Journal of Modern Technology
Vol. 01, No. 02, Dec 2024, pp. 75-86.

Homepage: https://review.journal-of-modern-technology.com

Enhancing Cyber Attack Detection in Microgrids for Resilient Energy Networks

Mohammad Parhamfar [1*], Alireza Zabihi [2], Milad Taheri [3], Benneth C. Oyinna [4]

[1*] Independence Researcher and Entrepreneur, Iran, Website: www.parhamfar.com , E-mail: drparhamfar@gmail.com , ORCID: https://orcid.org/0000-0002-3442-8270
[2] PhD Scholar, Department of Electrical Engineering and Intelligence Systems, University of Coimbra, Portugal. E-mail: alireza.zabihi@student.uc.pt , ORCID: https://orcid.org/0000-0003-4800-5583
[3] PhD scholar, Department of Electrical Engineering, Islamic Azad University of Najafabad, Isfahan, Iran. E-mail: milad.taheri@iau.ir, ORCID: https://orcid.org/0009-0001-0619-6601
[4] Centre for Power Systems Studies, University of Port Harcourt, Nigeria
E-mail: benneth.oyinna@nesconigeria.com, ORCID: https://orcid.org/0009-0006-4064-702X

Article Info

Article history:

Received Oct 16, 2024
Revised Nov 08, 2024
Accepted Nov 10, 2024
First Online: Nov 25, 2024

Keywords:

Cyber-attacks
Detection
Energy networks
Smart grid
Security

ABSTRACT

The threats posed by cyber-attacks on energy networks, especially microgrids, have become a significant concern as the global energy landscape becomes more interconnected and reliant on technological advancements. This study investigates the fundamental vulnerabilities in energy networks and the potential impact of cyber-attacks on power generation, consumption, and backup systems. The importance of robust identification systems cannot be overstated; real-time identification, mitigation, and response to cyber-attacks rely on advanced detection technology. This research underscores the critical role of active security protocols in safeguarding energy networks from cyber-attacks, focusing on coding in MATLAB and the development of best practices. The paper explores two scenarios - normal operations and attack situations - for three key units: power generation, power consumption, and power storage. The methodology involves: primary detection through statistical analysis and secondary detection through SPC. These findings emphasize the essential role of strong cybersecurity measures in ensuring the stability and dependability of microgrids, particularly in the face of escalating cyber threats.

[*] ***Corresponding Author:***

E-mail address: drparhamfar@gmail.com (Mohammad Parhamfar)

1. INTRODUCTION

The common improvements in cybersecurity, examined obstacles, vulnerabilities, and advantages, discussed a new descendant assault, and contrasted safety structures with first-generation techniques are well discussed in the literature [1]. Authors in [2] connected numerous study suggestions to a single theme by exploring the possible effects of CAs on electrical grid processes, such as condition estimates, autonomous power control, voltage management, and energy markets. While the paper assesses how false data injection can jeopardize stability, it may not deliver a detailed analysis of the cascading effects these attacks could have on the overall power grid. Li et al. [3], investigated a range

of CAs techniques, such as man-in-the-middle, denial-of-service, and fake data injection, on CPPS. There is a necessity to investigate successful approaches for preventing or addressing CAs in CPPS. Mitigation techniques might not be thoroughly evaluated for their effectiveness in real-time scenarios, where rapid response is crucial.

Reference [4] offered a method for risk identification that considers protective systems when assessing the cybersecurity of PSs. The research could fail to account for the complexities of real-world systems, and the protection systems can be more complex in realistic circumstances (e.g., including transformer protection, ground protection, and circuit breaker malfunction protection). The consequence of CAs on the dependability of generators and transmission lines is examined by using a FOR framework that is generated utilizing loss of load probabilities curves from ten distinct attacks [5]. While the study proposed a FOR model that considers the impacts of CAs on generator and transmission line reliability, there is a lack of comprehensive understanding regarding how various types of CAs specifically affect different components of the PS. In addition to offering some fresh ideas for scholars in related subjects, [6] aims to present an overview of CAs in CPPS through the viewpoints of the description, categories, frequent situations, and possibilities. In [7], the authors introduced a new malware identification method for electrical power distribution systems that effectively replicates complicated activities by using a real-time baseline framework. The system used chi-square testing as a residual-based ongoing identification of attack approach to assess data gathered from measurement results to regulate orders. Future research could explore its effectiveness, accuracy, and performance in detecting attacks within larger networks with more nodes and varying configurations.

Chen et al. [8] investigated load LFC for CAs and suggested a novel detection technique based on changeable properties. It's possible that the proposed changeable property-based detection method hasn't been thoroughly tested against a variety of attack scenarios outside the selected ones. The efficacy and dependability of the identification technique might not be known in the absence of careful evaluation. Zhou et al. [9] investigated the online detection of false data injection attacks and coordinated CPAs on PSs, proposing a cyber-physical FDIA with CCPA as a special case. While the article focused on FDIAs and CCPAs, there may be other types of CAs that also affect PSs but remain unaddressed. In [10], Bi and his colleagues utilized LFC methods shielded from dynamic CPAs through a unique detecting mechanism that uses the dynamic features of ACE to identify tainted content. The research gap could encompass more diverse and adaptive attack vectors that may evolve over time. Presekal et al. [11] suggested an innovative strategy for online CA scenario awareness. It employs a deep convolutional network and an integrated deep learning framework for real-time detection of anomalies. While the method demonstrated high accuracy in specific test cases, its ability to generalize across different power grid configurations, operational technologies, or geographical locations may not be established. Variations in network architecture and operational practices could affect the model's performance. Ref [12] offered a centralized process for CPA detection in ENs that leverages decentralized output injection and a sparse residual filter for distribution robustness without demonstrating uncertainty and limitations regarding interaction ability. Farrukh et al. [13] applied two-layer structured ML techniques with an accuracy rating of 95.44% for automated CA detection. Reference [14] provided a deep learning framework that uses both RNN and LSTM simultaneously to defend CPPSs against FCI assaults. The research gap could be addressed in future studies by redesigning the approach for MGs to focus on utilizing HIL laboratories. Wang et al. [15] described an online data-driven approach that employs semi-supervised clustering using K-means and local interaction among peers to recognize CAs in frequency management and PS balance. In a dynamic environment like PSs, generator behaviors can evolve, which may cause the model to become outdated. By employing an AC load flow-oriented simulation, [16] evaluated the smart grid 's resistance against FDI attacks and incorrect information recognition. It finds that CAs can cause overloading or large -scale breakdowns. The suggested model can be integrated with transient voltage stability and frequency stability to analyze the efficacy of the FDI paradigm. The purpose of [17] was to demonstrate a 98.19% accuracy rate in false data detection using FFN for replay CAs. Saber et al. [18] proposed an ABS that employs the isolation forest method to identify false-tripping assaults on LCDRs. In [19], Ntalampiras utilized a computationally intelligent approach that considers structural and temporal connections and combines linear time-invariant methods with NN. Reference [20] examined the difficulty

of designing and detecting centered secret CAs in shifting CPS, with an emphasis on the hidden strategies of hackers . On the other hand , reference [31] focused on how IoT integration improves the reliability and efficiency of smart grids, emphasizing important developments and practical applications. Zabihi et al. [32] analyzed the impact of integrating PHEVs and RESs on the power system, assessing load flow, short circuit scenarios, and economic implications to highlight the importance of smart grid adaptation. While RESs [35], such as hydropower [33] and PV [34] , can serve as power generation systems, there is a need for robust CA detection to protect the reliability and resilience of these RESs in interconnected microgrids [36]-[39].

According to the SOA, there are several techniques available for identifying CAs, including ML techniques, FNN, NN, AC load flow-oriented simulations, online data-driven approaches, RNN, LSTM, CNN, LFC, and FOR, etc, as discussed in the introduction along with the associated research gaps. This study concentrates on developing an enhanced framework capable of identifying CAs, which distinguishes it from previous research efforts. The key contributions of this research are as follows:

- The impact of CA on the microgrid, including power generation, power consumption, and energy storage.
- The provision of a primary detection method based on mathematical principles.
- The provision of secondary detection method based on SPC.
- The testing of fluctuations and variations in three units, and the verification of the framework.

This paper commences with an introductory section, followed by the presentation of the system model and mathematical equations in Section 2. Section 3 delves into the simulation results, while Section 4 is dedicated to the discussion. The paper concludes by summarizing the main findings.

2. MODELING FRAMEWORK

Concentrated ENs , known as MGs , can operate either independently from the primary network or in conjunction with it. Preserving their ability to withstand CAs is essential for maintaining a continuous electricity supply . The system model and mathematical formulas employed to analyze the effects of a CA on a MG are presented. The MG system comprises power generation, power consumption, and power storage components. The normal operation of the MG is disrupted by a simulated CA at a designated time, affecting power generation and consumption. The simulation runs for 24 hours. Under normal circumstances , power generation, power consumption, and power storage are outlined in equations (1) and (2) based on [23] to describe the standard condition. Equation (3) is also derived from (1) and (2).

$$P_{gen-norma}\ (t) = 50 + 10\sin\left(\frac{\pi t}{12}\right) \quad (1)$$

$$P_{cons-normal}(t) = 45 + 5.\sin\left(\frac{\pi t}{12} + \frac{\pi}{6}\right) \quad (2)$$

$$P_{stor-norma}\ (t) = Max\ (Min\big(P_{gen-normal}(t)_- P_{cons-normal}(t), 10\big), 0) \quad (3)$$

While in the simulation, the attack time is considered to be 12 hours, so:

$$P_{gen-attack}(t) = P_{gen-normal}(t) * 0.7 \quad (4)$$

$$P_{cons-attack}(t) = P_{cons-normal}(t) * 1.2 \quad (5)$$

$$P_{stor-attack}(t) = Max\ (Min\big(P_{gen-attack}(t)_- P_{cons-attac}\ (t), 10\big), 0) \quad (6)$$

In equations (4), (5), and (6), power generation, power consumption, and power storage within the attack situation are calculated. Figure 1 shows different units in MGs.

2.1. Primary Attack Detection

Tracking variations in power generation and consumption from their typical operating patterns is part of the detection method. The variances are expressed as a percentage of the actual (under attack) against anticipated (normal) values. If these variances exceed specified limits, the attack is identified. Equations (7), (8), and (9) are used to calculate the deviation for each unit.

$$Deviation_{generation}(t) = \frac{(P_{gen-attack}(t) - P_{gen-normal}(t))}{P_{gen-normal}(t)} \quad (7)$$

$$Deviation_{consumption}(t) = \frac{(P_{cons-attac}(t) - P_{cons-norma}(t))}{P_{cons-norma}(t)} \quad (8)$$

$$Deviation_{generation}(t) \geq threshold_{generation} \quad or \quad Deviation_{consumption}(t) \geq threshold_{consumption} \quad (9)$$

The threshold is considered 0.25 in this case, through trial and error in this section.

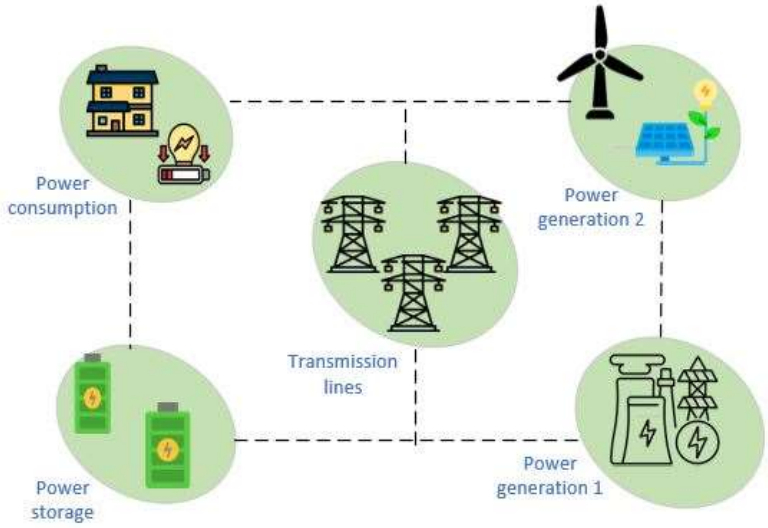

Fig. 1: MGs components.

2.2. Enhanced Methodology

The primary approach models latent association patterns in information by using PCA, which is derived from multivariable SPC [24]. SPC is a technique that monitors , regulates, and enhances a process by examining its data to identify trends and ensure it stays within predetermined parameters for reliable results [25]. SPC involves the use of measurement technology to continuously monitor and improve production processes, guaranteeing high-quality products and meeting the increasingly high standards for quality across various industries, including services, education, and public administration. SPC can support efficient quality management and ongoing improvements [26]. Managing data quality, handling complex process variability, adapting to changing circumstances, integrating with modern equipment, addressing false alarms, and the time and cost involved in setup are some of the challenges associated with using SPC for control and monitoring purposes [27, 28]. The aim of [29] is to offer a novel approach to problem detection for industrial plants that is based on SPC and time series models. It takes into account both dynamic and non-linear system aspects to reduce costs and enhance efficiency, and it has been validated on standard platforms. Through the analysis of sensor data from 31 wind turbines, the integration of servicing assessments into data mining management, the achievement of high accuracy with predictive algorithms, and the demonstration of the potential to enhance operational efficiency and reduce downtime, reference [30] employed SPC and machine learning techniques to recognize wind turbine faults and predict service

requirements. CA on MGs has the potential to compromise the reliability and stability of power systems. This research describes an SPC-based mechanism for identifying such types of attacks. SPC is a quality control technique that can be adapted to monitor variations in power generation and consumption. At a specified attack time, it creates variations in power generation and consumption, resulting in a 30% reduction in generation and a 20% increase in consumption. The next stage is the calculation of the moving average and moving standard deviation of the combined power generation and consumption data, followed by establishing control limits (upper and lower) based on the moving average and standard deviation. The final stage involves identifying anomalies by checking whether the power generation or consumption data points fall outside the control limits. Equations (9) to (13) are applied for the enhanced methodology. Figure 2 presents the detection approach flowchart. ω is 10 during this part. In this study, the authors adopt the methodology based on the enhanced approach, which is referenced in [21, 22].

$$Moving_{average}(t) = \frac{1}{\omega}\sum_{i=t-\omega/2}^{t+\omega/2} data\ (i) \tag{10}$$

$$Moving_{standard-deviation}(t) = \sqrt{\frac{1}{\omega}\sum_{i=t-\omega/2}^{t+\omega/2}(data\ (i) - (Moving_{average}(t))^2} \tag{11}$$

$$\begin{Bmatrix} upper_{limit}(t) = Moving_{average}(t) + 2 * Moving_{standard-deviati}\ \ (t) \\ lower_{limit}(t) = \ Moving_{average}(t) - 2 * Moving_{standard-deviation}(t) \end{Bmatrix} \tag{12}$$

$$Anomalies\ (t) = \ data\ (t) > upper_{limit}(t)\ \ or\ data\ (t) < lower_{limit}(t) \tag{13}$$

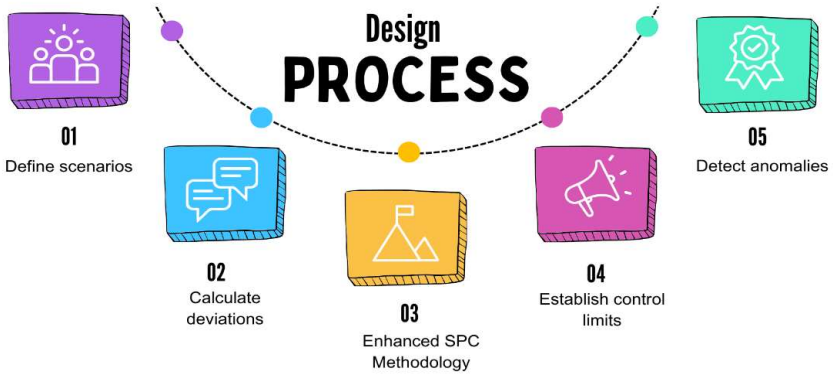

Fig. 2: Flowchart of detection methodology.

2.3. Simulate Real-Scenario

To validate and simulate the real scenario, which involves unit fluctuations, this section applies a fluctuation component for each unit to capture this concept and observe the results of the enhanced detection methodology. To implement this scenario $\epsilon_{gen}, \epsilon_{cons}$ are added to each section to introduce random noise, simulating fluctuations to validate the methodology.

How can SPC be utilized by technicians? To address this issue, real-time data from various locations, including distribution lines, transformers, and substations, can be monitored in a smart grid system using IoT-enabled devices. Engineers can identify potential cyber intrusions, such as attacks on the system's SCADA network, by employing control charts to monitor voltage, power flows, and data packet transfers. Abnormalities in predicted internet traffic or power flow indicate potential data manipulation.

3. RESULTS

The results of the simulation are presented in this section under two scenarios: normal operation and an attack situation. Different cases are examined for three key units: power generation, power consumption, and power storage. The primary detection method relies on statistical analysis and variation to identify the attack time by flagging a transition from zero to one. The secondary detection method is based on SPC, which was described in the previous section. This method aims to detect the specific area and time of occurrence of anomalies by monitoring the three units of the MG. To validate the framework, fluctuations are introduced to each unit to assess the results and performance of the enhanced detection method. The following figures illustrate the simulation results.

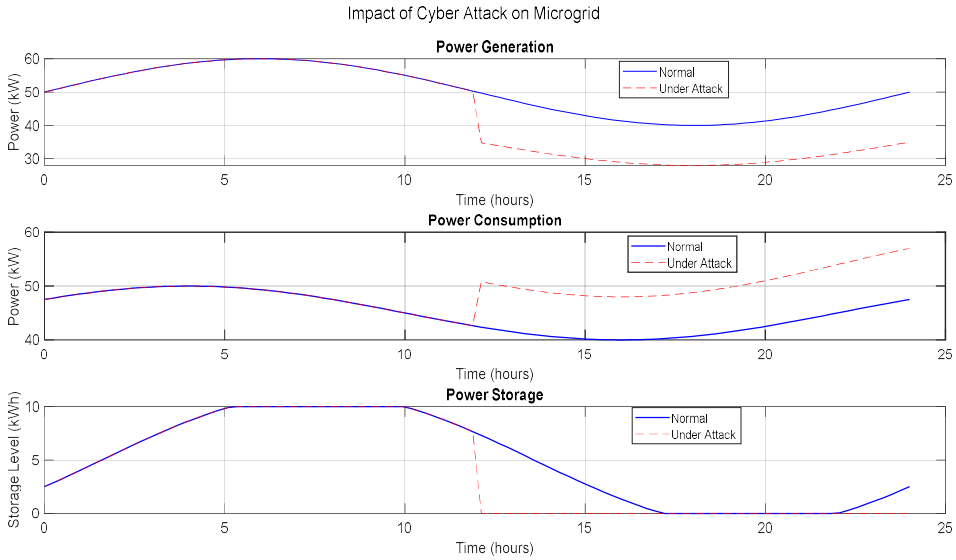

Fig. 3: Power generation, power consumption, and power storage under normal, and attack situation.

According to Figure 3, under normal conditions, power generation peaks at around 50 kW between 5 and 10 hours and then gradually decreases to a minimum at around 15 hours before increasing again toward the end of the period. When under attack, power generation drops sharply after 10 hours, reducing to zero and remaining low until nearly the 20th hour before slightly recovering. Power consumption starts at around 40 kW, peaks at about 10 hours, and then decreases gradually until the 15th hour before slightly rising again. During attacks, power consumption initially follows a similar pattern but diverges after 10 hours, showing an increase rather than a decrease, peaking around 15 hours and then continuing to rise steadily. The power storage level increases steadily, reaching a peak at 10 hours and then decreasing steadily until it hits zero at around 15 hours, before starting to increase again. The storage level shows a similar initial increase but then drops sharply to zero at 10 hours and remains depleted throughout the observed period.

Figure 4 illustrates all previous situations while adding the detection of a CA on the MG over a 24-hour period. The last plot, which shows attack detection, uses a binary flag (0 or 1) to indicate whether an attack is detected at any given time. The detection flag remains at 0 (indicating no attack) from the start of the observation period until approximately the 11th hour. Around the 11th hour, the detection flag sharply rises to 1, indicating the detection of a CA on the MG. This change is depicted with a magenta line. Once the detection flag reaches 1, it remains at this value for the rest of the observation period, suggesting that the attack persists, or the system remains in a detected state without

recovery. Figure 5 illustrates anomaly detection using SPC for the MG over a 24-hour period. Furthermore, the figure emphasizes the detection of anomalies in power levels, comparing normal operations to those under a CA. Both lines begin similarly, but they start to diverge after the 5-hour mark. Under attack conditions, the power level drops significantly around the 10-hour mark and remains low for the rest of the period. The shaded region begins around the 10th hour, indicating the identification of anomalies in the power levels. This region persists until around the 18th hour, suggesting a prolonged period of identified anomalies. The blue shaded area emphasizes the effectiveness of SPC in detecting deviations from normal power levels, which are indicative of a CA.

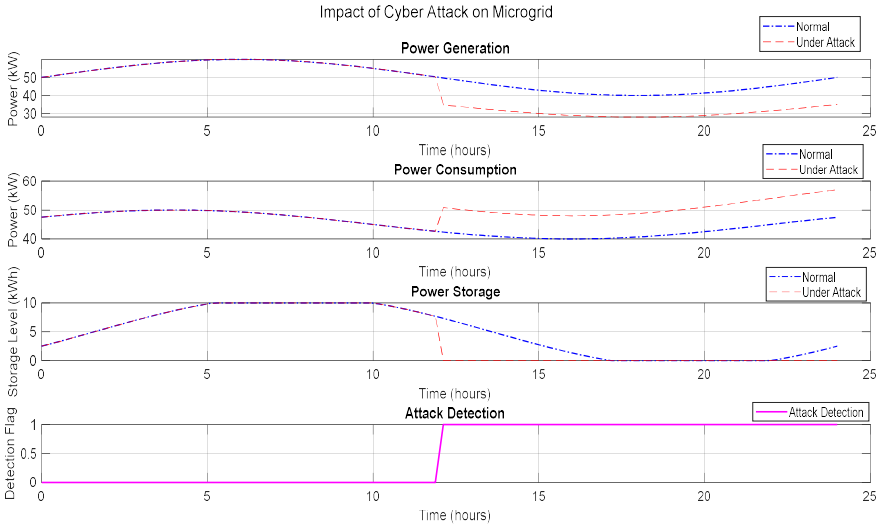

Fig. 4: Power generation, power consumption, and power storage under normal, and attack situation including the primary attack detection.

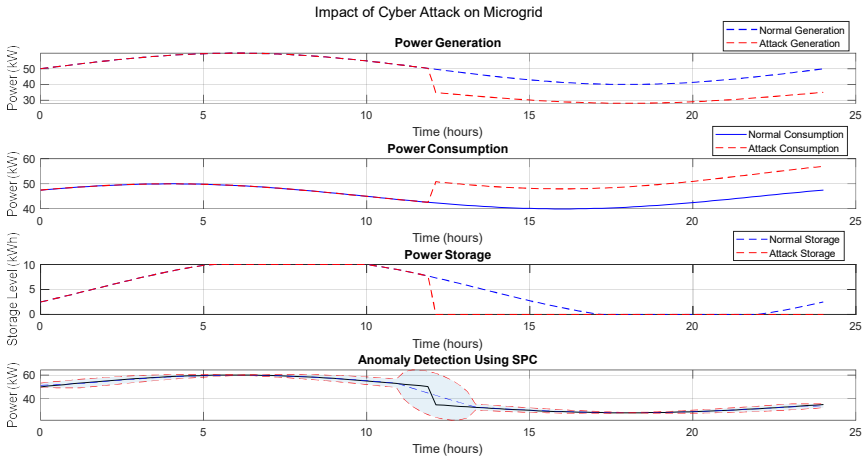

Fig. 5: Applying enhanced detection approach based on SPC.

The continuous detection flag value of 1 beyond this point indicates a sustained recognition of the attack, emphasizing the importance of real-time monitoring and rapid response mechanisms in safeguarding the MG against such disruptions. To validate the enhanced approach for the detection of CA in MG, fluctuations for each unit were applied to observe whether the methodology was functioning properly. After applying the changes, the results showed that the methodology worked well under fluctuations for each unit. Around the tenth hour, the shaded area began to appear, signifying the discovery of anomalies in the power levels. Figure 6

presents the improved detection technique , employing SPC and introducing variations for each section to simulate a real-world scenario.

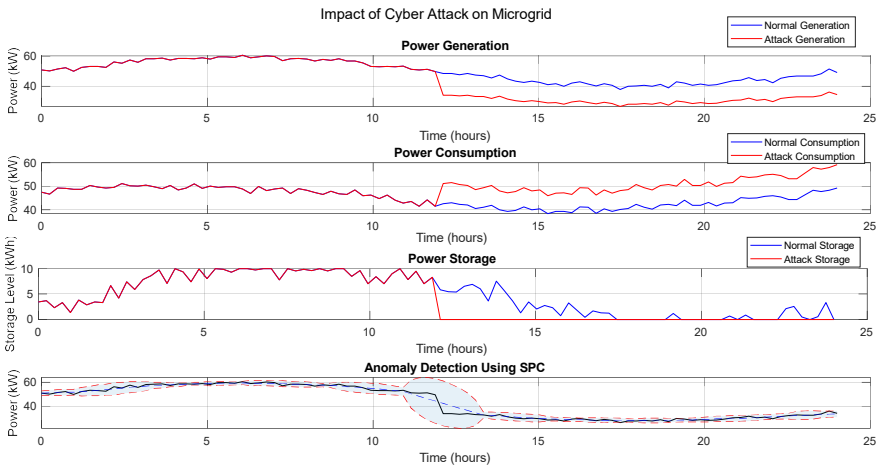

Fig. 6: Applying enhanced detection approach based on SPC, while simulating real situation.

4. DISCUSSION

This study examines power generation, consumption, and storage under normal and attack scenarios. The results show that power generation drops drastically after 10 hours, indicating disruption caused by a CA. Consumption rises to a peak and then declines gradually, while storage levels drop sharply and remain low, impacting the system's ability to store power. The primary detection method uses statistical analysis and variation to identify the attack time, flagging the transition from a non-attack state to an attack state around the 11th hour. The secondary method, based on SPC, monitors the specific area and time of anomalies by observing the three units of the MG. The enhanced detection method, which simulates real-world conditions, ensures robustness against normal variations and can identify genuine attacks. The simulation results emphasize the importance of robust cybersecurity measures in maintaining the stability and reliability of MGs, especially in the face of increasing cyber threats.

This study has some limitations. Instead of setting the values of certain parameters, such as ω, manually, future work could focus on optimizing these parameters. The enhanced method also has some limitations, such as the inability to apply various types of CAs with different strengths. It might be more effective to employ ML techniques to observe and test this scenario. According to Figure 4, the final plot illustrates the results of the primary detection method, which successfully detects CAs in a timely manner. Challenges associated with SPC implementation are illustrated in Figure 7.

The research gap, according to the SOA, is provided in Table 1. Future work could focus on exploring to bridge gaps:

- Implement ML techniques to enhance anomaly detection by learning from historical data and adapting to new threats.
- Analyses the methodology under various types of CAs.
- Investigate how different types of CAs specifically impact power quality.

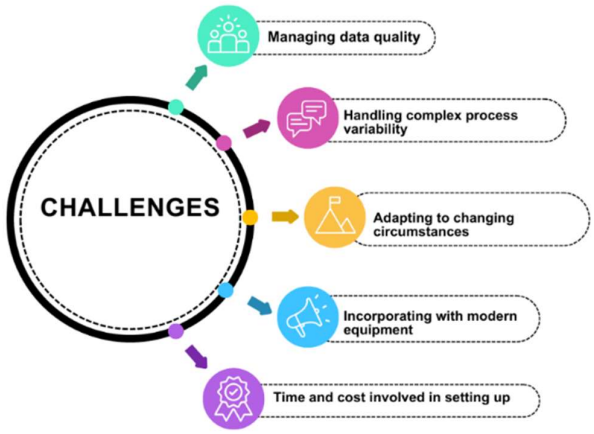

Fig. 7: Challenges in the application of SPC.

Table 1. The shortcomings in the SOA.

Ref	Research gap
[1]	The potential research gap refers to the impacts of CAs on the power grid.
[2]	It does not provide a detailed analysis of CAs.
[3]	Mitigation techniques may not have been thoroughly evaluated for their effectiveness in real-time scenarios, where a rapid response is crucial.
[4]	The research may have overlooked the practical aspects of protection systems, such as transformer, ground, and circuit breaker malfunction protection, which are essential in real-world systems.
[5]	There is a lack of detailed knowledge about how multiple types of CAs directly impact various PS components.
[7]	Further investigations might examine how well it performs, its accuracy, and how effectively it detects assaults in larger networks with additional nodes and diverse setups.
[8]	The proposed property-based identification system might not have been adequately evaluated across all prospective attack cases, not just the selected types.
[9]	Although CCPAs and FDIAs were the article's main topics, other CA types that might also impact PSs were not addressed.
[10]	The lack of research may include more varied and adaptable assault routes in the future.
[11]	Although the approach showed excellent accuracy in certain test instances, it remains unclear whether it can be applied to other power grid topologies, operational technologies, or regions.
[12]	A centralized method was provided for detecting CPA in ENs while avoiding ambiguity and limiting interaction by utilizing a sparse residual filter for distribution robustness and decentralized result injection.
[13,14]	Future studies may modify the strategy for MGs to focus on leveraging HIL laboratories, addressing the research deficit.
[15]	Generator characteristics can change in dynamic environments such as PSs, causing the framework to become outdated.
[16]	The effectiveness of the FDI paradigm can be examined by integrating the proposed model with transient voltage stability and frequency stability.
[19]	Introducing additional complexity makes finding the optimal configuration challenging and time-consuming.

5. CONCLUSION

The simulation results are presented for two scenarios: normal operation and a situation involving an attack. Various scenarios are analyzed for three main components: power generation, power consumption, and power storage. Under normal circumstances, power generation exhibits a consistent pattern, peaking during midday and decreasing towards the evening. However, during an attack, power generation experiences a sharp decline after 10 hours, suggesting a disruption caused by the attack. Typically, power consumption increases to a peak and then gradually decreases. In the event of an attack, the consumption pattern deviates significantly after 10 hours, displaying an abnormal increase not observed during normal operations. The storage level during normal operation rises to a peak and then decreases steadily. Conversely, during an attack, storage levels plummet rapidly and remain low, indicating a substantial impact on the system's power storage capability. The primary detection method relies on statistical analysis and variation to identify the attack time. This method effectively flags the transition from a non-attack state (zero) to an attack state (one) around the 11th hour, indicating the onset of the CA. The secondary method, based on SPC, aims to detect the specific area and time of occurrence of anomalies by monitoring the three units of the MG. This method is visualized in the anomaly detection plot, where the gray shaded area indicates the detection of anomalies in power levels. To validate the framework, fluctuations were introduced to each unit to assess the results and performance of the enhanced detection method. This approach simulates real-world conditions, ensuring that the detection method is robust against normal variations and capable of identifying genuine attacks. The simulation results highlight the critical role of advanced detection methods in safeguarding MG operations. The primary detection method effectively identified the onset of CAs, while the enhanced SPC-based approach provided a detailed analysis of the anomalies, ensuring timely and accurate detection. These findings underscore the importance of robust cybersecurity measures in maintaining the stability and reliability of MGs, especially amid increasing cyber threats.

DECLARATIONS

Conflict of Interest: The authors declare that there is no conflict of interests.

Funding: This research received no external funding.

Availability of data and materials: No data is available in this article.

Publisher's note: The Journal and Publisher remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

[1] Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." *Energy Reports* 7 (2021): 8176-8186. DOI: https://doi.org/10.1016/j.egyr.2021.08.126

[2] Chatterjee, Kaustav, V. Padmini, and S. A. Khaparde. "Review of cyber-attacks on power system operations." In *2017 IEEE Region 10 Symposium (TENSYMP)*, pp. 1-6. IEEE, 2017.

[3] Li, Feng, Xinteng Yan, Yunyun Xie, Zi Sang, and Xiaoshu Yuan. "A review of cyber-attack methods in cyber-physical power system." In *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, pp. 1335-1339. IEEE, 2019. DOI: 10.1109/APAP47170.2019.9225126

[4] Liu, Xindong, Mohammad Shahidehpour, Zuyi Li, Xuan Liu, Yijia Cao, and Zhiyi Li. "Power system risk assessment in cyber attacks considering the role of protection systems." *IEEE Transactions on Smart Grid* 8, no. 2 (2016): 572-580.

[5] Zhang, Yichi, Lingfeng Wang, and Weiqing Sun. "Investigating the impact of cyber attacks on power system reliability." In *2013 IEEE international conference on cyber technology in automation, control and intelligent systems*, pp. 462-467. IEEE, 2013. DOI: 10.1109/TSG.2016.2545683

[6] Tang, Yi, Qian Chen, Mengya Li, Qi Wang, Ming Ni, and XiangYun Fu. "Challenge and evolution of cyber attacks in cyber physical power system." In *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, pp. 857-862. IEEE, 2016. DOI: 10.1109/APPEEC.2016.7779616

[7] Khan, Mohammed Masum Siraj, Jairo A. Giraldo, and Masood Parvania. "Attack detection in power distribution systems using a cyber-physical real-time reference model." *IEEE Transactions on Smart Grid* 13, no. 2 (2021): 1490-1499. DOI: 10.1109/TSG.2021.3128034

[8] Chen, Chunyu, Kaifeng Zhang, Kun Yuan, Lingzhi Zhu, and Minhui Qian. "Novel detection scheme design considering cyber attacks on load frequency control." *IEEE Transactions on Industrial Informatics* 14, no. 5 (2017): 1932-1941. DOI: 10.1109/TII.2017.2765313

[9] Zhou, Tailin, Kaishun Xiahou, L. L. Zhang, and Q. H. Wu. "Real-time detection of cyber-physical false data injection attacks on power systems." *IEEE Transactions on Industrial Informatics* 17, no. 10 (2020): 6810-6819. DOI: 10.1109/TII.2020.3048386

[10] Bi, Wenjun, Kaifeng Zhang, Yaping Li, Kun Yuan, and Ying Wang. "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis." *IEEE Systems Journal* 13, no. 3 (2019): 2859-2868. DOI: 10.1109/JSYST.2019.2911869

[11] Presekal, Alfan, Alexandru Ştefanov, Vetrivel Subramaniam Rajkumar, and Peter Palensky. "Attack graph model for cyber-physical power systems using hybrid deep learning." *IEEE Transactions on Smart Grid* 14, no. 5 (2023): 4007-4020. DOI: 10.1109/TSG.2023.3237011

[12] Dörfler, Florian, Fabio Pasqualetti, and Francesco Bullo. "Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach." In *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1486-1491. IEEE, 2011.DOI: 10.1109/Allerton.2011.6120343

[13] Farrukh, Yasir Ali, Zeeshan Ahmad, Irfan Khan, and Rajvikram Madurai Elavarasan. "A sequential supervised machine learning approach for cyber attack detection in a smart grid system." In *2021 North American Power Symposium (NAPS)*, pp. 1-6. IEEE, 2021. DOI: 10.1109/NAPS52732.2021.9654767

[14] Naderi, Ehsan, and Arash Asrari. "Toward detecting cyberattacks targeting modern power grids: A deep learning framework." In *2022 IEEE World AI IoT Congress (AIIoT)*, pp. 357-363. IEEE, 2022. DOI: 10.1109/AIIoT54504.2022.9817309

[15] Wang, Pengyuan, Manimaran Govindarasu, Aditya Ashok, Siddharth Sridhar, and David McKinnon. "Data-driven anomaly detection for power system generation control." In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 1082-1089. IEEE, 2017. DOI: 10.1109/ICDMW.2017.152

[16] Shahinzadeh, Hossein, Arezou Mahmoudi, Jalal Moradi, Hamed Nafisi, Ersan Kabalci, and Mohamed Benbouzid. "Anomaly detection and resilience-oriented countermeasures against cyberattacks in smart grids." In *2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS)*, pp. 1-7. IEEE, 2021. DOI: 10.1109/ICSPIS54653.2021.9729386

[17] Sengan, Sudhakar, V. Subramaniyaswamy, V. Indragandhi, Priya Velayutham, and Logesh Ravi. "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning." *Computers & Electrical Engineering* 93 (2021): 107211. DOI: https://doi.org/10.1016/j.compeleceng.2021.107211

[18] Saber, Ahmad Mohammad, Amr Youssef, Davor Svetinovic, Hatem H. Zeineldin, and Ehab F. El-Saadany. "Anomaly-based detection of cyberattacks on line current differential relays." *IEEE Transactions on Smart Grid* 13, no. 6 (2022): 4787-4800. DOI: 10.1109/TSG.2022.3185764

[19] Ntalampiras, Stavros. "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling." *IEEE Transactions on Industrial Informatics* 11, no. 1 (2014): 104-111. DOI: 10.1109/TII.2014.2367322

[20] Eslami, Ali, Mohamad Ghasem Kazemi, and Khashayar Khorasani. "Event-Based Covert Cyber-Attack in Switching Cyber-Physical Systems: Design and Detection Mechanisms." In *2024 IEEE International Systems Conference (SysCon)*, pp. 1-7. IEEE, 2024. DOI: 10.1109/SysCon61195.2024.10553591

[21] Hassan, Adnan, M. Shariff Nabi Baksh, Awaluddin Mohd Shaharoun, and Hishamuddin Jamaluddin. "Improved SPC chart pattern recognition using statistical features." *International Journal of Production Research* 41, no. 7 (2003): 1587-1603. DOI: https://doi.org/10.1080/0020754021000049844

[22] Sachs, Emanuel, Albert Hu, and Armann Ingolfsson. "Run by run process control: Combining SPC and feedback control." *IEEE Transactions on Semiconductor Manufacturing* 8, no. 1 (1995): 26-43. DOI: 10.1109/66.350755

[23] Chen, Leian, and Xiaodong Wang. "Quickest attack detection in smart grid based on sequential Monte Carlo filtering." *IET Smart Grid* 3, no. 5 (2020): 686-696. DOI: https://doi.org/10.1049/iet-stg.2019.0320

[24] Hansen, Henrik Hviid, Murat Kulahci, and Bo Friis Nielsen. "Statistical process control versus deep learning for power plant condition monitoring." *Computers & Chemical Engineering* 178 (2023): 108391. DOI: https://doi.org/10.1016/j.compchemeng.2023.108391

[25] Oakland, John, and John S. Oakland. *Statistical process control*. Routledge, 2007. DOI: https://doi.org/10.4324/9780080551739

[26] Dönmezer, Semih. "Statistical Process Control (SPC) and Quality Management Systems as a Specialty of Quality Management and Case Turkey." *European Journal of Engineering and Formal Sciences* 4, no. 1 (2021): 1-16. DOI: https://doi.org/10.26417/ejef.v3i1.p6-17

[27] Tran, Phuong Hanh, Adel Ahmadi Nadi, Thi Hien Nguyen, Kim Duc Tran, and Kim Phuc Tran. "Application of machine learning in statistical process control charts: A survey and perspective." In *Control charts and machine learning for anomaly detection in manufacturing*, pp. 7-42. Springer, Cham, 2022. DOI: https://doi.org/10.1007/978-3-030-83819-5_2

[28] He, Q. Peter, Jin Wang, Devarshi Shah, and Nader Vahdat. "Statistical process monitoring for IoT-Enabled cybermanufacturing: opportunities and challenges." *IFAC-PapersOnLine* 50, no. 1 (2017): 14946-14951. DOI: https://doi.org/10.1016/j.ifacol.2017.08.2546

[29] Sánchez-Fernández, Alvar, Francisco Javier Baldan, Gregorio Ismael Sainz-Palmero, Jose Manuel Benitez, and M. J. Fuente. "Fault detection based on time series modeling and multivariate statistical process control." *Chemometrics and Intelligent Laboratory Systems* 182 (2018): 57-69. DOI: https://doi.org/10.1016/j.chemolab.2018.08.003

[30] Hsu, Jyh-Yih, Yi-Fu Wang, Kuan-Cheng Lin, Mu-Yen Chen, and Jenneille Hwai-Yuan Hsu. "Wind turbine fault diagnosis and predictive maintenance through statistical process control and machine learning." *Ieee Access* 8 (2020): 23427-23439. DOI: 10.1109/ACCESS.2020.2968615

[31] Zabihi, Alireza, and Amirhossein Shafiei Alavijeh. "Enhancing Reliability and Efficiency in Power Systems: The Role of IoT in Optimizing Smart Grids."

[32] Zabihia, Alireza, and Mohammad Parhamfarb. "Empowering the grid: toward the integration of electric vehicles and renewable energy in power systems." *International Journal of Energy Security and Sustainable Energy* 2, no. 1 (2024): 1-14. DOI: https://doi.org/10.5281/zenodo.12751722

[33] Zabihi, Alireza. "Assessment of Faults in the Performance of Hydropower Plants within Power Systems." *Energy* 7, no. 2 (2024). DOI: http://dx.doi.org/10.25729/esr.2024.02.0001

[34] Zabihi, Alireza, Mohammad Parhamfar, SSSR Sarathbabu Duvvuri, and Milad Abtahi. "Increase power output and radiation in photovoltaic systems by installing mirrors." *Measurement: Sensors* 31 (2024): 100946. DOI: https://doi.org/10.1016/j.measen.2023.100946

[35] Peng, Li, Alireza Zabihi, Mahdi Azimian, Hadis Shirvani, and Farhad Shahnia. "Developing a robust expansion planning approach for transmission networks and privately-owned renewable sources." *IEEE access* 11 (2022): 76046-76058. DOI: 10.1109/ACCESS.2022.3226695

[36] Patthi, Sridhar, VB Murali Krishna, Lokeshwar Reddy, and Sairaj Arandhakar. "Photovoltaic String Fault Optimization Using Multi-Layer Neural Network Technique." *Results in Engineering* (2024): 102299. DOI: https://doi.org/10.1016/j.rineng.2024.102299

[37] Sree, P. Bhavya, K. Balaji, Naveen Banoth, and Mohammad Parhamfar. "A Light Weight Mobile Net SSD Algorithm based dentification and Detection of Multiple Defects in Ceramic Insulators." *Journal of Modern Technology* (2024): 59-74.

[38] I. I. Al Barazanchi and W. Hashim. "Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach.", *SHIFRA*, (2023):1–8 DOI: 10.70470/SHIFRA/2023/002.

[39] Khalaf, M. A, Steiti, "Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks. " *Babylonian Journal of Machine Learning* (2024): 63–68. DOI: https://doi.org/10.58496/BJML/2024/006