3-2020

Design of Attack-Resilient System for Wide-Area Monitoring, Protection, and Control in Smart Grid

Vivek Kumar Singh
Iowa State University, vsingh@iastate.edu

Manimaran Govindarasu
Iowa State University, gmani@iastate.edu

Design of Attack-Resilient System for Wide-Area Monitoring, Protection, and Control in Smart Grid

Abstract

Can you imagine that a simple cyber-attack can turn your lights off? Do you know more than a dozen U.S. utilities have been constantly targeted through cyber-attacks within the past year? The solution - an attack-resilient grid infrastructure that can quickly detect stealthy cyber-attacks and provide an intelligent incident response to restore the normal grid condition.

Design of Attack-Resilient System for Wide-Area Monitoring, Protection, and Control in Smart Grid

Authors: Vivek Kumar Singh and Manimaran Govindarasu

Can you imagine that a simple cyber-attack can turn your lights off? Do you know more than a dozen U.S. utilities have been constantly targeted through cyber-attacks within the past year? The solution - an attack-resilient grid infrastructure that can quickly detect stealthy cyber-attacks and provide an intelligent incident response to restore the normal grid condition.

Today's energy infrastructure is undergoing a massive transformation across all generation, transmission, and distribution systems to provide reliability, efficiency, and sustainability to the power system network. In recent years, several wide-area monitoring, protection, and control (WAMPAC) applications, such as state estimation (SE), automatic generation control (AGC), remedial action scheme (RAS), synchrophasor-based applications, etc., are developed at the energy management system (EMS) layer to provide a real-time monitoring and grid condition-based automated responses to maintain the stability and reliability of power system. The existing vulnerabilities, due to their dependence on the unencrypted SCADA communication and insecure data sharing devices, have exposed them to countless cyber-attacks. Therefore, an attack-resilient system (ARS) is necessary to provide a defense-in-depth architecture for the WAMPAC applications by adding advanced security layers in the application layers with possible countermeasures, while considering advanced persistent threats (APT) in inside and outside grid environment.

In general, an attack resilient system (ARS) is defined as the integration of anomaly detection system (ADS) and attack mitigation system (AMS). The ADS includes a set of seamlessly-integrated detection algorithms and models that detect cyberattacks based on deviations in the observed data. Once an anomaly is detected, the attack mitigation system (AMS) is triggered based on the situational awareness and possible countermeasures against cyberattacks.

Attack-Resilient System = Anomaly Detection System + Attack Mitigation System

Conceptual architecture of attack-resilient system

Fig. 1 shows the conceptual architecture of the attack-resilient system for WAMPAC-Energy Management System (EMS) applications. In this architecture, several WAMPAC applications are running at the control center, which receive measurements from field sensors, perform analytical functions, and provide control signals, if necessary, to close the loop. Based on the given attack surfaces, a smart attacker can manipulate measurements or disable the communication, more in a stealthy manner, that can affect the usual operation of WAMPAC. It motivates the need to develop an ARS and the following are possible approaches to develop the ADS and AMS.

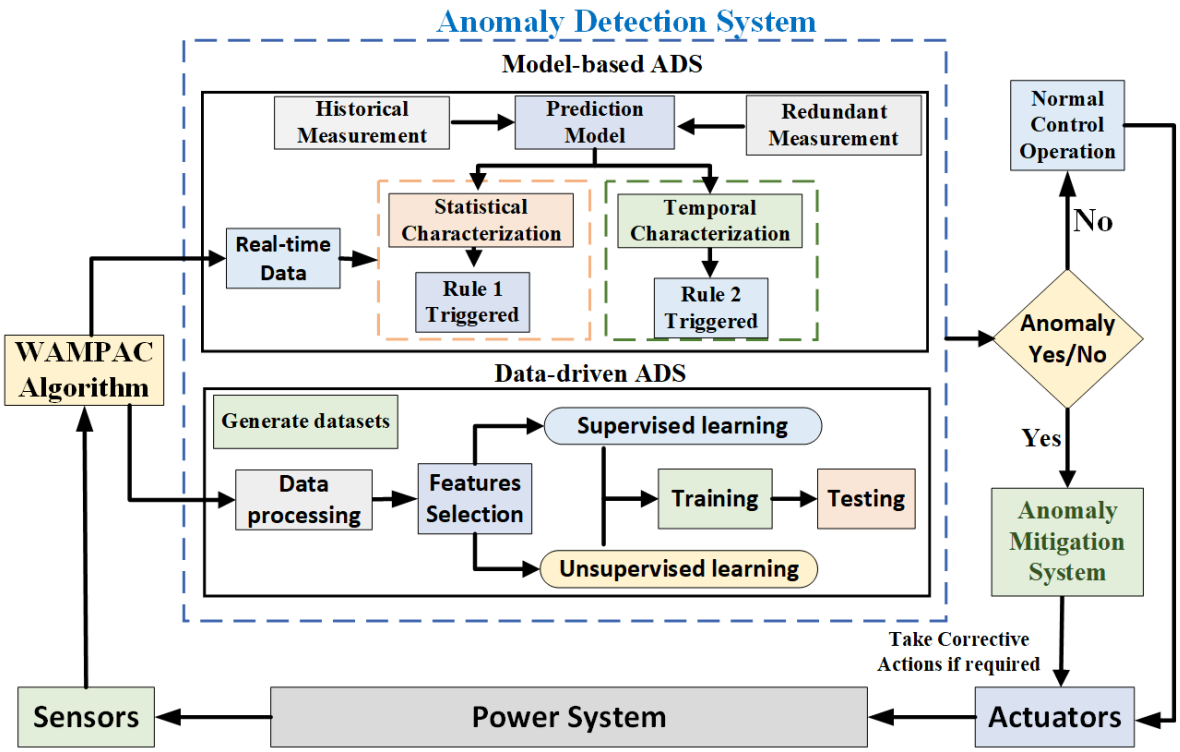

Fig. 1. Conceptual architecture of attack-resilient system for WAMPAC-EMS.

Anomaly Detection System (ADS): Based on the type and nature of WAMPAC applications, two different types of ADS methods: model-based and data-driven ADSs are presented. It is based on the notion of capturing cyberattack signatures by developing accurate models and leveraging power system measurements and network packets to detect different classes of cyberattacks.

a) Model-based ADS: The model-based ADS leverages historical or secure and redundant measurements to develop a prediction model and cyber-attacks are detected based on rules defined during the statistical and temporal correlation-based comparative analysis of incoming data streams.
b) Data-driven ADS: The data-driven ADS applies state-of-the-art machine learning and data-mining techniques, such as decision trees (supervised), K-means clustering (Unsupervised), principal component analysis (PCA), etc., to detect anomalies using an immense volume of the data. This method involves data pre-processing, input feature selection, training and real-time testing of different participating classifiers and based on their performances, the best classifier is selected for optimal decision making.

Attack Mitigation System (AMS): Several mitigation strategies can be considered at the infrastructure and application layers to minimize the impact of undesired events. For example, during the attack reconnaissance, such as ping or nmap network scanning, alerts can be sent to the control center operator to provide situational awareness about the possible threats. Similarly, during data integrity or denial of service (DoS) attacks, the given system can be re-configured, such as restoring the system or network topology, to maintain the normal operation. Table I shows the proposed model-based and data-driven ARS for different WAMPAC applications. For example, in case of automatic generation control (AGC) cyber-physical security, real-time load

forecasts are leveraged to design model-based ARS [2], and K-means clustering-based machine learning classifier is utilized for data-driven ARS [3].

Table I. Proposed Attack-Resilient System for WAMPAC Applications

Cases	WAMPAC	Measurements & Inputs	Control Actions	Model-based ARS	Data-Driven ARS
1	Automatic Generation Control	Frequency & Tie-Line Power Measurement	Raise/lower Generation	Load Forecasts [2]	SCADA measurements, K-means clustering [3]
2	Remedial Action Scheme	Power/load measurement & Lines status	Shed generation/load	Multi-agent System (MAS) [4]	Phasor measurements, Decision Tree (DT) [5]
3	State Estimation	Voltage & Power, VAR or Current-Flow	Generation Re-Dispatch and Open/Close Breakers	PMU measurements, load forecasts [6]	Physics based features, Dimension Reduction Technique
4	Oscillations Damping	Phasor measurements	FACTS, Power system stabilizer (PSS), High-voltage direct current system (HVDC)	Redundant PMU measurements	Physics-based Features, Principal component Analysis (PCA) [7]

Conclusion

Developing an attack-resilient system for WAMPAC applications in smart grid is a difficult task since it requires in-depth knowledge and understanding of their operations and grid network topology. This article presents the conceptual architecture of an attack resilient system that is as a combination of anomaly detection system (ADS) and attack mitigation system (AMS). Further, it presented different types of ADS, and also threw light on different mitigation strategies, as a part of AMS. Finally, this article highlighted the proposed attack resilient methods and technology for different WAMAPC applications to prevent the propagation of cyberattacks in the smart grid network.

References

1. A. Ashok et al., "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," in *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389-1407, July 2017.
2. S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," in *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, March 2014.
3. P. Wang, M. Govindarasu, A. Ashok, S. Sridhar and D. McKinnon, "Data-Driven Anomaly Detection for Power System Generation Control," *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, New Orleans, LA, 2017, pp. 1082-1089.
4. V. K. Singh, A. Ozen and M. Govindarasu, "A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid," *2018 Resilience Week (RWS)*, Denver, CO, 2018, pp. 63-69.
5. V. K. Singh and M. Govindarasu, "Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data," *2018 IEEE Power & Energy Society General Meeting (PESGM)*, Portland, OR, 2018, pp. 1-5.
6. A. Ashok, M. Govindarasu and V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," in *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, May 2018.
7. K. Mahapatra et al., "Malicious Corruption Resilience in PMU Data and Wide-Area Damping Control," in *IEEE Transactions on Smart Grid*.

Vivek Kumar Singh (Member, IEEE) received the B.E. degree in electrical engineering from the National Institute of Technology (NIT) Durgapur, India in 2014. He is currently pursuing his PhD in Electrical Engineering with a minor in Computer Engineering from Iowa State University (ISU). His research interests include smart grid, cyber-physical security for smart grid, wide-area monitoring, protection, and control (WAMPAC) applications, synchrophasor applications in power system, and smart-grid cyber-physical federation testbeds. He received the journeyman fellowship award from US Army Research Laboratory, published 14 research papers and 1 provisional patent in smart grid cybersecurity, given nearly dozen oral presentations, and organized 6 cybersecurity training sessions for utilities, companies, and co-operatives. He has received 2nd place lightening talk award at Resilience Week 2019, best paper award at Resilience Week 2020, and 3rd place poster award at TPEC 2020. He is also serving as a reviewer in IEEE conference and journal papers.

Manimaran Govindarasu is currently the Mehl Professor of Computer Engineering in the Department of Electrical and Computer Engineering at Iowa State University. He received his Ph.D degree in Computer Science and Engineering from the Indian Institute of Technology (IIT), Madras, India in 1998. He has been on the faculty of Iowa State University since 1999. His research experiences are in the areas of cyberphysical system (CPS) security for the smart grid, cyber security, real-time systems and networks, and Internet of Things. He has co-authored over 150 peer-reviewed research publications, and has given several invited talks and tutorials at reputed IEEE conferences, and delivered nearly two dozen training sessions and shortcourses on the subject of cybersecurity for the power grid. At Iowa State, he has built a CPS security testbed for smart grid and

demonstrated several realistic attack-defense use-cases, and made the testbed accessible to R&D community. He is a co-author of the text “Resource Management in Realtime Systems and Networks,” MIT Press, 2001. He served as a Guest CoEditor for several flagship IEEE publications (IEEE Network, IEEE Power & Energy, IEEE Trans. on Secure and Dependable Computing), and served as an Associate Editor for IEEE Transactions on Smart Grid and IEEE Transactions on Mobile Computing. He served as the Chair of Cybersecurity Working Group within IEEE Power & Energy Society AMPS Committee. He is a Fellow of the IEEE.