28th Electrical Power Distribution Conference, April 23-25, 2024, Zanjan, Iran

A Review and Analysis of Attack and Countermeasure Approaches for Enhancing Smart Grid Cybersecurity

Amir Meydani, Hossein Shahinzadeh, Ali Ramezani, Hamed Nafisi, Gevork B. Gharehpetian
Department of Electrical Engineering
Amirkabir University of Technology (Tehran Polytechnic)
Tehran, Iran
meydani@ieee.org, h.s.shahinzadeh@ieee.org, ali.ramezani@aut.ac.ir, nafisi@aut.ac.ir, grptian@aut.ac.ir

2024 28th International Electrical Power Distribution Conference (EPDC) | 979-8-3503-8550-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/EPDC62178.2024.10571761

Abstract—**The Smart Grid (SG) is an advanced power network that facilitates the two-way exchange of energy and information between consumers and providers. The field of cyber-physical smart grid has witnessed significant progress in recent times, leading to the development of various innovative gadgets that rely on information and communication technology. Yet, the utilization of ICT devices has greatly increased the vulnerability of SGs to potential attacks and broadened their range of potential threats. This study conducts a comprehensive analysis, based on reviews, of 184 contemporary attack and countermeasure strategies in the field of cybersecurity for smart grids. This article aims to examine the latest and most effective strategies of offensive and defensive maneuvers, as they undergo continuous advancements.**

Keywords—Smart Grid (SG); Cyber-Physical Smart Grid (CPSG); Cyber-Physical System (CPS); Cybersecurity; Power System (PS)

I. Introduction

The escalating global energy crisis and climate change have underlined the urgency for improved energy efficiency, harnessing renewable energy sources (RES), and introducing distributed generation (DG). The Traditional Power System (TPS), with its aging infrastructure, is struggling to keep pace with the burgeoning electrical demands of the modern world. Its limited ability to tap into RESs and inherent inefficiency in rectifying defects and issues further compound the problem. A significant paradigm shift has been brought about by the integration of Information and Communication Technology (ICT) and Cyber-Physical Systems (CPSs), transforming the TPS into the Smart Grid (SG) [1]. This transformation has given rise to an advanced, automated, and operational network that enables a mutual exchange of energy and data between suppliers and consumers. However, this innovative model known as the Cyber-Physical SG (CPSG), which marries a cyber-infrastructure with physical systems, is not without its vulnerabilities [2]. With the increased reliance on wireless connectivity, autonomous systems, and the integration of software and virtualization functions, the risk quotient for power networks has sharply escalated. Security of the CPSG can be compromised by both intentional and unintentional actions. On one hand, deliberate attacks can originate from multiple sources, including disgruntled employees, espionage agencies, hackers, and terrorist groups [3]. On the other hand, unintentional threats can originate from natural disasters or equipment malfunctions, each posing a significant risk to the security of the Smart Grid. Moreover, threats are not confined to the supply side alone. Vulnerabilities exist on the customer-side as well, with intrusions against smart inverters and Distributed Energy Resources (DER) being enabled by a number of factors. Despite the increasing potential for these cyber-physical attacks (CPAs), there exists an alarming gap in research into CPAs and the development of robust security mechanisms [4]. Therefore, it is critically important to stay updated with the latest advancements in SG security, particularly due to the intertwined nature of cyber and physical security aspects. This heightened understanding of the security challenges posed to the CPSG paves the way for the development of robust countermeasures and resilience strategies. The study of cyber threats to SG systems has focused mainly on various types of attacks, including false data injection, denial of service, data framing, man-in-the-middle, load altering, false command injection, load redistribution, coordinated cyber-physical (CP) topology attacks, and replay attacks, as shown in Fig. 1. By doing so, we can better protect our energy infrastructure, thereby addressing the global energy crisis, mitigating the impacts of climate change, and ensuring a secure, reliable, and sustainable energy future [5-6]. In the long run, these efforts will contribute to the broader goals of energy security, economic stability, and environmental sustainability.

II. Security and Cyber-Physical Concerns in SG

A. Security Requirements of SG: CIA

Service providers and consumers must adhere to the principle of *confidentiality*, which prevents unauthorized disclosure of information and restricts access to authorized users only. Unauthorized access to operational data of SG could potentially enable adversaries to discern the weak points of networks or gain privileged access to the system to execute malicious operations. *Integrity* ensures the precision and uniformity of data while safeguarding it against unauthorized tampering, deletion, or loss. Any tampered message transmitted into the SG is capable of causing system functionality to be disrupted. Crucial determinations, like pricing policies and power generation, are formulated on the basis of data acquisition and measurements from the SG environment. The system's regular operation may be jeopardized by any unauthorized modification of this data. It is essential that all authorized users have access to a dependable network. High *availability* is a fundamental goal of the SG, as it ensures the steadiness and dependability of the grid [7]. SG operates in numerous sectors of society, including enterprise, healthcare, transportation, education, and the households of its clients. Insufficient provision of services in critical infrastructure can result in substantial economic and societal repercussions.

B. Cyber-Physical Security Concerns

The essential layers upon which CPS operates are perception (physical), data transmission (network), and application (cyber). Physical, Detection, and Control and Communication elements are the three categories into which a CPS is composed. Device configurations that facilitate the physical process constitute the physical components of a CPS. A multitude of loads, including generators, transformers, switchgear, transmission line (TL), circuit breakers, motors, and cylinders, comprise the main components of Cyber–physical power system (CPPS). The sensing elements, which are tangibly connected to the physical system and tasked with observing and extracting data from the

979-8-3503-8550-2/24/$31.00 ©2024 IEEE

process, are devices. This unit focuses on actuators, sensors, and aggregators. The Control and Communication elements of CPS include devices tasked with the task of supervising and regulating the physical system. Programmable logic controller (PLC), distributed control systems (DCS), and remote terminal unit (RTU) are notable components for control, while the supervisory control and data acquisition (SCADA) and phasor measurement unit (PMU) undertake the task of data acquisition within CPS [8].

CP attacks are classified into *three* categories within CPSGs. *Control signal attacks* leverage the capacity to circumvent data authentication and integration checks to obtain authority over a physical device, enabling the perpetrator to manipulate its functionality. Mission-critical devices in power systems (PSs), including automatic generation control, relays, smart inverters, flexible AC transmission system (FACTS) devices, and circuit breakers, are the intended targets of the attack. Cases of *measurement attacks* focus on the falsification of RTU in the field or the manipulation of sensor measurement data over communication channels. To transmit fake messages, physical communication links are compromised (e.g., through RA, GPS deception, and FDI). *Control-measurement-loop attacks* involve the coordinated engagement of adversaries with the control signal and measurement. Immediate physical layer repercussions result from the control signal attack, while measurement attacks can obscure the ongoing control signal assault. The manipulated measurements evade the system's current anomaly detection mechanisms [9]. This attack (e.g., Stuxnet and line outage masking attack) augments the covert nature of control signal attacks through the concealment of attack repercussions and the deception of attack detection and mitigation systems.

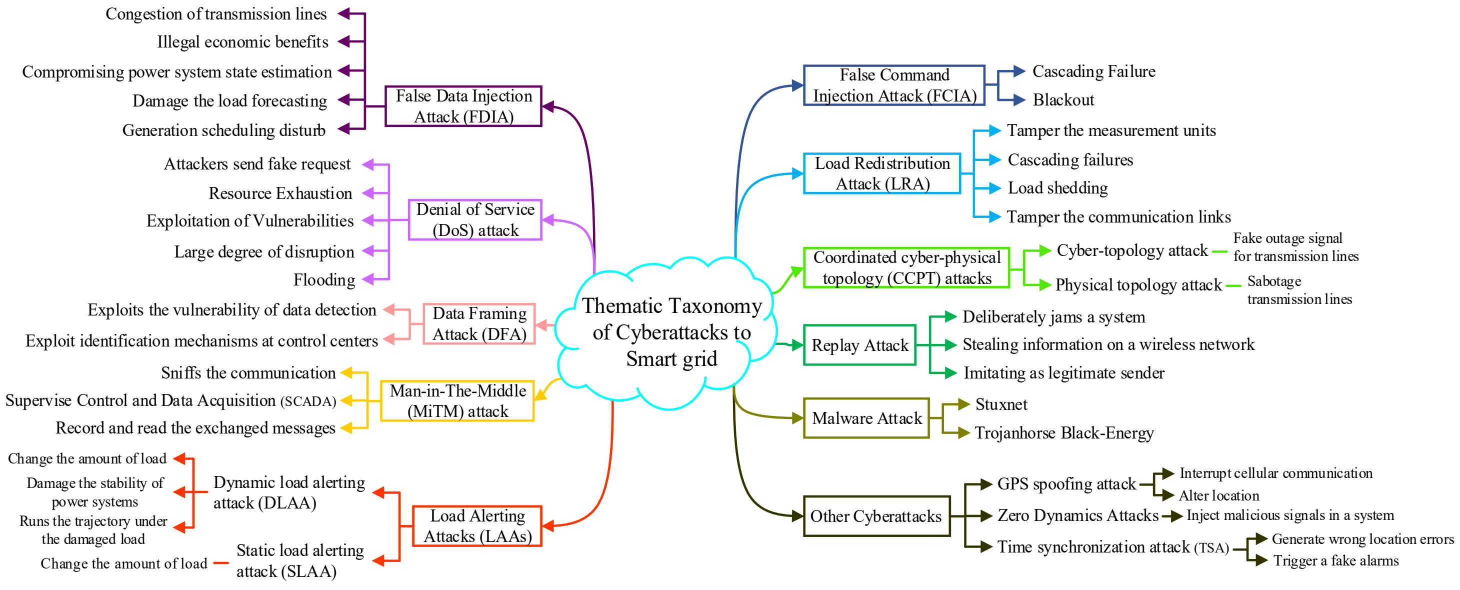
Thematic Taxonomy of Cyberattacks to Smart grid
False Data Injection Attack (FDIA)
Congestion of transmission lines
Illegal economic benefits
Compromising power system state estimation
Damage the load forecasting
Generation scheduling disturb
Denial of Service (DoS) attack
Attackers send fake request
Resource Exhaustion
Exploitation of Vulnerabilities
Large degree of disruption
Flooding
Data Framing Attack (DFA)
Exploits the vulnerability of data detection
Exploit identification mechanisms at control centers
Man-in-The-Middle (MiTM) attack
Sniffs the communication
Supervise Control and Data Acquisition (SCADA)
Record and read the exchanged messages
Load Alerting Attacks (LAAs)
Dynamic load alerting attack (DLAA)
Change the amount of load
Damage the stability of power systems
Runs the trajectory under the damaged load
Static load alerting attack (SLAA)
Change the amount of load
False Command Injection Attack (FCIA)
Cascading Failure
Blackout
Load Redistribution Attack (LRA)
Tamper the measurement units
Cascading failures
Load shedding
Tamper the communication links
Coordinated cyber-physical topology (CCPT) attacks
Cyber-topology attack
Fake outage signal for transmission lines
Physical topology attack
Sabotage transmission lines
Replay Attack
Deliberately jams a system
Stealing information on a wireless network
Imitating as legitimate sender
Malware Attack
Stuxnet
Trojanhorse Black-Energy
Other Cyberattacks
GPS spoofing attack
Interrupt cellular communication
Alter location
Zero Dynamics Attacks
Inject malicious signals in a system
Time synchronization attack (TSA)
Generate wrong location errors
Trigger a fake alarms

Fig. 1. A Thematic Categorization of Cyberattacks That Specifically Target Smart Infrastructure

III. Attack and Defense Strategies

A. Non-Technical Loss (NTL)/Electricity Theft Detection (ETD)

[10] examines an ETD algorithm that utilizes a contrastive learning architecture and non-intrusive load monitoring (NILM). To identify obvious fraudulent users, a semi-supervised learning architecture is utilized. This design incorporates Gramian angular field (GAF) encoding and contrastive learning, which effectively distinguishes between different appliance operation states during instances of electricity theft. Also, Kendall's W is used to filter out common regular-switched appliances. Operation routines of typical appliances are then introduced as an additional foundation to thoroughly assess suspected users. Ultimately, the chance of electricity theft is determined by merging the two phases. In [11], a three-module outlier-based detector was devised. To detect larceny at the end-user infrastructure, the method used the KNN algorithm and the local outlier factor (LOF). Before proceeding, outlier candidates were identified by calculating the deviation of each consumer from the respective cluster centers, after which consumption profiles were analyzed using k-means. The LOF algorithm was then used to compute the anomaly ranking of the chosen candidates. Despite the satisfactory detection accuracy of 0.9184, it remains incapable of identifying linear larceny, which occurs when an assailant consistently reduces the consumption profile. To analyze the ETA behavior, a broad and deep CNN model was devised in [12]. The model's broad component is an FCL that uses 1D electricity use data to acquire global knowledge. By converting the 1D data to 2D data in weeks, the deep CNN component is capable of distinguishing between the aperiodic nature of ETA and the periodic nature of typical electricity use. Using a weighted sum of their output as hidden features that are fed into a logistic loss function as a classifier to identify ETA behaviors, the two components are subsequently combined.

To identify instances of electricity fraud, [13] specifies the need for multiple detection stations and two servers. Consumers employ differential privacy (DP) specifically to safeguard the confidentiality of their readings prior to transmitting them to the detection stations. The received data is utilized to train local ML models by the detection stations. Subsequently, utilizing FL, the servers and detection stations construct a global electricity fraud detection model in collaboration. Using DP to protect privacy compromises the accuracy of electricity fraud detection; thus, a compromise exists between accuracy and privacy. In [14], On the basis of MLP, LSTM, and GRU, a three-stage ETA detection system is devised. The first one is a multi-DL model forecasting system for the next twenty-four hours of energy use; the second stage is a key decision-making model for determining energy theft predictions; and the third stage increases detection accuracy by conducting additional checks for potential energy theft. For ETA, a data-driven regression model was devised in [15]. As opposed to relying on unreliable secondary network topology information and parameters, the method used a modified linear regression algorithm. By using solely voltage data and consumer use data, this approach enhances its feasibility for adoption. In conclusion, real-world SM training data was used to validate the method, and the outcomes show the efficacy of the identification of energy fraud cases. Yet, the reliance on voltage measurements exposes consumer information to the risk of privacy breaches.

In [16], a hybrid DL model that combines CNN and GRU was proposed to effectively detect cyberattacks targeting ETAs in RE-based DG units. The model has the capability to extract and analyze the temporal connection that exists between the readings of DG SMs, irradiance data, and SCADA meter readings. This analysis is aimed at improving the performance of detection methods. A classification system for identifying energy fraud occurring at the end-user infrastructure was devised in [17]. The performance of the solution was evaluated using simulations that replayed the Irish Smart Energy Trail dataset. Its functionality was dependent on the combined utilization of a support vector machine (SVM) classifier, a power optimization algorithm, and a voltage sensitivity analysis component. In practice, the SVM classifier generated a weight function indicating the probability of fraudulent activity based on the annual active energy use of a consumer. The accuracy of the system under consideration was 0.994. In [18], a novel model utilizing graph convolutional neural networks (GCNs) is built to detect instances of electricity theft. The method offers a fresh perspective by leveraging the principles of graph theory (GT). More precisely, a method is devised to transform the one-dimensional electricity consumption data into a standardized graph, consisting of a feature matrix of nodes and an adjacency matrix. Also, graph convolutional layers and an adjacency matrix are utilized to capture the periodic patterns and temporal relationships of power load curves at each time point. An Euclidean CNN (ECNN) is introduced to extract underlying characteristics of power load curves by transforming the original 1-D power load curves into 2-D matrices. A hybrid structure is proposed to incorporate the GCN and ECNN to simultaneously model latent properties, cyclical nature, and temporal correlation of power load curves. Prior to transmitting the encrypted fine-grained readings to the electric utility company, [19] suggests an electricity deception scheme that protects privacy. Specifically, the SMs inform two entities of the encrypted measurements. Unconditional trust is placed in the initial entity, the server gateway. The reported fine-grained measurements may therefore be decrypted and the results reported to the electric utility company via a CNN-based electricity fraud detector. Without the ability to access the individual plaintext readings, the second entity or the gateway is only authorized to aggregate the encrypted individual readings for a group of consumers in a specific area and report the aggregated reading in plain text to the electric utility company for energy management. In actuality, the supposedly trustworthy entity may potentially abuse the data.

B. False Data Injection (FDI)

The minimal attack resources are determined using a deep reinforcement learning (DRL)-based approach in [20], proposing a coordinated CP topology attack strategy. By inducing a fault signal in another line within the cyber layer via FDI attack, the method tangles a physical TL and obfuscates the outage signal. Modeling the PS as the dynamic environment, tripped lines as the action, and grid topology information as the state, an MLP-based DRL model is used to ascertain physical and cyber-tripped lines to minimize attack resources. The method enhances the likelihood of effective attacks by managing load uncertainty. Isolation Forest, an unsupervised algorithm that operates on unlabeled data, was devised in [21] as a means to identify covert data integrity assaults (CDIA) and FDI attacks that threaten the system's integrity and circumvent the bad data detection (BDD) of SG. The underlying premise of the scheme's detection hypothesis is that the assault traverses the shortest path length possible within a RF structure. The results of the evaluation indicate that this algorithm outperforms the supervised schemes.

A framework for detecting FDIA in DN is proposed in [22]. The concept is based on collaboration between end devices, edge devices, and cloud resources. Its primary focus is to optimize the computational capabilities of dispersed edge devices to alleviate the computational burden on the control center. By facilitating collaboration between the control center and edge devices, the detection framework enhances the ability to identify FDIA in large-scale DN. A Federated Learning (FL)-based mechanism for cooperation between the edge and cloud is proposed based on the framework for collaboration between the end, edge, and cloud; it utilizes the local storage of private measurement data on each edge device to enable collaborative training of the FDIA detection model among multiple stakeholders. Finally, an extensive FDIA detection model is aggregated, effectively addressing the issues of data privacy and data isolation. A FDIA detection model, using data-driven approach and is built on temporal spatial graph convolutional network (TSGCN), is specifically developed to operate on the edge side. The NN may analyze the measurement data of the buses in the DN to identify temporal-spatial patterns. This analysis improves the detection performance of FDIA and enhances the DN's ability to detect and respond to attacks.

By expanding upon the issue of attack detection, [23] then determines the real-time location of FDIA. To accomplish the goal, a DL-based Locational Detection architecture (DLLD) was developed. The DLLD comprises CNN and BDD, after which a multi-label classifier is implemented. On IEEE-14 and 118 bus systems, simulations demonstrated that the method attains a high degree of detection precision. Nonetheless, this approach fails to alter the existing BDD system and does not capitalize on any previous statistical research. A hybrid ML model for FDI detection was devised in [24]; it combines LSTM and a seasonal AutoRegressive Integration Moving Average (SARIMA) model with a dynamically adjusted threshold. The algorithm is assessed for its validity through experimentation with a realistic testbed comprising three systems: urban transit systems, gas pipeline systems, and power generation systems. The evaluation includes scenarios like network anomalies, malicious operating behavior, and cyberattack. While the adaptive thresholding algorithm is used to label data, LSTM is used for supervised learning. LSTM has the benefit of sequential learning coupled with an amnesia mechanism capability, enabling systems to remain compatible with data changes at all times. Dual-attention multi-head graph attention network (DAMGAT) is an interpretable DL scheme proposed in [25] for the identification of FDIAs in SGs. The DA and the MGAT are two essential sub-modules that comprise the model. The DA is integrated into the input layer, incorporating attention to node features and spatial topology. Through the implementation of adaptive weighting during model training, DA greatly prioritizes significant nodes and spatial characteristics derived from grid measurements and topology data, while attenuating extraneous information. The attention-processed node and topology features are integrated with MGAT to extract spatial features to identify FDIs. By using the attention mechanism of the graph, spatial feature representation is improved, leading to enhanced detection accuracy and interpretability. In [26], an efficient location detection method called Fast-Lightweight Location Detection Framework (FLLF) is developed for SG FDIA location detection. This framework incorporates an early exiting mechanism and a mixed-precision quantization (EEMPQ) model, along with an autonomous search method for architectural optimization. The EE-MPQ is a compact model that offers rapid and precise attack detection by using the early exiting mechanism with mixed-precision quantization. A genetic algorithm (GA)-based model architecture automatic search algorithm is created to match EE-MPQ models to SGs with varying architectures.

Spatial data was utilized predominately in previous studies regarding the detection of FDI attacks. [27] proposed a DNN-based detector that integrates GRU and FCL as a response to it. The method can distinguish between FDI attack and normal operational occurrences by extracting temporal-spatial properties and acquiring knowledge from temporal data correlation in consecutive states. [28] trained an LSTM-autoencoder (AE) model with feature vectors extracted from normally estimated states in an effort to identify FDI attacks that could cause load shedding and rescheduling. The refined model has the capability to analyze the extracted spatial and spectral characteristics to compute and revise the measurement deviation. Additionally, the logistic regression classifier is capable of distinguishing FDI attacks from routine system operation occurrences. For the aim of predicting FDI attacks, a succession of feedforward networks (FNNs) were trained using ELM theories in [29]. Initial input weights for the ensemble of ELMs are generated using Gaussian Random Distribution (GRD) and Latin Hypercube (LH) to optimize weight optimization. To designate samples prior to feeding the ELMs, a faulty data identification method based on Contaminated State Separation (CSS) is implemented. ELM is an exceptional method for training FNNs due to its ability to decrease algorithmic complexity. In [30], a proactive defense system is devised to provide an additional layer of protection between the communication network and the actuator. It aims to minimize its own expenses by deliberately blocking or allowing control signals that may be corrupted, without detecting or diagnosing the FDIA. A dynamic Stackelberg game model is built between the FDI attacker and the active interdiction defender, without any predetermined constraint on the FDIA. The Stackelberg equilibrium is then identified. A condition is established adequate to ensure the physical plant's asymptotic stability when the controller closes the control loop and implements the corresponding Stackelberg equilibrium strategies.

For the aim of detecting cyberattacks, [31] examines a hybrid approach that combines the symbolic dynamic filtering (SDF) method with RBMs techniques. To discern fault line patterns from those associated with intrusions, the entire procedure was predicated on unsupervised learning. RBMs are used to fine-tune a DBN for the classification process, following the data labeling procedure. To verify the accuracy of the method, numerous classification metrics have been implemented. A model for real-time FDI attack detection is developed in [32] using an LSTM-embedded DNN to represent the dynamic behaviors of SG that are impacted by RES or system reconfiguration. By integrating the RES and identifying the attacked vehicles, the detection method is able to accommodate uncertainties. In [33], a sub-grid-oriented paradigm was presented for FDIA detection by jointly learning the relationship between a target sub-grid and all other subgrids. To model the spatial connection between bus/line representations, MLP is employed, while LSTM is used to learn the temporal connection from time-series measurement data. Each subgrid maintains the confidentiality of its collected measurement data. For the aim of collaborative training, solely the feature representation related to each subgrid is transmitted, ensuring the confidentiality of each sub-grid and decreases data latency. A DL model was devised in [34] to detect sporadic cyberattacks in SG networks. The model was to accommodate both complete and incomplete data. Interval estimation based on thresholding is represented as an optimization problem. In the context of nonlinear mapping, deep extractors, like Stacked AEs (SAEs), are implemented. Then, LR is used to approximate the data. Simulation systems based on IEEE benchmarks were used; experimental parameters were extracted from MATPOWER.

To replace tampered data with non-tampered data, [35] devises a generative adversarial network (GAN)-based recovery model against FDIAs that can capture deviations from ideal measurements. A seamless training method and an adaptive window are executed to expedite the GAN training procedure due to the computational burden of DL. Evidently, the recovered measurements are close enough to the actual measurements to preserve SE integrity. [36] devises a method for detecting FDIAs using unsupervised learning. The dual graph AE (GAE) algorithm is devised to greatly reduce the dimensionality and represent high-dimensional data by considering the complex nature and nonlinear relationships of the measurement data. An approach is created, which calculates the encoder loss by reconstructing latent features that may be concealed inside the data. A method called adversarial training, using adversarial feature loss, is devised to enhance the training of models and enhance their resilience in noisy situations. The method suggests using an adaptive threshold based on support vector regression (SVR) to account for the periodic fluctuations in grid data. It may dynamically adjust to changes in data performance, causing improved accuracy in discriminating performance and detecting attacks.

C. Denial-of-Service (DoS) & Delay Attacks

In [37], an RL-based online detection algorithm is executed to identify DoS and other types of attacks. SARSA is a model-free RL algorithm that underpins the training method for the detector. After every training episode, the adversary acquires knowledge of a Q-table identified by the cost of its environmental interactions. The method's efficacy is superior to that of the detectors based on Euclidean and cosine similarity. A DoS predicated on the detection of integrity attacks is discussed in [38]. To train an ML model as a specific agent, SVM and DT are used. Numerous agents were cloned to scan a multitude of hyperparameter combinations. Following the fusion of results, a determination is reached based on a solitary output. The test shows model's capability to identify massive data in network operating states and adjust its corrective actions to account for potential attacks. From an algorithmic point, the inclusion of adaptive learning capability is evident to accommodate changes in the data. The model shows algorithmic adaptability and simplicity, which are conducive to the detection of anomalies in large data. In [39], cyberattacks, like FDI and DoS attacks, can be detected in SGs utilizing a DQN-based DRL algorithm. To model dynamic state transients in SG and identify cyberattacks in real time, a DQN-based RL method is developed using dynamic AC PS model, allowing the algorithm to minimize the average detection delay while maintaining a low probability of false alarm. Using the Markov decision process (MDP) framework, the DQN-based RL algorithm is created by formulating a sliding window of Rao-statistics to capture the power grid's dynamic state evolution in real time.

[40] focuses on the design of an intermittent observer for a MG system that is subjected to a DoS attack and features stochastic gain floating. A strategy is devised where the frequency of attacks is irregular and the size of each attack remains constant. The intermittent observer is suggested for MG systems affected by DoS attacks, when only partially quantifiable information is available. The observer gain part in the design experiences uncertain floating, which is characterized by random uncertainty. Two distinct sufficient criteria are formulated to guarantee the stabilization performance of the observation error system, and the intermittent observer based on MG is established.

A hybridization of the CNN and GRU algorithms was used to propose a method in [41] for distributed DoS (DDoS) detection in SG. The supervised ML method is implemented after the normalization of the data. The algorithm under consideration exhibits a classification accuracy of 0.997 and a detection rate of 0.999 when applied to attacks, surpassing those of alternative intrusion detection techniques currently in use. The strategic interaction between a hypervisor monitoring its vSDN controllers and the origin of new flow requests sent from switches compromised by DDoS attackers was conceptualized in [42] as a non-cooperative dynamic Bayesian game of intrusion detection in order to thwart the exploitation of an SG architecture based on virtual software defined network (vSDN) technology. By using the game model, a hypervisor can simultaneously reduce its monitoring costs and enhance the likelihood of detecting distributed attacks while minimizing false positives. This is achieved by allocating resources to monitor vSDN controllers in accordance with the hypervisor's observational assessment regarding the origin of the attacks. [43] introduces a strategy for designing H_∞ LFC control in sampled-data systems to address multi-area PSs subject to partially known DoS attacks. Only the intervals during which DoS attacks are actively occurring are restricted, and only the minimum and maximum durations of these periods are presumed to be known. A sampled data-based transmission paradigm is created to enable the sampling and transmission of the PS condition of each control region over specific communication networks. The DoS attacks are defined as sporadic data transmissions occurring at specific sampling intervals, leading to the creation of numerous corrupted data packets. To conduct thorough stability and performance analysis, we make full use of the bound information regarding confined times of DoS activity and attack instances. This information is utilized in the construction of the Lyapunov functional, which in turn allows us to generate analysis and design needs. Utilizing the complete range of attack knowledge could result in more precise analysis and design criteria, with less emphasis on caution.

With the aum of enhancing the precision and efficacy of DDoS attack detection in the SG network, [44] devised a system using multilevel DL technology. Unsupervised feature learning is accomplished by the algorithm through the utilization of both shallow and deep AEs. Multiple Kernel Learning (MKL), which learns the weights of the ensemble's features automatically, is employed to integrate the features of multilevel AEs. In terms of accuracy and simplicity, the method shows great efficacy. The application of CNNs and ResNet to the security of cellular networks was investigated in [45] in a coarse-grained manner in order to detect various DDoS-causing attacks, such as voice, Internet, and SMS, with an accuracy of 0.91. The study helps to resolve an issue regarding the mitigation of DDoS attacks in cellular networks. Besides main subscriber devices, it holds significant implications for safeguarding cellular-dependent CPS devices, used in vertical industries and vital infrastructures, from cellular DDoS attacks, used as a beachhead or smokescreen to compromise the CPS infrastructure and impede its services.

[46] presents a dynamic and robust control approach for the wind turbine (WT) system to counteract time-delay attacks (TDA). A TDA model is created to investigate the delay in transmitting the rotor speed sensor data to the WT controller. A real-time adaptive state observer is designed to compensate for the loss or delay of sensor input caused by the considered time-domain analysis in the WT control system. A method for adaptive resilient control is devised to provide optimal tracking of rotor speed in WTs. The level of resilience against attacks is assessed, taking into account both the duration of delays and the time it takes to implement the attack. To fortify the network's resistance to delay attack, [47] devised a mathematical model for PMU communication routing in WAMS. Invalid measurements are those that are received subsequent to the expiration of the PDC timer or the end-to-end delay threshold. The aim of this model is to reduce the quantity of such signals. The model is capable of locating trees that mitigate the impact of delays while meeting real-time requirements. In [48], a load frequency control method was devised to address the occurrence of random time-delay attacks (TDA) on PSs. The control scheme effectively reduces the impact of random TDA through the estimate and compensation of perturbations. Also, the control scheme exhibits a high level of robustness in external disturbances. A learning-based solution that analyzes pertinent sensor outputs in a closed-loop CPS to detect and characterize TDAs simultaneously was proposed in [49]. Practicality for real-world systems such as power plant control systems (PPCS) and AGC is the focus of the study, which is also adaptable to various objectives in accordance with user-specific needs. A dynamic and robust control system utilizing time-delay compensation (TDC) is devised in [50] for regulating load frequency control (LFC) with synthetic time delays (STDs). The technique can offset the unpredictable disturbances and achieve great control performance. The TDC-based LFC system utilizes a timestamp technique to assess the STDs in the actuator section of the LFC. It is capable of compensating for the STDs in both the sensing loop and control line, and the computational TD and waiting TD. The updating period of the actuator is set to a substantial one of 2–4 s, which is considered in modeling and control system design of the scheme. Thus, the approach accommodates the need to update power orders in the LFC system and guarantees optimal control performance even during long updating periods. The use of a dual-loop open communication network is recommended for the TDC-based LFC system. To enhance the system's dependability and resilience in the face of severe STDs, the main communication channel will be redirected to the standby communication channel when TDs are identified as surpassing the specified maximum TD in the main channel.

In [51], a secure adaptive event-triggered control for cyber–physical PSs (CPPSs) vulnerable to energy-limited DoS assaults is proposed. An initial assessment is conducted on the deficiencies of traditional event-triggered mechanisms (ETMs) with respect to defense against attacks and communication efficacy. Second, a unified secure adaptive ETM (SAETM) is devised in support of the DoS-dependent adaptive protocol to thwart DoS attacks and improve communication efficiency. Also, adequate conditions are established to ensure that CPPSs possess ultimate boundedness uniformly. Also, the time parameter is specified, beyond which the state trajectories are assured to remain within a secure region.

D. False Command Attack (FCA)

In [52], an ultrafast active response method was developed using an LSTM-enabled DRL model to create real-time response action in the event that fault current limiters (FCLs) were targets of FCAs. The key aspects of the SCC can be retrieved in a 7ms time window using an LSTM network, and an online decision is generated using a DRL-based method to enable fault clearance. Results show that the technique clears the fault in diverse scenarios with the least impact on PS stability. [53] creates a DL-based security system to identify and rectify PMU data tampering assaults. The scheme comprises two complex artificial neural network (ANN) models. The first model is a multi-label binary classifier designed for attack detection, whereas the second model is a regression neural network used for data recovery. The security system processes PMU voltage readings and related attributes to determine if each PMU is under assault or secure. It also provides reconstructed signals to the wide-area monitoring and control (WAMC) system. A distributed anomaly measurer utilizing an AE-DNN and installed across all TLs of the PS is devised in [54] to identify the FCA anomaly of each PMU measurements. From two RBMs, the AE structure was unrolled. The RBM probability mechanism exhibits greater flexibility in collaborating with additional information sources to improve the performance of detection. A delayed alert triggering algorithm is executed to prevent false positives and enhance the method’s resistance to noise. A method is devised in [55] to enhance CNN-LSTM with PSO to identify anomalous measurement values in PMU. The PSO-CNN-LSTM method exhibits great robustness in detecting remote tripping command injection, data injection, attack sub-type (CIA against a single relay), and relay configuration change attacks compared to other methods; it predicted samples with greater accuracy in the face of natural occurrences like SLG disturbances and line maintenance. To learn from data under the challenging conditions of partially labeled samples and asymmetrical class distributions, [56] presents a GAN-based semi-supervised (GBSS) approach. Based on the proposed data-driven method, a data-driven diagnostic scheme is created wherein GBSS is modified to diagnose cyber-attacks and defects. An exhaustive comparison is also possible due to the framework's utilization of the GAN and six semi-supervised learners. By producing a substantial quantity of synthetic minority class samples (i.e., faults and assaults), the adversarial network rebalances the training samples. These samples are subsequently gathered and inputted into various semi-supervised learners.

In [57], a detection system is devised targeting transmission protective relays in substations. The system uses a 1D CNN-embedded AE structure as its foundation and inputs consisting of current and voltage measurements that simulated different types of faults occurring on TLs. FCAs are distinguishable from single-phase-to-ground, three-phase-to-ground, phase-to-phase, and two-phase-to-ground faults by the detection system. In [58], a detection algorithm is developed with the ability to identify anomalous phase shifts that occur in response to intrusions. The algorithm is designed to identify and prioritize specific detection features, consisting of four indices calculated using branch ratio and injection currents to terminals. Reference values are included into the evaluation of discrete indices during phase shift selection. DNN-based FALCON is devised in [59] to identify and categorize physical and cyber anomalies, like FCAs on distribution lines, replay attacks on communication networks, and FCAs on protection devices. FALCON uses the transient short-circuit current and voltage detected by protection relays, the fault indicator (FI) malfunction alarm, and the relay command status as input. Voltage and current can provide adequate information to distinguish between defects and attacks, as well as pinpoint the location of attacks, even in the absence of FIs. [60] devises a lightweight algorithm capable of identifying instances of covert malicious tap modified directives. The algorithm is constructed upon intuition-based principles, wherein attacks involving erroneous data and commands exclusively impact the estimation and measurement of specifically designated variables, rather than affecting the entire set. The branch current to the voltages of the end nodes of the tap-modifying transformers is used by the algorithm.

An FCA-based DRL-based recovery strategy for substation control authority to optimally reestablish faulted TL is devised in [61]. Through the optimization of the reclosing time, the method obtains a higher level of recovery performance compared to alternative recovery strategies. The DRL enables real-time optimal or near-optimal decision making and provides the strategy with excellent adaptability across various FCA scenarios. The algorithm in [62] utilizes multi-agent DRL to generate coordinated stealthy destabilizing FCAs on islanded DC MGs protected by the discordant detection algorithm and automatically identify vulnerable areas in classic index-based cyberattack detection schemes. Notwithstanding its efficacy in detecting conventional deceptive and destabilizing FDI attacks, the discordant scheme cannot detect coordinated FDI attack generated by this scheme. An additional RL-DQN detection method is used as a solution to the inadequacy of the discordant method in precisely detecting the coordinated FDIs. Confronted with autonomously identified FDI vulnerabilities, the hybrid detection strategy significantly improved the dependability of all index-based detection algorithms. In [63], a federated deep learning (FDL) method, termed DeepFed, is devised to identify and mitigate cyberattacks to industrial CPSs, as each SG often has limited attack instances and is unwilling to share such attack samples due to highly sensitive information. Also, a novel CNN-GRU based intrusion detection model is designed, facilitating the reliable detection of a wide range of cyberattacks aimed against industrial CPSs. A Paillier-based secure communication protocol is developed for the FL framework to further ensure the safety of the model parameters during training. Nevertheless, the method primarily targets industrial CPSs in the same domain when constructing its federated intrusion detection model.

E. Adversarial Attacks (AAs)

A cyber-secure hybrid electric load forecasting (LF) model, AE-CLSTM, was devised in [64], utilizing DL models to predict LF for the ultra-short-term and short-term time horizons. The first layer consists of an AE network, executed to preprocess and de-noise the data. Using a CNN model, the subsequent stratum discerns behavioral patterns and extracts features from the data. The fully-connected layers in the CNN model were substituted with an LSTM model to execute the training and LF procedures. [65] devises an adversarial ML (AML) strategy that incorporates perturbation vectors into FDIAs in order to deceive DL-based detectors while achieving targeted attack effects on SE results, as FDIAs can circumvent conventional BDDs but might be detected by DL-based detectors. A joint adversarial example for FDIAs was similarly presented in [66]. In PSs, which utilize neural attack detection (NAD) methods for SE, the state perturbation performs admirably when BDD and NAD methods are applied, indicating a pressing security risk; nevertheless, measurement perturbation can be effectively mitigated by using NAD methods while disregarding BDD methods in a system. The vulnerability of FL electricity theft detectors to evasion attacks (EAs) is shown in [67] (attack success rates of 0.98 and 0.975 for the independent and identically distributed [IID] and Non-IID scenarios); thus, the implementation of the adversarial training (AT) led to a significant reduction in the attack success rate, earning values of 0.03 and 0.079 for the IID and Non-IID scenarios. Also, three attacks are employed to examine the case of misbehaving FL participants. In the presence of adversaries, the study highlights the vital need for auxiliary countermeasures that fortify the security of the AT process against EAs.

The credibility and attack needs of six adversarial example attacks on the voltage stability assessment (SA) are systematically examined in [68]. Also, an ensemble-based method for jointly detecting adversarial examples via majority vote and thwarting adversarial examples on the basis of predictive uncertainty was devised. The evaluation shows that the MC-dropout DNN unit-based strategy can defend against all the adversarial examples with an average execution latency of less than 1ms. FDIAI is an adversarial example generation method proposed in [69] that integrates the physical constraints of the PS into a targeted adversarial perturbations generation problem against the DRL-based security-constrained optimal power flow (SCOPF) model. This is done through the transformation of unconstrained optimization problems and the design of constructor functions. Utilizing this method is feasible for both value-based and policy-based approaches. The results show the superior performance of FDIAI in terms of stealthiness and consequence severity in SG (FDIA) and the AI community (CW attack). Before the practical implementation of DRL models, the method in [70] seeks to identify the vulnerabilities of such models so that power grid administrators can reduce or eliminate the security risks. The indices based on probability and gradient criteria assess the operational vulnerability and performance of the DRL models. A criticality-based adversarial perturbation model is used to detect perturbation characteristics that have the potential to induce hazardous situations. FDIAs and ambiguous data perturbation compromise PS control approaches based on DRL.

To construct attack vectors and model dependency variables like network voltage, current, real power, and reactive power, [71] devised an ML-based FDIA against the SG measurement matrix. Three approaches—linear regression, time-stamped linear regression, and delta threshold—have been contemplated for inputting inaccurate data into the measurement system. Linearity between sensor measurements, partial linearity, and nonlinear considerations informed the design of these defective samples.

Also, defense methods including BDD, SVM, temporal behavior, and AC SE were evaluated against these attack models. Defenders fail to detect these samples as the nonlinearity of the attack vectors increases. The defense strategy in [72] uses randomized smoothing to address the issues posed by errors/noise and AAs in PS-SA. Also, the proposed effectiveness index is used to quantify the highest level of resilience exhibited by data-driven SA models against AAs; it can be used to choose the most resilient data-driven sentiment analysis algorithms. A mitigation strategy based on causal structure learning is proposed in [73] due to the susceptibility of the PS's ML-based network attack detection model to AAs, which can render it ineffective. This mitigation strategy does not need adversarial examples for training, thereby conserving computing resources. To perform an FDIA without knowledge of the PS's underlying information, [74] devises an architecture to generate tampered measurement vectors. To regulate the attack measurement vectors, the architecture is structured within an optimization framework that incorporates two regularization terms and the Wasserstein GAN (WGAN) loss function. The fraudulent measurements in PSs, which circumvents the residual error test used to identify erroneous data, provides entirely inaccurate estimated state variables and measurements without knowledge of the underlying PS model. Such measurements threatened the reliability of the electric grid.

The robustness of existing DL-based LF models against malicious attacks was enhanced in a Bayesian learning approach in [75]. This enhanced resilience is applicable to a range of attacking goals and algorithms, while maintaining the prediction performance in the absence of any attacks. The computational load is decreased by implementing a training scheme based on approximations. Bayesian learning exhibits superior robustness in its ability to retain forecasting performance at a higher level. A strategy for preemptive protection and blindside assault against DL-based soft sensors (DLSSs) is developed in [76]. The system considers realistic scenarios that attackers may face and utilizes a proxy model and attack transferability to achieve its goals. The knowledge-guided adversarial attack (KGAA) method possesses the features of imperceptibility, stability, and rationality. The strategy solves the optimization problem in DL-based semantic segmentation caused by the lack of labels during testing. The DLSS demonstrates resilience to further attacks and maintains prediction accuracy when subjected to the KGAA adversarial training approach, which effectively defends against KGAA. [77] devised two universal attacks—one using principal component analysis (PCA) and the other accumulative perturbation—to make universal adversarial perturbations in a black-box fashion, after analyzing DL-based models for a regression problem concerning downlink power allocation in massive multiple-input-multiple-output (MIMO) systems. Adversarial perturbations can be generated using the UAP algorithms that are independent of input and require only a small number of random samples. High success rate can be attained with the attacks, even in the lack of knowledge regarding the positions of the user equipment.

A DNN-based one-day-ahead prediction algorithm for a fast-response battery energy storage system (BESS) in an intelligent energy management system (EMS), SIEMS, which receives weather data and uses LSTM for one-day-ahead predictions, was devised in [78] for hybrid, grid-tied MGs. The defense algorithm is developed through the execution of adversarial training algorithms and defensive distillation. SIEMS was then subjected to FGSM, BIM, and DeepFool attacks, during which the MG's integrity was compromised to an optimal degree of 0.3 from an attacker's perspective; the models achieve a prediction accuracy over 0.95. Though the prediction accuracy of the models decreases to nearly 0.3 to 0.4 after attacks are applied to training data, defense methods improve the system's robustness; by applying them to attack-affected case data, the prediction accuracy increases to over 0.8. To strengthen EM in SGs in opposition to AAs and FDI, an IoT architecture for demand side management (DSM) is devised in [79]. The architecture is implemented using Contact Elements, an IIoT platform. CWT is an image processing strategy that processes the data acquired from end users' SM to alleviate the big data computational burden. To enhance the reliability of the IoT architecture and verify if the data received from the consumer is true due to the cyberattack, the extracted features from the CWT are used as input for a devised DCNN. In [80], a defense strategy and a data-driven attack are used for the issue of destabilizing attacks on droop gains in inverter-based MGs. Following the derivation of the full-order model and linearized reduced order small-signal model of typical multi-inverter systems, an analysis is done on the destabilizing attack on droop gains and its defense strategy. A DRL method TD3 is devised to identify the least effort attack path for the system and develop a resilient defense strategy. The optimal combination of droop gains for attack and defense sets are done by the method, causing a shift in the system spectral abscissa to the intended position. The adversarial training-obtained defense strategy is resistant to the destabilizing attack.

In [81], a novel attack, GradMDM, is devised, focusing on manipulating the energy aspect of the attack by modifying the magnitude (through Power Loss) and direction (via Complexity Gradient Masking) of gradients. The aim is to identify a subtle perturbation that can activate a greater number of compute units in dynamic networks during the inference process. A method to attack data-driven control strategies in PSs is devised in [82]. To execute real-time black box attack, a GAN designs and trains a generator comprising a node selector, an encoder, and a decoder. The attack experiment on the CCT prediction strategy shows the method's efficacy with respect to calculation speed, number of attacked nodes, success rate, and detection rate. Also, the real-time performance remains unaffected by the scalability of the power grid. Methods for attacking learning models used in power quality (PQ) signal classification through the generation of adversarial signals in SG and black-box attacks using transferable characteristics and signal-specific adversarial attack (SSA) and signal-agnostic adversarial attack (SAA) are devised in [83]. To fortify learned models against adversarial signals, adversarial training is executed, thereby enhancing the models' robustness. The SAA can produce the universal perturbation that deceives learned models, whereas the SSA produces less perturbation than the FGSM. A substantial and practical threat to CNN-based PQ classification is posed by the attack method based on the universal signal-agnostic algorithm, which has a higher transfer rate of black-box attacks than the attack method based on the signal-specific algorithm. [84] explores the utilization of a denoising AE (DAE) framework to reduce the impact of AAs on deep neural network (DNN) regression models used for power allocation in massive MIMO (maMIMO) networks. The DAE is created as a layer-based DNN architecture designed to transform disturbed adversarial samples into their original clean representations through training. The DAE is trained to preserve performance on non-adversarial samples by mapping clean data to itself. During inference, the sample undergoes forward propagation through the DAE, and the DAE's output is used as input for the DNN regression model representing the base station. A method for diagnosing transformer faults is suggested in [85], involving using an IoT monitoring system and ensemble machine learning (EML). The model considers various scenarios of AAs to verify the prediction model's robustness. A feature engineering strategy is suggested to enhance the diagnosis accuracy of transformer problems by focusing on gases' concentrations and their ratios. By isolating the overlap among different transformer faults, these added values can enhance accuracy rates. Utilizing EML-based IoT greatly visualizes the status and faults of power transformers, aiding in making informed decisions regarding maintenance and prolonging their lifespan. [86] presents a framework for robust online SA (ROSA) utilizing label-independent self-supervised learning. Based on emerging contrastive learning, an auxiliary objective is created for the consistent contrastive learning (CCL) module, which generates an appropriate signal to adaptively assist the initial SA decisions. In support of the CCL aim, specific data augmentation techniques are executed in the interim to process the time-series PMU measurements. To mitigate computational burdens and systematically counter adversarial disturbances, a purification algorithm is iteratively developed and implemented on clean and adversarial samples. It reduces the likelihood of an adversarial disturbance succeeding online, thereby strengthening the model's resilience against adversarial samples.

F. Operational Control Attacks

1) Automatic Generation Control (AGC)

A co-design of Micro-AGC (μAGC) and its cyber solutions is presented in [87]. The sensory obstacles and cyber susceptibilities that the μAGC design encounters are identified. Using the structure of microgrid (μG) dynamics, specifically the rank-one deficiency property, a μG modelling approach is devised to tackle these obstacles. Such a modeling strategy yields an optimal AGC that is simple to execute, since it does not need the acquisition of difficult-to-obtain rapid frequency measurements. For the AGC, an end-to-end cyber security solution is devised for FDIA detection and mitigation. The initial obstacle to using commercially available algorithms for detecting cyberattacks is eliminated through the execution of a data-driven modeling strategy. A collaborative mitigation scheme and an observer-based corrective control are suggested for islanded μGs and AC-μG systems, respectively. μG frequencies can be regulated by AGC despite load/renewable power fluctuations and FDIA. A data-driven AGC scheme resilient to FDI is devised in [88]. A reconfigured compensation-based control mechanism to attenuate the influence and regression for signal recovery are the key elements. Once the regression model is trained offline, the estimation can be rapidly done, resulting in time savings for the online applications. In large-scale PSs, it surpasses model-based controllers without requiring a basic redesign of the PI controller, owing to its engineering feasibility advantages. Devising a cluster driven ensemble learning method, [89] focuses on a decentralized intrusion detection system (IDS) for the AGC system. Locally at the generating stations, the IDS performs attack classification to detect data intrusions in the networks prior to their use for generation corrections. The method maintains its predictive accuracy while the telemetered signals have a signal-to-noise ratio exceeding 40 dB. The implementation of an optimal two-stage Kalman filter (OTS-KF) in the AGC of the benchmark PS models with two, three, and five areas is devised in [90]. The estimation of load variations and outliers in OTS-KF is modified in response to the integration of DG systems into the power grid. While the magnitude of the system will not hinder computation speed or efficiency, extremely large-scale systems necessitates the division of the system into subsystems; filters in each subsystem can also enhance detection capabilities. To address the issues posed by multiarea multichannel FDIAs in an interconnected PS, [91] devises an observer-based decentralized detection and mitigation (ODDM) scheme based on state and attack observer (SAO). For the ODDM scheme to effectively counter multichannel attacks, SAO can concurrently estimate the unknown input and unknown output of the system that is vulnerable to FDIAs. Also, the decentralized structure of the ODDM scheme ensures that the implementation of SAO solely necessitates local measurements. Identification and mitigation of potential FDI and DOS attacks targeting the AGC loop of CP layers was proposed in [92] using CDMP. To detect any malicious activity in the operation of the PS, the CDMP examines the real-time area control error (ACE) estimation, sum, and mean. The actual ACE input to the generators is substituted with the estimated ACE once the algorithm detects any anomaly in the ACE signal caused by attacks. To maintain the frequency deviation near zero, CDMP also includes a frequency correction multiplier (FCM).

2) Automatic Voltage Control (AVC)

A secure distributed scheme is devised in [93]. Cyberattack locations are identified and disturbances and attacks during SVC of MGs are differentiated using an efficient detection method based on the multi-resolution mathematical morphology gradient. A resilient consensus VC strategy (VCS) based on medians is used to mitigate the detrimental impact on system operations in the event of a communication network attack. A cyberattack is considered an occurrence, and a methodical event-driven mitigation strategy is formulated to execute the transitioning of VCSs. A resilient distributed method is used in [94] for autonomous AC MGs to mitigate the effects of disturbance and deception attacks on actuators and sensors. A distribution system operator (DSO) is used to estimate the behavior of each unit; then, a mixed robust adaptive controller is executed to mitigate the impact of actual attack and ensure L2-gain performance despite disturbances. The results indicate that the algorithm enables the MGs to restore voltage and frequency fluctuations and maintain its stability facing deception attacks involving both small and large signal disturbances. A learning-based AVC approach shown in [95] converges with a higher mean reward and a comparatively low reward standard deviation, albeit at a slower rate than the most prevalent DRL methods. Also, by training an AVC NN controller with the AVC policy derived from the optimal GA agent, it becomes feasible to manage the bus voltages of the IEEE 8500 Node DS even in the face of randomly perturbing cyber-adversaries and naturally occurring inherent voltage signal noise. SOA is devised in [96] as a preventative measure against a series of DoS attacks that, left unattended, can compromise data availability, causing control loss and degradation. The SOA properly mitigated the control degradation caused by DoS attack in situations where as many as 0.24 of the customer population is affected. By alleviating congestion caused by the storage of up to 16,000 messages, the SOA enhanced response times between the AA and CA layers by 8.2s. Therefore, the SOA effectively mitigates the computational burden indicator by an average of 89.6%, thereby showing its ability to reduce computational needs. For the coordinated regulation of voltage, [97] devises a two-stage ML-based strategy. The method identifies and locates both coordinated and uncoordinated attacks, given that an assailant can modify a single device or multiple devices in a coordinated fashion. A RF regressor model is used during the regression phase to forecast voltage measurements of the present state using historical voltage measurements, current solar irradiance, and ambient temperature. Logistic regression operates during the classification phase to identify and localize assaults in real time by comparing the predicted voltage to the measured voltage.

3) Load Frequency Control (LFC)

A set of cyberattack-resistant controllers is devised in [98] to ensure continuous operation for various types of disruptions, cyberattacks, and TDAs. False step or ramp signals were presumably injected into the sensor's measured output by the assailant. After the intrusion signal is estimated by the observer of the tolerant state, resilient control eliminates FDI. Sliding mode predictor control is thus intended to maintain the frequency within the acceptable range in the event that a delay in the system occurs due to the formation of a delay signal on the controller-actuator side or a TDA. A model predictive control (MPC)-based unified rapid FC is proposed in [99]. During large disturbances, the method not only restores the system frequency to its nominal value, also effectively repels all known time-delay switch attacks (TDSAs); it compensates for the hacker-injected attacks through precise estimation of the unknown TDSA, allowing for the maintenance of the electricity system's resilience. ESS specifications, including peak rate and power, and frequency limits established by the grid code, enable the method to additionally optimize ESS power allocation. A method is devised in [100] to mitigate the stringent requirements related to solving the bilinear matrix inequalities (BMI) problem representing the DOFC for the AC–MG system. To reduce the intricacy of solving the initial BMI problem, it decomposes the problem into a smaller one and a linear MI problem. Also, the provision of a viable initial solution was rendered unnecessary by the method. An observer is implemented to supplement the control center's measurements for LFC issues to mitigate the impact of intrusions like FDIA. Deception attacks and random communication delays are analyzed in [101] in relation to the decentralized H_∞secure LFC of networked PS (NPS). Using the delay probability density, the stochastic transmission delay model is devised. Two distributed delay terms are utilized to represent conventional control signals and deception attacks, with the probability density serving as the distributed delay kernel. Then, the Lyapunov method was used to propose novel probability-density-dependent conditions deemed adequate for the design of a decentralized H_∞ secure controller, which aimed to preserve the frequencies of the system. Islanded AC-MGs that are susceptible to FDIAs and DoS attacks are the subject of a novel joint estimation and LFC control framework devised in [102]. Despite the duration-constrained DoS attack, an initial step involves the development of a piecewise observer that co-estimates the state of the AC-MG system under consideration and the actuator FDIA signal. Then, a time-varying Lyapunov function analysis method is used to establish a resilient LFC design criterion. [103] used 5G technology to construct a model of the shipboard MG (SMG) under hybrid cyberattacks. Besides developing an adaptive RL (ARL) method to fine-tune the ADRC's parameters, the secondary controller proposed a control scheme based on active disturbance rejection control (ADRC) to regulate the SMG frequency. A control scheme was devised, utilizing the parallel SL structure, to mitigate attacks, including DoS and FDI, enhancing the system's resilience. The strategies enhance the system's control performance in the field of marine technology and fortify it against highly damaging intrusions. [104] devises an analysis method for networked PSs experiencing communication delay that incorporates the switching-like event-triggered mechanism (ETM) and an acknowledgment character (ACK) detection technique. It ensures communication efficiency while permitting a certain degree of data loss caused by energy-limited DoS attacks. When energy-limited DoS assaults threaten LFC power systems, the sliding mode control (SMC) method is utilized to address the issue. SMDs with communication latency are then modeled mathematically within a unified framework comprised of the switching-like ETM and SMC method. A SMC law is formulated utilizing linear matrix inequalities to ensure the system attains asymptotically stable $L_2 - L_\infty$ performance, in consideration of the established mathematical model. Also, the predetermined sliding surface is guaranteed to be accessible.

G. *Cyber-Physical Attack (CPA)*

A networked topology optimization (NTO)-based model is devised in [105] to improve the resilience of SG and alleviate the effects of coordinated CPA (CCPA). It greatly enhances the PS's resistance to attacks in comparison to the classic OR-based and the OTS-based approach. The load loss caused by the attacks is also mitigated, resulting in a more rapid restoration of power supply to customers. As the initial few NTO actions have the major impact on bolstering the resilience of the PS, a large number of switching operations are unnecessary. [106] devises three cyber-topology attack strategies exploiting the TL connection status in the cyber layer. Two attack scenarios to cause economic losses to the system and consumers and security issues were used. The use of NAA, DE algorithm, and the multi-objective evolutionary algorithm based on decomposition (MOEA/D) is proposed to address the attack models. The line-switching attack has the potential to cause more substantial adverse impact compared to the line-addition attack and the line-removal attack. The EXPOSE algorithm was devised in [107] by using the algebraic properties of AC power fluxes to detect line failures and restore voltages after an attack. It can precisely recover the information, irrespective of the grid size and number of line failures, even in more complex attacked zones, if the compromised area possesses particular topological characteristics. It can also be used for line failure detection and optimal placement of measurement devices. Yet, the EXPOSE method depends on the PS returning to a stable state following an attack, which becomes increasingly unlikely when line failures multiply. The polynomial time REACT Algorithm is devised in [108], combining the ATAC and LIFD modules for DC Power Flow (PF), to estimate the attacked area and identify line failures after CPAs on the grid. It can approximate the attacked area and detect line failures with minimal false negatives and positives despite the increasing number of line failures and the enlargement of the attacked area, even in a cycled attack area. ATAC module, weight randomization method and confidence metric (used in LIFD module) is expandable to the analysis of AC-PFs. A NN-decoder-ensemble variational autoencoder (DE-VAE) is devised in [109] to safeguard the data privacy of publicly shared data. The numerous decoders are put together and linked to the same encoder, which is fine-tuned using the gradients of the decoder-ensemble, in order to achieve multi-objective optimization using the strong connections between data sources in cyber-physical power grids (CPPG). The encoder is used to create disturbances and alter the publicly released datasets in order to hinder the simultaneous deduction of connected confidential information. A multi-optimization method is created to train the entire DEVAE network, based on maximizing mutual data. The conservation of usable information in the original data and the mitigation of sensitive data leakage risks can be achieved through the use of the loss functions that incorporate the mutual information and Fano inequality terms. The balance between data privacy and usability is attained through the training of the noise generator using several optimizers in the DE-VAE algorithm. To establish a secure cooperative control strategy in DC-MGs, [110] devises a decentralized method based on ANNs to detect and eliminate coordinated FDIA on current measurements. Prior to executing a PI controller to remove the attack from the attacked unit, a NN is used in each unit to estimate the output DC current of each converter based on the estimated value. When any of the units is under attack, the strategy is capable of ascertaining the value of the deceptive data. Despite the adversary's unfair attempt to inject erroneous data into all units simultaneously via high domains, it can detect and eliminate attacks even if all units are compromised.

Based on the AC model, [111] proposed a joint line-removing and line-maintaining attack strategy in which adversaries inject malevolent false data into the cyber layer to obscure a physical event in SG. The aim of the strategy is to initially cause a system failure and then trigger a cascade of failures. The process of initiating the attack involves identifying the target lines using the LODF matrix, obtaining the attack region via a method devised by the BFS algorithm, and adjusting the measurements derived from the PF equations. A covert physics-manipulated attack (SPMA) against FACTS was devised in [112] through the coordination of physical and cyber assaults using the DC and AC models; to conceal the command manipulated attack (CMA) against the thyristor-controlled series compensator (TCSC) device, a strategic measurement manipulation attack (MMA) was developed. SPMA was established through the coordinated execution of CMA and MMA. Tri-level optimization is used in

[113] to identify the most secure PMU placement for outage prevention (PPOP) to defend against CCPA. An alternating optimization algorithm is used to resolve PPOP by generating supplementary constraints for each impractical PMU placement. A scalable heuristic algorithm generates a potentially suboptimal solution for PPOP. An algorithm is used to assess the suitability of a given PMU placement for the AC-PF model to meet the defense needs. Even with the AC-based augmentation, the method can significantly reduce the number of required PMUs while preventing CCPA from causing disruptions.

To improve the CPPS resilience, [114] devoses a hierarchical CPPS network architecture utilizing time-sensitive networking (TSN). By using the impact of a compromised communication network, a power grid model is devised that takes into account the interdependence of CP. To mitigate the effects of uncertain CP coordinated attacks, the model co-optimizes the PF distribution scheduling strategy and the TSN transmission method. Based on all probability distributions of link failures on the power grid and TSN-based communication network, an ambiguity set is devised to model the N-K attack. An enhanced level of precision in CP interdependence is done through the TSN scheduling algorithm using hot standby redundant routing to ensure dependable and deterministic transmission of sensor data and control instructions. A distributionally robust coordinated defense (DRCD) strategy using CP interdependence is created to deal with uncertainties by identifying the worst-case probability distribution of the N-K attack. A distributed adaptive robust restoration scheme featuring voltage/var control is devised in [115] to address the issues posed by extreme events. First, a comprehensive CP system model is suggested to examine the dynamics of communication between the physical and cyber systems. A two-stage robust restoration scheme featuring voltage/var control is suggested, grounded in the CP system paradigm. The model is solved utilizing the column and constraint generation (C&CG) algorithm, which takes into account multidimensional uncertainties in physical and cyber space. To augment the robustness of the cyber-physical active DS (CPADS) in the face of cyber disruptions, the execution of a distributed restoration and control framework is suggested. The distributed optimization is resolved using the alternating direction method of multipliers (ADMM), and the alternating optimization procedure (AOP) ensures convergence of the discrete problem.

IV. Additional Varieties of Attacks and Defenses

A. CPSG Attack Methods

Man-in-the-Middle (MITM): Flow-based hybrid network IDS (NIDS) methods detect and classify known and unknown MITM attacks without compromising customer privacy in the private area networks (PANs) [116]. it is compatible with various client-server protocols using a request-response communication model. By categorizing MITM attacks into four classes—MITM two-way attack, MITM attacking the router, MITM attacking the controller, and unknown MITM attack technique—hybrid NIDS methods can discern eavesdropped packets and victims. Yet, it is restricted to client-server communication protocols. In [117], a multilayer event-driven resilient control scheme to detect two categories of MITM attack on voltage and current measurements in CP-DC MGs is devised. Prioritizing attacks as events, it uses a DF-based detection to identify the attacks and notifies adjacent agents of the authenticity of communicated measurements. In a multilayer paradigm, it causes the remaining agents to realign their operations and aid the compromised cyber link in reconstructing an error signal triggered by events. The controller was built using the consensus theory's adherence to identical arrangements. Many adversarial scenarios are analyzed in [118] regarding the mitigation of MITM attacks against hierarchical controllers. To evaluate the real-time operation and mitigation of a variety of MITM attack templates, including unidirectional, bidirectional, concurrent, and stealthy, the system is executed in RTDS and WAVECT. By minimizing the MITM financial hazards, the solutions integrated into the controllers provide economic benefits to the DC-MG industry and its stakeholders. Technical innovations will not only provide a competitive edge, also stimulate market demand and prevent expensive disruptions and equipment damage caused by MITM attacks. The method in [119] involves the use of network metrics, like average RTT and ARP data, and Snort IDS alerts, to detect MITM attack traffic. The automated tool to evaluate cyberattack scenarios based on MITM attack is correlated with DNP3 packet data and integrates with ARP. As successive packets from different outstations reach the adversary before the MITM script can modify and forward the initial packet, an increase in the number of polled outstations results in delayed DNP3 packets and a decline in the MITM attack efficacy, requiring more DNP3 retransmissions.

Load Altering Attack (LAA): A novel defense strategy for load frequency control (LFC) systems is devised in [120]; it is based on the model-free technique. The defender's goal is to acquire knowledge of various LAAs and use the evidence to implement attack attenuation as an active defense (AD). Also, an approach known as model-free passive defense (PD) is utilized, in which the defender enhances system redundancies to withstand a load-altering attack. An analytical framework to examine the effects of IoT-based static/dynamic load altering attacks (S/DLAAs) on the dynamic response of the PS was devised in [121], showing the application of outcomes derived from second-order dynamical systems in the analysis of load altering attacks against power grids that are based on IoT. It provides an easy analytical method for identifying nodes associated with the least-effort destabilizing DLAAs and the least-effort SLAAs that induce unsafe frequency excursions. The evaluation of DLAAs and SLAAs is highly reliant on the system's eigensolutions and their responsiveness to variations in the attack parameters. A cyber-resilient economic dispatch (CRED) model is devised in [122]. The efficacy of the CRED is illustrated by dynamic simulations. System stability is more significantly affected by LAAs in systems characterized by high wind penetration. The additional operational expenses to ensure system stability are impacted by the energy storage and SI provision enabled by the wind turbine. A protective scheme against closed-loop DLAA with feedback from SG frequency is devised in [123] through the formulation and resolution of a non-convex pole placement optimization problem for coordinated multi-point and single-point attacks. An iterative algorithm is employed to solve the non-convexity by addressing a series of convex feasibility optimization and semi-definite optimization issues. Additionally, uncertainty regarding the location of the attack sensor is addressed.

Load Redistribution Attack (LRA): The system cascades into failure due to the proposed LRA in [124], which is intended to identify the optimal LRA (worst case) with a drastic physical impact. To identify the most effective LRAs, the power disparity of islands formed by severe disruptions following an attack is used. A 0.99 detection rate estimated-load and DL-based detection mechanism is proposed as an effective, practicable, and rapid method. A statistical method was devised in [125] for the aim of localizing the attacked bus, along with an enhanced data-driven algorithm for identifying LRAs. On a large number of assaults from two distinct categories—random LRAs and intelligently designed attacks—the detector based on the nearest-neighbor algorithm and a grouping strategy is evaluated. In order to determine the probability that a given load is targeted for an attack, the statistical method for attack localization assigns each load a likelihood value. A sophisticated LRA model is suggested in [126] considering the concealment property and resource constraint of practical attack behaviors. Bilevel optimization is used to identify critical attacking moments and specific target TLs to create attack vectors. A method for detecting attacks is created by utilizing power load pattern learning. It involves establishing a multichannel power load predictor using SARIMAX to capture spatial and temporal correlations of power load for precise prediction. An attack detector based on DL is utilized to identify attacks, greatly addressing the issue of class imbalance. In [127], LRA is devised against the conservation voltage reduction (CVR) in DER-equipped DSs. The adversary devises malevolent load data into the advanced metering infrastructure (AMI) network and deceives the CVR into generating an erroneous control signal that affects the set points of the smart inverter and voltage regulator. The CVR results are significantly skewed, leading to an augmentation in the active PF emanating from the substation. [128] establish conditions that ensure the stealthiness of LR attacks and devise the paradigm for LR attacks against the integrated electricity-gas systems (IEGS). Unit commitment (UC) variables are utilized, and nonconvex gas transmission constraints are piecewise linearized utilizing the piecewise linear (PWL) method. Also, a bi-level MILP is created to determine the most severe LR attack regarding economics. A potential upper-level attack is not ruled out by the model, even under a moderate assumption. To address the bilevel MILP within a master-subproblem framework, a modified reformulation and decomposition (R&D) algorithm is devised. To mitigate potential impracticability concerns in the overarching problem, a novel subproblem is created. It verifies whether all upper-level assaults are feasible with lower-level binary variables held constant. To ensure the solution's optimality and the algorithm's feasibility, two categories of cuts are incorporated into the master problem.

GPS Spoofing Attack (GSA): An algorithm with enhanced computational efficiency is devised in [129] to identify and rectify PMU data in DSs using multiple GSAs. Unlike the impracticable brute force search for every possible combination of counterfeit PMU locations and magnitudes of GSA phase shifts, this method is hierarchical. The identification method effectively refines the scale of the phase shifts while identifying the locations of numerous counterfeit PMUs. The spoofing-matched algorithm (SpM) is proposed in [130] due to the fact that, in contrast to random gross errors and statistically distributed small phase mismatch, a single GSA imparts the same GSA phase shift to all synchrophasor measurements originating from the spoofed PMU. The findings show that the algorithm under consideration not only successfully pinpoints the location of the counterfeit GPS annals but also efficiently and precisely recovers the data from the spoof synchrophasor, thereby enhancing the estimate of the PS state. An algorithm for the power grid, residual-based spoofing detection and measurement correction (RSDMC), is devised in [131]. Correcting the PMU measurements and determining a GSA are the subalgorithms that comprise the algorithm. The spoofing detection algorithm relies on measurement residuals, while the correction of PMU measurements under GSAs is accomplished iteratively through the minimization of residual norms by the measurement correction algorithm. For multiple GSAs, RSDMC-corrected measurements are an order of magnitude more precise than SpM. Comparing RSDMC with SpM on the IEEE 118 and Illinois 200 bus test cases, RSDMC performs better in terms of calculation time, voltage RMSE, and phase RMSE. In [132], an optimization problem to determine the most susceptible PMUs for constructing a TSA is formulated. The vulnerability is assessed using the SE error, and the issue is resolved using a greedy algorithm. For the aim of concurrently estimating the network state and reconstructing the attack, an alternating minimization algorithm is devised as the solution to the nonconvex constrained least squares problem.

Time-Synchronization Attack (TSA): The urgency for early stage detection of TSAs is underscored by real-world experiments in [133] that show how quickly stealthy TSAs can inflict severe damage on the PS and how difficult it is for modern servers to detect them; within a few tens of seconds after the TSA commences, the server is subjected to unacceptable timing errors, but no alarms are generated. A combined-signal-statistics method for detecting TSA interference, extremely sensitive and reduces false alarms, was devised: the rapid detection of signal distortions (RDSD). Signal quality monitor (SQM) statistics are employed to facilitate the monitoring of initial signal distortions induced by TSAS. In [134], the potential of using a three-phase state estimator to identify TSAs was analyzed. The equivalence of vulnerability conditions between the three-phase and direct-sequence state estimators in a balanced three-phase system show that both are capable of detecting a greater number of TSAs than traditional direct-sequence state estimator. Yet, in an unbalanced system, the vulnerability of direct-sequence SE does not always indicate the vulnerability of three-phase SE. Undetectable TSAs on direct-sequence measurements may become detectable with the execution of three-phase SE. While increasing the detection of TSAs through the use of a three-phase state estimator is practical, it may not always be adequate to fully secure the grid. Regarding PMU-enabled wide-area damping controllers (WADC), [135] highlights the susceptibility of data aggregation protocols and standards to TSAs. Aiming to obstruct the WADC's ability to observe low-damping oscillation (DLO) modes, the adversary executes an optimal TSA against PMUs in the attack model to maximize data dropout in critical PMU measurements. For the purpose of constructing the TSA vector, which comprises manipulated timestamps and targeted PMUs, the adversary employs a stochastic mixed-integer linear (MIL) model. The presence of this TSA may lead to undamped oscillation or system instability by compromising the modal observability of the WADC. Co-optimizing PMU-phasor data concentrator (PDC) data forwarding trees and PDC buffer waiting time is proposed as a novel preventive countermeasure against this family of TSAs.

Blind FDIA (BFDIA): Based on matrix reconstruction and subspace estimation, [136] devised a data-driven BFDI method; it addresses the issue of mitigating measurement noise when the quantity of data is minimal, without requiring any knowledge of the system parameters. The method's suitability for large-scale system with significant measurement noise and the ability to achieve a higher attack success rate are proven by studies done on the European 1354-bus network, the IEEE 14, 57, 118, 300-bus, and the Polish 3120-bus systems. It also operates efficiently with reduced measurement data requirements. A process for pre-processing data prior to independent component analyses (ICA) was suggested in [137]. Dimension reduction is implemented via T-distributed stochastic neighbor embedding (T-SNE) for the goal of data classification. Although there are circumstances in which adversaries can acquire topology information, it is possible for attackers to develop FDIAs using minimal topology data. It was established in [138] that the modification of the state variable on a bus or superbus is only possible with knowledge of the susceptance of each TL that is incident to it. Thus, a novel approach to counter FDIAs involves concealing from the adversary the susceptances of $n-1$ interconnected TLs that encompass all buses. Normal operations of a PS regulated by the OPF-based AVC can be distorted by the FDIA method in [139]. The attack can be able to devise an approximate optimal strategy by using a Q-learning algorithm coupled with the nearest sequence memories and conceiving the attack as a partial observable MDP (POMDP). With poor information of the PS, FDIs can potentially cause voltage collapse events from specific substations. Automated selection of viable assault moments and stealthy execution are additional benefits of online learning.

Pricing Attack: An attack strategy was devised in [140] that ensures the assailants worst-case robustness against uncertainties regarding grid dynamics by simulating the discrepancy between the actual network dynamics and the one they know to be within a bounded error. An adversary can manipulate nodal prices of real-time markets without being detected by BDDs, even when network dynamics are subject to constrained uncertainty. When coupled with a virtual bidding mechanism, the attacks still generate profits for the attackers. To evaluate the resilience of SGs against social network-based false price attacks (SNFPAs), [141] proposed an integrated Monte Carlos Simulation (MCS)-based method and a stochastic multi-level influence propagation model. To mitigate the potential threat, a minimize optimization problem was devised to ascertain the load shedding that would occur on each individual node. The aggressors' ability to inflict damage is constrained through the implementation of a price change rate (PCR) increase. As the impact of SNFPA saturates when PCR exceeds a certain threshold, attacks is dissuaded from attempting to publish extremely low false prices. A Blockchain (BC)-enabled TE framework to enhance energy security and privacy protection against cyberthreats was devised in [142]. Each MG derives advantages from the execution of the bilateral trading pricing mechanism, which increases the aggregate energy cost savings. The integration of BC into the TE system shows an extraordinary accomplishment in the face of attacks. A range of operational case studies are presented, incorporating severe occurrences like MG outages and FDIAs, to illustrate the system's defensive prowess. The system's efficacy is evaluated via the trade-off between resilience and cost, and the likelihood of successful attacks. The effects of two types of cyberattacks—malicious bid quantity and malicious bid price—on transactive energy have been analyzed in [143]. Operational parameters like system voltage and frequency are impacted adversely when the bid price or quantity for prosumers is manipulated, resulting in alterations to the locational marginal price and overall load demand. To identify various types of anomalies in the market and physical signals that prompt additional root cause analysis and event classification, an intrusion detection model using the SAE methodology was devised. As a self-supervised method, SAE reads raw data directly as input and uses the input data as the goal value; thus, it is applicable to a wide range of scenarios and does not require additional effort to construct features.

Replay Attack (RA): To tackle the cybersecurity vulnerability, [144] devises a security solution using hash algorithms to ensure the integrity of GOOSE protocol message and a digital signature algorithm (DSA) to ensure authenticity. By adhering to the IEC62351 framework, it identifies RAs, separating them through the use of a packet switch enabled by high traffic, and preventing masquerade attacks through the implementation of hash and DSA, executed using RSA with various key sizes and ECDSA with various elliptic curves. Malicious packets can be discarded while the solution detects and reports the attack. The system exhibits complete scalability across all nodes of SG if public keys remain publicly accessible. Based on the real-time validation setup in [145] using the OP5700 OPAL-RT target, RAs enter a quiescent state within the communication link once they detect modifications in the system information, instigated by load fluctuations. RAs, once triggered, impede the system's capacity to sustain a consistent voltage setpoint necessary for reliable operation. Also, compared to its average value, the line current shows an increase of more than one hundredfold. By observing an increase in residue, the attack is identified; it is deemed resolved when the residue value returns to zero. A DC-CNN is used to devise a novel intrusion detector and classifier in [146]. Spatially accurate data characteristics are preserved by the network via sophisticated capsule layers. Also, the detector and classifier are capable of differentiating malicious data and identifying different types of intrusions through the extracted spatial and temporal features. The mechanism can accomplish distinct identification and classification accuracy for a single and multiple cyberattacks. The method achieves a training accuracy of 0.9977 and a test accuracy of 0.9975 in RA detection. A method for assessing the resilience of PSs against sequential assaults is proposed in [147] employing a double deep-Q-network (DDQN) architecture. A cascading failure simulator based on DC-PF is created to simulate changes in topology and PF. This simulator can incorporate the regulator droop coefficient and lower bound generation of generators. Also, for evaluating resilience, a number-of-attacks-based index is suggested; this index signifies the PS's capacity to withstand attacks. A DDQN-based agent is then creayed to perform the resilience assessment across various operational scenarios. Also, for the purpose of training the DDQN-based agent, an enhanced prioritized experience replay (PER) method is devised. This method considers the average episode reward and temporal difference-error to identify the priority of transitions.

Stealth Attack: By accessing to one of the devices linked to the same network link used by the BESS controller, an MITM covert attack between the local supervisory controller of a BESS and its battery control units are executed [148]. The electricity bill experienced a 36% increase, power use and injection peaked at a 46% rate, and the SSI and SCI decreased by a 23% margin. Due to the attack's covert nature, two strategies are required: prevention and detection via increased cross-checks conducted coupled with DSOs. [149] concocts an unsupervised deep latent space clustering algorithm to identify stealthy FDIA in SGs. The strategy entails training a stacked AE network by a greedy layer wise training method, followed by an end-to-end finetuning of the stacked encoder-decoder system. A KL Divergence error between the soft cluster assignment outputs of the clustering head and an auxiliary target distribution is then minimized to fine-tune the pretrained encoder network and a clustering head with trainable cluster centers. Through this process of self-training, the encoder network weights and cluster centers are updated, enhancing the performance of clustering. In order to jointly detect and localize FDIAs in power systems, [150] proposes a graph neural network (GNN)-based model that integrates the spatial correlations of its measurement data and the underlying graph topology of the grid. The full AC-PF equations are utilized to account for the network's physics. To accurately represent the spatial relationships among smart grid data in a non-Euclidean space and make an end-to-end data-driven determination of the unknown filter weights, a scalable model utilizing auto-regressive moving average (ARMA) graph filters (GFs) of the infinite impulse response (IIR) type is proposed; it concurrently locates and detects the FDIAs within a few millisecond timespans. The architecture forecasts the presence of the attack for the entire grid and for each individual bus in an efficient manner. The multidimensional data processed by the implemented models are embedded in a 2D space utilizing the t-SNE algorithm for improved visualization and analysis.

A novel stealth attack construction with sparsity constraints is introduced in [151]. By distilling the knowledge gained from the challenge of adding an extra sensor to the attack, heuristic greedy constructions have been developed for the independent and correlated attack cases. In both cases, the greedy phase generates a convex optimization problem that is efficiently solvable and produces an attack update rule with minimal complexity. The efficacy of the attack is determined by the topology and SNR regime. A cyber-physical security framework is devised in [152] with a focus on networking; it uses a comprehensive, network-wide strategy to real-time identify, isolate, and recover from a pole dynamics attack (PDA). To validate the method, a physical emulator and SDN were integrated into a testbed. In real time, the framework ensures the robustness of a CPS against the PDA. Yet, the SDN switch has constrained computational resources. Increasing the workload related to packet inspection results in a decline in network efficiency, affecting the control performance of the underlying physical system. The UIO-based detector's susceptibility stems from its inability to accurately identify genuine inputs [153]. Zero trace stealthy (ZTS) attacks can be executed without affecting the detection residual by stealthily simulating the unknown inputs. The DC-MG is destabilized by a single ZTS attack, and collaborated ZTS attacks have precise and targeted effects. A timely and automatic countermeasure against ZTS attacks is devised, using the average PCC voltage (APV) derived from the dynamic average consensus (DAC) estimator. To ensure the integrity of the communicated data used in DAC estimators can be verified by UIO-based detectors, the DAC parameters are perturbed for a predetermined period of time in a manner that is concealed from the adversary. Using asymptotic random matrix theory (RMT) tools, [154] examines the learning prerequisites for information theoretic data injection attacks (DIAs). Within this framework, the assailant constructs attacks utilizing the estimated second-order statistics of the state variables that are learned from a restricted set of prior realizations of said variables. The performance of the assaults, as determined by the estimated statistics, is a random variable, as the sample covariance matrix is randomly generated. To gain insight into the distribution of the performance, the closed-form ergodic performance of the attacks is characterized using the estimated statistics, and the variance of the performance is constrained. [155] enhances dummy data assaults in order to create more covert, destructive malicious data that can be seamlessly masked with benign data to evade detection; such data can have catastrophic effects on the system. Furthermore, the integrity of simulated data is validated using established anomaly detection techniques. By integrating more practicable pre-dispatch and post-corrective actions in response to a specified level of cyber risk, this scheme can secure the flow levels and ensure the security of the power system's operation. The model is formulated as a bi-level mixed integer linear programming (MILP) problem to address the overarching issue. The global optimal solution can be obtained through a decomposition method in which the upper and lower-level problems are solved in a limited number of iterations.

B. CPSG Defense Method

Moving Target Defense (MTD): In the context of Microgrid MGs (DCMGs), [156] proposes a converter-based MTD (CMTD) strategy against deceptive (stealthy) FDIAs and RAs. Without compromising the voltage stability in DCMGs, the monitoring capability of an unknown input observer (UIO)-based detector against deception attacks is greatly improved by perturbing the PCGs of converter devices with the proper magnitudes and frequencies. In [157], to safeguard the SG against CPAs, double-benefit MTD is devised, benefiting from the generation cost. To model the CPA, the tripping attack on TLs is concealed by a data manipulation attack. MTD deployment is then optimized in accordance with GT to decrease the quantity of vital D-FACTS devices. By judiciously adjusting the reactances of TLs, the optimization problem is formulated in a manner that significantly reduces the cost of generation. To examine the efficacy of MTD in thwarting covert FDIAs, [158] develops an Extended MTD strategy to bolster the defensive capabilities of SG for AC SE. Proposed rationality constraints aim to prevent potential negative consequences of EMTD on SG. Also, active power loss, the impact of EMTD on the electricity market, and device costs are considered system defense costs. Minimizing system defense costs while ensuring adequate defense efficacy is the aim of EMTD. A method is devised in [159] that establishes an event-triggering connection between the physics-based MTD and the design of a data-driven detector. By eliminating erroneous positive outcomes generated by the data-driven detector and decreasing the use and expenditure To MTD, the framework surpasses the individual one. To identify attacks via normality projection, a measurement recovery method is created. Embedded PS physics information ensures the accuracy of the recovered attack while the FDIA detector and identifier are incorporated into a single LSTM-AE DL model. To designe the MTD, a bilevel optimization problem is stated. At an elevated echelon, the concealment of information is enhanced, while at a lower tier, the accuracy of detection is firmly ensured with regard to the most severe assault encompassing the identified vector of attack. Also, linear matrix inequalities and duality are integrated into two consecutive semidefinite programming to ensure convergence and feasibility of the nonlinear nonconvex bilevel optimization. An efficient and economical MTD against intended FDIAs (iFDIA) is devised in [160]. An adversary could only modify the SEs with targeted biases if they possess knowledge of the branch parameters in a power transmission network disruption. This result establishes a vital and sufficient condition for safeguarding a bus against iFDIAs with MTD, thereby instigating the development of a novel metric to quantify the level of protection offered by MTD. Also, operational and infrastructure expenses are minimized to achieve a cost-effective MTD. To compute the minimum number of D-FACTS devices required to protect a specific set of buses, an efficient algorithm is proposed. Additionally, two strategies are devised to ensure that activating the MTD incurs no increasing operation cost.

For complete and incomplete MTDs, D-FACTS placement algorithms and an MTD-based ACOPF model as a DFACTS operating approach are devised in [161] to maximize the rank of the composite matrix. For optimal MTD efficacy, system operators may install D-FACTS devices on less than 0.4 of TLs. The solutions ensure that even the most basic MTDs continue to function if the D-FACTS setpoints are not inactive. The D-FACTS placement and operational methods compromise the efficacy of the MTD in exchange for system loss. By utilizing a reduced number of D-FACTS devices and ensuring the highest rank of the composite matrix at a modest increase in system loss, the approaches effectively decrease the expenditure associated with deploying D-FACTS devices. The methods can be seamlessly integrated into control room energy management system (EMS). By utilizing various communication channels, the DMTDR in the [162] framework duplicates and transmits data originating from multiple data sources within the power network. Dual algorithms—random replica activation and path selection—are used to enable the transmission and selection of replicated data. Signals with the greatest impact, like battery control commands and frequency deviation measurement, are allocated replicas in the optimal replica allocation problem. As per the results, the attack impact is reduced by 80% by using only four replicas on certain devices. Also, for residual-based BDD strategies, the DMTDR enables the detection of covert attacks and may even scale back the effects. Also, by using only local information and eliminating the requirement for a SE, the lightweight decentralized detection strategy based on replicated data can rapidly identify attacks in a decentralized fashion, and the DMTDR is extensible to other CPSs. Proactive FDD (PFDD) approach to detect FDIAs on SGs was systematically examined in [163]. The profiles illustrating the minimum effort needed to activate D-FACTS devices for FDIA detection were derived by considering three varieties of FDIAs: uncoordinated multiple-bus, coordinated multiple-bus, and coordinated single-bus FDIAs. The deployment of D-FACTS devices across branches that comprise a minimum of one spanning tree of the grid graph enables PFDD to detect all three of types of FDIAs. Nevertheless, effective FDI operations that target buses or super-buses with a degree of 1 cannot be detected using the PFDD method.

After Stuxnet-like (SL) attack construction techniques, the MTD-based SL attack detection framework is proposed in [164]. The study of the performance of MTD against SL attacks (MISA and MDSA) against the secondary voltage control (SVC) in SG indicate that MTD is only effective when the attacker is able to compromise the data links and is not intended to provide faultless security. If adversaries can gain access to physical infrastructure or sensors, they will be capable of executing more potent attacks, rendering MTD defenseless against the system. Therefore, the execution of MTD raises the barrier to entry for malicious actors seeking to successfully compromise the system. [165] introduces a sophisticated attack model called parameter-estimate-first-FDI (PEF-FDI) to manipulate AC state estimation (SE) results in the presence of MTD. This attack may efficiently and effectively generate stealthy FDI attacks by promptly acquiring updated branch parameters. The PEF-FDI attack model minimizes the time delay (TD) in constructing attacks by estimating recently altered branch parameters. PEF-FDI attack circumstances are studied in AC-SE using MTD. The eavesdropped measurements in PEF-FDI attack set expose the attackers' limitations. The analysis provides the bare minimum number of measurements necessary for the construction of PEF-FDI attacks.

C. Other Methods of Attack and Defense

A mathematical model of a wind power (WP) system under zero-dynamics attack (ZDA) is devised in [166]. An equivalent circuit is derived from a semi-direct drive permanent magnet synchronous generator (D-PMSG). The equation of state is separated into a stable component and an unstable component using the system's relative degree ρ. The conditions are outlined in which ZDA is harmful in terms of the magnitude of change in system output and the duration from the start of the attack until the rated output is surpassed. The zero dynamics parameter matrix is modified to enhance the attack devastation within specified constraints. The Byrnes-Isidori normal form is integrated with MLR to accurately represent hidden internal state changes in the expected output of wind generating systems. The alteration in the undetected ZDA signal pattern is precisely mirrored in the detection output at the start of the attack. For vehicle-to-grid-enabled CPSs (V2G-CPSs), [167] creates a robust detection and mitigation mechanism for CCAs. To identify and mitigate CCAs in the system, a digital twin (DT) replica of V2G-CPSs is devised. A virtual replica of V2G-CPSs operates in the DT framework, utilizing the LSTM-based DRL algorithm. Identifying the precise states of V2G-CPS is the responsibility of the LSTM algorithm. The DRL algorithm trains its agent to identify aberrant behavior in V2GCPSs, subsequent to which corrective measures are implemented in response to the identified impact, using the estimated states as a basis. To further enhance the convergence time and system efficacy of the LSTM-DRL algorithm, the actor-critic method is executed. [168] devises a feature selection-based ML method to detect covert cyber deception attack (CCDA) in SG communication network. GA is utilized to discriminative characteristics and identify distinctive, and SVM input for BDD is comprised of the selected optimal features. Then, the SVM classifies test data as compromised or uncompromised using the decision boundary it automatically discovers, which maximizes the geometric deviation between unassailed and compromised data points, through observation of the SE-MF dataset in both normal and assaulted conditions. [169] uses the Takagi-Sugeno (T-S) fuzzy approach to tackle the dynamic event-triggered finite-time filter design problem for discrete-time nonlinear networked systems that are susceptible to quantization effect and DoS attacks. The $l_2 - l_\infty$ filtering and finite-time H_∞ filtering issues have been consolidated into a single framework utilizing a generalized performance index. To ensure that the finite-time stochastic bounded (FTSB) filtering error system operates at the specified performance level (H_∞ or $l_2 - l_\infty$), the necessary conditions are deduced. Solving these sufficient conditions for the inequality yields the corresponding filter gains and the event-triggered communication parameter.

The SeCDM scheme with enhanced resilience is proposed in [170]. Classic FDI and two varieties of collusive FDI (CFDI) attacks (DM-CFDI and DD-CFDI) against SGs are detected and mitigated by it. A hierarchical knowledge sharing algorithm and a decentralized homomorphic computation paradigm are devised to detect FDIA securely. The communication overheads and computational complexity are comparatively minimal. In [171], a hierarchical structure consisting of two layers was proposed for networked control in AC-MGs, comprising of a protagonist layer, which consists of several inverters, and an antagonist layer that involves interacting attackers. The AC-MG layer undergoes coordinated sensor attacks and unbounded injections in both communication and control input channels. A novel distributed resilient secondary control architecture is devised; its aim is to ensure the MG stability and to achieve the uniformly ultimately bounded (UUB) convergence result for the frequency regulation and voltage containment control goals. To detect of dynamic cyberattacks in SGs, [172] devised integrating delayed feedback reservoir (DFR) and MLP. Various temporal encoding schemes are examined to encode the measurements of SG. DFR can be used to transfer the data to a higher dimensional space, enabling the classification of compromised data from uncompromised data, whereas ISI promotes superior training performance by conveying more information than alternative encoding scheme. Changes in delay value cause the observation of erratic dynamic behavior in DFR responses, i.e., DFR being delay-dependent.

A secondary layer of isolated CP-AC-MGs is devised in [173] with an event-triggered (ET) resilient distributed voltage and frequency consensus-based control scheme, susceptible to DoS attacks. Besides precise active power management and state of charge matching, voltage regulation and frequency syncing were done through the control schemes. To predict the states of the MG and mitigate the impact of attack, a state estimator is used during the attack's initiation. Without Zeno behavior, the ET mechanism greatly reduces the quantity of control updates. A technique using ANNs is devised in [174] to detect and mitigate FDIA in DC-MGs. After the computation of FDI by the ANN, the resulting value of erroneous data is utilized to eliminate the intrusion. The countermeasure is capable of swiftly eliminating the attack and operates at an exceptionally high rate of speed. Also, the lack of supplementary controllers (like PI and MPC) contributes to the decreased complexity of the system. Utilizing the LUBE and GAN algorithms, [175] proposes an intelligent real-time intrusion detection system. Combining PIs for forecasting future power use constraints with a probability that enables the model to identify false monitored data that induces anomalies in the behavior of the recorded data is the foundation of the model's construction. Fixing the GAN-based LUBE model parameters and locating the optimal compromise for PICP and PIAW criteria, the method employs the MTLBO algorithm. A resilient defense strategy against FDIA in SG is devised in [176] using the virtual hidden network (VHN). The Kron reduction method is used to derive a simplified model. To defend SG against FDI in a resilient manner, a well-designed controller based on VHN is devised, given the structural SG vulnerability; to further exacerbate it, an efficient interconnection method comprising network zero-sum games is executed. The effective defense against FDI is achieved through the strategic selection of the topology of VHN and the bipartite engagement network. BC is executed in networked control systems (NCSs) as a solution to the system's unaddressed security concerns [177]. BC's intrinsic qualities of security, traceability, and anonymity may enable NCSs to proactively defend against cyber threats. To ensure the security of the NCSs, BC-based control technology could eradicate tainted and corrupted data prior to its use in the controller or actuator, while acquiring authentic information. Yet, the incorporation of BC diminishes the real-time capability of the entire NCS in the absence of human intervention. A skillfully designed observer-based networked predictive control strategy is implemented to rectify this flaw. The control technique has low computational complexity, requiring minimal processing power for algorithm implementation.

To detect FDIAs in smart DSs, [178] devised a semi-supervised AAE-based algorithm. By using a cutting-edge GAN framework, it successfully identifies unobservable FDIAs that evade the conventional BDD method when only a minute portion of labeled measurement data is involved. The method is entirely data-centric and is not contingent upon estimation technique or system expertise. Anomalies in SGs are identified by the decentralized FL-based method in [179]. For training SM devices using their local datasets, a global model is obtained from the server; the parameters of the local models are then transmitted to the server to enhance the global model. To protect against adversary, the server-client communication is encrypted using the SSL/TLS protocol. The model exhibits high efficiency regarding power use (0.33 to 2.34W), memory usage (10% to 31%), and CPU usage (5.56% to 88.78%) executed on edge hardware. Significant bandwidth savings are achieved due to the communication overhead ranging from 48.8 to 1191 kbps. For CP-DC-MGs, Hilbert-Huang transform-based FDIA detection is devised in [180]. The method identifies a variety of FDIA in the controller and voltage and current sensors of the converters. by classifying clients using label data, an efficient more granular data-exchanging method is devised using a community detection framework and BC. Four phases—initialization, identification, signature, and information exchange—are executed to ensure the security and efficacy of data sharing. The community detection server functions to retrieve and analyze the label data of all clients. It then uses cosine similarity to diagnose the community.

In [181], a DRL method improved by SA-GAN was proposed to assure the survival of critical loads via NMGs to increase grid resilience during the sequential extreme event (SEE) process. To enhance the learning of sequential features of system data in the SEE process, the GAN is built incorporating the Attention Mechanism. SA-GAN is also included into the DRL method to facilitate effective learning with restricted data. The SA-GAN-DRL method provides a robust and adaptive scheme for the survival of critical load during SEE processes, while suitably expanding the dataset by generating new and distinct additional data that captures the inherent characteristics of the original data. The cybersecurity implications of NMGs are examined in [182] through the implementation of directed acyclic graph and modified BC model. To model the uncertainties related to hourly load demand and RE output power, a stochastic framework is used that uses the unscented transform method, and an incentive price is devised whereby the cost of selling decreases as the purchasing power increases. Primarily as the hash addresses are modified with each iteration, unauthorized users outside the system are unable to access the data. A central node is unnecessary for the decentralized network, resulting in an increase in the system's security. To identify stealthy cyberattack (SCA) in SG networks, [183] devised a DR-based ML scheme. The data was transformed into a lower-dimensional space using the KPCA method so as to resolve the computational complexity introduced by the high-dimensional space in large-scale PSs. Extra-Trees is a rapid and effective algorithm to detect SCA, and its input is comprised of the data transformed by KPCA. When training data is contaminated with noisy labels, the scheme shows resilient performance against noisy labels in a practical situation as KPCA does not consider the labels during dimension reduction, and the Extra-Trees algorithm can handle noisy labels by adjusting the parameter related to the minimum number of instances needed in a child node to execute the split.

In [184], a method for detecting and mitigating FDIAs in DC-MGs based on MPC was devised; the reference for the model predictive controller was generated using a feedforward-based ANN. To enhance the performance of the ANN, the inputs of the data were evaluated based on their historical value. The model predictive-based controller is tasked with injecting the proper data into the system to mitigate the impact of cyberattacks. By employing the MPC/ANN-based strategy, MPC and ANN are able to effectively collaborate in the detection and elimination of FDIAs. Also, the framework can be modified and adjusted to ensure the security of operations for various other types of CPSs. To identify and eliminate FDI in SGs, [185] devised a rapid intrusion detection algorithm. With the aim of a maximum false alarm rate, the algorithm was designed to mitigate worst-case detection delays (WDD). A time-varying dynamic model was modeled to depict the dynamic state transitions to differentiate between an FDIA and a sudden system failure. To estimate and monitor the time-varying and nonstationary state transitions, a dynamic state estimator was then created. A new normalized Rao-CUSUM detector was devised to reduce the detection latency of the FDIA and distinguish it from abrupt system changes, based on the statistical properties of the SE results. Even FDI into correlated measurements can be detected by the method. Although sensor failures and line outages are examples of system defects that the algorithm can detect, it is incapable of distinguishing them from the FDIA. SGs' security and resilience can be enhanced by implementing the algorithm to fortify IEDs and SCADA systems. The ETradeChain [186] provides a secure and efficient energy trading system for the local energy market (LEM) in the SGs. It enables residential units equipped with RESs to engage in energy trading with each other. ETradeChain tackles a range of LEM security issues like as transaction integrity, user authentication, double spending, forking, and non-repudiation. An energy-backed virtual currency called Pcoin is developed to enable energy trading in the LEM. Prosumers generate Pcoins to assist this trade. ETradeChain utilizes a modified double auction method, where Pcoin is used as a stake to establish consensus on energy transactions. ETradeChain demonstrates the practicality of real-time peer-to-peer trading by utilizing BC.

Utilizing the differential private FL (DPFL) paradigm as its foundation, [187] creates an AMI value-added service model that safeguards privacy. The computation and communication capabilities of the cloud server are diminished due to the edge computing enabled by the decentralized topological structure of the method. A FL framework is used by the decentralised service model to facilitate communication between the SMs and the central cloud server. Private consumer energy usage data (CEUD) is exclusively transmitted to the local model and not shared with the central cloud server. It effectively mitigates the potential for external attackers to intercept personal information. Also, random Gaussian noise is integrated into the secure aggregation procedure to withstand inference and membership assaults on the shared model parameters by an honest-but-curious (HBC) third party. A K-means clustering detection algorithm is employed to identify nefarious clients prior to the commencement of the training round, thereby safeguarding the global model against potential collapse. Using a BC-based method, [188] proposes a strategy to fortify DC-MGs against prospective cyberattacks. To verify the integrity of blocks, it employs a consensus-based verification method in which the acceptance of said blocks by the receiving node is contingent on the majority of nodes concurring on the validity of their hash indices. Yet, the method of verification can potentially be compromised by hijacking attacks. Also, this access may be exploited to forge the nodes' assent to accept or reject illegitimate blocks. By combining the general features of the BC with distinct attack detection metrics informed by physics, it becomes possible to identify the attacks and initiate mitigation measures in their presence. A method for model-free control is created, seamlessly integrated into the self-healing strategy to safeguard against potential DoS attacks and stochastic TDs, ensuring that any computational latency introduced by the BC-based configuration is effectively reduced. In [189], a multiregional pricing model is devised that incorporates realistic considerations of RE distribution, based on energy supply and demand. Energy trading and consensus activities are considered concurrently, with energy trading occurring at the virtual layer and consensus activities at the network layer. A two-stage Proof-of-Energy consensus model is created to operate the BC in an environmentally friendly and effective manner by integrating energy trade. The PoE chooses delegates based on their significant past energy production to enhance efficiency. Delegates are then offered a variable block reward as an incentive to encourage competition while keeping energy usage within a tolerable range. An iterative method with two layers is created to determine the ideal block rewards that maintain a balance between system safety and social welfare, contributing to the development of a low-energy BC.

An AE-enhanced GAN-based method for detecting intrusions based on market-level behaviors is introduced in [190]. Training for this data-driven strategy consists of typical historical real-time locational marginal prices (RTLMPs). More precisely, it utilizes a reconstructor to reconstruct the normal RTLMPs by acquiring knowledge of the spatial-temporal correlations of the RTLMPs. By employing a discriminator, the reconstructor is improved via adversarial training. Once the reconstructor has been effectively trained, a detector is devised with the aim of discerning whether RTLMPs have been compromised through cyberattacks. To examine the security of MGs in the face of abnormal deception assaults (ADCAs), [191] suggests a secure aperiodic sampling control. The existing constraint condition is further weakened by constructing a novel relaxed condition that is contingent on state TD. Also, a bilateral delay-dependent looped-function (BDDLF) $V_c(x_t)$ is constructed in the second step. An additional enhanced BDDLF $V_d(x_t)$ is concurrently developed in order to obtain more state information, based on the properties of the aperiodic sampling control. Proper integral inequalities and the convex combination method are used in the development of an optimized control algorithm. In order to ensure the actual power-sharing between DGs and ESSs in MG, a new secure aperiodic sampled-data (SASD) controller is completed under ADCAs. Voltage balancing deviation (VBD) and current sharing deviation (CSD) are two attack detection indicators in [192] for each DER to quantify the impact of covert deception attacks on the two control aims in DCMGs. The average point of common coupling (PCC) voltage is estimated in a distributed fashion using the dynamic average consensus (DAC) observer, and the sliding time window (STW) technology is implemented to reduce the impact of daily operations on VBD and CSD. To expose the compromised DERs to the UIO-based locators, the primary control gains (PCGs) are perturbed with the optimal magnitudes, identified by maximizing the locatability of attacks while limiting the induced transient fluctuations on PCC voltage and currents. The quantification of the locatability of attacks occurs through the residual increments of UIOs when subjected to PCG perturbation. The quantification of the induced transient fluctuations is achieved by quantifying the variations in the primary control input (PCI) that are brought about by PCG perturbation. A proactive distributed detection and localization (PDDL) framework is used to incorporate the attack detection and localization phases; upon anomaly detection, the PCG perturbation is triggered.

V. Conclusion

CPSGs comprise a wide variety of networks and rely heavily on the integration of physical and cyber layer features, while characterized by heterogeneous and communication networks, machine-type service, and automated remote control units. With the growing prevalence of SG technologies and the growing number of physical devices connected to CP infrastructures, there is a notable expansion of attack surfaces, presenting an array of challenges, underscoring the importance of conducting a thorough examination and categorization of protective measures and threats. This research performs an in-depth analysis of 184 contemporary scholarly papers to study the latest advancements in operational attacks and countermeasure strategies within the field of cybersecurity for CPSG. To ensure the continued effectiveness of these tactics, it is imperative to frequently update and enhance them. Moving forward, our methodology will involve undertaking a comprehensive examination of scholastic articles, placing special emphasis on thoroughly evaluating the limitations and exploring the potential of each unique approach.

References

[01] A. Meydani *et al.,* "Comprehensive Review of Artificial Intelligence Applications in Smart Grid Operations," *Proc. 9th Int. Conf. Technol. Energy Manage. (ICTEM),* pp. 1-13, Feb. 2024.

[02] S. Paul *et al.,* "On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review," *IEEE Syst. J.*, vol. 16, no. 2, Jun. 2022.

[03] M. Nozarian *et al.,* "Exploring Social Capital in Situation-Aware and Energy Hub-Based Smart Cities: Towards a Pandemic-Resilient City," *Energies*, vol. 16, no. 18, p. 6479, Sep. 2023.

[04] H. Shahinzadeh *et al.,* "An Agile Black-Out Detection and Response Paradigm in Smart Grids Incorporating IoT-Oriented Initiatives and Fog-Computing Platform," *Proc. Int. Conf. Protection Autom. Power Syst. (IPAPS),* Jan. 2022.

[05] J. Moradi *et al.,* "Attributes of big data analytics for data-driven decision making in cyber-physical power systems," *Proc. 14th Int. Conf. Protection Autom. Power Syst. (IPAPS)*, pp. 83-92, Dec. 2019.

[06] H. Shahinzadeh *et al.,* "Anomaly Detection and Resilience-Oriented Countermeasures against Cyberattacks in Smart Grids," *Proc. 7th Iranian Conf. Signal Process. Intell. Syst. (ICSPIS)*, 2021.

[07] J. Moradi *et al.,* "Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency for Financial Transactions in Smart Grids," *Proc. 24th Electr. Power Distrib. Conf. (EPDC)*, pp. 47-53, Jun. 2019.

[08] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," *IEEE Access*, vol. 10, pp. 99875–99896, 2022.

[09] M. Amin *et al.,* "CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review," *IEEE Access*, vol. 9, pp. 38571–38601, 2021.

[10] A. Gao *et al.,* "Electricity Theft Detection Based on Contrastive Learning and Non-Intrusive Load Monitoring," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4565–4580, Nov. 2023.

[11] Y. Peng *et al.,* "Electricity Theft Detection in AMI Based on Clustering and Local Outlier Factor," *IEEE Access*, vol. 9, pp. 107250–107259, 2021.

[12] Z. Zheng *et al.,* "Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids," *IEEE Trans. Industr. Inform.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[13] M. Wen *et al.,* "FedDetect: A Novel Privacy-Preserving Federated Learning Framework for Energy Theft Detection in Smart Grid," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6069–6080, Apr. 2022.

[14] W. Li *et al.,* "A Novel Smart Energy Theft System (SETS) for IoT-Based Smart Home," *IEEE Internet of Things J.*, vol. 6, no. 3, Jun. 2019.

[15] Y. Gao, B. Foggo, and N. Yu, "A Physically Inspired Data-Driven Model for Electricity Theft Detection With Smart Meter Data," *IEEE Trans. Industr. Inform.*, vol. 15, no. 9, pp. 5076–5088, Sep. 2019.

[16] M. Ismail *et al.,* "Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.

[17] G. M. Messinis, A. E. Rigas, and N. D. Hatziargyriou, "A Hybrid Method for Non-Technical Loss Detection in Smart Distribution Grids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6080–6091, Nov. 2019.

[18] W. Liao *et al.,* "Electricity Theft Detection Using Euclidean and Graph Convolutional Neural Networks," *IEEE Transactions on Power Systems*, vol. 38, no. 4, pp. 3514-3527, July 2023.

[19] D. Yao *et al.,* "Energy Theft Detection With Energy Privacy Preservation in the Smart Grid," *IEEE Internet of Things J.*, vol. 6, no. 5, Oct. 2019.

[20] Z. Wang *et al.,* "Coordinated Topology Attacks in Smart Grid Using Deep Reinforcement Learning," *IEEE Trans. Industr. Inform.*, vol. 17, 2021.

[21] S. Ahmed *et al.,* "Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, Oct. 2019.

[22] H. Li *et al.,* "End-Edge-Cloud Collaboration-Based False Data Injection Attack Detection in Distribution Networks," *IEEE Trans. Industr. Inform.*, vol. 20, no. 2, pp. 1786–1797, Feb. 2024.

[23] S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach," *IEEE Internet Things J.*, vol. 7, no. 9, Sep. 2020.

[24] W. Hao, T. Yang, and Q. Yang, "Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyber–Physical Systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 1, Jan. 2023.

[25] X. Su *et al.,* "DAMGAT Based Interpretable Detection of False Data Injection Attacks in Smart Grids," *IEEE Trans. Smart Grid*, pp. 1–1, 2024.

[26] J. Zhu, W. Meng, M. Sun, J. Yang, and Z. Song, "FLLF: A Fast-Lightweight Location Detection Framework for False Data Injection Attacks in Smart Grids," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 911–920, Jan. 2024.

[27] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," *IEEE Trans. Industr. Inform.*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.

[28] L. Yang, Y. Zhai, and Z. Li, "Deep learning for online AC False Data Injection Attack detection in smart grids: An approach using LSTM-Autoencoder," *J. Netw. Comput. Appl.*, vol. 193, p. 103178, Nov. 2021.

[29] T. Wu *et al.,* "Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system", *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1892-1904, Mar. 2021.

[30] Y. Huang and J. Zhao, "Active Interdiction Defence Scheme Against False Data-Injection Attacks: A Stackelberg Game Perspective," *IEEE Trans. Cybern.*, vol. 54, no. 1, pp. 162–172, Jan. 2024.

[31] H. Karimipour *et al.,* "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.

[32] M. Mohammadpourfard *et al.,* "Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids," *Sustain. Cities Soc.*, vol. 75, Dec. 2021.

[33] X. Yin, Y. Zhu, and J. Hu, "A Subgrid-Oriented Privacy-Preserving Microservice Framework Based on Deep Neural Network for False Data Injection Attack Detection in Smart Grids," *IEEE Trans. Industr. Inform.*, vol. 18, no. 3, 2022.

[34] H. Wang *et al.,* "Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks," *IEEE Trans. Industr. Inform.*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018.

[35] Y. Li, Y. Wang, and S. Hu, "Online Generative Adversary Network Based Measurement Recovery in False Data Injection Attacks: A Cyber-Physical Approach," *IEEE Trans. Industr. Inform.*, vol. 16, no. 3, Mar. 2020.

[36] H. Feng *et al.,* "Detection of False Data Injection Attacks in Cyber-Physical Power Systems: An Adaptive Adversarial Dual Autoencoder With Graph Representation Learning Approach," *IEEE Trans. Instrum. Meas.*, vol. 73, 2024.

[37] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[38] P. Wang and M. Govindarasu, "Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020.

[39] Y. Li and J. Wu, "Low latency cyberattack detection in smart grids with deep reinforcement learning," *Int. J. Electr. Power Energy Syst.*, vol. 142, Nov. 2022.

[40] K. Ding, Q. Zhu, and T. Huang, "Partial-Information-Based Non-Fragile Intermittent Estimator for Microgrids With Semi-Aperiodic DoS Attacks: Gain Stochastic Float," *IEEE Trans. Power Syst.*, vol. 39, no. 1, Jan. 2024.

[41] S. Y. Diaba and M. Elmusrati, "Proposed algorithm for smart grid DDoS detection based on deep learning," *Neural Netw.*, vol. 159, Feb. 2023.

[42] R. A. Niazi and Y. Faheem, "A Bayesian Game-Theoretic Intrusion Detection System for Hypervisor-Based Software Defined Networks in Smart Grids," *IEEE Access*, vol. 7, pp. 88656–88672, 2019.

[43] S. Hu, X. Ge, W. Zhang, and D. Yue, "DoS-Resilient Load Frequency Control of Multi-Area Power Systems: An Attack-Parameter-Dependent Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 3423–3434, 2024.

[44] S. Ali and Y. Li, "Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network," *IEEE Access*, vol. 7, 2019.

[45] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network," *IEEE Trans. Industr. Inform.*, vol. 17, no. 2, pp. 860–870, Feb. 2021.

[46] S. Zhao *et al.,* "Adaptive Observer-Based Resilient Control Strategy for Wind Turbines Against Time-Delay Attacks on Rotor Speed Sensor Measurement," *IEEE Trans. Sustain. Energy*, vol. 14, no. 3, Jul. 2023.

[47] R. Kateb *et al.,* "Enhancing WAMS Communication Network Against Delay Attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, May 2019.

[48] K. S. Xiahou, Y. Liu, and Q. H. Wu, "Robust Load Frequency Control of Power Systems Against Random Time-Delay Attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 909–911, Jan. 2021.

[49] P. Ganesh *et al.,* "Learning-Based Simultaneous Detection and Characterization of Time Delay Attack in Cyber-Physical Systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, Jul. 2021.

[50] X.-C. Shangguan *et al.,* "Resilient Load Frequency Control of Power Systems to Compensate Random Time Delays and Time-Delay Attacks," *IEEE Trans. Ind. Electron.*, vol. 70, no. 5, pp. 5115–5128, May 2023.

[51] A. Wang, M. Fei, Y. Song, C. Peng, D. Du, and Q. Sun, "Secure Adaptive Event-Triggered Control for Cyber–Physical Power Systems Under Denial-of-Service Attacks," *IEEE Trans. Cybern.*, vol. 54, no. 3, pp. 1722–1733, Mar. 2024.

[52] F. Wei *et al.,* "Ultrafast Active Response Strategy against Malfunction Attack on Fault Current Limiter," *IEEE Trans. Smart Grid*, vol. 11, 2020.

[53] M. Elimam *et al.,* "Deep Learning-Based PMU Cyber Security Scheme Against Data Manipulation Attacks With WADC Application," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2148–2161, May 2023.

[54] J. Wang *et al.,* "Distributed Framework for Detecting PMU Data Manipulation Attacks With Deep Autoencoders," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019.

[55] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *Int. J. Crit. Infrastruct.*, vol. 40, p. 100582, Mar. 2023.

[56] M. Farajzadeh-Zanjani *et al.,* "Adversarial Semi-Supervised Learning for Diagnosing Faults and Attacks in Power Grids," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3468–3478, Jul. 2021.

[57] Y. M. Khaw *et al.,* "A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2554–2565, May 2021.

[58] S. Chakrabarty and B. Sikdar, "Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 271–280, Jan. 2021.

[59] M. Ganjkhani *et al.,* "Integrated Cyber and Physical Anomaly Location and Classification in Power Distribution Systems," *IEEE Trans. Industr. Inform.*, vol. 17, no. 10, pp. 7040–7049, Oct. 2021.

[60] S. Chakrabarty and B. Sikdar, "Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov. 2020.

[61] F. Wei, Z. Wan, and H. He, "Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020.

[62] A. J. Abianeh *et al.,* "Vulnerability Identification and Remediation of FDI Attacks in Islanded DC Microgrids Using Multiagent Reinforcement Learning," *IEEE Trans. Power Electron.*, vol. 37, no. 6, Jun. 2022.

[63] B. Li *et al.,* "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems," *IEEE Trans. Industr. Inform.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[64] A. Moradzadeh *et al.,* "Electric load forecasting under False Data Injection Attacks using deep learning," *Energy Rep.*, vol. 8, Nov. 2022.

[65] J. Tian *et al.,* "Exploring Targeted and Stealthy False Data Injection Attacks via Adversarial Machine Learning," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 14116–14125, Aug. 2022.

[66] J. Tian *et al.,* "Joint Adversarial Example and False Data Injection Attacks for State Estimation in Power Systems," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13699–13713, Dec. 2022.

[67] A. H. Bondok *et al.,* "Novel Evasion Attacks Against Adversarial Training Defense for Smart Grid Federated Learning," *IEEE Access*, vol. 11, 2023.

[68] Q. Song *et al.,* "On Credibility of Adversarial Examples Against Learning-Based Grid Voltage Stability Assessment," *IEEE Trans. Dependable Secure. Comput.*, pp. 1–14, 2022.

[69] L. Zeng *et al.,* "Physics-Constrained Vulnerability Assessment of Deep Reinforcement Learning-Based SCOPF," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2690–2704, May 2023.

[70] Y. Zheng *et al.,* "Vulnerability Assessment of Deep Reinforcement Learning Models for Power System Topology Optimization," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3613–3623, Jul. 2021.

[71] R. Nawaz *et al.,* "Machine learning based false data injection in smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 130, p. 106819, Sep. 2021.

[72] C. Ren and Y. Xu, "A Universal Defense Strategy for Data-Driven Power System Stability Assessment Models Under Adversarial Examples," *IEEE Internet Things J.*,, vol. 10, no. 9, pp. 7568–7576, May 2023.

[73] R. Huang and Y. Li, "Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2367–2376, May 2023.

[74] N. Costilla-Enriquez and Y. Weng, "Attack Power System State Estimation by Implicitly Learning the Underlying Models," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 649–662, Jan. 2023.

[75] Y. Zhou *et al.,* "Robust Load Forecasting Towards Adversarial Attacks via Bayesian Learning," *IEEE Trans. Power Syst.*, vol. 38, no. 2, Mar. 2023.

[76] R. Guo, H. Liu, and D. Liu, "When Deep Learning-Based Soft Sensors Encounter Reliability Challenges: A Practical Knowledge-Guided Adversarial Attack and Its Defense," *IEEE Trans. Industr. Inform.*, 2023.

[77] P. M. Santos *et al.,* "Universal Adversarial Attacks on Neural Networks for Power Allocation in a Massive MIMO System," *IEEE Wireless Commun. Lett.*, vol. 11, no. 1, pp. 67–71, Jan. 2022.

[78] P. Asef *et al.,* "SIEMS: A Secure Intelligent Energy Management System for Industrial IoT Applications," *IEEE Trans. Industr. Inform.*, vol. 19, no. 1, pp. 1039–1050, Jan. 2023.

[79] M. Elsisi, C.-L. Su, and M. N. Ali, "Design of Reliable IoT Systems With Deep Learning to Support Resilient Demand Side Management in Smart Grids Against Adversarial Attacks," *IEEE Trans. Ind. Appl.*, 2023.

[80] Y. Wang and B. C. Pal, "Destabilizing Attack and Robust Defense for Inverter-Based Microgrids by Adversarial Deep Reinforcement Learning," *IEEE Trans. Smart Grid*, vol. 14, no. 6, Nov. 2023.

[81] J. Pan *et al.,* "GradMDM: Adversarial Attack on Dynamic Networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 9, 2023.

[82] Z. Liu *et al.,* "A GAN-Based Data Injection Attack Method on Data-Driven Strategies in Power Systems," *IEEE Trans. Smart Grid*, vol. 13, no. 4, Jul. 2022.

[83] J. Tian, B. Wang, J. Li, and Z. Wang, "Adversarial Attacks and Defense for CNN Based Power Quality Recognition in Smart Grid," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 807–819, Mar. 2022.

[84] R. Sahay *et al.,* "Defending Adversarial Attacks on Deep Learning-Based Power Allocation in Massive MIMO Using Denoising Autoencoders," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 4, pp. 913–926, Aug. 2023.

[85] M. N. Ali, M. Amer, and M. Elsisi, "Reliable IoT Paradigm With Ensemble Machine Learning for Faults Diagnosis of Power Transformers Considering Adversarial Attacks," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–13, 2023.

[86] T. Zhao, M. Yue, and J. Wang, "Robust Power System Stability Assessment Against Adversarial Machine Learning-Based Cyberattacks via Online Purification," *IEEE Trans. Power Syst.*, vol. 38, no. 6, pp. 5613–5622, Nov. 2023.

[87] T. Huang, D. Wu, and M. Ilić, "Cyber-Resilient Automatic Generation Control for Systems of AC Microgrids," *IEEE Trans. Smart Grid*, vol. 15, no. 1, 2024.

[88] C. Chen *et al.,* "Data-Driven Resilient Automatic Generation Control Against False Data Injection Attacks," *IEEE Trans. Industr. Inform.*, vol. 17, no. 12, pp. 8092–8101, Dec. 2021.

[89] S. D. Roy, S. Debbarma, and A. Iqbal, "A Decentralized Intrusion Detection System for Security of Generation Control," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18924–18933, Oct. 2022.

[90] A. S. L. V. Tummala and R. Kiran Inapakurthi, "A Two-stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System," *J. Mod. Power Syst. Clean Energy*, vol. 10, no. 1, 2022.

[91] K. Xiahou, Y. Liu, and Q. H. Wu, "Decentralized Detection and Mitigation of Multiple False Data Injection Attacks in Multiarea Power Systems," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 3, no. 1, 2022.

[92] S. D. Roy and S. Debbarma, "Detection and Mitigation of Cyber-Attacks on AGC Systems of Low Inertia Power Grid," *IEEE Syst. J.*, vol. 14, 2020.

[93] L. Sheng, W. Gu and G. Cao, "Distributed Detection Mechanism and Resilient Consensus Strategy for Secure Voltage Control of AC Microgrids," *CSEE J. Power Energy Syst.*, vol. 9, no. 3, May 2023

[94] A. Afshari *et al.,* "Resilient Synchronization of Voltage/Frequency in AC Microgrids Under Deception Attacks," *IEEE Syst. J.*, vol. 15, no. 2, 2021.

[95] J. Obert, R. D. Trevizan, and A. Chavez, "Noise-Immune Machine Learning and Autonomous Grid Control," *IEEE Open Access J. Power Energy*, vol. 10, 2023.

[96] C. Cameron *et al.,* "Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3010–3019, May 2019.

[97] N. Bhusal, M. Gautam, and M. Benidris, "Detection of Cyber Attacks on Voltage Regulation in Distribution Systems Using Machine Learning," *IEEE Access*, vol. 9, pp. 40402–40416, 2021.

[98] M. I. Ibraheem *et al.,* "A Sophisticated Slide Mode Controller of Microgrid System Load Frequency Control Under False Data Injection Attack and Actuator Time Delay," *IEEE Trans. Ind. Appl.*, pp. 1–10, 2023.

[99] R. K. Subroto and K. L. Lian, "An Improved Model Predictive Fast Frequency Control for Power System Stability Against Unknown Time-Delay Switch Attack," *IEEE Access*, vol. 10, pp. 99776–99789, 2022.

[100] H. Javanmardi *et al.,* "BMI-Based Load Frequency Control in Microgrids Under False Data Injection Attacks," *IEEE Syst. J.*, vol. 16, no. 1, 2022.

[101] S. Yan *et al.,* "Probability-Density-Dependent Load Frequency Control of Power Systems With Random Delays and Cyber-Attacks via Circuital Implementation," *IEEE Trans. Smart Grid*, vol. 13, no. 6, Nov. 2022.

[102] S. Hu *et al.,* "Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial-of-Service Attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 690–700, Jan. 2023.

[103] J. Heidary *et al.,* "Shipboard Microgrid Frequency Control Based on Machine Learning Under Hybrid Cyberattacks," *IEEE Trans. Ind. Electron.*, 2023.

[104] H. Shen *et al.,* "Switching-Like Event-Triggered Sliding Mode Load Frequency Control for Networked Power Systems Under Energy-Limited DoS Attacks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 54, no. 3, Mar. 2024.

[105] Z. Liu and L. Wang, "Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1552–1564, Mar. 2021.

[106] G. Liang *et al.,* "A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios," *IEEE Trans. Smart Grid*, vol. 10, no. 2, Mar. 2019.

[107] S. Soltan and G. Zussman, "EXPOSE the Line Failures Following a Cyber-Physical Attack on the Power Grid," *IEEE Trans. Control. Netw. Syst.*, vol. 6, no. 1, pp. 451–461, Mar. 2019.

[108] S. Soltan, M. Yannakakis, and G. Zussman, "REACT to Cyber Attacks on Power Grids," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 3, Jul. 2019.

[109] B. Hu *et al.,* "Data Protection Method Against Cross-Domain Inference Threat in Cyber-Physical Power Grid," *IEEE Transactions on Smart Grid*, 2024.

[110] M. R. Habibi *et al.,* "Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 9, no. 4, 2021.

[111] H.-M. Chung *et al.,* "Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019.

[112] Z. Zhang *et al.,* "SPMA: Stealthy Physics-Manipulated Attack and Countermeasures in Cyber-Physical Smart Grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 581–596, 2023.

[113] Y. Huang *et al.,* "Preventing Outages Under Coordinated Cyber–Physical Attack With Secured PMUs," *IEEE Trans. Smart Grid*, vol. 13, Jul. 2022.

[114] X. Li, Q. Xu, X. Lu, M. Lin, C. Chen, and X. Guan, "Distributionally Robust Coordinated Defense Strategy for Time-Sensitive Networking Enabled Cyber-Physical Power System," *IEEE Trans. Smart Grid*, 2024.

[115] Y. Tao *et al.,* "Distributed Adaptive Robust Restoration Scheme of Cyber-Physical Active Distribution System With Voltage Control," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 2170–2184, Jan. 2024.

[116] M. F. Elrawy *et al.,* "Detecting and classifying man-in-the-middle attacks in the private area network of smart grids," *Sustain. Energy, Grids Netw.*, vol. 36, p. 101167, Dec. 2023.

[117] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522–2532, Mar. 2021.

[118] S. Jena, N. P. Padhy, and J. M. Guerrero, "Multi-Layered Coordinated Countermeasures for DC Microgrid Clusters Under Man in the Middle Attack," *IEEE Trans. Ind. Appl.*, pp. 1–14, 2023.

[119] P. Wlazlo *et al.,* "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Phys. Syst.: Theor. Appl.*, vol. 6, no. 3, pp. 164–177, Jun. 2021.

[120] C. Chen *et al.,* "Load altering attack-tolerant defense strategy for load frequency control system," *Appl. Energy*, vol. 280, p. 116015, Dec. 2020.

[121] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems," *IEEE Trans. Smart Grid*, vol. 12, no. 5, 2021.

[122] Z. Chu *et al.,* "Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3164–3175, Jul. 2023.

[123] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, Jul. 2018.

[124] A. Khaleghi, M. S. Ghazizadeh, and M. R. Aghamohammadi, "A Deep Learning-Based Attack Detection Mechanism Against Potential Cascading Failure Induced by Load Redistribution Attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4772–4783, Nov. 2023.

[125] A. Pinceti, L. Sankar, and O. Kosut, "Detection and Localization of Load Redistribution Attacks on Large-scale Systems," *J. Mod. Power Syst. Clean Energy*, vol. 10, no. 2, pp. 361–370, 2022.

[126] W. Deng *et al.,* "Detecting Intelligent Load Redistribution Attack Based on Power Load Pattern Learning in Cyber-Physical Power Systems," *IEEE Trans. Ind. Electron.*, vol. 71, no. 6, pp. 6285–6293, Jun. 2024.

[127] D. Choeum and D.-H. Choi, "Vulnerability Assessment of Conservation Voltage Reduction to Load Redistribution Attack in Unbalanced Active Distribution Networks," *IEEE Trans. Industr. Inform.*, vol. 17, no. 1, 2021.

[128] R.-P. Liu, X. Wang, B. Zeng, and R. Zgheib, "Modeling Load Redistribution Attacks in Integrated Electricity-Gas Systems," *IEEE Trans. Smart Grid*, 2024.

[129] Y. Zhang, J. Wang, and J. Liu, "Attack Identification and Correction for PMU GPS Spoofing in Unbalanced Distribution Systems," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 762–773, Jan. 2020.

[130] X. Fan, L. Du, and D. Duan, "Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4538–4546, Sep. 2018.

[131] S. V. S. Chauhan and G. X. Gao, "Synchrophasor Data Under GPS Spoofing: Attack Detection and Mitigation Using Residuals," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3415–3424, Jul. 2021.

[132] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, Jul. 2019.

[133] W. Gao *et al.,* "An Underestimated Cybersecurity Problem: Quick-Impact Time Synchronization Attacks and a Fast-Triggered Detection Method," *IEEE Trans. Smart Grid*, vol. 14, no. 6, Nov. 2023.

[134] M. Delcourt *et al.,* "Time-Synchronization Attack Detection in Unbalanced Three-Phase Systems," *IEEE Trans. Smart Grid*, vol. 12, no. 5, Sep. 2021.

[135] M. Zadsar, M. Ghafouri, A. Ameli, and B. Moussa, "Preventing Time-Synchronization Attacks on Synchrophasor Measurements of Wide-Area Damping Controllers," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–14, 2023.

[136] H. Yang *et al.,* "Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3174–3187, Jul. 2022.

[137] M. Higgins, F. Teng, and T. Parisini, "Stealthy MTD Against Unsupervised Learning-Based Blind FDI Attacks in Power Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1275–1287, 2021.

[138] R. Deng and H. Liang, "False Data Injection Attacks With Limited Susceptance Information and New Countermeasures in Smart Grid," *IEEE Trans. Industr. Inform.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.

[139] Y. Chen *et al.,* "Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[140] M. R. Mengis and A. Tajer, "Data Injection Attacks on Electricity Markets by Limited Adversaries: Worst-Case Robustness," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5710–5720, Nov. 2018.

[141] D. Tang *et al.,* "Resilience of Smart Power Grids to False Pricing Attacks in the Social Network," *IEEE Access*, vol. 7, pp. 80491–80505, 2019.

[142] D. K. Mishra *et al.,* "Resilience-Driven Scheme in Multiple Microgrids with Secure Transactive Energy System Framework," *IEEE Trans. Ind. Appl.*, 2023.

[143] Y. Zhang *et al.,* "Cyber Physical Security Analytics for Transactive Energy Systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[144] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[145] Md. A. Taher *et al.,* "Analyzing Replay Attack Impact in DC Microgrid Consensus Control: Detection and Mitigation by Kalman-Filter-Based Observer," *IEEE Access*, vol. 11, pp. 121368–121378, 2023.

[146] G. Zhang *et al.,* "Identification and classification for multiple cyber attacks in power grids based on the deep capsule CNN," *Eng. Appl. Artif. Intell.*, vol. 126, p. 106771, Nov. 2023.

[147] L. Zeng *et al.,* "Resilience Assessment for Power Systems Under Sequential Attacks Using Double DQN With Improved Prioritized Experience Replay," *IEEE Syst. J.*, vol. 17, no. 2, pp. 1865–1876, Jun. 2023.

[148] M. Pasetti *et al.,* "Artificial Neural Network-Based Stealth Attack on Battery Energy Storage Systems," *IEEE Trans. Smart Grid*, vol. 12, 2021.

[149] A. Bhattacharjee *et al.,* "Deep Latent Space Clustering for Detection of Stealthy False Data Injection Attacks Against AC State Estimation in Power Systems," *IEEE Trans. Smart Grid*, vol. 14, no. 3, May 2023.

[150] O. Boyaci *et al.,* "Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids Using Graph Neural Networks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.

[151] X. Ye *et al.,* "Stealth Data Injection Attacks With Sparsity Constraints," *IEEE Trans. Smart Grid*, vol. 14, no. 4, Jul. 2023.

[152] S. Kim, Y. Eun, and K.-J. Park, "Stealthy Sensor Attack Detection and Real-Time Performance Recovery for Resilient CPS," *IEEE Trans. Industr. Inform.*, vol. 17, no. 11, pp. 7412–7422, Nov. 2021.

[153] M. Liu *et al.,* "False Data Injection Attacks and the Distributed Countermeasure in DC Microgrids," *IEEE Trans. Control. Netw. Syst.*, vol. 9, no. 4, Dec. 2022.

[154] K. Sun, I. Esnaola, A. M. Tulino, and H. Vincent Poor, "Asymptotic Learning Requirements for Stealth Attacks on Linearized State Estimation," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3189–3200, Jul. 2023.

[155] M. Du *et al.,* "Robust Mitigation Strategy Against Dummy Data Attacks in Power Systems," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3102–3113, Jul. 2023.

[156] M. Liu *et al.,* "Converter-Based Moving Target Defense Against Deception Attacks in DC Microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, 2022.

[157] Z. Zhang *et al.,* "A Double-Benefit Moving Target Defense Against Cyber–Physical Attacks in Smart Grid," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17912–17925, Sep. 2022.

[158] M. Zhang *et al.,* "Extended Moving Target Defense for AC State Estimation in Smart Grids," *IEEE Trans. Smart Grid*, vol. 14, no. 3, 2023.

[159] W. Xu, M. Higgins, J. Wang, I. M. Jaimoukha, and F. Teng, "Blending Data and Physics Against False Data Injection Attack: An Event-Triggered Moving Target Defence Approach," *IEEE Trans. Smart Grid*, vol. 14, no. 4, Jul. 2023.

[160] Z. Zhang *et al.,* "Security Enhancement of Power System State Estimation With an Effective and Low-Cost Moving Target Defense," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 53, no. 5, pp. 3066–3081, May 2023.

[161] B. Liu and H. Wu, "Optimal D-FACTS Placement in Moving Target Defense Against False Data Injection Attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4345–4357, Sep. 2020.

[162] J. Giraldo, M. E. Hariri, and M. Parvania, "Decentralized Moving Target Defense for Microgrid Protection Against False-Data Injection Attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, Sep. 2022.

[163] B. Li *et al.,* "On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices," *IEEE Trans. Industr. Inform.*, vol. 16, no. 2, Feb. 2020.

[164] J. Tian *et al.,* "Moving Target Defense Approach to Detecting Stuxnet-Like Attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[165] C. Liu, Y. Li, H. Zhu, Y. Tang, and W. Du, "Parameter-Estimate-First False Data Injection Attacks in AC State Estimation Deployed With Moving Target Defense," *IEEE Trans. Circuits Syst. I Regul. Pap.*, pp. 1–10, 2024.

[166] Z. Wang *et al.,* "Modeling and Detection Scheme for Zero-Dynamics Attack on Wind Power System," *IEEE Trans. Smart Grid*, vol. 15, no. 1, Jan. 2024.

[167] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5258–5271, 2023.

[168] S. Ahmed *et al.,* "Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning," *IEEE Access*, vol. 6, pp. 27518–27529, 2018.

[169] X. Zhang and H. Han, "Event-Triggered Finite-Time Filtering for Nonlinear Networked System With Quantization and DOS Attacks," *IEEE Access*, vol. 12, pp. 1308–1320, 2024.

[170] B. Li *et al.,* "Detection of False Data Injection Attacks on Smart Grids: A Resilience-Enhanced Scheme," *IEEE Trans. Power Syst.*, vol. 37, 2022.

[171] S. Zuo *et al.,* "Resilient AC Microgrids Against Correlated Attacks," *IEEE Access*, vol. 11, pp. 1603–1612, 2023.

[172] K. Hamedani *et al.,* "Detecting Dynamic Attacks in Smart Grids Using Reservoir Computing: A Spiking Delayed Feedback Reservoir Based Approach," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, Jun. 2020.

[173] M. Jamali *et al.,* "Distributed Cooperative Event-Triggered Control of Cyber-Physical AC Microgrids Subject to Denial-of-Service Attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 6, Nov. 2023.

[174] M. R. Habibi *et al.,* "Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2580–2591, Jun. 2022.

[175] Z. Tang *et al.,* "Securing Microgrid Optimal Energy Management Using Deep Generative Model," *IEEE Access*, vol. 9, pp. 63377–63387, 2021.

[176] X. Luo et al., "Resilient Defense of False Data Injection Attacks in Smart Grids via Virtual Hidden Networks," *IEEE Internet Things J.*, vol. 10, no. 7, Apr. 2023.

[177] Y. Yu, G.-P. Liu, X. Zhou, and W. Hu, "Blockchain Protocol-Based Predictive Secure Control for Networked Systems," *IEEE Trans. Ind. Electron.*, vol. 70, no. 1, pp. 783–792, Jan. 2023.

[178] Y. Zhang, J. Wang, and B. Chen, "Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[179] J. Jithish *et al.,* "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," *IEEE Access*, vol. 11, 2023.

[180] M. Ghiasi *et al.,* "Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform," *IEEE Access*, vol. 9, 2021.

[181] J. Zhao *et al.,* "Self-Attention Generative Adversarial Network Enhanced Learning Method for Resilient Defense of Networked Microgrids Against Sequential Events," *IEEE Trans. Power Syst.*, vol. 38, no. 5, Sep. 2023.

[182] B. Wang *et al.,* "Cybersecurity Enhancement of Power Trading Within the Networked Microgrids Based on Blockchain and Directed Acyclic Graph Approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, Nov. 2019.

[183] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020.

[184] M. R. Habibi *et al.,* "Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1487–1498, Mar. 2022.

[185] S. Nath, I. Akingeneye, J. Wu, and Z. Han, "Quickest Detection of False Data Injection Attacks in Smart Grid with Dynamic Models," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, Feb. 2022.

[186] U. R. Barbhaya, L. Vishwakarma, and D. Das, "ETradeChain: Blockchain-Based Energy Trading in Local Energy Market (LEM) Using Modified Double Auction Protocol," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 1, Mar. 2024.

[187] X.-Y. Zhang *et al.,* "Privacy-Preserving Federated Learning for Value-Added Service Model in Advanced Metering Infrastructure," *IEEE Trans. Comput. Soc. Syst.*, vol. 11, no. 1, pp. 117–131, Feb. 2024.

[188] S. Rath *et al.,* "Self-Healing Secure Blockchain Framework in Microgrids," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4729–4740, Nov. 2023.

[189] Z. Bao *et al.,* "Toward Green and Efficient Blockchain for Energy Trading: A Noncooperative Game Approach," *IEEE Internet Things J.*, vol. 10, no. 22, pp. 20021–20032, Nov. 2023.

[190] Z. Zhang, S. Bu, Y. Zhang, and Z. Han, "Market-Level Integrated Detection Against Cyber Attacks in Real-Time Market Operations By Self-Supervised Learning," *IEEE Trans. Smart Grid*, 2024.

[191] X. Cai *et al.,* "Secure Aperiodic Sampling Control for Micro-Grids Under Abnormal Deception Cyber Attacks," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 70, no. 3, pp. 1392–1402, Mar. 2023.

[192] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng, and J. Chen, "PDDL: Proactive Distributed Detection and Localization Against Stealthy Deception Attacks in DC Microgrids," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 714–731, Jan. 2023.