Operational Mitigation of Cyberattack-Induced Cascading Failures in Power Systems

Hashemi, Sina; Panteli, Mathaios; Rajkumar, Vetrivel S.; Stefanov, Alexandru

DOI
10.1109/SEST61601.2024.10694287

Publication date
2024

Document Version
Final published version

Published in
Proceedings of the 2024 International Conference on Smart Energy Systems and Technologies (SEST)

Operational Mitigation of Cyberattack-Induced Cascading Failures in Power Systems

Sina Hashemi and Mathaios Panteli
Department of Electrical and Computer Engineering
University of Cyprus
Nicosia, Cyprus
{hashemi.seyedsina, panteli.mathaios}@ucy.ac.cy

Vetrivel S. Rajkumar and Alexandru Ştefanov
Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
{v.subramaniamrajkumar, a.i.stefanov}@tudelft.nl

2024 International Conference on Smart Energy Systems and Technologies (SEST) | 979-8-3503-8649-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/SEST61601.2024.10694287

***Abstract*—Cyber-physical power systems are susceptible to cyber threats and attacks that can lead to cascading failures and widespread power outages. Therefore, mitigating the impact of such attacks requires the timely implementation of operational strategies to prevent cascading blackouts. One Such strategy is the controlled islanding of the affected power grid, serving as a last resort against the propagation of the cascading outages. In this context, this paper introduces a novel detection-informed operational mitigation strategy, i.e., controlled islanding, against cyberattack-induced cascading failures, addressing "when" and "where" to implement controlled islanding. The proposed strategy leverages dynamic cascading failure modeling to quantify the impact of ongoing cyberattacks on power grids, using quantitative metrics such as demand-not-served (DNS). For effective operational mitigation, the strategy initiates controlled islanding when any attack, including fabricated protection trip commands and measurements' replay attacks, are detected, and any operating limits, such as line loading, are violated. It then proceeds to the implementation of controlled islanding, where identified cyberattack-affected elements are effectively surrounded by stable and self-sufficient islanded areas, while minimizing the system DNS. Numerical results on the IEEE 39-bus system demonstrate the effectiveness of the proposed strategy, reducing the DNS value by up to 47% when the controlled islanding strategy is implemented.**

Keywords— cascading failures, cyberattacks, anomaly detection, operational mitigation, controlled islanding.

I. INTRODUCTION

In future power systems with increased digitalization, cyberattacks may become one of the most common causes of cascading failures [1]. These events are classified as high-impact low-probability (HILP) events that threaten power systems and may lead to severe blackouts, especially in cyber-physical power systems (CPPS). The most recent impactful cyberattacks on power systems globally were associated with Ukraine in 2015 and 2016 [1], emphasizing the critical need for effective countermeasures against such incidents. To mitigate the impact of cyberattacks, especially when adversaries successfully breach network security and hack into the cyber network, it is necessary to implement an operational strategy applicable to power grids, thereby halting the spread of cascading failures. In general, cyberattacks may involve compromising communication links, such as those between phasor measurement units (PMUs) and Phasor Data Concentrator (PDC), as well as fabricating, altering, or deleting measurement data from PMUs or PDC, thereby impacting the integrity of data. Moreover, the system is susceptible to manipulation of control signals and protection commands through techniques like blocking controllers and replaying a trip command packet [2]. As power system operators cannot rely on measurement data following events that raise suspicions of cyberattacks, they can instead initiate the implementation of mitigation strategies surrounding the affected elements. This ensures the prevention of a system collapse resulting from the spread of a severe cascading blackout, providing an opportunity for direct communication between the control center and power plant or substations. Consequently, this facilitates a more in-depth investigation of evolving incidents, resulting in improved situational awareness of the power grid and informed decision-making for effective operations ahead.

The cascading failure phenomenon poses a constant threat to power systems, particularly as grids become more complex and the frequency of weather-related and cyberattack events continues to rise. Controlled islanding serves as an operational mitigation strategy in both preventive [3] and corrective [4] control actions. It can effectively alleviate cascading blackouts triggered by various initiating events, including extreme operating conditions, severe weather-related incidents, and cyberattacks. For an effective operational mitigation strategy applicable to the power grid in near-real-time, the computational time of the controlled islanding method needs to be as short as possible [4], [5]. In [5], different controlled islanding methods suitable for online Wide-Area Monitoring, Protection, and Control (WAMPC) application are evaluated. Fig. 1 illustrates conceptually how the implementation of an operational mitigation strategy, such as corrective controlled islanding, can affect system resilience, specifically during the disturbance progress phase. It can effectively halt cascading propagation, thereby reducing degradation in system performance and contributing to the improvement of system resilience. Drawing from an extensive review of existing literature in [1], [2], [6], various types of attacks within the CPPS context are addressed in terms of detection, prevention, and mitigation. However, a notable proportion of these studies, exemplified by [3]–[5], do not explore or emphasize an operational mitigation strategy, such as controlled islanding, specifically designed to seamlessly quantify, detect, and mitigate the impacts of cyberattack-induced cascading failures in power systems. This work aims to bridge this gap by exploring such an impactful phenomenon through dynamic cascading failure modelling (DCFM). In this paper, we introduce an effective mitigation strategy based on controlled islanding to suppress the progressive impact of cascading outages by confining the cyberattack-affected elements within limited islanded areas.

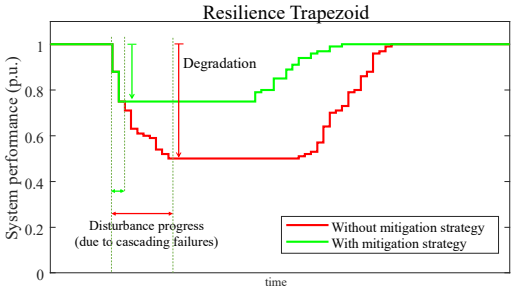

Fig. 1. Resilience trapezoid without and with the implementation of a reactive mitigation strategy on the power grid.

This work was funded by the Horizon Europe project "HVDC-based Grid Architectures for Reliable and Resilient WIdeSprEad Hybrid AC/DC Transmission Systems" (HVDC-WISE) (Grant agreement ID: 101075424).

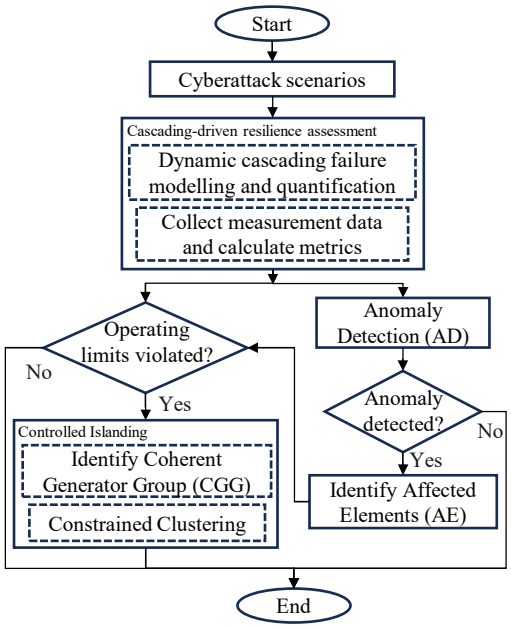

Fig. 2. Flowchart of the proposed methodology.

This paper develops a novel detection-informed mitigation strategy for power grids, incorporating the following items as its main contributions:

- A cascading-driven resilience assessment is performed through dynamic modeling and time-domain simulation of cyberattack-induced cascading failures to quantify the degradation in system performance following attacks, such as fabricated protection trip commands and measurements' replay attacks.
- The proposed strategy involves identifying affected elements to be included in the constraints of the controlled islanding problem. This enables the mitigation strategy to effectively split the system surrounding the affected elements, thereby limiting the propagation of cascading events.
- The methodology is developed based on corrective controlled islanding as an operational mitigation strategy against evolving cyberattacks, providing near-real-time applicability while ensuring the stability and self-sufficiency of islanded subnetworks during system split.

II. Controlled Islanding Methodology Against Cyber-Induced Cascading Outages

The methodology introduced in this work primarily focuses on mitigating cascading impacts in power systems induced by cyberattacks through an operational strategy, which involves controlled islanding with near-real-time applicability to power grids. Fig. 2 shows the flowchart of the proposed methodology, which mainly encompasses cascading-driven resilience assessment, anomaly detection (AD), identification of affected elements (AE), and controlled islanding. The aim of the methodology is to reduce the impacts of cascading failures by splitting the system into stable and self-sufficient islands, thereby containing the evolving events triggered by the cyberattack-affected elements. To attain this, the identification of assets affected by cyberattacks needs to be incorporated into the controlled islanding framework, formulated as a constrained spectral clustering problem. The data needed to identify AE using the AD method and to detect operating limit violations involve the voltage of power system nodes and the flow of power network branches. Upon detecting any attack and subsequent violation of operating limits, such as line loading, controlled islanding is performed.

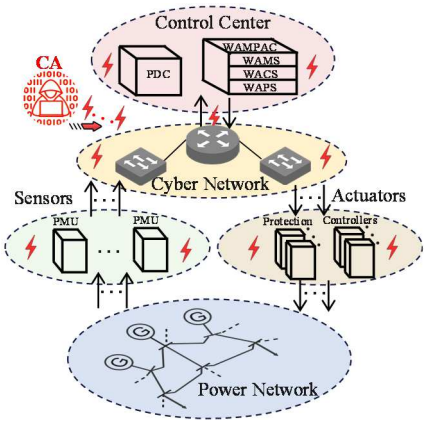

Fig. 3. Vulnerable points to launch cyberattacks on a conceptually represented typical CPPS.

A. Cyberattack modelling and considerations

Fig. 3 conceptually illustrates vulnerable points in CPPSs that adversaries can target to carry out their planned attacks. These vulnerabilities may include compromising communication links between PMUs and PDC, fabricating, altering, or deleting measurement data from PMUs or PDC, and manipulating control signals and protection commands. In this study, two types of cyberattacks, i.e., fabricated trip commands and replay attacks, are considered, targeting protection relays and measurement data, respectively. It is also assumed that network security is compromised and breached by adversaries through gaining necessary access to launch the cyberattacks, due to vulnerabilities within the cyber layer. In the attacker model, attack resources limited by the maximum available number are considered due to the attack budget [7]. This work explores different scenarios by setting the maximum number of concurrent attacks at different values ($\bar{R}$) [8]. It is also assumed that a maximum of only one generator can be attacked in each scenario. The cyberattack-affected elements are defined randomly, as formulated below:

$$A = \arg\ rand(E)$$

Subject to

$$\begin{aligned} \textstyle\sum_i e_i \le \bar{R} \quad , \quad e_i \in E \quad , \quad \forall\, i \in I \\ \textstyle\sum_\gamma e_\gamma \le 1 \quad , \quad e_\gamma \in E \quad , \quad \forall\, \gamma \in \Gamma \end{aligned} \tag{1}$$

where, A denotes a random integer vector representing cyberattack-affected elements, with values of 0 and 1 indicating not-affected and affected elements, respectively; E is a vector including binary numbers corresponding to all transmission lines and generators; I refers to a set of all network elements, comprising all transmission lines and generators, while Γ represents a set of all generators; $\bar{R}$ refers to the maximum number of concurrent attacks.

B. Cascading-driven resilience assessment

This work leverages dynamic cascading failure modeling to examine the proposed methodology's effectiveness in mitigating cascading impacts. Indeed, it conducts a cascading-driven resilience assessment of the power grid by measuring system degradation following cyberattack incidents. In essence, dynamic modeling of cascading failures captures entire cascade mechanisms and transient dynamics following a disturbance. This involves incorporating all relevant controllers and protective relays, such as the generator's governor and AVR, underfrequency and undervoltage load

shedding (UFLS and UVLS), over- and under-frequency generator tripping (OFGT and UFGT), and overcurrent relays [9]. The model is developed in the DIgSILENT software using time-domain RMS simulation [10]. It then quantifies the impacts of cyberattack-induced cascading failures through the DNS metric.

C. Identification of Affected Elements (AE)

As the proposed methodology is designed for near-real-time applications, the computational burden of the anomaly detection method needs to be low. To this end, the overall methodology employs the Pearson correlation as a data-driven online detection comparison metric for cyberattacks. It is used to measure the strength and direction of a linear relationship between two variables. This AD method is nearly instantaneous and effectively locates affected elements by calculating correlations of data within a moving window of PMU measurements [11]. Given that attack resources are limited and only a few elements can be targeted [7], detection of anomalies caused by cyberattacks, including fabricated trip commands and replay attacks, can be achieved by tracing correlations in measurement data. The method distinguishes between data packets originating from an actual fault or disturbance and those fabricated or altered by attackers. As a consequence of the cyberattack, a sudden drop in the correlation value between two successive instants is detected. This drop reflects a low or poor correlation, indicating a loss of a common trend and unison in the system's response at respective measurement points [11]. If the correlation value of a specific measurement compared to that of other neighboring measurements exhibits a distinctive trend, the corresponding element is identified as being attacked. The pseudocodes presented in Algorithm 1 outline the process of identifying affected elements due to cyberattacks. It is worth mentioning that, in this work, the cybersecurity measures are not taken into account for the current study. To assess the effectiveness of the anomaly detection algorithm, performance evaluation metrics such as True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR), and False Negative Rate (FNR) are employed, based on the confusion matrix [12].

D. Controlled islanding

The method of controlled islanding (CI) developed in this work, depicted in Fig. 2, employs constrained spectral clustering due to its low computational time [5], making it suitable for near-real-time applications in network splitting. The constraints in the CI problem, here, encompass coherent generators within each island and cyberattack-affected elements.

1) Identification of coherent generator group (CGG)

To maintain rotor angle stability following controlled islanding, it is crucial to cluster coherent generators together in the same group. Due to data availability and similarity to rotor angle behavior, phase angles of terminal voltage from generators, as measured by PMUs, are utilized for CGG identification [13]. This work employs the Intraclass Correlation Coefficient (ICC) and the K-medoids clustering algorithm [14] to develop a CGG identification method. The ICC measures the coherency between each pair of generators on a scale from 0 to 1, where values closer to 1 indicate higher coherency. Moreover, the K-medoids clustering algorithm is employed to partition the calculated ICC values into k-distinct clusters of coherent generators by identifying medoids that minimize the sum of dissimilarities between data points and their nearest medoid. For this purpose, a set of 100 samples, each spanning 10 milliseconds, is processed over a moving time window.

Algorithm 1: Identification of Affected Elements (AE)

- Collect phasor measurement data
- Calculate correlations between each pair of measurements within the moving window
- **if** a distinctive trend in correlations is detected **then**
  - **if** any tripping occurred **then**
    - Identify the tripped elements with the detected anomaly as Affected Elements (AE)
    - Proceed with the implementation of operational mitigation strategies
  - **end if**
- **end if**

2) Spectral clustering

In essence, the spectral clustering method utilizes the graph-cut of an undirected edge-weighted graph that is built according to Eq. (2) by ignoring the direction of power flow [15]. In this study, the arithmetical sum of the active power across a transmission line connecting nodes i and j serves as the edge weight (w_{ij}). The dynamic weighting of edges, based on power flow, incorporates the effects of changes in actual operating conditions on controlled islanding.

$$w_{ij} = w_{ji} = (|P_{ij}| + |P_{ji}|)/2 \tag{2}$$

The objective function, which focuses on minimizing the power flow disruption—represented by the absolute value of the active power flow across the splitting boundary branches—is expressed as follows:

$$\min\left(\sum_{i,j \in S_B} (|P_{ij}| + |P_{ji}|)/2\right) \tag{3}$$

where, S_B is the set of buses at both ends of the splitting boundary branches.

In the proposed methodology, constrained spectral clustering is employed with two types of pairwise constraints: Must Link (ML) and Cannot Link (CL) [16]. An ML constraint between two vertices ensures that these vertices will belong to the same cluster, while a CL constraint guarantees that the vertices will be assigned to different clusters. Given the objective of mitigating the progressive impact of cascading outages by confining affected elements within limited islanded areas, the identified coherent generator groups and cyberattack-affected elements are applied to the constrained controlled islanding problem through the pairwise constraints.

III. Results and Discussion

A. Case study application

The test system used in this study to demonstrate the effectiveness of the proposed methodology is the IEEE 39-bus system with a peak demand of 6259.4 MW. The study explores different values of the maximum number of concurrent attacks by setting $\bar{R}$ to 2, 3, and 4 [8] in the definition of three cyberattack scenarios. It is also assumed that only one generator can be attacked in each scenario, derived from historical cyberattack incidents [6]. The proposed methodology is simulated on a PC with an Intel core i7, 2.8 GHz CPU, and 16 GB RAM, taking a maximum computational time of around 5 seconds from detection to implementation. To extensively explore the methodology from an effective implementation perspective, three different scenarios of cyberattacks are randomly defined as follows:

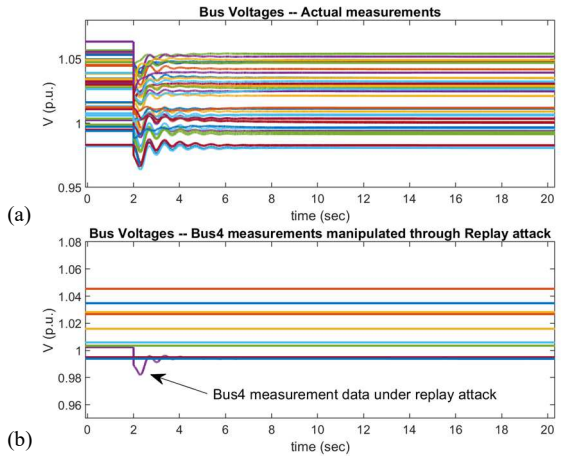

Fig. 4. Comapring the manipulated measurement data for bus voltages with the actual data.

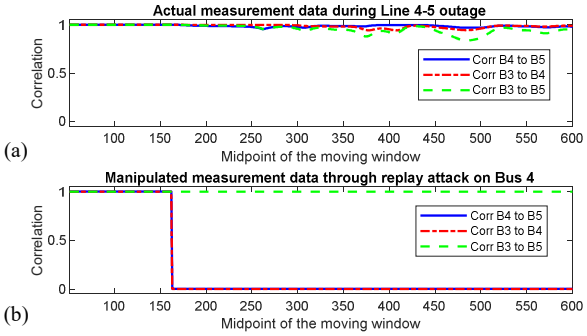

Fig. 5. Comapring the correlations between each pair of voltages for Bus 4 that are under replay attack with those of its beighbouring buses.

- Scenario 1: two concurrent attacks ($\bar{R} = 2$). Line 6-11 and Transformer 6-31 are targeted by a trip command attack on their relays, located at Bus 6.
- Scenario 2: three concurrent attacks ($\bar{R} = 3$). Gen 7, Line 4-5, and Line 1-39 are subject to a trip command attack, targeting their relays located at Bus 36, Bus 4, and Bus 39, respectively.
- Scenario 3: four concurrent attacks ($\bar{R} = 4$). Line 17-18 and Line 21-22 are subject to a trip command attack. In addition, two more replay attacks are launched at Bus 21 and Bus 18 to manipulate the measurement data.

B. Affected Elements' Identification

As described in Section II-C, the elements affected by a cyberattack are initially identified and then added to the operational mitigation strategy. This identification involves calculating the correlation between time-series voltage signals within a moving window. Subsequently, the elements identified as affected, which exhibit distinctive correlation trends compared to those of other neighboring buses, are incorporated into the constraints of the controlled islanding problem. Fig. 4 depicts the time-series bus voltages of the IEEE 39-bus system under line outage disturbances at 2 seconds of simulation. It compares the actual measurement data, shown in Fig. 4-(a), with the manipulated data without disturbances through the replay attack on Bus 4, as illustrated in Fig. 4-(b). Fig. 5 illustrates how a distinctive trend in correlations can be detected by comparing the respective values for actual data, depicted in Fig. 5-(a), with the manipulated data, shown in Fig. 5-(b). As can be seen in Figs. 4-(a) and 5-(a), following a disturbance, all actual measurement data undergo changes, and the corresponding correlations for neighboring buses experience nearly identical trends. This indicates that any bus losing correlations with other neighboring buses and exhibiting a distinctive trend, as illustrated in Fig. 5-(b), is identified as being anomalous. Similarly, in the case of fabricated trip commands, if no transients are detected from grid measurements but an element is tripped, it signifies an anomaly.

In this study, 100 test scenarios are used to evaluate the anomaly detection algorithm, consisting of 10 scenarios with anomalies and 90 scenarios without anomalies. The test results reveal that 11 scenarios are positive, with 9 scenarios classified as true positives (TP) and 2 as false positives (FP). Additionally, 89 scenarios are negative, with 88 scenarios classified as true negatives (TN) and 1 as false negative (FN). The evaluation metrics are then calculated as follows: TPR is 90%, FPR is 2.2%, TNR is 97.8%, and FNR is 10%. These values indicate the satisfactory performance of the algorithm, as the high TPR and TNR values, along with the low FPR and FNR values, demonstrate its effectiveness. In the exemplary case, as shown in Fig. 4, the affected element, Bus 4, is then assigned to the pairwise constraints of the controlled splitting problem. This effectively surrounds the identified affected elements with an islanded area, providing an opportunity for improved situational awareness of the power grid. This is essential as the system operator cannot rely on the measurement data and availability status of the targeted element. Therefore, by confining it within an island, the potential impacts of cascading failures are mitigated, providing more time for the implementation of appropriate security countermeasures.

C. Comparative studies of cyberattack-induced cascading failures with and without controlled islanding

This section thoroughly explores the effectiveness of the proposed reactive mitigation methodology, i.e., corrective controlled islanding. To this end, the randomly generated cyberattacks, as described in Section II-A and outlined earlier in three scenarios, are applied to the test system. Subsequently, the cascading-driven resilience assessment is conducted to demonstrate how the system performance degrades after cyberattacks, both with and without the controlled islanding strategy. Initially, the comparative study delves into more details, specifically focusing on Scenario 2. Then, the results of the same study for all scenarios are compared. According to Scenario 2, the attacks on G7, Line 4-5, and Line 1-39 are successfully launched through the manipulation of protection commands, leading to the tripping of these elements at 2 seconds of the simulation. Fig. 6 depicts the impacts of this attack scenario on the test system, showcasing the initiation and propagation of the cascade across a significant portion of the system, involving the outages of 3 generators, 14 buses, and 21 branches. This results in approximately a 52% demand loss.

To mitigate the cascading impacts, the system is split into three islands by opening Line 3-4, Line 3-18, Line 14-15, and Line 17-27 as shown in Fig. 7. The three islanded areas demonstrate how these stable and self-sufficient networks can absorb the impacts of the events and minimize the resultant DNS value. As described in Section II-D-1, to maintain rotor angle stability following controlled islanding, coherent generator groups are initially identified. In this scenario, {G1, G2, G3}, {G4, G5, G6}, and {G8, G9, G10} swing closely together and are grouped as shown in Fig. 8. Figs. 8 to 11 illustrate the system responses, both with and without

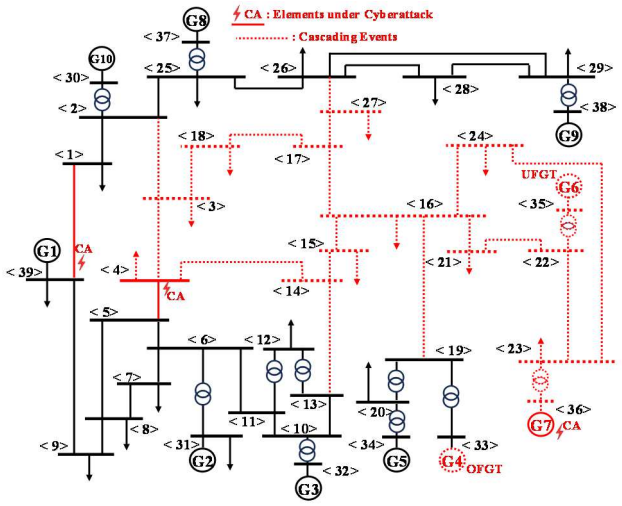

Fig. 6. Cascading propagation across a significant portion of the system under Scenario 2 of cyberattacks.

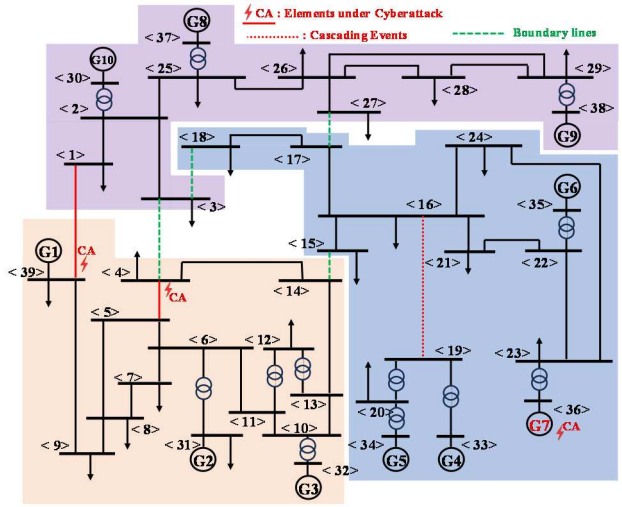

Fig. 7. Three identified islanded areas confining the cyberattack-affected elements related to Scenario 2.

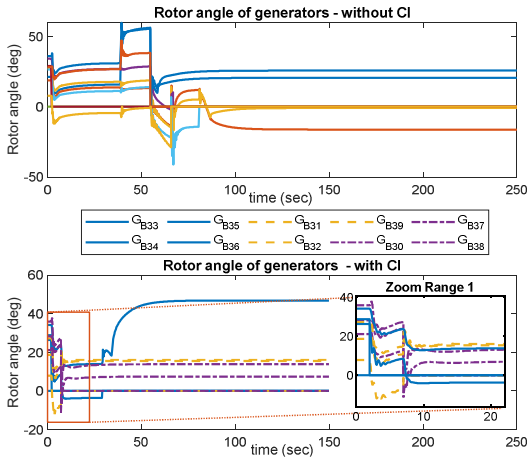

Fig. 8. Identification of coherent generators during the islanding process.

controlled islanding following the events, through time-domain RMS simulation. At 2 seconds of the simulation, the system is subjected to the cyberattack events. Approximately 5 seconds later, due to the algorithm's computational time, the controlled islanding strategy is implemented at 7 seconds, resulting in the system splitting into three islanded areas. In Fig. 9, the frequency responses of the system under the events in Scenario 2, both with and without controlled islanding, are compared. According to Fig. 9-(a), at each instant when the cascading failures propagate, the system frequency at each bus undergoes different changes across the system, depending on the value of load-generation imbalance. This imbalance arises from uncontrolled system splitting, as well as uncontrolled loss of load and generation following events during cascading propagation. At 66.7 and 81.7 seconds of the simulation, generators G4 and G6 are tripped due to the over-frequency generator tripping relay (OFGT) and the under-frequency generator tripping relay (UFGT) operations, respectively. As a result, a major part of the system, as depicted in Fig. 6, experiences a cascading blackout. In comparison, Fig. 9-(b) shows the same study with the controlled islanding implementation mentioned earlier in this section. It represents the transient deviations in frequency for each islanded area following the system splitting at 7 seconds of the simulation. In this case, the only element tripped by the overcurrent protection relay is Line 16-19 at 29 seconds of the simulation due to overloading.

Fig. 10-(a) elaborates on the variations of the total load over the simulation time resulting from the dynamic mechanisms of the cascade, which involve system controllers and protection relays such as governors and under-frequency load shedding. It clearly demonstrates system degradation due to cascading failures, comparing the total load with and without the islanding mitigation strategy. In Fig. 10-(b), the DNS values for the base case are compared, both without and with controlled islanding, corresponding to the entire system and at each individual bus once the system remains stabilized

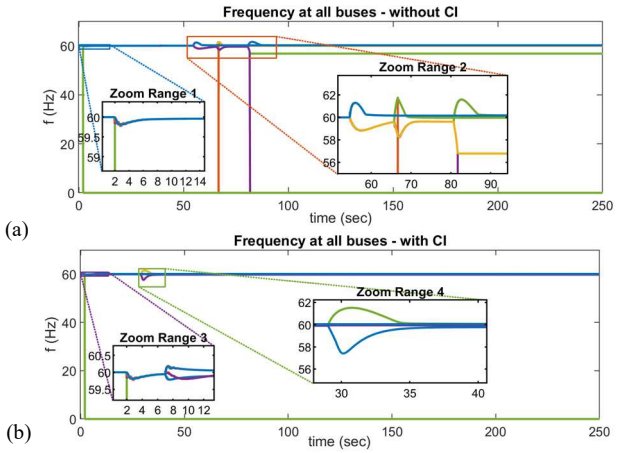

Fig. 9. Frequency deviations during cascading failures across the system corresponding to (a) without and (b) with corrective controlled islanding.

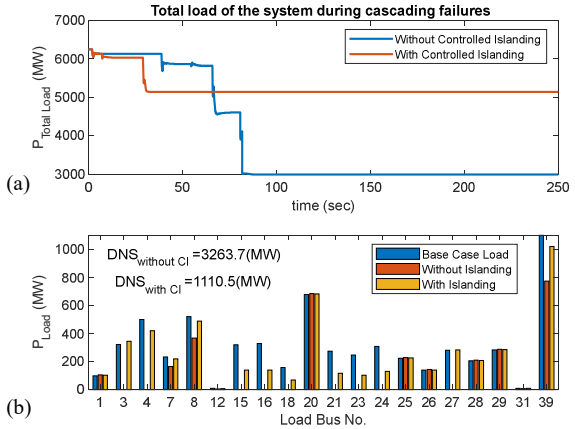

Fig. 10. Change in total system load during cascading failures corresponding to (a) without and (b) with corrective controlled islanding.

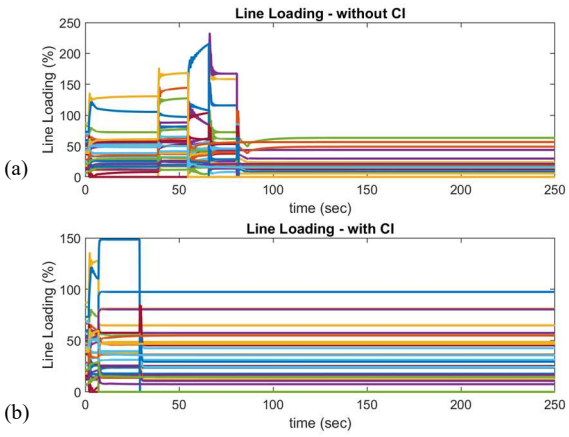

Fig. 11. Change in line loading during cascading failures corresponding to (a) without and (b) with corrective controlled islanding.

TABLE I. STUDY RESULTS FOR THE THREE DIFFERENT SCENARIOS

Cyberattack scenario no.		1	2	3
Maximum concurrent attacks		2	3	4
Targeted Elements		Line 6-11 Trans. 6-31	Gen. 7 Line 4-5 Line 1-39	Line 17-18 Line 21-22 Bus 21 * Bus 18 *
Type of attacks	* Replay	0	0	2
	Trip commands	2	3	2
DNS in MW (% of total demand)	Without CI	1381.7 (22.1%)	3263.7 (52.2%)	4751.2 (76%)
	With CI	1183.2 (18.9%)	1110.5 (17.8%)	1815.5 (29%)
	Improvement	198.5 (3.2%)	2153.2 (34.4%)	2935.7 (47%)

and the cascade halts. As a result of the controlled islanding, the total DNS value decreases from 3263.7 to 1110.5 MW, representing a 2153.2 MW reduction in loss of load or a 34.4% improvement in the system performance with ICI implemented. Fig. 11 illustrates the loading of the network lines, comparing the studies conducted without and with controlled islanding. It highlights the lines that are tripped due to overloading during the cascading propagation. It is worth noting that, owing to the inverse-time characteristics of overcurrent relays, the lines and transformers experiencing overload are tripped with varying delays based on the extent of overloading. Table I summarizes the results of the same cascading failure analysis for all attack scenarios, comparing the cases both without and with controlled islanding. The system DNS under the events of Scenarios 1, 2, and 3 is reduced from 1381.7 MW, 3263.7 MW, and 4751.2 MW to 1183.2 MW, 1110.5 MW, and 1815.5 MW, respectively, as a result of implementing the proposed methodology. Considering the total load, the overall improvements of 3.2%, 34.4%, and 47% in DNS are attained for Scenarios 1, 2 and 3, respectively. Thus, the study explicitly demonstrates that the controlled islanding strategy, serving as a last resort for power systems to endure, is particularly effective in mitigating highly impactful events, such as Scenario 3.

IV. CONCLUSION

This paper introduces a novel operational mitigation strategy against cyberattack-induced cascading failures through the seamless integration of dynamic cascading failure analysis, an anomaly detection technique, and a constrained controlled islanding method. The AD technique facilitates the identification of elements targeted by cyberattacks, such as fabricated protection trip commands and measurements' replay attacks, aiding in the effective implementation of an operational mitigation strategy. The mitigation strategy employed in this study involves corrective controlled islanding, constrained to identified coherent generator groups and cyberattack-affected elements, which can serve in near-real-time operation. These constraints enhance the methodology's effectiveness in system splitting by surrounding the affected elements with stable and self-sufficient islanded areas. This work leverages the dynamic cascading failure modelling developed in the DIgSILENT software to quantify the cascade impacts, capturing system dynamics stemming from cascade mechanisms after initiating events. The simulation results on the IEEE 39-bus system clearly highlight the benefits of the proposed operational mitigation strategy in alleviating the impact of cyberattack-induced cascading failures, resulting in a maximum reduction of 47% in DNS for the studied scenarios. This improvement is primarily attributed to isolating the affected elements and halting the propagation of cascading failures to other healthy parts of the system. Notably, a methodology for implementing cybersecurity measures, alongside the proposed operational mitigation strategy against a broader range of cyberattacks, will be considered as an extension of the paper in future work.

REFERENCES

[1] V. S. Rajkumar, A. Stefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures," IEEE Access, vol. 11, no. September, pp. 103154–103176, 2023.
[2] S. Vahidi et al., "Security of Wide-Area Monitoring , Protection , and Control (WAMPAC) Systems of the Smart Grid : A Survey on Challenges and Opportunities," IEEE Commun. Surv. Tutorials, vol. 25, no. 2, pp. 1294–1335, 2023.
[3] Z. Wang and Z. Wang, "A novel preventive islanding scheme of power system under extreme typhoon events," Int. J. Electr. Power Energy Syst., vol. 147, no. September 2022, p. 108857, 2023.
[4] S. Ranjbar, "Online estimation of controlled islanding time intervals using dynamic state trajectories through cascading failures from WAMS data," Electr. Power Syst. Res., vol. 214, no. PA, p. 108890, 2023.
[5] L. Ding, Y. Guo, and P. Wall, "Performance and suitability assessment of controlled islanding methods for online WAMPAC application," Int. J. Electr. Power Energy Syst., vol. 84, pp. 252–260, 2017.
[6] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications," IEEE Access, vol. 8, pp. 151019–151064, 2020.
[7] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach," Phys. Commun., vol. 47, p. 101394, 2021.
[8] K. Lai et al., "A Robust Energy Storage System Siting Strategy Considering Physical Attacks to Transmission Lines," 2018 North Am. Power Symp. NAPS 2018, pp. 1–6, 2018.
[9] Y. Dai, M. Noebels, M. Panteli, and R. Preece, "Benefits and Challenges of Dynamic Modelling of Cascading Failures in Power Systems," 11th Bulk Power Syst. Dyn. Control Symp. (IREP 2022), no. Irep, pp. 1–10, 2022.
[10] Y. Dai, M. Panteli, and R. Preece, "Python Scripting for DIgSILENT PowerFactory : Enhancing Dynamic Modelling of Cascading Failures," 2021.
[11] K. Chatterjee and S. A. Khaparde, "Data-driven Online Detection of Replay Attacks on Wide-Area Measurement Systems," 2018 20th Natl. Power Syst. Conf. NPSC 2018, pp. 1–6, 2018.
[12] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Comput. J., vol. 10, no. 1, pp. 1–35, 2010.
[13] M. R. Aghamohammadi, S. Fazel Mahdavizadeh, and Z. Rafiee, "Controlled Islanding Based on the Coherency of Generators and Minimum Electrical Distance," IEEE Access, vol. 9, no. November, pp. 146830–146840, 2021.
[14] H. S. Park and C. H. Jun, "A simple and fast algorithm for K-medoids clustering," Expert Syst. Appl., vol. 36, no. 2 PART 2, pp. 3336–3341, 2009.
[15] A. Esmaeilian and M. Kezunovic, "Prevention of power grid blackouts using intentional islanding scheme," IEEE Trans. Ind. Appl., vol. 53, no. 1, pp. 622–629, 2017.
[16] X. Wang, B. Qian, and I. Davidson, "On constrained spectral clustering and its applications," Data Min. Knowl. Discov., vol. 28, no. 1, pp. 1–30, 2014.