A Short Review on Cybersecurity of Cyber-Physical Power Systems

Mengxiang Jiang
Department of EECS
Texas A&M University-Kingsville
Kingsville, USA
mengxiang.jiang@students.tamuk.edu

Rajab Challoo
Department of EECS
Texas A&M University-Kingsville
Kingsville, USA
rajab.challoo@tamuk.edu

***Abstract*—The Cyber-Physical System (CPS) is an emerging digital technology gaining traction in various sectors, from academia to government and industry, with applications spanning areas like agriculture, energy, and transportation. These systems evolve traditional power mechanisms by merging them with information and communication technologies, leading to the Cyber-Physical Power System (CPPS). The CPPS, while facilitating efficient and reliable monitoring and control of power grids through its integration of physical and cyber systems, also introduces vulnerabilities to cybersecurity threats. Existing methods typically separate the physical and cyber domains when modeling and analyzing these systems, which is not optimal for modern CPPS. This paper offers a short overview of two papers that model, simulate, and analyze cyber threats and security measures for the CPPS.**

I. INTRODUCTION

In recent years, power and control system engineers have worked diligently to enhance the tools and techniques for the improved performance of monitoring and control of the physical power system. Concurrently, professionals in computer science and electronics have been innovating in the cyber realm to amplify the performance of computing and communication systems. This convergence has made computing ubiquitous, with most daily gadgets and electronic devices now integrated with efficient computing and communication networks. This trend

undoubtedly will have a profound impact on energy systems [1].

This merging of physical and cyber dimensions has given birth to a new digital technology known as the Cyber-Physical System (CPS). This system is gaining momentum across sectors such as agriculture, energy, medicine, and transportation. CPS is a heterogeneous system combining the cyber realm (control, computing, communication) to enhance stability, efficiency, and reliability in various physical system applications [2]. Within the CPS framework, the cyber component collects data from the physical system and, in turn, feeds back control signals to achieve mutual objectives.

This harmonization between the physical power system and the cyber component evolves into the Cyber-Physical Power System (CPPS) [3], [4]. The CPPS encompasses all facets of the electric power systems, from generation to utilization. At its essence, a CPPS combines and coordinates internet technologies with physical power system components. These systems are not merely about adding computing and communication methods to existing structures but represent a holistic fusion of these domains to bring forth innovations in science, technology, and application.

The primary limitation of the Cyber-Physical Power System (CPPS) pertains to cyber-attacks and cybersecurity vulnerabilities. CPPS, being a large and diverse networked transmission and distribution system, is susceptible to cyber threats. These threats, while not directly harming the physical power system, can, when combined with physical attacks, lead to significant damage and system instability. There's a pressing need to delve into cyber threats and security measures for CPPS.

This paper will summarize two recent works directed towards detecting and mitigating cyber threats. The first is by Roberts et al. using data from Phasor Measurement Unit (PMUs) as inputs to algorithms to learn the control logic of voltage regulators and switched capacitor banks in order to detect attacks [5]. The second is by Zhang et al. using electricity bid price measurments to train deep stacked autoencoders (SAEs) to detect attacks [6].

II. Learning Behavior of Distribution System Discrete Control Devices for Cyber-Physical Security

The key event mentioned by the researchers was the 2015 Urkaine blackout. It was a significant cyber attack that targeted several regional power companies in Ukraine, leading to a power outage affecting approximately 230,000 residents for several hours on December 23, 2015. It was the first known successful cyber attack on a power grid. Hackers utilized malware to compromise systems and destroy data, alongside spear-phishing emails to gain access to the power infrastructure. The attackers also disrupted the power companies' customer service lines using a denial-of-service attack, making it challenging for customers to report outages. The incident marked a concerning evolution in cyber warfare capabilities, illustrating the potential for cyber attacks to cause tangible disruptions in essential services [7].

In order to prevent such attacks, it is necessary to monitor the physical voltage, current measurements, and Supervisory Control and Data Acquisition (SCADA) data to identify false data attacks and other irregularities in both transmission and distribution grids. The researchers chose to employ a model-based method, which generally needs less data than machine learning techniques, making it easier to update after intentional control changes.

This is done through the use of distribution Phasor Measurement Units (PMUs) as an isolated sensor network to supplement existing intrusion detection systems that primarily monitor SCADA traffic. PMUs monitor the actions of control devices on the distribution grid, like On-Load Tap Changing (OLTC) transformers and capacitor banks. If these devices are densely placed, they can be manipulated to impact the voltage range of Distributed Energy Resources (DER), affecting power quality and potentially tripping a significant number of DERs.

A key insight of this work is to detect potential threats within the SCADA network even before an attack starts, such as during reconnaissance when an attacker gathers information about a network. Such subtle actions might not immediately trigger alarms but can indicate potential threats. For instance, slightly adjusting the settings of an OLTC transformer could be a sign of verifying control, which usually goes unnoticed by operators.

The researchers implement a series of algorithms designed to learn and observe the control logic of distribution system regulation equipment, particularly OLTC transformers and capacitor banks. The process involves detecting and associating control actions with specific devices, estimating their time delay, refining this estimation for accuracy, and determining the actuation thresholds of the devices.

The solution was validated on simulated and utility recorded data. In particular, the more discrete jump events the better the estimation voltage ranges becomes, with 60 total events stabilizing the estimation. However, this is still a reliance on many of these discrete jump events in order for the algorithms to learn the system. Addressing this limitation requires examining the statistical characteristics of events in order to reduce the learning period.

III. Cyber Physical Security Analytics for Transactive Energy Systems

The 2015 Ukraine blackout was also mentioned by the researchers of this paper, but they offer a different approach for detecting such attacks.

The main focus is on transactive energy systems (TESs), which use economic and control strategies to adjust the electric grid's supply and demand in real-time. This modern control method relies heavily on distributed computing and Internet of Things (IoT) devices to make independent or semi-independent decisions about energy output and consumption. But these cyber components, including the IoT devices, are becoming increasingly susceptible to cyber threats. Given the financial motivations behind these interactions, TESs are also vulnerable to cyberattacks, which can disrupt the power grid. There's a pressing need for methods to continually monitor these systems and identify suspicious activities.

In order to meet these challenges, the researchers model and simulate various components of TESs in detail, building around the transactive energy simulation platform (TESP) designed by Pacific Northwest National Laboratory (PNNL). They train a deep stacked autoencoder (SAE) in order to detect cyberattacks. A brief overview of SAE is given next.

An SAE consists of an input layer, an output layer, and several fully connected hidden layers. The SAE

structure consists of two main elements: the encoder and the decoder. The encoder transforms the data into a compressed codebook, and the decoder then attempts to recreate the original data from this codebook. Unlike conventional supervised learning techniques that demand pre-set labels or values for the model's target, the SAE uses its input data as the target, making it a self-supervised approach. Additionally, SAE does not necessitate extra steps for feature creation and can accept raw data directly. However, unlike the more well-known variational autoencoders (VAEs), SAEs cannot generate new data samples by sampling from the latent representation of the compressed codebook.

The researchers train the SAE on the bid prices and bid quantities of normal operation data and evaluate the performance using unseen normal, outage, and attack data. Despite never seeing any outage and attack data during training, it was able to identify 79% of outages and 96.9% of attacks as anomalous, although around 3% of normal events were incorrectly detected as anomalous as well. A major limitation of this solution however, is that although the attack is detected, this seems to be in the late stages where the attackers is already exploiting the system rather than detecting during the reconnaissance stage of the previous paper.

IV. Conclusion

The comprehensive cybersecurity aspect of the CPPS is distinct from traditional information security, incorporating advanced data analytics and machine learning techniques. It is highly likely that more cyberattacks on CPPS will happen in the future, and this will also motivate more research in other preventative measures.

References

[1] E. F. Orumwense and K. Abo-Al-Ez, ‘‘A systematic review to aligning research paths: Energy cyber-physical systems,’’ Cogent Eng., vol. 6, no. 1, pp. 1–21, Dec. 2019.

[2] L. Shi, Q. Dai, and Y. Ni, ‘‘Cyber–physical interactions in power systems: A review of models, methods, and applications,’’ Electr. Power Syst. Res., vol. 163, pp. 396–412, Oct. 2018.

[3] S. Suryanarayanan, R. Roche, and T. M. Hansen, ‘‘Cyber-physical-social systems and constructs in electric power engineering,’’ Inst. Eng. Technol., London, U.K., Tech. Rep., 2016.

[4] Y. Cao, Y. Li, X. Liu, and C. Rehtanz, Cyber-Physical Energy and Power Systems. Singapore: Springer, 2020.

[5] C. Roberts, A. Scaglione, M. Jamei, R. Gentz, S. Peisert, E. M. Stewart, C. McParland, A. McEachern, and D. Arnold, ‘‘Learning behavior of distribution system discrete control devices for cyber-physical security,’’ IEEE Trans. Smart Grid, vol. 11, no. 1, pp. 749–761, Jan. 2020.

[6] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, ‘‘Cyber physical security analytics for transactive energy systems,’’ IEEE Trans. Smart Grid, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection attacks,” IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317–3318, Jul. 2017.