchrophasor-based power system protection and control applications,” *2010 63rd Annual Conference for Protective Relay Engineers*, College Station, TX, 2010, pp. 1-10.

[3] J. O'Brien et al., "Use of synchrophasor measurements in protective relaying applications," *2014 67th Annual Conference for Protective Relay Engineers*, College Station, TX, 2014, pp. 23-29.

[4] F. Tang, J. M. Guerrero, J. C. Vasquez, D. Wu, and L. Meng, “Distributed active synchronization strategy for microgrid seamless reconnection to the grid under unbalance and harmonic distortion,” *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2757–2769, 2015.

[5] E. Alegria, T. Brown, E. Minear, and R. H. Lasseter, “Certs microgrid demonstration with large-scale energy storage and renewable generation,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 937–943, March 2014.

[6] National Electric Sector Cybersecurity Organization Resource (NESCOR), “Electric Sector Failure Scenarios and Impact Analyses”, September 2013, ver. 1.0, Electric Power Research Institute (EPRI).

[7] T. H. Morris, S. Pan and U. Adhikari, “Cyber security recommendations for wide area monitoring, protection, and control systems,” *2012 IEEE Power and Energy Society General Meeting*, San Diego, CA, 2012, pp. 1-6.

[8] M. D. Hadley, J.B. McBride, T. W. Edgar, L. R. O’Neil, J. D. Johnson, “Securing Wide Area Measurement Systems”, Pacific Northwest National Laboratory, June 2007, PNNL-17116.