Recent Advances in Cyberattack Detection and Mitigation Techniques for Renewable Photovoltaic Distributed Energy CPS

Jessica Whitaker[1] and Danda B. Rawat[2]

Department of Electrical Engineering and Computer Science
Howard University, Washington DC 20059, USA
[1]jessica.whitaker1@bison.howard.edu, [2]danda.rawat@howard.edu

Abstract. Cyberattacks targeted to the energy cyber-physical system (ECPS), also known as the smart grid, could interrupt the electricity supply with major ramifications. Attackers identify and exploit any vulnerable portion of the energy power grid, including the inverters with solar-powered photovoltaic (PV) panels. PV presents unique challenges as electricity consumers have also become providers of solar energy for utilities. As mandates require increased PV penetration across the world for positive environmental impacts, increased cyberattacks targeted at PV systems impact reliability and efficiency within the ECPS. The new technologies continuously being introduced to manage the ECPS and ensure bi-directional communications and energy flow between components also lead to more attack surfaces, system vulnerabilities, and heightened malicious attacks. Data integrity attacks are increasing within PV systems. In this paper, we present a survey of different methods that are proposed and explored for identifying and preventing cyberattacks targeted at PV systems. The attack detection methods include voltage control, data diodes, and voltage measurement algorithms. Furthermore, we present blockchain, cyber switching, and other attack mitigation techniques for PV systems.

Keywords: Smart Grid, Coordinated Cyberattacks, Attack Detection, Renewable, Photovoltaic, Energy Cyber-Physical System.

1 Introduction

Cyberattacks have been increasing at a rapid pace with the rise in the number of devices and connectivity in cyber-physical systems (CPS) [1], [2], [3] and Internet of Things (IoT) [4], [5]. Energy CPS (ECPS) devices control vital infrastructure and include both the physical and digital cyber portions. The extensive composition of the ECPS makes it susceptible to cyber-physical attacks [6], [7], [8]. The conventional model of the energy grid is unidirectional. However, the emerging smart grid ECPS has bidirectional electricity and information flow. The ECPS continues to experience more severe cyberattacks because of the impact it could have on the nation, industry, government, and people [1], [6], [7].

The modern smart power grid uses a combination of information and communication technology. This combination enables an automatic response in many scenarios and supports the overall goals of the ECPS. These goals are to continuously seek improvement in efficiency, sustainability, economics, and reliability when producing and distributing electricity. The communication infrastructure leverages various media and modes of transmission for signals and data. The network infrastructure allows the power flow and measurements to have better operations, monitoring, and control. Several technologies, like smart meters and substation automation, enhance the function of the smart grid. The supervisory control and data acquisition (SCADA) system is another tool that improves the electronic monitoring and control of the power grid. SCADA can be attacked through unauthorized access, the interception of communication channels, and the injection of a false signal. The ECPS control center regulates and monitors this significant amount of communication, making it vulnerable to being attacked by hackers. Malicious attacks cause system interruption or disruption. The cyberattacks have increased in complexity with more successful attempts on the power grid.

The evolution of distribution and transmission power system networks is swift based on increasing demand, reliability issues, and environmental policies requiring carbon emission reductions. The increased desire to expand distributed generation or distributed energy resources (DER) introduces both obstacles and advantages, as shown in [9]. The obstacles for DER include voltage rise, system faults, bidirectional power flow, and feeder constraints which contribute to safety concerns. As climate challenges worldwide increase, the demand for distributed renewable energy from natural resources is also growing. The electric power grid has been a complex web of communication and automation even before evolving into what is now referred to as the smart grid. The primary goals of the electric power grid are evolving. As cyber technology and the electricity network are intertwined, they produce a much smarter grid that is much more efficient and reliable. Distributed energy resources, including wind, PV generation, and battery energy storage, are often interconnected for increasing hybrid options in ECPS [10]. New security concerns require continuous monitoring as the controllers for the various hybrid grid devices are managed through the SCADA system. The possibility of cyberattacks on SCADA components continues to increase exponentially.

Fig. 1 shows historical milestones for photovoltaic (PV) systems [11], [12]. In the past, the cyber risk for PV systems was relatively minor as those systems were not connected to ECPS or deployed minimally. However, cyber risk has been growing with the connection of PV with ECPS, where inverters are the interface between solar panels and the energy grid CPS. Attackers could intercept and manipulate inverters, and the inverter could spread malware into ECPS through embedded code. The cyberattacks could cause physical as well as financial damage. Microgrids are also a potential target for cyberattacks.

The smart grid ECPS is increasingly dependent on the digital grid infrastructure for control and monitoring as complex measuring and management

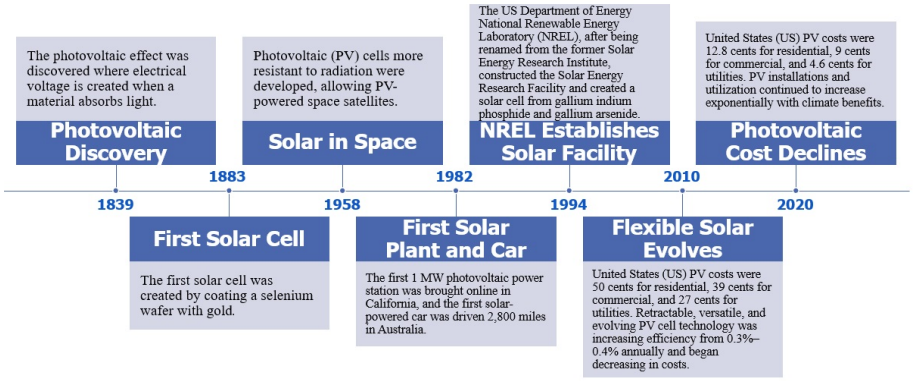

Fig. 1. The Evolution of Photovoltaic

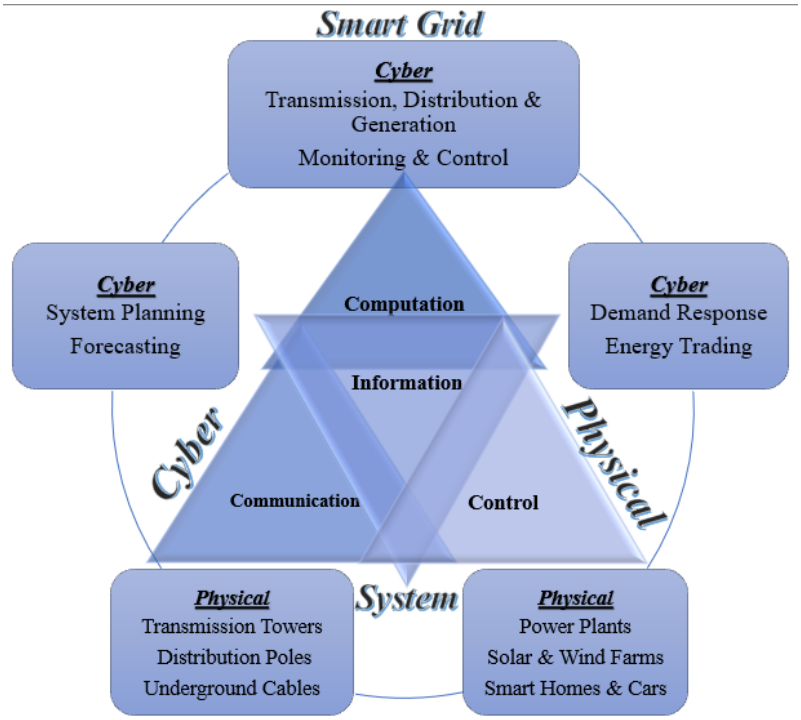

Fig. 2. Smart Grid Energy Cyber-Physical System

components are introduced into the ECPS, as shown in Fig. 2. Enhanced communication infrastructure requires investment for generating companies to adhere to operational requirements. With every expansion of any portion of the ECPS with DER connected to the smart grid, the attack surface also expands,

which is available to adversaries for malicious attacks. Work in [13] details how power systems must be designed with attack resilience and tolerance.

The National Science and Technology Council (NSTC) released a typical Federal Cybersecurity Research and Development Strategic Plan with deter, protect, detect, and adapt to cyberattacks [14] as shown in Fig. 3. This Strategic Plan applies to any CPS, including energy CPS with PV systems.

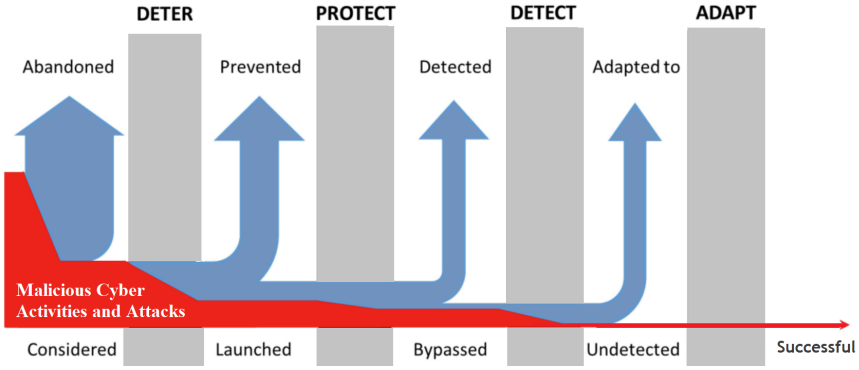

Fig. 3. Continuously strengthening cyber defense through deter, protect, detect, and adapt stages to minimize the malicious cyber activities and attacks, per the NSTC plan.

2 Smart Grid ECPS Analysis

2.1 Attack Assessment

A ranking system was created in [15] through a voltage-based index for nine cyberattacks. The ranking highlighted the severity of the deterioration of the smart grid due to attacks to improve mitigation within a hybrid power grid consisting of PV. The denial of service (DoS) attack was the most severe, and the packet drop attack had the least (most negligible) impact on the ECPS. The framework was presented for a smart grid cyberattack impact analysis focused on both cyber and physical attacks. A method and model were proposed in [16] for evaluating the dynamic vulnerability of ECPS to protect the power grid network from infrastructure failures. Advancements and challenges with ECPS were reviewed by [17] to determine optimal techniques and designs to benefit the smart power grid for researchers and grid operators. In [18], event tree analysis enabled the exploration of the impact of smart grid attacks on information assets.

Furthermore, the PV grid overvoltage protection issues were summarized in [19] and [20] to document the output power loss due to voltage rise for increased DER penetration. Various PV inverters were categorized to review a multitude of

platforms for introducing single and three-phase photovoltaic technology within the electrical grid in [10], [21], and [22]. Mitigating attacks within an automated grid with numerous DER scenarios was evaluated in [23], [24], [25], and [26].

2.2 Cyberattack Mitigation

Cyber switching attack mitigation techniques were proposed in [27], [28], and [29] to prevent the destabilization of the smart grid. Man-in-the-middle (MITM) and data integrity attacks in [30] and [31] were reviewed to introduce countermeasures against these smart grid ECPS cyberattacks. In [18], [32], and [33], defense mechanisms for challenges of smart grid data injection attacks were presented for proactive protection or mitigation with late detection. In [34], a new coordinated voltage control scheme for enabling efficient voltage regulation of multiple feeders with DER was introduced by placing a remote terminal unit at each DER and line capacitor.

Attack resilient control was addressed in [35] by identifying cyberattacks directed at industrial control systems, power system key control loops, and effective attacks against control loops. An ECPS substation attack resulting in an overheated transformer was modeled utilizing a hybrid attack graph to identify opportunities for increased security in [36]. Within [37], [38], and [39], grid ECPS cyberattacks were analyzed based on various methods to determine their effectiveness.

3 Smart Grid ECPS Photovoltaic Attack Detection

In this section, we present different photovoltaic attack detection and mitigation techniques and summarize different approaches in Table 1.

3.1 Multi-layer Long Short-Term Memory Network Attack Detection

Secure power electronics converters are critical within the ECPS. A PV solution for attacks with deep sequence learning-based diagnosis was proposed in [29] for a data integrity attack (DIA). This included converters which were AC/DC and DC/DC. PV current and voltage sensors provided time-series electric waveform data using multi-layer long short-term memory networks (MLSTM). A DIA diagnosis was combined with a detection method and tailored to determine whether attacks occurred. This modified DIA performance was determined by comparing the methods, including multiple forms of neural networks.

The analysis began with DIA on the smart grid. The MLSTM approach was applied to detect the PV attack and type with the attack diagnosis model. At the PV point of common coupling, one voltage and one current sensor were used for DIA mitigation. Encryption was recommended for the communication channel for waveform data security. MLSTM was proposed for streaming sensor data intrinsic sequential characteristics.

3.2 Voltage Control Attack Detection

Distribution PV attacks in [40] employed a centralized control scheme with switches containing sensors. The attacks could result in inaccurate measurements being introduced by the hacker, causing system voltage violations. The tap controller received incorrect sensor measurements from switches. A detection algorithm on the control confirmed reduced impact. The impact was further reduced if a limited number of sensors experienced the attacks.

The standard system behavior determined the simple algorithm. Optimization problems were devised to specify which attacks were effective against the algorithm. Attacks were investigated that minimized power output for PV with overvoltage protection functions. Attacks resulted in inaccurate node voltage with minimal nodes. With increased attacks on nodes, PV damage occurred due to node voltage violation.

3.3 High-Dimensional Data-Driven Cyber-Physical Attack Detection

A high-dimensional data-driven cyber-physical attack detection and identification approach (HCADI) was introduced in [40]. The impact of attacks was evaluated on power grid electric waveforms and solar inverter harmonics. The streaming data matrix was based on the network signal analysis of sensors. The new method contained score-based attack detection and diagnosis based on binary matrix factorization.

The HCADI method contrasted with the machine and deep learning-based methods by not requiring the training stage for detection and root cause determination. HCADI avoided this stage by utilizing binary coding and data structure. The same data was leveraged with the existing structure to examine streaming waveform data features utilizing a matrix. The leverage score identified that the attack impacts were highlighted by a score, and binary coding results identified attack types.

3.4 IEC 61850 Photovoltaic Inverter Installations Attack Detection

In [41], attack detection for the IEC 61850 specification was analyzed. This specification is widely applicable to Smart Grid communication services. Hackers were proven to impact physical and cyber systems through MITM and data attacks. The lab was configured for a MITM attack. An attack use case was developed for the power utility automation standard (IEC 61850) with inverter-based distributed energy resource devices, including PV.

Testing showed a physical impact on system operation and electrical devices. The PV physical operation was altered with changes to power limits perpetrated by hackers. These changes could also cause the PV to stop generating electricity. The SCADA system would not recognize this shutdown to notify the appropriate system operexperiencedx-like malware payload was created for additional research with IEC 61850 PV in modeling, testing, and security against malicious attacks. The lab configuration for a MITM attack is shown.

3.5 Grid-Tied PV Systems Attack Detection

Mitigation techniques to protect systems connected to the power grid specifically focused on distribution-level PV were proposed in [34]. The dynamic watermarking approach determined alterations of the measurements for the current and voltage sensors, which were inputs for inverter operation. The solution was tested on a distribution scale single-phase grid-tied 5kW inverter. This size was considered for residential PV connections. The proposed defense identified attacks in under 0.016 seconds. The replay attack model implementation included the current measurement sent to the controller being replaced by a measurement recorded in the past due to the attack.

As PVs and other distributed energy resources increase, the number of power electronic converter interfaces will also increase. Real power is introduced at various points within the power system when PV generates extra electricity. Reactive power injection capability exists for smart inverters to maintain voltage control across the smart grid. Early detection helps with the mitigation of cyber threats. A single distribution node was investigated by [34] to mitigate the malicious activity on the current measurement, current sensing manipulation, and inverter instability within the grid.

3.6 Commercial PV Inverter Providing Ancillary Services Attack Detection

Cyberattacks in the ECPS could cause inefficient grid operations, unauthorized access to smart meter data in [42], feeder tripping, and blackouts within the smart grid. A MITM cyberattack on a sizeable commercial PV inverter was discussed in [30], which tripped a feeder offline and led to a regional blackout. The communication flow of packets was explained before the attack and after the false measurements were injected. The PV inverter provided ancillary services to the grid. Ancillary services help the electricity generators and grid operators maintain reliable electricity throughout the interconnected power grid. With electricity, these services are critical to ensuring the proper flow and direction, maintaining the balance between supply and demand, and restoring the system after outages.

A risk analysis was conducted to determine the influence of PV inverter capacity and feeder loading on the attack severity. The ancillary services controller had not operated properly during the attack, which overloaded the feeder. The feeder breaker tripped the feeder offline for all of the connected consumers when the feeder became overloaded. This feeder outage occurred without the hacker having cyber access to the feeder breaker. The risk analysis concluded that the attack had a more significant outcome due to the tighter loading margin when a feeder had a substantial number of connected consumers, limited inverter capacity, and high reactive power production. A feeder with a unity power factor loading condition reduced the risk of tripping the feeder.

3.7 Blockchain Attack Detection

DER is converting consumers into a combination of consumers and producers of electricity. This scenario with resources like PV creates unmanageable smart grid conditions in the presence of a malicious cyberattack. In [43], blockchain technology (BCT) was manipulated to handle grid data and enable substations that could operate without human intervention. Grid communication was still available on blockchain during the implementation of the distributed denial of service (DDoS) attack.

Two test methodologies were modeled with a cyberattack. For the first test with the single machine infinite bus (SMIB), the system was vulnerable to hardware and software access during the attack. The hacker accessed both software and hardware to manipulate the switch. The malicious lines of code introduced by the attacker produced non-functional switches and removed the load from the target generator. A non-functioning switch would cause the rotor to oscillate and potentially damage the generator shaft. The generator could also lose synchronism. BCT was proven to stabilize the SMIB system and cease the oscillations. The distributed ledger computing with BCT decreased the vulnerability in [43].

The DDoS cyberattack occurred with a power distribution system in the second test. Data communication input and output channels were shown not to function and display a busy signal. The monitoring, control, and data transmission of the power distribution system could malfunction due to system imbalance. Protection devices could trip the system, and the frequency could become unsustainable, resulting in a smart grid power outage. BCT features were proven in [43] to make the smart grid more reliable by utilizing the distributed app of dApp. dApp ran on distributed computing techniques and served as a communication link between consumers and producers of electricity.

3.8 µPMU Data Attack Detection

In [35], attack detection was proposed to mitigate PV cyberattacks. The ECPS security framework examined data integrity attacks on various control loops. A µPMU lower sampling rate of µPMU data was incorporated into the detection algorithm. The methods of support vector machine (SVM) and long short-term memory (LSTM) confirmed the µPMU data was effective in detecting cyberattacks. SVM separated multiple data classes with increased training time. SVM poorly handled image classification and other larger data.

For LSTM, the vanishing gradient problem was solved for the recurrent neural network in [44]. A manner of carrying past information across time steps was developed by saving information for later, which stopped old data from vanishing during training. LSTM provided the flexibility of processing single, multiple, and time-series data points. With µPMU, the data was collected from sensors. SVM was used for attack detection, and LSTM was used for attack diagnosis experimentation.

3.9 Data Diodes Attack Detection

In [45], a survey was completed for both a PV system that utilizes data diodes for cyberattacks and a system that does not use data diodes for attacks. A typical PV system was displayed, including the PV panel, performance monitoring and reporting services (PMRS), and other components. A comparison was made between eight different data diodes.

The cost of the diodes was investigated for feasibility. The purchase of data diodes was not determined to be feasible for small, residential, or community PV. However, the data diodes for large-scale utility providers were feasible. Data diodes protected IoT, SCADA networks, and other applications by enforcing unidirectional strict network communication. Data diodes forced data to flow in one direction by translating bidirectional protocol into a unidirectional protocol [45].

Another implementation in [45] with data diodes included modifying communication cables connecting multiple devices. The devices interfacing must have communication lines to both transmit and receive. The receiving line on one side of the cable would have to be removed, and the transmitting line on the other side of the same communication cable would also be removed. The diode would then direct traffic in one-direction loops.

3.10 Voltage Measurement Algorithm Attack Detection

In [46], a cyberattack analysis occurred on the PV measures engaged in regulating voltage. There was a focus on PV with reactive power capability. An algorithm was proposed to detect cyberattacks utilizing a centralized method for controlling the system. Distribution voltages across the grid were leveraged. The operation of the PV inverters and reactive power were impacted by measurement modifications implemented during an attack. The reactive power control loop was evaluated for attack impact.

The work in [46] studied cybersecurity issues in distribution networks with PV units with reactive power capability. Inaccurate sensor measurements resulted in a tap change generating a voltage violation. This tap change caused PV reactive power compensation. Command signals changed the PV inverter output reactive power, causing damage to the grid and PV unit owners. An attack could lead to financial loss and real power curtailment if the inverter capacity was not higher than the PV real power. The increased PV inverter capacity resolved this problem.

3.11 Volt-Var Control Attack Detection

In [17], centralized volt–var control (VVC) led to optimal distribution feeder operation and included vulnerable metered data. During an attack on the metered data, the VVC could become useless. The distribution system state estimation (DSSE) provided the foundation for centralized VVC. DER injection measurements were DSSE-based calculations. Two solutions offered a VVC optimization

DSSE malicious attack mitigation. This approach was necessary when DER injection measurements were attacked. One solution involved using past or future forecasted data. Another solution included set-points to control and regulate the voltage.

Table 1. Summary of Smart Grid ECPS Photovoltaic Attack Detection Methods

Attack Detection Method	**Attack Type**	**Detection Approach**
Multilayer Long Short-Term Memory Network Attack Detection [29]	Data Integrity Attack	Deep Sequence Learning-Based Diagnosis
Voltage Control Attack Detection [40]	Data Integrity Attack	Control Detection Algorithm
High-Dimensional Data-Driven Cyber-Physical Attack Detection [40]	Data Integrity Attack	Score-Based Detection and Factorization Diagnosis
IEC 61850 Photovoltaic Inverter Installations [41]	Man-in-the-Middle Attack	Havex-like Malware Payload
Grid-Tied PV Systems [34]	Replay Attack	Dynamic Watermarking Approach
Commercial PV Inverter Providing Ancillary Services [30]	Man-in-the-Middle Attack	Risk Analysis to Adjust PV Inverter Capacity and Feeder Loading
Blockchain Attack Mitigation [43]	Distributed Denial of Service Attack	Blockchain Manages Data to Produce Autonomous Decentralized Units
µPMU Data Attack Detection [35]	Data Integrity Attack	µPMU Data with Support Vector Machine for Detection and Long-Short Term Memory for Diagnosis
Data Diodes Attack Detection [45]	Data Integrity Attack	Data Diodes Direct Data or Traffic Flow
Voltage Measurement Algorithm Attack Detection [46]	Data Integrity Attack	Centralized Control Scheme with an Attack Detection Algorithm Focused on Reactive Power
Volt-Var Control Attack Detection [17]	Data Integrity Attack	Stochastic Optimal Solution and Local Setting Solution

The goal was to limit power loss with a cumulant-based probabilistic optimal power flow. The communication network was at risk of a cyberattack when it

provided network control. A knowledgeable hacker familiar with the ECPS could negatively impact the network and VVC. State estimation failures would result from altered measurements and a faulty VVC. DER injection measurements endured similar attacks, and the two solutions of cyberattack mitigating stochastic optimal solution (CAMSOS) and local setting solution (LSS) were offered. The CAMSOS procedure was explained.

System states were estimated, and corrupted measurement data was identified. Probability density functions were proposed instead of using these states. The CAMSOS offered DER generation and load forecast probability density functions. CAMSOS also utilized historical measurements for the probability density function. Voltage control device set-points were calculated with the stochastic optimal. Another solution involved monitoring devices for control. With corrupted measurements, this prevented data control and produced the demand for predetermined set points. VVC was operational after the attack, as detailed in [17].

4 Challenges for Detection Methods

Real-time cyberattack detection and mitigation is a challenge in securing distributed energy CPS. As the ECPS evolves, necessities such as big data analytics processing become some of the many obstacles to effectively securing the smart power grid. The proposed attack detection techniques need to be able to handle big data (with volume, velocity, veracity, and variety).

The machine learning-based detection methods require more in-depth data analysis due to the limited data available for attack scenarios.

Investigating voltage control detection requires the application of more complex distribution systems with several feeders and devices. Utilizing battery energy storage devices and sectionalizing switches equipped with smart-meter sensors should be explored with voltage control detection.

With HCADI detection, the statistical analysis was influenced by unbalanced amplitudes among various observations and required shifting techniques for visualizing high-dimensional matrices. Further designs for modeling for threats and testing for penetration were needed for IEC 61850 PV inverter installation detection. We need validation and verification in a realistic ECPS since some simulation-based approaches discard real parameters. Commercial PV inverters providing ancillary services detection focused only on the configuration where most devices used non-secured Modbus TCP protocol for communication. Intruders conducting attacks should be considered for detection and mitigation.

With data diode detection, the expense of the data diode was excessive for residential use compared to other low-cost options. The system adequacy portion of reliability should be addressed with voltage measurement algorithm detection, and additional measures to quantify subsystem effects on system operation could be considered. Volt-Var control detection can be expanded to detect affected sensors with the authentication signal technique.

5 Conclusion

This paper presented a survey of DER PV attack detection and mitigation within the smart grid ECPS. To adequately explore this topic, we began with the connection between the ECPS and the smart grid, including the evolution of PV. The NSTC plan discussed to minimize attacks included strengthening cyber defense through deter, protect, detect, and adapt stages. The topics of attack assessment and mitigation have been presented during the analysis.

We examined the various types of smart grid PV attack detection techniques of MLSTM network, voltage control, HCADI, IEC 61850 PV inverter installations, grid-tied PV systems, commercial PV inverter providing ancillary services, blockchain, µPMU data, data diodes, voltage measurement algorithm, and Volt-Var control attack detection. The smart grid ECPS PV attack detection methods were summarized in a tabular form, including the method, attack type, and detection approach. The detection challenges detailed future research areas for each attack detection method studied in the paper.

6 Acknowledgement

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) at Howard University under Contract W911NF-20-2-0277 with the U.S. Army Research Laboratory, NSF grant #1828811, VMware research gift funds, NNSA Grants and DHS Grant 2017-ST-062-000003. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

References

1. Felix Olowononi, Danda B. Rawat, and Chunmei Liu. "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps." IEEE Communications Surveys & Tutorials 23.1 (2020): 524-552.
2. Rawat, Danda B., Joel JPC Rodrigues, and Ivan Stojmenovic, eds. Cyber-physical systems: from theory to practice. CRC Press, 2015.
3. Rawat, Danda B., Chandra Bajracharya, and Gongjun Yan. "Towards intelligent transporneedn cyber-physical systems: Real-time computing and communications perspectives." SoutheastCon 2015. IEEE, 2015.
4. Danda B. Rawat, et al. "Payoff optimization through wireless network virtualization for IoT applications: A three layer game approach." IEEE Internet of Things Journal 6.2 (2018): 2797-2805.
5. Bimal Ghimire and Danda B. Rawat. "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things." IEEE Internet of Things Journal (2022).

6. Rawat, Danda B., and Chandra Bajracharya. "Cyber security for smart grid systems: Status, challenges and perspectives." SoutheastCon 2015 (2015): 1-6.
7. Rawat, Danda B., and Chandra Bajracharya. "Detection of false data injection attacks in smart grid communication systems." IEEE Signal Processing Letters 22.10 (2015): 1652-1656.
8. Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity in big data era: From securing big data to data-driven security." IEEE Transactions on Services Computing 14.6 (2019): 2055-2072.
9. Walling, R., Saint, R., Dugan, R., Burke, J., Kojovic, L.: "Summary of Distributed Resources Impact on Power Delivery Systems." In: IEEE Transactions on Power Delivery, vol. 23, no. 3, pp. 1636–1644 (2008).
10. Mechouma, R., Azoui, B., Chaabane, M.: "Three-Phase Grid Connected Inverter for Photovoltaic Systems, a Review." In: 2012 First International Conference on Renewable Energies and Vehicular Technology, pp. 37–42 (2012).
11. U.S. Department of Energy Solar Energy Technologies Office (DOE SETO), Solar Futures Study, September 2002.
12. U.S. Department of Energy (DOE) Energy Efficiency and Renewable Energy, The History of Solar, 2002.
13. Khaitan, S., J. McCalley, J.: "Cyber Physical System Approach for Design of Power Grids: A Survey." In: 2013 IEEE Power Energy Society General Meeting, pp. 1–5, (2013).
14. National Science and Technology Council (NSTC), Federal Cybersecurity Research and Development Strategic Plan, February 2016.
15. Ghosh S., Ali, M., "Exploring Severity Ranking of Cyber-Attacks in Modern Power Grid." In: 2019 IEEE Power Energy Society General Meeting (PESGM), pp. 1–5 (2019).
16. Rodriguez, V., Cheng, A., Doan, B.: "Work-in-Progress: Combining Two Security Methods to Detect Versatile Integrity Attacks in Cyber-Physical Systems." In: 2019 IEEE Real-Time Systems Symposium (RTSS), pp. 596–599 (2019).
17. Farraj, A., Hammad, E., Daoud, A., Kundur, D.: "A Game-Theoretic Analysis of Cyber Switching Attacks and Mitigation in Smart Grid Systems." In: IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 1846–1855 (2016).
18. Langer, L., Smith, P., Hutle, M., Schaeffer-Filho, A.: "Analysing Cyber-Physical Attacks to a Smart Grid: A Voltage Control Use Case." In: 2016 Power Systems Computation Conference (PSCC), pp. 1–7 (2016).
19. Liu, S., Chen, B., Kundur, D., Zourntos T., Butler-Purry, K.: "Progressive Switching Attacks for Instigating Cascading Failures in Smart Grid." In: 2013 IEEE Power Energy Society General Meeting, pp. 1–5 (2013).
20. Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., Butler-Purry, K.: "A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid." In: IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 273–285 (2013).
21. Venkatesan, M., Rajeswari, R., Keerthivasan, K.: "A Survey of Single Phase Grid Connected Photovoltaic System." In: 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET), pp. 404–408 (2012).
22. Kjaer, S., Pedersen, J., Blaabjerg, F.: "A Review of Single-Phase Grid-Connected Inverters for Photovoltaic Modules," In: IEEE Transactions on Industry Applications, vol. 41, no. 5, pp. 1292–1306 (2005).
23. Hao, J., Piechocki, R., Kaleshi, D., Chin, W., Fan, Z.: "Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids." In: IEEE Transactions on Industrial Informatics, vol. 11, no. 5, pp. 1198–1209 (2015).

24. Jiang, J., Qian, Y.: "Defense Mechanisms Against Data Injection Attacks in Smart Grid Networks." In: IEEE Communications Magazine, vol. 55, no. 10, pp. 76–82 (2017).
25. Ansari, M., Vakili, V., Bahrak, B., Tavassoli, P.: "Graph theoretical Defense Mechanisms Against False Data Injection Attacks in Smart Grids." In: Journal of Modern Power Systems and Clean Energy, vol. 6, no. 5, pp. 860–871 (2018).
26. Xu, A., Jiang, Y., Zhang, Y., Hong, C., Cai, X.: "A Double-Layer Cyber Physical Cooperative Emergency Control Strategy Modification Method for Cyber-Attacks against Power System." In: 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–5 (2020).
27. Pasqualetti, F., Dorfler, F., Bullo, F. "Attack Detection and Identification in Cyber-Physical Systems." In: IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729 (2013).
28. Larkin, R., Wagner, T., Mullins, B.: "Securing photovoltaic system deployments with data diodes." In: 2020 47th IEEE Photovoltaic Specialists Conference (PVSC), pp. 2525–2531 (2020).
29. Li, F., Li, Q., Zhang, J., Kou, J., Ye, J., Song, W., Mantooth, H.: "Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network." In: IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2495–2498 (2021).
30. Tertytchny, G., Karbouj, H., Hadjidemetriou, L., Charalambous, C., Michael, M., Sazos, M., Maniatakos, M.: "Demonstration of Man in the Middle Attack on a Commercial Photovoltaic Inverter Providing Ancillary Services." In: 2020 IEEE CyberPELS (CyberPELS), pp. 1–7 (2020).
31. Zhang, J., Li, Q., Ye, J., Guo, L.: "Cyber-Physical Security Framework for Photovoltaic Farms." In: 2020 IEEE CyberPELS (CyberPELS), pp. 1–7 (2020).
32. Teymouri, A., Mehrizi-Sani, A., Liu, C.: "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability." In: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 2872–2877 (2018).
33. Majumdar, A., Agalgoankar, Y., Pal, B., Gottschalg, R.: "Centralized Volt-Var Optimization Strategy Considering Malicious Attack on Distributed Energy Resources Control." In: 2018 IEEE Transactions on Sustainable Energy, vol. 9, no. 1, pp. 148–156 (2018).
34. Elkhatib, M., El-Shatshat, R., Salama, M.: "Novel Coordinated Voltage Control for Smart Distribution Networks with DG," In: IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 598–605 (2011).
35. Sridhar, S., Hahn, A., Govindarasu, M.: "Cyber Attack-Resilient Control for Smart Grid." In: 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1–3 (2012).
36. Hawrylak, P., Haney, M., Papa, M., Hale, J.: "Using Hybrid Attack Graphs to Model Cyber-Physical Attacks in the Smart Grid." In: 2012 5th International Symposium on Resilient Control Systems, pp. 161–164 (2012).
37. Sarangan, S., Singh, V., Govindarasu, M.: "Cyber Attack-Defense Analysis for Automatic Generation Control with Renewable Energy Sources." In: 2018 North American Power Symposium (NAPS), pp. 1–6 (2018).
38. Wang, D., Guan, X., Liu, T., Gu, Y., Sun, Y., Liu, Y.: "A Survey on Bad Data Injection Attack in Smart Grid." In: 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–6 (2013).
39. Huang, Y., Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z., Li, H., Song, L.: "Bad Data Injection in Smart Grid: Attack and Defense Mechanisms." In: IEEE Communications Magazine, vol. 51, no. 1, pp. 27–33 (2013).

40. Li, F., Xie, R., Yang, B., Guo, L., Ma, P., Shi, J., Ye, J., Song, W.: "Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids with PVs: An Online High-Dimensional Data-Driven Approach." In: IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 1, pp. 1282–1291 (2019).
41. Kang, B., Maynard, P., McLaughlin, K., Sezer, S., Andren, F., Seitl, C., Kupzog, F., Strasser, T.: "Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations." In: 2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA), pp. 1–8 (2015).
42. Lee, C., Zappaterra, L., Choi, K., and Choi, H.: "Securing smart home: Technologies, security challenges, and security requirements." In: 2014 IEEE Conference on Communications and Network Security, pp. 67–72 (2014).
43. Singh, K., Choube, S.: "Using Blockchain Against Cyber Attacks on Smart Grids." In: 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1–4 (2018).
44. Kundur, D., Feng, X., Liu, S., Zourntos, T., Butler-Purry, K.: "Towards a framework for Cyber Attack Impact Analysis of the Electric Smart Grid." In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 244–249 (2010).
45. Jianfeng, D., Jian, Q., Jing, W., Xuesong, W.: "A Vulnerability Assessment Method of Cyber Physical Power System Considering Power-Grid Infrastructures Failure." In: 2019 IEEE Sustainable Power and Energy Conference (iSPEC), pp. 1492–1496 (2019).
46. Oyewole, P., Jayaweera, D.: "Power System Security with Cyber-Physical Power System Operation." In: IEEE Access, vol. 8, pp. 179970–179982 (2020).