Review

Review of Data Injection Attacks in Power Systems: Research Status, Challenge, and Prospects

Yunchang Dong *

Posted Date: 28 January 2025

doi: 10.20944/preprints202501.2043.v1

Keywords: data injection attacks; cyber-physical security; smart grids; false data injection; machine learning in power systems; proactive cyber defense

 doi:10.20944/preprints202501.2043.v1

Review

Review of Data Injection Attacks in Power Systems: Research Status, Challenge, and Prospects

Yunchang Dong

State Grid Jilin Electric Power Research Institute, Changchun 130000, China; dycdd359@126.com

Abstract: This review provides a comprehensive overview of data injection attacks (DIAs) in power systems, addressing their evolution, detection, and mitigation within the broader context of cyber-physical system security. With the integration of advanced information technologies and smart grid components, power systems are increasingly vulnerable to cyber threats that can disrupt their operational integrity. The article discusses various forms of DIAs, including false data injection attacks (FDIAs) and dummy data injection attacks (DDIAs), and their impact on system reliability and security. It explores the development of sophisticated attack modeling that accounts for multiple types of DIAs, enhancing detection methodologies through data-driven approaches and machine learning algorithms. Additionally, it highlights the importance of precise attack localization and proactive defense mechanisms that adapt dynamically to detected threats. The review also addresses the integration of cyber and physical security measures as a unified approach to safeguard against these evolving cyber threats. By providing a detailed examination of current challenges and emerging trends, the review sets the stage for future research directions that focus on enhancing the resilience and security of power systems against complex and coordinated cyber attacks.

Keywords: data injection attacks; cyber-physical security; smart grids; false data injection; machine learning in power systems; proactive cyber defense

1. Introduction

With the widespread application of advanced information and communication technologies in power systems, the development towards smarter power systems has progressed, transforming traditional systems into cyber-physical systems (CPSs) closely integrated with information technology [1–3]. As illustrated in Figure 1 [4], based on conventional systems dominated by thermal power generation, the new power systems comprise a large array of distributed renewable energy sources, electric vehicles, and storage systems, with an information network that facilitates data acquisition, state perception, and decision-making control in power systems. The high integration of information and physical systems enhances the capabilities of broad perception, efficient communication, and high-performance computing within the power system, improving the observability, measurability, and controllability of its monitoring and control functions. Concurrently, the strong coupling between information and physical systems, and the frequent interactions between information flows and power flows, increase the vulnerabilities of these integrated systems. The safe and robust operation of power systems heavily relies on the integrity, accuracy, and reliability of measurement data [5–7]. Attackers can exploit these vulnerabilities through malicious and premeditated cyber-attacks targeting sensors, communication facilities, and smart metering devices within information systems, leading to physical failures and cascading faults, thereby exposing the system to greater cybersecurity risks.

 doi:10.20944/preprints202501.2043.v1

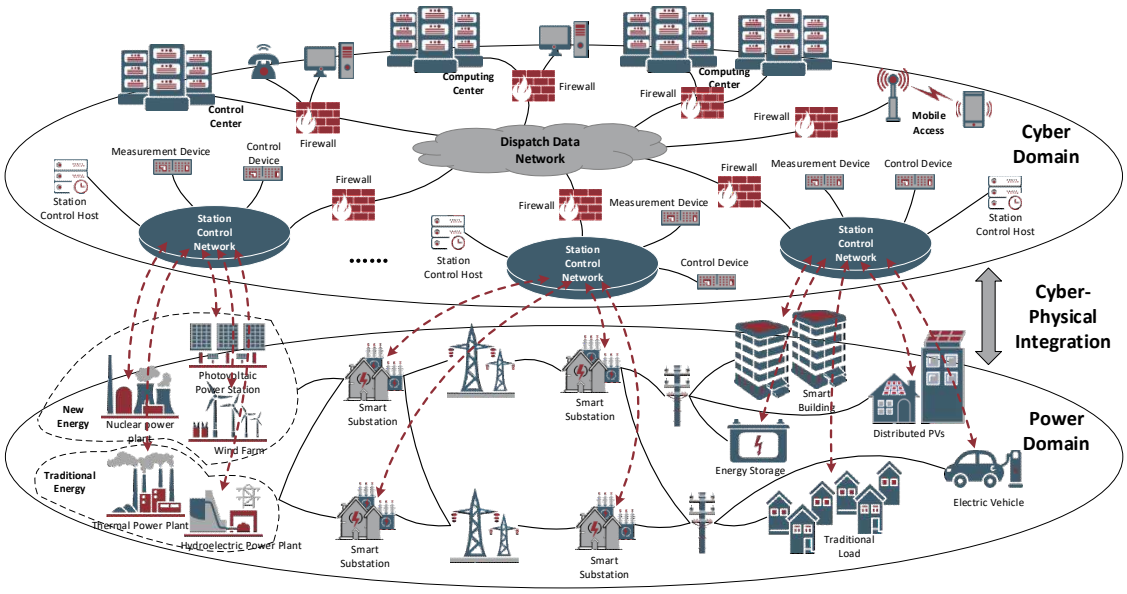

Figure 1. Cyber-physical power system.

The cybersecurity risks primarily manifest in several aspects [8]: (1) A current power CPS encompasses a diverse and abundant array of connected devices such as sensing equipment and smart terminals, increasing security risks; (2) The source code of many IoT devices in power CPS is not fully open, leading to non-uniform standards for security detection and validation, with numerous vulnerabilities in the systems and protocols of smart terminals, resulting in illegal intrusions and deliberate destructive actions; (3) The integration of interfaces between public and private networks within power CPS provides opportunities for cyber attackers; (4) External societal elements, physical entities, unexpected incidents, and attack-defense tactics pose severe threats to power CPS, requiring the handling and consideration of numerous non-secure data sources. Consequently, security measures for power systems need to extend beyond the energy sector to societal aspects, where traditional passive protection methods such as isolation and elimination mainly defend against known threats or attacks. However, facing an exponentially growing number of malicious codes and new security risks [9], the existing power system monitoring and security protection methods are increasingly inadequate for today's power CPS defense systems [10–12].

In recent years, numerous security incidents in industrial control systems and power systems have occurred globally due to cyber-attacks [13,14]. As detailed in Figure 2 [4], significant incidents include the 2010 Stuxnet worm attack on Siemens' SIMATIC WinCC Supervisory Control and Data Acquisition (SCADA) system, which launched a destructive assault on its industrial control system; the 2010 hacking of Schneider Electric's SCADA system, severely disrupting normal workflows; the 2010 attack by the Stuxnet virus on centrifuge motors at Iran's nuclear facilities; the 2012 sustained cyber-attack on Canada's Telvent SCADA system; the 2012 malicious cyber-attack on Saudi Arabia's Aramco oil company, leading to the erasure of most of the company's computer-stored data; the multiple remote attacks in 2014 by the malware BlackEnergy, which is highly flexible and customizable; the 2014 attacks by a Russian hacking group using the malicious code Havex on multiple Western energy companies, aiming to disrupt the energy supply in Europe and America; the over 4000 cyber-attacks within a month on the U.S. PJM in 2015; the catastrophic blackout caused by a data injection attack (DIA) in Ukraine in 2015 [15], resulting in a three-hour-wide outage as shown in Figure 3, where the attackers employed a diversified network attack strategy from the information domain of the power CPS, implementing a composite multi-step cross-domain attack that caused maximum outage losses in the physical domain; the massive ransomware attack on Israel's power system in 2016, which led to computer systems going offline and losing control; the 2017 attack on a U.S. wind farm by an ARP cache poisoning virus, which forged normal industrial control signals for wind turbines; and the 2019 twin hacker attacks on a major hydroelectric station in Venezuela, causing large-scale blackouts across 20 states. These incidents highlight that complex and variable network

 doi:10.20944/preprints202501.2043.v1

attacks have posed a severe threat to the safety of power systems, making defensive research against attacks on power systems urgently necessary [16–18].

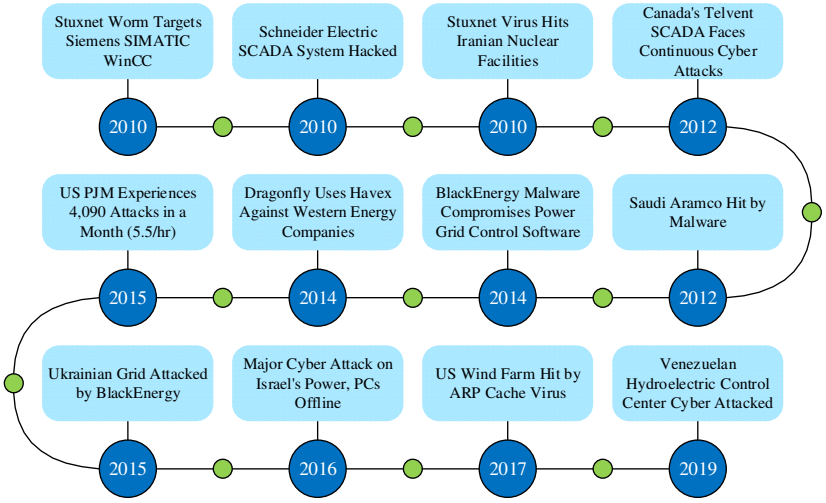

Figure 2. Safety incidents in industrial control systems and power systems worldwide.

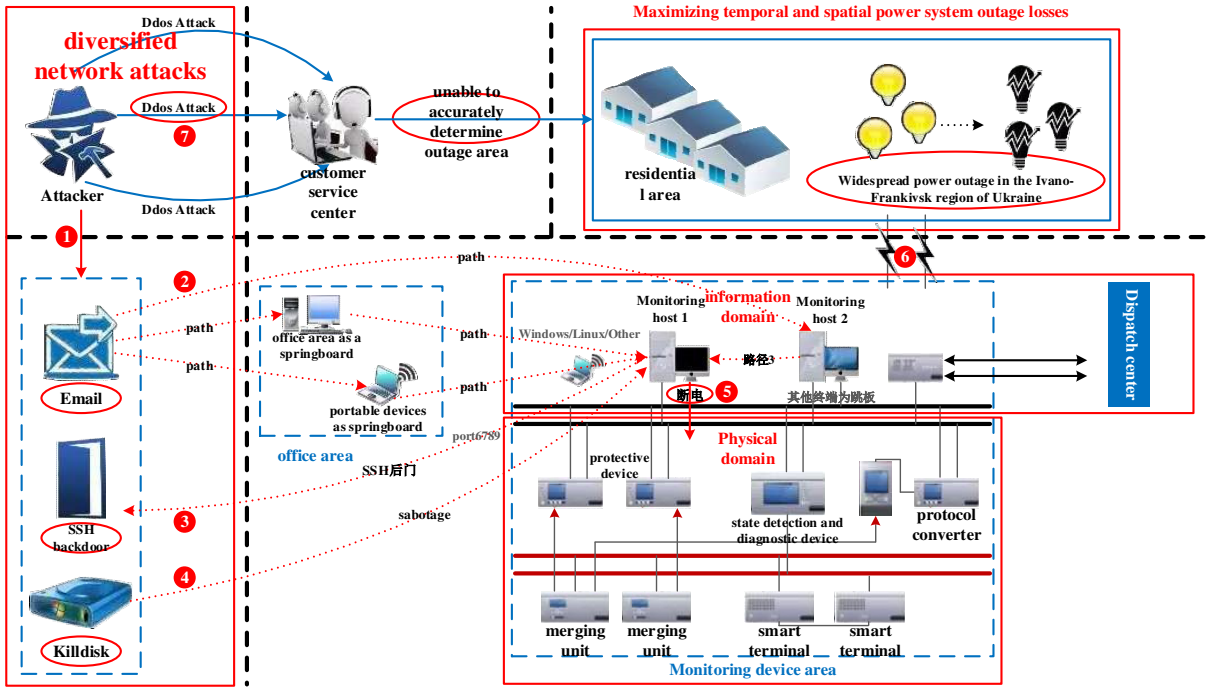

Figure 3. Ukraine blackout attack process.

According to the three key elements of cybersecurity, attacks can be categorized into integrity, availability, and confidentiality attacks. Currently, DIAs represent a typical form of integrity attack in cyber-attacks, distinct from the erroneous data already present in systems; the injected data often possess deceptive and purposeful characteristics [19–21]. As illustrated in Figure 4 [4], DIAs can penetrate the information system by targeting power system endpoint sensors, remote terminal control units, or information and communication devices, subsequently altering the collected measurement data from Remote Terminal Units (RTUs) and Phasor Measurement Units (PMUs) among other power terminals [22–24]. This bypasses the bad data detection module in the energy management system, leading to incorrect state estimations at the power dispatch control center, influencing the decision-making of monitoring personnel [25–27]. This alters the operational flow of the power system, resulting in incorrect or failed actions like circuit breaker misoperations, potentially causing

 doi:10.20944/preprints202501.2043.v1

regional or even widespread power outages, severely impacting the safety and stability of the power system [28–30].

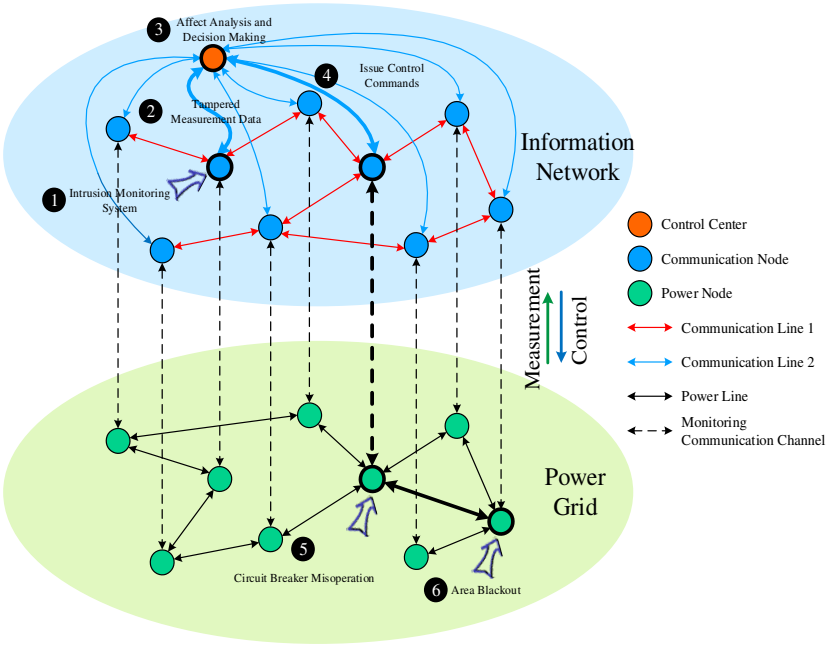

Figure 4. Typical power CPS DIA process.

Traditional DIAs primarily refer to False Data Injection Attacks (FDIAs), characterized by their stealthiness, flexibility, clear consequences, random attack locations, and wide-ranging destructive capabilities [31,32]. The main targets of FDIAs are the electrical measurement data collected by monitoring systems. As attack methods have evolved, the types and scope of power FDIAs have expanded [33]. These attacks aim to destabilize the power system or gain economic benefits by tampering with critical data such as power system measurement data, control signals, and equipment information [34–36]. Recent research indicates that FDIA has evolved into a new form known as Dummy Data Injection Attacks (DDIAs), first proposed by Liu et al. [37]. Malicious data in DDIAs can blend seamlessly with normal measurement data, significantly increasing the difficulty of detecting anomalous data. DDIA builds on traditional FDIA by creating dummy data that is extremely close in the measurement data space, fulfilling the constraints of virtuality and allowing attacked and normal data to mix perfectly. This enhancement of data stealthiness leads to the ineffectiveness of existing cluster- and distance-based attack detection and defense methods, presenting new challenges for the security of power systems.

In summary, various types of FDIA and DDIA are collectively referred to as DIA. By analyzing the attack process, objectives, and impacts, the characteristics of DIA can be summarized as follows:

(1) **Attack Variety and Complexity**: The types of DIAs are numerous and the targets of intrusion vary, making the attack mechanisms complex. DIAs may include forms such as brute-force attacks on passwords, injection of measurement data, topology tampering, forgery of Global Positioning System (GPS) synchronization clocks, denial of service, and control delay attacks. These attacks target communication transmission channels, electrical quantities, switches, clock signals, and computing storage resources. They exploit vulnerabilities in information or control systems to inject fraudulent data, making the intrinsic effectiveness and patterns of attack actions difficult to control.

(2) **Low Probability, High Risk**: The occurrence of DIAs in power systems is extremely rare, and the number of attack samples accumulated by analysis centers is limited, far fewer than the normal operating data. Additionally, the high dimensionality of operational data increases the difficulty of extracting and analyzing attack behavior patterns.

(3) **Complex Spatio-temporal Evolution**: From the perspective of power system operational states, attacks are strongly related to flow sequence and grid topology and evolve continuously along temporal and spatial dimensions. This evolution can lead to cascading failures across the information and physical domains, making it challenging to discern the intent behind attack behaviors.

 doi:10.20944/preprints202501.2043.v1

(4) **Purposeful and Damaging**: DIA attacks are not random disruptions but are carefully designed covert strategies by attackers. They bypass protections such as bad data detection, maliciously manipulate state estimation results, and cause severe consequences like system load shedding and line overloads [38]. Identifying and defending against DIAs is a critical concern.

Due to these complex characteristics of DIAs, existing methods for attack analysis and security defense show limitations [39,40]. Especially, as the integration of renewable energy sources and electric vehicles into modern power systems leads to increased operational uncertainty, this further compounds the complexity [41–43]. In There is an urgent need to explore new methods for power system security defense and develop an integrated security system that encompasses DIA modeling, identification, localization, and defense. This approach aims to address the pain points of existing defense technologies, such as inaccurate attack modeling, difficulty in identifying multiple types of attacks, weak spatio-temporal correlation analysis, and poor adaptability of defenses, thereby mitigating attack risks to ensure the safe and stable operation of power CPS [44–46].

2. Current Research on DIA in Power Systems

2.1. Attack Targets of DIA in Power Systems

In the context of power CPS, vulnerabilities in both the information and physical systems can lead to DIA penetration in various sectors of the smart grid, including generation, transmission, distribution, consumption, markets, and operations [47–50]. The targets most susceptible to attacks include, but are not limited to [51]: generators, transmission lines, substations, renewable energy sources, monitoring and control centers, smart electronic devices, and information and communication systems.

Current research primarily focuses on the energy management system within power control centers as a critical target of DIAs. State estimation serves as a crucial link between the information and physical systems, relying on trustworthy outputs from SCADA and PMU data [52–54]. The reliability of subsequent modules and advanced applications depends on the accuracy of state estimation outputs. Liu et al. first proposed the concept of DIAs targeting state estimation in 2009, analyzing its attack mechanisms [55]. By injecting carefully designed attack vectors into measurements that satisfy system constraints like flow equations, covert DIAs can deceive and bypass traditional residual-based bad data detection, leading to incorrect state estimation results. This may cause frequency instability, line overloads, grid component failures, and load shedding, resulting in severe physical consequences. Reference [56] has explored the impact of DIAs on the static security assessment of power systems, proposing two types of attack scenarios: false security signals and false insecurity signals. The former misleads operators into believing the system is secure, while the latter deceives them into taking corrective actions such as generator rescheduling or load shedding.

In automatic generation control systems, DIA poses threats by directly attacking the automatic generation control (AGC) decision system, tampering with frequency control data in information and communication systems, altering area control error data, and maliciously injecting false error data. Literature [57] has introduced ensemble filtering to detect DIA in AGC systems, determining hidden DIAs by checking if the intersection between measurement updates and prediction updates exists. Research [58] has established a model-based framework for detecting and mitigating attacks on AGC systems, discussing extended, random, ramp, and pulse attacks, and analyzing their principles in modifying AGC system measurements and generator node implementations. Studies [59] have developed a synchronous algorithm based on joint state and unknown input estimation to detect and mitigate measurement DIAs in AGC systems, enabling control centers to make decisions based on corrected sensor signals. Literature [60] examined the impacts of DIA and DOS attacks on low-inertia AGC systems and considered intermittent photovoltaic designs in attack detection algorithms to mitigate the effects of attacks on the grid. Research [61] proposed a semi-supervised ensemble learning framework based on OC-SVM to detect DIAs in AGC system loops, also designing cooperative stealthy DIAs aimed at destabilizing system stability and manipulative DIAs targeting the economic efficiency of power markets. Literature [62] modeled optimal attack strategies as observable Markov decision processes and introduced a kernel density estimation-based method for detecting and correcting DIAs in automatic voltage control (AVC) systems, ensuring the safety of AVC systems even under high system loads. Literature [63] addressed covert limitations by continuously injecting false data across multiple AGC periods to attack flow measurements, defining an emergency response time metric to assess attack effectiveness.

 doi:10.20944/preprints202501.2043.v1

Emergency analysis in power systems, a crucial component of grid security, is divided into emergency selection and assessment. DIAs circumvent state estimation bad data detection by injecting false data, adding or removing emergency elements in emergency analysis lists to disrupt the transmission flow analysis process. Literature [64] modeled the minimum cost DIA as an optimization problem based on mixed-integer linear programming, minimizing the number of attacked sensors to successfully manipulate targeted emergency elements. Manipulated emergency actions embedded as safety constraints in economic dispatch with security constraints quantitatively analyzed the impacts of these DIAs on the safety and economics of power systems. When emergency analysis transitions to a normal safety state, it triggers a safety-constrained optimal flow program. Literature [65] proposed a collaborative distributed AC optimal flow solver based on dual decomposition and introduced a credibility information-based DIA identification method.

Distribution energy management systems and distribution control systems are also prone to DIA attacks, presenting several cybersecurity issues [66–68]: 1) Standardized communication protocols allow network intruders to understand the architecture of distribution systems; 2) Exposed field devices reduce the difficulty for intruders to access the backbone communication network of distribution systems; 3) Purposeful intruders can destroy distribution control centers by injecting malware viruses; 4) Protection device passwords are default or weak, making them easy to crack. Unlike the widely studied state estimation in transmission systems, the scale of distribution networks is large and lacks real-time redundant measurement data, presenting numerous challenges and difficulties. Studies have shown [69] that DIA can create imbalances between the supply and demand sides, increasing transmission and distribution costs and affecting the reliable supply of electric power. Research [70] assessed the security impact of DIA on dynamic microgrid partitioning, leading to increased energy losses in supply-demand balance. Literature [71] proposed a DIA method for three-phase unbalanced distribution network state estimation from a CPS perspective, comparing it with traditional direct and linear attack methods. The proposed attack method can bypass the maximum normalized residual detection while achieving the desired effect. In addition to these detection methods, advanced cryptographic techniques, such as those described in [72], using a 9D complex chaotic system with Quaternion, are also being integrated into smart grid systems to bolster security against DIAs and ensure the integrity of communication and control data within the power CPS.

Power market management systems aim to facilitate standardized transactions between energy industry service providers and public utility consumers, becoming a primary target for attackers to manipulate utility market intelligence or obtain illegal economic gains through other means. Research [73] studied the economic impact of DIA on power market operation state estimation, analyzing how attackers manipulate real-time market prices without being detected by state estimation, and developed a heuristic method for calculating the optimal injection of DIAs from an attacker's perspective. Literature [74] introduced pricing attacks by sending real price scaling values and introducing old price delays. Research [75] modeled DIAs to disrupt communication channels and deploy attack time series to manipulate price signals, increasing the mismatch between production and consumption power. In contrast to snapshot-type single DIAs, literature [76] analyzed that DIAs can be continuously injected over a long period, causing excess generation, poor power quality, and economic losses. It proposed transforming sensitivity functions to simulate system dynamics and quantify the impact of DIAs. Research [77] studied the economic impact of DIA on transmission line ratings in dual settlement power markets, assuming the opponent has complete system load and generation cost information, manipulating real-time nodal marginal prices through forged DIA. Additionally, attackers could manipulate multiple sensors to send erroneous measurement values to convergence centers [78], aiming to gain economic benefits from the power market.

2.2. DIA Modeling Methods

Extensive research has explored the principles and conditions for FDIAs, laying the groundwork for subsequent detection, localization, and defense strategies by constructing DIA models. For instance, DIAs based on the direct current state estimation model [79] allow attackers, who have complete knowledge of the system's topology and configurations, such as topology information, system parameters, state estimation, and bad data detection algorithms, to effectively inject DIAs by crafting specific attack vectors. To expedite the computation of state variables, the nonlinear relationships between measurements and state variables are approximated using the direct current model. Previous studies have shown that DIAs based on the direct current model are easily captured by nonlinear

 doi:10.20944/preprints202501.2043.v1

alternating current state estimations [80], prompting researchers to develop AC-based attack models. In traditional residual testing methods, random DIAs are detectable, whereas covert DIAs remain undetected, with research primarily focusing on the latter.

The assumption that attackers know complete configuration information is not entirely feasible in practice. If attackers have limited attack resources and protected information, launching DIAs with incomplete information becomes more crucial. Literature [81] assumes that attackers can access grid topology information and line parameters, constructing optimal DIAs by calculating the minimum generalized eigenvalue of the characteristic function. Literature [82] constructs covert AC state estimation attack vectors based on measurements of multiple boundary nodes in the attack area, with vector construction depending on angle differences rather than actual phase angles. Literature [83] proposes a RTU tampering attack method based on graph theory, which determines the number of measurements that need to be modified by the attacker, depending on the system topology and the presence of power injection nodes. To minimize the state estimation residuals after an attack, literature [84] develops an optimal attack strategy using principal component analysis and the Lagrange multiplier method, effectively targeting specific areas in real-time. Literature [85] constructs AC-based DIA models under both complete and incomplete topology information, using the angular difference between attacked and non-attacked nodes along lines to calculate line flows and determine power injections at attacked nodes. Literature [86] considers energy distribution and local load redistribution, establishing an attack model that isolates critical nodes and uses regional minimal residuals as the objective function. Reference [87] utilizes incomplete information to mathematically characterize DIA from the perspectives of attackers and operators. It analyzes how the attackers' lack of complete knowledge impacts the power grid and proposes a new vulnerability index that can compare the resistance of various topological structures to attacks.

Research has shown that blind DIAs can be successfully implemented without network information of the attack area; here, no network information means the attack method relies solely on the connections and power measurement data between the attack and non-attack areas. Literature [88], based on adversarial generative networks, proposes a blind AC-based DIA generation method without network topology information. Through the adversarial process between the generative and discriminative networks, physical laws embedded in measurement data are captured, and self-attention mechanisms determine the associations between nodes and lines, verifying the effectiveness of the constructed attacks under various measurement error conditions. Literature [89] separates normal and anomalous values through alternating direction sparse optimization, using principal component analysis on measurement data to retrieve system information and construct DIA vectors. Literature [90] employs kernel principal component analysis to project measurement data into a high-dimensional data space via kernel functions, calculating an approximate grid topology matrix, and constructing a blind online DIA. Literature [91] designs a matrix reconstruction method to mitigate the impact of measurement noise, proposing a subspace estimation-based blind DIA method that can operate without knowing system parameters. This method modifies the eigenvalues of the covariance matrix of the data to reduce the impact of measurement noise, with example analyses showing that the proposed method can achieve a high success rate and operate effectively under limited measurement data, demonstrating robustness against noise levels and grid sizes.

Load redistribution (LR) attacks were first proposed by Yuan et al. in 2011 [92]. Measurement data entering power system state estimations primarily includes generator active power, load node power, and branch active power. However, not all these data can be tampered with by attacks, as real-time communication between power plants and control centers makes it difficult to tamper with generator output power. Literature [93] models and analyzes three-stage delayed LR attacks using Karush-Kuhn-Tucker (KKT) conditions and dual-based methods to identify destructive LR attacks that can be effectively prevented with limited protection resources. To overcome the limitation of attackers knowing all topology information, literature [94] proposes a local LR attack model with incomplete topology information, adjusting the power injection measurement frequency of non-attackable nodes within a threshold to achieve selective attack areas. Literature [95] establishes a coordinated LR attack model with generators and lines, formulated as a bi-level optimization problem where the upper layer aims to maximize load shedding by attackers and the lower layer minimizes load shedding by defenders. Example analysis shows that attackers can coordinate attack measurements with basic power transmission elements, disrupting the physical power system and misleading

 doi:10.20944/preprints202501.2043.v1

power dispatch, maximizing damage with limited attack resources, offering viable strategies for preventing and mitigating high-impact, low-frequency coordinated attacks.

Topology manipulation attacks, a recent research focus, involve most DIA models centered on a constant grid topology, where attackers can only inject DIAs into measurement data. However, due to routine maintenance and unexpected equipment failures, the topology and configuration information may change at any time. DIA models for power systems have further developed to reflect real-time grid topology, aiming to tamper with information such as transformer tap settings, circuit breakers, and switches, ensuring that the estimated topology matches the received data. By tampering with measurements, control systems are misled about the current system topology state, although it does not result in actual physical switching operations. This type of attack was proposed in literature [96], creating an undetectable line removal attack in the control center by attackers with only local information, who can conceal grid topology through false data injection. In literature [97], a topology attack model is designed using heuristic methods to determine the likely attack areas of lines with minimal information resources. When attackers know partial information, they can modify the injected power at both ends of the line and distribute the attacked line's flow to other measurements, making the flow distribution uniform and not exceeding limits, reducing the likelihood of detection. Research considers both increasing and decreasing lines as attack methods [98], using natural aggregation algorithms to solve the DIA model with generation costs, marginal electricity prices, and flows as targets. Literature [99] injects false data to conceal the actual physical disconnections in the power system and constructs DIA vectors based on changed topology and flow data, causing delays in fault response and handling, potentially inducing larger-scale cascading failures. Additionally, injecting false tripping commands to cause real system tripping actions is another form of such attacks. Modeling methods mainly target the process of confidentiality breach, using attack trees, Markov models [100,101], and other tools to intrude into the power system and calculate the success rate of attacks. For consequence modeling, metrics such as component downtime and recovery time are calculated to quantify the probability of lost loads as a measure of attack consequences.

GPS synchronized clock spoofing attacks involve attackers forging GPS signals at receivers, injecting false data into the power grid monitoring system, often deceiving PMUs with incorrect clock signals, leading to deviations in the calculation results for state estimation amplitude, phase angle, frequency, and other measurements. Literature [102] sets an optimization problem to identify PMUs vulnerable to attacks within the grid, developing a joint state estimation and attack reconstruction algorithm based on alternating minimization, analyzing the vulnerability of the grid to GPS spoofing attacks, and extending it to use SCADA and GPS-spoofed PMU combined measurements for state estimation and attack detection. Literature [103] analyzes the impact of GPS synchronized clock spoofing attacks on system dynamic behavior, changing multiple PMUs' measurement readings by transforming the system matrix of the measurement equation, and develops a hypothesis testing procedure based on the generalized likelihood ratio to detect behavioral changes during attacks. Literature [104] optimizes the search for multiple attack targets in PMU measurements, constructing undetectable GPS synchronized clock spoofing attacks.

2.3. DIA Detection Methods

From the perspective of power system operators, accurately and efficiently detecting FDIA is crucial in the defense process. Extensive research has been conducted globally on the detection of FDIAs in power systems, focusing mainly on model-driven and data-driven detection methods [105–107]. Specific methods include Kalman filtering and its variants, low-rank decomposition, mixed Gaussian models, Euclidean detectors, Kullback-Leibler divergence, sparse optimization, similarity matching, data mining, and deep learning [51,108–111]. Model-driven detection approaches typically include state estimation detection, graph theory-based detection, and physical property detection; data-driven methods predominantly involve deep learning and machine learning.

2.3.1. State Estimation-Based DIA Detection

This approach uses the deviation between state estimation and predicted system states for attack detection. Traditional residual testing compares state estimation residuals against measurement error thresholds, identifying anomalies when these exceed predefined limits. Due to increasing system size, data heterogeneity, and varying sources, improvements have been made on existing state estimation methods. For large-scale systems, literature [112] introduced a new robust linear static

 doi:10.20944/preprints202501.2043.v1

estimation framework based on PMU data, segmenting the system into multiple areas to ensure minimal redundancy at least at one subsystem boundary node, effectively detecting DIAs. Literature [113] designed a parallel robust least trimmed squares estimator with different fault points, improving DIA detection for Jacobian matrices, measurement functions, and vectors, thereby enhancing network cybersecurity and reducing necessary sensor numbers to lower capital investments. Literature [114] proposed a cross-layer detection mechanism for GPS clock synchronization attacks, combining state estimation with receiver signal-to-noise ratios for joint physical and application layer DIA detection. To address the issue of undetected attacks due to tampered measurements in centralized control receiving collaboration, literature [115] designed a distributed direct current optimal power flow algorithm, using different updating rules and exchange mechanisms to detect and mitigate DIAs, proposing an embedded resilient control mechanism for information sharing without violating privacy, identifying attacked controllers and restoring optimal power dispatch. Literature [116] based on distributed voltage control in microgrids, constructed a two-stage DIA model comprising deception and terminal attacks, proposing a distributed synchronous detection method to identify covert DIAs and attacked nodes in microgrids, avoiding the complexities of centralized methods by requiring only neighbor information for DIA detection. Literature [117] utilized gated recurrent neural networks for real-time detection of data streams in power grids, classifying predicted residuals using a wavelet-transformed convolutional neural network, with prediction and classification processes completed at the edge, enhancing the effectiveness and real-time performance of DIA detection. Other static state estimation methods such as median filters [118] and maximum likelihood estimation [119] are noted for their simplicity and versatility; however, these may suffer performance degradations when system parameters are uncertain.

2.3.2. Dynamic State Estimation

As the integration of renewable energies increases the uncertainty in power systems, using dynamic state estimation can address the limitations of static methods by establishing time-series based state prediction models. These models dynamically and real-time adjust state prediction results by combining measurements from previous and current moments. The principle is that deviations between measured and attacked state estimates exceeding a preset threshold indicate an attack. Literature [120] combined Kalman filters with Euclidean distance detectors to detect DIAs, and to quickly mitigate attacks and restore system states, literature [121] proposed a new low-complexity online detection and estimation algorithm for DIAs and coordinated attacks, introducing a CUSUM-based detector for rapid response to covert attacks. To enhance DIA detection accuracy and reduce errors due to model linearization, extended Kalman filter [122] and unscented Kalman filter-based DIA detection methods [123] have been proposed. The extended Kalman filter detects DIAs by calculating deviations between dynamic and static estimates, while the unscented Kalman filter, which does not require Jacobian matrix calculations, approximates state variables using unscented transformations to quantify all state fluctuations for DIA detection. Literature [124] proposed a hybrid DIA detection method combining adaptive Kalman filters and convolutional neural networks, achieving parallelized knowledge-driven and data-driven detection.

2.3.3. Graph-Theoretical Models

Given the network topology inherent in power grids, DIA implementation requires knowledge of a set of measurements in the attack area and adjacent nodes and branches. Researchers abstract the power system as a graph network model and explore DIA detection methods from a graph-theoretical perspective. Literature [125] computed the graph Fourier transform of the network state and filtered out high-frequency components of the graph, comparing the maximum norm of the filtered signal to a threshold to detect DIAs. To enhance detection efficiency, literature [126] used graph theory to deconstruct the entire system into interconnected subsystems, generating residual signals for attack detection and designing a distributed attack detection method. To further reduce detection complexity and ensure the applicability of maximum likelihood estimation for real-time DIA detection in large-scale grids, literature [127] utilized the approximate cosparse nature of the grid to accelerate finding optimal solutions for maximum likelihood estimation, applying phase angle Markov graph reduction to decompose the DIA detection problem into local marginal estimation issues. In reality, the edges of the power system graph model have weights, and literature [128] integrated the grid admittance matrix as an adjacency matrix into the graph model, developing a stochastic gradient

 doi:10.20944/preprints202501.2043.v1

descent-based stealth DIA detection algorithm, verifying the scalability and effectiveness of graph model-based attack detection. Literature [129] proposed a graph-theoretical method to detect DIAs in power system AC state estimation, using historical data to calculate the difference in continuous state estimates, identifying whether anomalies in the current timestep's state estimation were caused by an attack.

2.3.4. Physical Property-Based Detection

The consequences and impacts of DIAs manifest through certain physical properties, prompting researchers to detect DIAs based on changes in physical laws post-attack. Literature [130], based on the exponential parameters of the ratio of branch and injected currents to node voltages, could detect abnormal phase shifts caused by DIAs, verifying the algorithm's reliability and lightweight nature through example analysis; the algorithm is developed based on controlled and control variable principles of power system analysis, thus scalable to any phase-shifting device based on power electronics. Literature [131], independent of critical instrument protection and historical data, proposed a two-stage real-time DIA detection method based on multiple alarm indicators and sensitivity factors. Literature [132] studied the impact of DIAs on the performance of line current differential relays, using local currents and voltages, remote currents, and line parameters, based on measurements and calculations to obtain the difference between superimposed voltages at relay terminals for DIA detection. To detect PMU data manipulation attacks, literature [133] tested data integrity in a distributed and non-iterative manner based on continuous monitoring of transmission line equivalent impedance, achieving classification and detection of PMU manipulation attacks. To address the lack of consideration for system stability related to DIAs, literature [134] identified vulnerability levels of advanced metering infrastructure based on different degrees of DIA attacks, studied the interdependence between nodes, and considered the voltage stability index to understand physical vulnerabilities under DIAs. For AC smart island DIAs, which may disrupt central control system performance, literature [135] proposed a wavelet singular entropy analysis of continuous-time system states, adjusting singular value matrices and wavelet transform coefficients, decomposing sliding mode controller switching surfaces, and calculating expected entropy values through stochastic processes to characterize DIAs' switching current and voltage levels. To more comprehensively analyze DIA behavior, from a matrix analysis perspective, literature [136] extracted three attack characteristics: sparsity, persistence, and temporal variability, based on which it analyzed the structural sparsity of the attack matrix and proposed a new structural sparse matrix separation algorithm to enhance detection accuracy. Literature [137] used an adaptive cumulative sum method to detect mean distribution changes in residual vectors under DIAs, based on traditional weighted least squares for state estimation.

2.3.5. Data-Driven Detection Methods

Data-driven methods rely on big data and artificial intelligence technologies to automatically learn hidden features in data and mine abnormal characteristics of DIAs, distinguishing attack events from normal events through classification or clustering algorithms. Classic machine learning algorithms such as support vector machines, K-nearest neighbors, decision trees, artificial neural networks, extreme learning machines, convolutional neural networks, K-means clustering, autoencoders, and random forest algorithms have been applied to DIA detection [138]. More advanced data-driven detection methods have been developed in recent years. Literature [139] combined variational mode decomposition and extreme learning machines to identify DIAs. Literature [140] achieved multi-type DIA classification recognition based on a non-nested generalized exemplar data mining algorithm. From a game-theoretic learning perspective, literature [141] used an adversarially generated deep learning network model and a semi-supervised deep autoencoder combined, designing a diagnostic framework for attacks and faults in power systems. From a semi-supervised learning perspective, literature [142] proposed a mixed Gaussian distribution-based DIA detection method, training classifiers with attack-labeled test sets to set optimal detection thresholds; simulation results proved the method superior to traditional bad data detection and other classic machine learning methods. Literature [143] proposed an edge-based federated learning framework for DIA detection in power grid state estimation, achieving DIA detection with unknown system parameters and small, dispersed datasets, protecting user privacy while exploring and quantifying the impact of incentives on detection accuracy, designing a new preference criterion. As existing detection methods are limited by the input order restrictions of Euclidean space data, making it difficult to accurately describe

 doi:10.20944/preprints202501.2043.v1

spatial correlations between data, literature [144] combined graph data modeling and deep learning methods, designing graph network models for different topologies through multi-graph mechanisms and temporal correlation layers to better mine DIA data-related features and their attributes. To merge the advantages of data-driven and physical model approaches, literature [145] proposed a two-stage power system security state prediction and attack detection framework, aiming to predict power system states in the first stage and achieve binary classification detection of DIAs based on Kullback-Leibler distance in the second stage.

2.4. DIA Localization Methods

To minimize the damage and risks caused by malicious DIAs to power systems, accurately locating the attacked nodes immediately after detecting the attacks has become a critical need. Literature [146] maps the problem of DIA detection to a multi-label classification problem and, using a model-free deep learning approach that combines CNNs with traditional bad data detectors, executes precise attack localization under various noise and attack conditions. In literature [147], a DIA localization method based on extreme learning machines is proposed; however, a limited number of hidden layers restricts the capability to handle high-dimensional, large-scale power system measurement data. Literature [148] introduces a multi-granularity DIA localization algorithm based on graph theory techniques. As a multi-label classification method, literature [149] proposes an effective DIA location identification strategy using a CNN-BiLSTM model, which has passed sensitivity and robustness tests.

In the context of frequently changing power system loads, generation power, and topology, literature [150] uses an improved capsule network to detect and localize DIAs, maintaining stable and accurate attack location detection rates even when attack sparsity and disturbance size change. Literature [151] proposes a cluster-based architecture for false data injection attack detection and localization in smart grids, representing the state vector of the grid as a multivariate time series, using vector autoregression for DIA detection and localization.

To address the challenges of the multimodal probability distribution of measurements and state variables in state estimation for DIA localization, literature [152] constructs a generative adversarial network-based autoencoder that generates normal distributions of multimodal measurements offline under unknown power system topologies, building a candidate set to localize and recover forged measurement data. For efficient DIA localization, literature [153] proposes a model optimized with bidirectional gated recurrent units and a fully convolutional neural network, effectively extracting interrelated features from data. To overcome the limitations of preset thresholds and ensure DIA detection performance using modeling uncertainty, literature [154] considers internal state boundaries, modeling errors, and disturbances to design a series of interval observers, creating distributed interval observers for each measurement device and using a logic discrimination matrix for attack localization.

2.5. DIA Defense Methods

DIA defense strategies primarily include proactive protection of critical devices, optimization of attack-defense resource configuration, moving target defense, and measurement data recovery defense.

2.5.1. Proactive Protection of Critical Devices

This strategy involves protecting certain measurements from attacks to defend the system. Existing research has proposed mixed linear programming [155] and heuristic algorithms [156], with literature [156] introducing an efficient greedy search algorithm to quickly identify target measurement subsets for defense against covert DIAs.

2.5.2. Optimization of Attack-Defense Resource Configuration

Both attackers and defenders aim to maximize their benefits, constrained by their resources, optimizing their resource configuration in a dynamic game process. Literature [157], targeting PMUs as the attack objective, proposes a multi-stage game model from the attacker's perspective, including data tampering, attack strategy adjustment, and multi-path attacks, based on two-person zero-sum

 doi:10.20944/preprints202501.2043.v1

game theory. It considers overall profits and multi-path attacks, finding the optimal attack-defense strategy through Nash equilibrium.

2.5.3. Moving Target Defense

This involves installing Distributed Flexible AC Transmission System (D-FACTS) devices on transmission lines to actively change power system reactance and other parameters, misleading attackers with incorrect parameter information to construct DIAs, which are then easily detected due to significant residuals in state estimation. To address the instability of net load system voltages caused by approximate perturbations of transmission line impedances in traditional moving target defenses, literature [158] constructs a voltage stability-constrained moving target defense framework, deriving a sensitivity matrix of the voltage stability index to line impedance, proposing an index optimization method and load margin constraint method to maintain moving target defense performance while ensuring system voltage stability. To ensure the economic placement of D-FACTS while maintaining the effectiveness of moving target defense, literature [159] uses graph theory to analyze system topology, proposes sufficient conditions for complete and incomplete moving target defenses, and designs a new D-FACTS placement algorithm to minimize system power loss and enhance economic benefits.

2.5.4. Active Defense through Measurement Data Recovery and Correction

This new approach to defense involves recovering attacked measurement data using generative adversarial networks, integrating new smooth training techniques to maintain the integrity of state estimation in real-time. Literature [160] achieves effective recovery of attacked measurement data. Literature [161] mines historical state quantities and predicted state quantities together, integrating measurements from SCADA and PMU instruments for online DIA detection, removal, and correction. Literature [162] proposes a data-driven defense framework for state estimation against DIAs, with a graph model using edge-condition filters to extract data features, detecting abnormal DIAs and effectively restoring attacked data to normal operation values by combining Bayesian inference and variational autoencoder models.

3. Existing Issues and Trends in Research on DIA in Power Systems

The current state of research on DIA in power systems highlights several issues with existing security defense methods:

3.1. Modeling Limitations

Current DIA modeling primarily focuses on traditional types of FDIAs and does not adequately consider multiple forms of attacks. Newer forms of DDIA are often modeled without considering realistic constraints, leading to inaccuracies in the models that may omit critical information about attack behaviors. This can significantly impact the effectiveness of defensive measures, with potential cascading effects.

3.2. Detection Challenges

Attack detection methods based on physical mechanism models struggle with explicitly modeling complex attack behaviors, and the uncertainty in detection thresholds can impact detection accuracy, leading to false positives and missed detections. Although data-driven methods can uncover inherent attack patterns, their detection accuracy heavily relies on the quantity of training samples and the quality of data feature selection, making accurate attack detection challenging. Additionally, the interpretability of data-driven computational approaches remains poor, and machine learning models often lack personalized settings for specific tasks.

3.3. Analysis Limitations

Existing machine learning methods tend to analyze the system's operational data focusing solely on temporal sequences or Euclidean spatial characteristics, often overlooking the inherent non-Euclidean spatial relationships tied to grid topology. This lack of exploration into spatio-temporal coupling mechanisms can lead to inaccurate localization of attack origins, complicating the development of effective defense strategies.

 doi:10.20944/preprints202501.2043.v1

3.4. Traditional Defense Shortcomings

Conventional defense methods mostly focus on pre-deployment of defense resources or on detecting and alerting to attacks, struggling to mitigate and counteract the impacts of attacks on the grid once they occur. There is a lack of effective defensive response methods to attacks. Moreover, the growing volume of data and the frequent interaction between CPS information and energy flows inevitably raise issues of privacy security. Addressing the computational and communication pressures during defense and protecting data privacy remain challenging areas needing breakthroughs.

4. Future Research Directions

4.1. Advanced Attack Modeling

Research in attack modeling is rapidly evolving beyond the confines of single-type FDIA models to embrace a more diverse array of multi-category and novel DIA models. This expansion is critical as it encompasses a wider variety of attack vectors that are becoming increasingly sophisticated in the context of modern power systems. Future studies should not only focus on incorporating a broader spectrum of attacks but also delve into the nuanced characteristics specific to different attack types. This approach will significantly enhance the robustness and adaptability of current detection and mitigation strategies. Furthermore, it will enable researchers and practitioners to develop more comprehensive defense mechanisms that are capable of anticipating and countering attacks effectively, ensuring the resilience and security of power systems against a more complex landscape of cyber threats.

4.2. Enhanced Attack Identification Techniques

As the landscape of cyber threats evolves, the emphasis is increasingly shifting towards leveraging data-driven methods that utilize sophisticated algorithms, including machine learning and artificial intelligence, to detect multiple types of attacks. These technologies are capable of analyzing vast datasets to identify subtle anomalies that may indicate a cyber attack. To address challenges posed by limited data, which is common in highly secure environments, there is a growing need to refine machine learning models that can deliver high accuracy even when trained on small sample sizes. This is particularly crucial for ensuring robust detection capabilities under varied operational conditions where traditional models might fail. Future research should also explore unsupervised and semi-supervised learning models that can continuously adapt to new attack patterns without the need for frequent retraining.

4.3. Precise Attack Localization

Current efforts are extending beyond basic data mining of operational timelines in power systems to more sophisticated analyses involving spatio-temporal correlations. This shift is aimed at developing precise localization algorithms that integrate advanced computational methods such as machine learning, graph theory, and statistical modeling, leveraging the increasing availability of sensor data. By enhancing the accuracy of localization techniques, researchers can more effectively pinpoint the origins and potential pathways of attacks, which is vital for timely intervention and mitigation. Future research should focus on the integration of these technologies to develop systems that not only detect but also visualize the attack progression in real-time across the network.

4.4. Proactive and Adaptive Defense Mechanisms

The field is moving towards proactive and adaptive defense strategies that not only detect attacks but also dynamically respond to them as they occur. This approach involves utilizing advanced technologies such as predictive analytics, automated response systems, and adaptive security architectures that can adjust their configurations in real-time to mitigate potential threats. Research should continue to develop these technologies to enable systems to anticipate attacks based on threat intelligence and behavioral analytics, ensuring continuous operation and system recovery during and after an attack. This will necessitate a layered defense strategy that integrates endpoint security, network security, and application security seamlessly.

4.5. Integrating Cyber-Physical Systems Security

 doi:10.20944/preprints202501.2043.v1

The increasing integration of information technology and operational technology in modern power systems demands a holistic approach to security that addresses both cyber and physical threats cohesively. Future research must focus on developing robust cyber-physical system designs that ensure operational integrity and cybersecurity in tandem. This includes the use of advanced encryption methods, secure communication protocols, and intrusion detection systems that are specifically tailored for the unique requirements of integrated cyber-physical environments. Ensuring that security measures are embedded within both the design and operational phases of system development is crucial for maintaining resilience against increasingly sophisticated cyber-physical threats.

5. Conclusion

This review has underscored the critical evolution of research on data injection attacks in power systems, highlighting the shift from basic models and detection methods to sophisticated multi-dimensional strategies that encompass modeling, detection, localization, and proactive defense mechanisms. The dynamic and increasingly complex nature of modern power systems, coupled with sophisticated potential cyber threats, necessitates a multi-disciplinary approach that spans engineering, computer science, and cybersecurity. As the grid continues to integrate more digital technologies and renewable energy sources, the strategies for its protection must also evolve to anticipate, detect, and mitigate threats dynamically. The ongoing commitment of the research community to innovate and adapt is essential for safeguarding the essential infrastructures that power our world.

References

1. Liu, Z.; Wang, L. Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks. *IEEE Trans. Smart Grid* **2020**, *12*, 1552–1564. https://doi.org/10.1109/tsg.2020.3028123.
2. Ti, B.; Li, G.; Zhou, M.; Wang, J. Resilience Assessment and Improvement for Cyber-Physical Power Systems Under Typhoon Disasters. *IEEE Trans. Smart Grid* **2021**, *13*, 783–794. https://doi.org/10.1109/tsg.2021.3114512.
3. Aslani, M.; Faraji, J.; Hashemi-Dezaki, H.; Ketabi, A. A novel clustering-based method for reliability assessment of cyber-physical microgrids considering cyber interdependencies and information transmission errors. *Appl. Energy* **2022**, *315*. https://doi.org/10.1016/j.apenergy.2022.119032.
4. Bo X. A Review of Detection, Evolution, and Data Reconstruction Strategies for False Data Injection Attacks in Power Cyber-Physical Systems. arXiv preprint arXiv:2501.10441, 2025.
5. Wang, L.; Xu, P.; Qu, Z.; Bo, X.; Dong, Y.; Zhang, Z.; Li, Y. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link. *Front. Energy Res.* **2021**, *9*. https://doi.org/10.3389/fenrg.2021.666130.
6. Qu Z, Zhao T, Zhang Y, et al. Determination Method of Network Risk Propagation Threshold in Power CPS Based on Percolation Theory . Automation of Electric Power Systems, 2020, 44(4): 16-23.
7. Li, Y.; Han, M.; Shahidehpour, M.; Li, J.; Long, C. Data-driven distributionally robust scheduling of community integrated energy systems with uncertain renewable generations considering integrated demand response. *Appl. Energy* **2023**, *335*. https://doi.org/10.1016/j.apenergy.2023.120749.
8. Qu Z, Dong Y, Liu S, et al. Security technology for ubiquitous electric power IoT based on biological immunology methods. Automation of Electric Power Systems, 2020, 44(2): 1-12.
9. Liu T, Tian J, Wang J Z, et al. Comprehensive security threats and defenses research for cyber-physical systems. Acta Automatica Sinica, 2019, 45(1): 5-24.
10. Qu, Z.; Zhang, Y.; Qu, N.; Wang, L.; Li, Y.; Dong, Y. Method for Quantitative Estimation of the Risk Propagation Threshold in Electric Power CPS Based on Seepage Probability. *IEEE Access* **2018**, *6*, 68813–68823. https://doi.org/10.1109/access.2018.2879488.
11. Lu A Y, Yang G H. False data injection attacks against state estimation without knowledge of estimators. IEEE Transactions on Automatic Control, 2022, 67(9): 4529-4540.
12. Qu Z, Dong Y, Qu N, et al. Quantitative Assessment of Survivability of Power CPS Considering Load Optimization and Reconfiguration . Automation of Electric Power Systems, 2019, 43(6): 15-24.

13. Wang Q, Li M Y, Tang Y, et al. A review on cyber-attack and defense research for electrical cyber-physical systems (Part I): Modeling and assessment. Automation of Electric Power Systems, 2019, 43(9): 9-21.
14. Guo Q, Xin S, Wang J, et al. Comprehensive security assessment of information-energy systems observed from the Ukraine blackout incident. Automation of Electric Power Systems, 2016, 40(5): 145-147.
15. Liu N, Yu X, Zhang J, et al. Network coordinated attacks: Deduction and insights from the Ukraine blackout incident. Automation of Electric Power Systems, 2016, 40(6): 144-147.
16. Bo, X.; Chen, X.; Li, H.; Dong, Y.; Qu, Z.; Wang, L.; Li, Y. Modeling Method for the Coupling Relations of Microgrid Cyber-Physical Systems Driven by Hybrid Spatiotemporal Events. *IEEE Access* **2021**, *9*, 19619–19631. https://doi.org/10.1109/access.2021.3053402.
17. Almutairy, F.; Scekic, L.; Elmoudi, R.; Wshah, S. Accurate Detection of False Data Injection Attacks in Renewable Power Systems Using Deep Learning. *IEEE Access* **2021**, *9*, 135774–135789. https://doi.org/10.1109/access.2021.3117230.
18. Li Y, Ma W, Li Y, et al. Enhancing Cyber-Resilience in Integrated Energy System Scheduling with Demand Response Using Deep Reinforcement Learning. Applied Energy, 2025, 379:124831.
19. Qu, Z.; Dong, Y.; Li, Y.; Song, S.; Jiang, T.; Li, M.; Wang, Q.; Wang, L.; Bo, X.; Zang, J.; et al. Localization of dummy data injection attacks in power systems considering incomplete topological information: A spatio-temporal graph wavelet convolutional neural network approach. *Appl. Energy* **2024**, *360*. https://doi.org/10.1016/j.apenergy.2024.122736.
20. Li, Y. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach. 2024 IEEE Power & Energy Society General Meeting (PESGM). LOCATION OF CONFERENCE, United StatesDATE OF CONFERENCE; pp. 1–1.
21. Wang, L.; Qu, Z.; Li, Y.; Hu, K.; Sun, J.; Xue, K.; Cui, M. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal&x2013;Topological Correlation. *IEEE Access* **2020**, *8*, 57260–57272. https://doi.org/10.1109/ACCESS.2020.2982057.
22. Qu, Z.; Dong, Y.; Qu, N.; Wang, L.; Li, Y.; Zhang, Y.; Mugemanyi, S. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation. *Math. Probl. Eng.* **2019**, *2019*, 1–15. https://doi.org/10.1155/2019/2817586.
23. Qu, Z.; Zhang, Z.; Qu, N.; Zhou, Y.; Li, Y.; Jiang, T.; Li, M.; Long, C. Extraction of typical operating scenarios of new power system based on deep time series aggregation. *CAAI Trans. Intell. Technol.* **2024**. https://doi.org/10.1049/cit2.12369.
24. Chen, L.; Gu, S.; Wang, Y.; Yang, Y.; Li, Y. Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid. *Math. Probl. Eng.* **2021**, *2021*, 1–8. https://doi.org/10.1155/2021/2014345.
25. Li, Y.; Li, Z.; Chen, L. Dynamic State Estimation of Generators Under Cyber Attacks. *IEEE Access* **2019**, *7*, 125253–125267. https://doi.org/10.1109/access.2019.2939055.
26. Zhao, J.; Srivastava, A.; Guo, Y.; Ćetenović, D.; Lin, Y.; Levi, V.; Yin, G.; Huang, M.; Zhang, T.; Li, Z.; et al. State Estimation for Integrated Energy Systems: Motivations, Advances, and Future Work. *IEEE Trans. Power Syst.* **2024**, *PP*, 1–17. https://doi.org/10.1109/tpwrs.2024.3524323.
27. Chen, L.; Li, Y.; Huang, M.; Hui, X.; Gu, S. Robust Dynamic State Estimator of Integrated Energy Systems Based on Natural Gas Partial Differential Equations. *IEEE Trans. Ind. Appl.* **2022**, *58*, 3303–3312. https://doi.org/10.1109/tia.2022.3161607.
28. Li Y, Zhang S, Li Y, et al. PMU measurements-based short-term voltage stability assessment of power systems via deep transfer learning. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 2526111.
29. Ahmadi, A.; Nabipour, M.; Taheri, S.; Mohammadi-Ivatloo, B.; Vahidinasab, V. A New False Data Injection Attack Detection Model for Cyberattack Resilient Energy Forecasting. *IEEE Trans. Ind. Informatics* **2022**, *19*, 371–381. https://doi.org/10.1109/tii.2022.3151748.
30. Li, Y.; Yang, Z. Application of EOS-ELM With Binary Jaya-Based Feature Selection to Real-Time Transient Stability Assessment Using PMU Data. *IEEE Access* **2017**, *5*, 23092–23101. https://doi.org/10.1109/access.2017.2765626.

31. Irfan, M.; Sadighian, A.; Tanveer, A.; Al-Naimi, S.J.; Oligeri, G. A survey on detection and localisation of false data injection attacks in smart grids. *IET Cyber-Physical Syst. Theory Appl.* **2024**, *9*, 313–333. https://doi.org/10.1049/cps2.12093.
32. Li Y, Li Z, Chen L, et al. A false data injection attack method for generator dynamic state estimation. Transactions of China Electrotechnical Society, 2019, 34: 3651-3660.
33. Liang, J.; Sankar, L.; Kosut, O. Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation. *IEEE Trans. Power Syst.* **2015**, *31*, 3864–3872. https://doi.org/10.1109/tpwrs.2015.2504950.
34. Tang Y, Li M, Wang Q, et al. A review of network attacks and defenses in cyber-physical power systems: Part II—Detection and Protection. Automation of Electric Power Systems, 2019, 43(10): 1-9.
35. Xu F, Xue A, Chang N, et al. Current research status and prospects of network attacks and defenses in power system automatic generation control. Automation of Electric Power Systems, 2021, 45(3): 3-14.
36. Chen L D, Liu N. False data injection attacks and their detection methods for interactive demand response. Automation of Electric Power Systems, 2021, 45(3): 15-23.
37. Liu, X.; Song, Y.; Li, Z. Dummy Data Attacks in Power Systems. *IEEE Trans. Smart Grid* **2019**, *11*, 1792–1795. https://doi.org/10.1109/tsg.2019.2929702.
38. Li, Y.; Li, J.; Qi, J.; Chen, L. Robust Cubature Kalman Filter for Dynamic State Estimation of Synchronous Machines Under Unknown Measurement Noise Statistics. *IEEE Access* **2019**, *7*, 29139–29148. https://doi.org/10.1109/access.2019.2900228.
39. Pasha S A, Safdar R, Ali S T. False data injection attacks on networked control systems. Journal of Control and Decision, 2024, 11(4): 650-659.
40. Zadsar, M.; Abazari, A.; Ameli, A.; Yan, J.; Ghafouri, M. Prevention and Detection of Coordinated False Data Injection Attacks on Integrated Power and Gas Systems. *IEEE Trans. Power Syst.* **2022**, *38*, 4252–4268. https://doi.org/10.1109/tpwrs.2022.3216118.
41. Li, Y.; Han, M.; Yang, Z.; Li, G. Coordinating Flexible Demand Response and Renewable Uncertainties for Scheduling of Community Integrated Energy Systems with an Electric Vehicle Charging Station: A Bi-level Approach. *IEEE Trans. Sustain. Energy* **2021**, *12*, 2321–2331. https://doi.org/10.1109/tste.2021.3090463.
42. Yang, X.; Li, Y.; Zhao, Y.; Li, Y.; Hao, G.; Wang, Y. Gaussian Mixture Model Uncertainty Modeling for Power Systems Considering Mutual Assistance of Latent Variables. *IEEE Trans. Sustain. Energy* **2024**, *PP*, 1–4. https://doi.org/10.1109/tste.2024.3356259.
43. Li Y, Bu F, Li Y, et al. Optimal scheduling of island integrated energy systems considering multi-uncertainties and hydrothermal simultaneous transmission: A deep reinforcement learning approach. Applied Energy, 2023, 333: 120540.
44. Wang, Y.; Cui, Y.; Li, Y.; Xu, Y. Collaborative optimization of multi-microgrids system with shared energy storage based on multi-agent stochastic game and reinforcement learning. *Energy* **2023**, *280*. https://doi.org/10.1016/j.energy.2023.128182.
45. Qu, Z.; Dong, Y.; Mugemanyi, S.; Yu, T.; Bo, X.; Li, H.; Li, Y.; Rugema, F.X.; Bananeza, C. Dynamic exploitation Gaussian bare-bones bat algorithm for optimal reactive power dispatch to improve the safety and stability of power system. *IET Renew. Power Gener.* **2022**, *16*, 1401–1424. https://doi.org/10.1049/rpg2.12428.
46. Fang, Z.; Zhao, D.; Chen, C.; Li, Y.; Tian, Y. Corrections to "Nonintrusive Appliance Identification With Appliance-Specific Networks" [Jul/Aug 20 3443-3452]. *IEEE Trans. Ind. Appl.* **2020**, *56*, 5678–5678. https://doi.org/10.1109/tia.2020.3011856.
47. Kou, L.; Wu, J.; Zhang, F.; Ji, P.; Ke, W.; Wan, J.; Liu, H.; Li, Y.; Yuan, Q. Image encryption for offshore wind power based on 2D-LCLM and Zhou Yi eight trigrams. *Int. J. Bio-Inspired Comput.* **2023**, *22*, 53–64. https://doi.org/10.1504/ijbic.2023.133505.
48. Chen L, Li Y, Cai J, et al. SCKF-LSTM Based Trajectory Tracking for Electricity-Gas Integrated Energy System. arXiv preprint arXiv:2412.18357, 2024.
49. Hao, G.; Li, Y.; Li, Y.; Guang, K.; Zeng, Z. Safe Reinforcement Learning for Active Distribution Networks Reconfiguration Considering Uncertainty. *IEEE Trans. Ind. Appl.* **2024**, *PP*, 1–13. https://doi.org/10.1109/tia.2024.3462663.

50. Cui, Y.; Xu, Y.; Wang, Y.; Li, Y.; Zhao, Y. Multi-microgrid optimization operation strategy considering nonlinear conditions and renewable energy uncertainty: A data-driven method. *IEEE Trans. Ind. Appl.* **2024**, *PP*, 1–13. https://doi.org/10.1109/tia.2024.3371966.
51. Musleh A S, Chen G, Dong Z Y. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Transactions on Smart Grid, 2019, 11(3): 2218-2234.
52. Bo, X.; Qu, Z.; Liu, Y.; Dong, Y.; Zhang, Z.; Cui, M. Review of active defense methods against power CPS false data injection attacks from the multiple spatiotemporal perspective. *Energy Rep.* **2022**, *8*, 11235–11248. https://doi.org/10.1016/j.egyr.2022.08.236.
53. Fahmeeda S, Bhagyashree B K. Detection and Prevention of False Data Injection Attack in Cyber Physical Power System[C]//2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE, 2021: 1-5.
54. Wang C, Wang X, Cao Y, et al. Critical link identification of power system vulnerability based on modified graph attention network. Power System Protection and Control 2024, 52(15):36-45.
55. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th of ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
56. Chen, J.; Liang, G.; Cai, Z.; Hu, C.; Xu, Y.; Luo, F.; Zhao, J. Impact analysis of false data injection attacks on power system static security assessment. *J. Mod. Power Syst. Clean Energy* **2016**, *4*, 496–505. https://doi.org/10.1007/s40565-016-0223-6.
57. Wu Y, Ru Y, Liu J, et al. Detection of false data injection attacks in automatic generation control systems based on ensemble filtering. Automation of Electric Power Systems, 2022, 46(01): 33-41.
58. Sridhar, S.; Govindarasu, M. Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. https://doi.org/10.1109/tsg.2014.2298195.
59. Khalaf, M.; Youssef, A.; El-Saadany, E. Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems. *IEEE Trans. Smart Grid* **2018**, *10*, 4985–4995. https://doi.org/10.1109/tsg.2018.2872120.
60. Roy S D, Debbarma S. Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid. IEEE Systems Journal, 2019, 14(2): 2023-2031.
61. Roy S D, Debbarma S. A novel OC-SVM based ensemble learning framework for attack detection in AGC loop of power systems. Electric Power Systems Research, 2022, 202: 107625.
62. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control. *IEEE Trans. Smart Grid* **2018**, *10*, 2158–2169. https://doi.org/10.1109/tsg.2018.2790704.
63. Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control. *IEEE Trans. Ind. Informatics* **2017**, *14*, 1932–1941. https://doi.org/10.1109/tii.2017.2765313.
64. Kang J W, Joo I Y, Choi D H. False data injection attacks on contingency analysis: Attack strategies and impact assessment. IEEE Access, 2018, 6: 8841-8851.
65. Cheng Z, Chow M Y. Resilient Collaborative Distributed AC Optimal Power Flow Against False Data Injection Attacks: A Theoretical Framework. IEEE Transactions on Smart Grid, 2021, 13(1): 795-806.
66. Qu, Z.; Bo, X.; Yu, T.; Liu, Y.; Dong, Y.; Kan, Z.; Wang, L.; Li, Y. Active and passive hybrid detection method for power CPS false data injection attacks with improved AKF and GRU-CNN. *IET Renew. Power Gener.* **2022**, *16*, 1490–1508. https://doi.org/10.1049/rpg2.12432.
67. Padhan, S.; Turuk, A.K. Design of False Data Injection Attacks in Cyber-Physical Systems. *Inf. Sci.* **2022**, *608*, 825–843. https://doi.org/10.1016/j.ins.2022.06.082.
68. Qu, Z.; Xie, Q.; Liu, Y.; Li, Y.; Wang, L.; Xu, P.; Zhou, Y.; Sun, J.; Xue, K.; Cui, M. Power Cyber-Physical System Risk Area Prediction Using Dependent Markov Chain and Improved Grey Wolf Optimization. *IEEE Access* **2020**, *8*, 82844–82854. https://doi.org/10.1109/access.2020.2991075.
69. Sun, H.; Zhang, B. Global state estimation for whole transmission and distribution networks. *Electr. Power Syst. Res.* **2005**, *74*, 187–195. https://doi.org/10.1016/j.epsr.2004.10.011.
70. Zhang X, Yang X, Lin J, et al. On false data injection attacks against the dynamic microgrid partition in the smart grid[C]//2015 IEEE International Conference on Communications (ICC). IEEE, 2015: 7222-7227.

71. Wei S, Xu J, Wu Z, et al. False data injection attack methods for state estimation of unbalanced three-phase distribution networks. High Voltage Engineering, 2021, 47(7): 2367-2377.
72. Zhang, F.; Huang, Z.; Kou, L.; Li, Y.; Cao, M.; Ma, F. Data encryption based on a 9D complex chaotic system with quaternion for smart grid. *Chin. Phys. B* **2023**, *32*, 010502. https://doi.org/10.1088/1674-1056/ac76b2.
73. Xie, L.; Mo, Y.; Sinopoli, B. Integrity Data Attacks in Power Market Operations. *IEEE Trans. Smart Grid* **2011**, *2*, 659–666. https://doi.org/10.1109/tsg.2011.2161892.
74. Tan R, Badrinath Krishna V, Yau D K Y, et al. Impact of integrity attacks on real-time pricing in smart grids[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. 2013: 439-450.
75. Giraldo, J.; Cardenas, A.; Quijano, N. Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures. *IEEE Trans. Smart Grid* **2016**, *8*, 2249–2257. https://doi.org/10.1109/tsg.2016.2521339.
76. Maharjan, S.; Zhu, Q.; Zhang, Y.; Gjessing, S.; Basar, T. Dependable Demand Response Management in the Smart Grid: A Stackelberg Game Approach. *IEEE Trans. Smart Grid* **2013**, *4*, 120–132. https://doi.org/10.1109/tsg.2012.2223766.
77. Ye, H.; Ge, Y.; Liu, X.; Li, Z. Transmission Line Rating Attack in Two-Settlement Electricity Markets. *IEEE Trans. Smart Grid* **2015**, *7*, 1346–1355. https://doi.org/10.1109/tsg.2015.2426418.
78. Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets[C]//2010 First IEEE International Conference on Smart Grid Communications. IEEE, 2010: 226-231.
79. Margossian, H.; Sayed, M.A.; Fawaz, W.; Nakad, Z. Partial grid false data injection attacks against state estimation. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 623–629. https://doi.org/10.1016/j.ijepes.2019.03.039.
80. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting False Data Injection Attacks in AC State Estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. https://doi.org/10.1109/tsg.2015.2388545.
81. Jia L, Thomas R J, Tong L. On the nonlinearity effects on malicious data attack on power system[C]//2012 IEEE Power and Energy Society General Meeting. IEEE, 2012: 1-8.
82. Liu, X.; Li, Z. False Data Attacks Against AC State Estimation With Incomplete Network Information. *IEEE Trans. Smart Grid* **2017**, *8*, 2239–2248. https://doi.org/10.1109/tsg.2016.2521178.
83. Hug, G.; Giampapa, J.A. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. *IEEE Trans. Smart Grid* **2012**, *3*, 1362–1370. https://doi.org/10.1109/tsg.2012.2195338.
84. Tian M, Wang X, Dong Z, et al. False data attack strategies based on the Lagrange multiplier method. Automation of Electric Power Systems, 2017, 41(11): 26-32.
85. James J Q, Hou Y, Li V O K. Online false data injection attack detection with wavelet transform and deep neural networks. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271-3280.
86. Fu, X.; Chen, G.; Yang, D. Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems. *IEEE Access* **2020**, *8*, 103285–103290. https://doi.org/10.1109/ACCESS.2020.2999585.
87. Rahman M A, Mohsenian-Rad H. False data injection attacks with incomplete information against smart power grids[C]//2012 IEEE Global Communications Conference (GLOBECOM). IEEE, 2012: 3153-3158.
88. Jiao, R.; Xun, G.; Liu, X.; Yan, G. A New AC False Data Injection Attack Method Without Network Information. *IEEE Trans. Smart Grid* **2021**, *12*, 5280–5289. https://doi.org/10.1109/tsg.2021.3102329.
89. Tian J, Wang B, Shang F. False data injection attacks in smart grids based on robust principal component analysis. Journal of Computer Applications, 2017, 37(7): 1943-1947+1971.
90. Li Y, Qiu R, Zeng J. Blind online false data injection attacks in smart grids based on kernel principal component analysis. Power System Technology, 2018, 42(7): 2270-2278.
91. Yang, H.; He, X.; Wang, Z.; Qiu, R.C.; Ai, Q. Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction. *IEEE Trans. Smart Grid* **2022**, *13*, 3174–3187. https://doi.org/10.1109/tsg.2022.3164874.
92. Yuan, Y.; Li, Z.; Ren, K. Modeling Load Redistribution Attacks in Power Systems. *IEEE Trans. Smart Grid* **2011**, *2*, 382–390. https://doi.org/10.1109/tsg.2011.2123925.
93. Yuan, Y.; Li, Z.; Ren, K. Quantitative Analysis of Load Redistribution Attacks in Power Systems. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1731–1738. https://doi.org/10.1109/tpds.2012.58.
94. Liu, X.; Li, Z. Local Load Redistribution Attacks in Power Systems With Incomplete Network Information. *IEEE Trans. Smart Grid* **2014**, *5*, 1665–1676. https://doi.org/10.1109/tsg.2013.2291661.

95. Xiang Y, Wang L, Yu D, et al. Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks[C]//2015 IEEE Power & Energy Society General Meeting. IEEE, 2015: 1-5.
96. Kim, J.; Tong, L. On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1294–1305. https://doi.org/10.1109/jsac.2013.130712.
97. Liu, X.; Li, Z. Local Topology Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2016**, *8*, 2617–2626. https://doi.org/10.1109/tsg.2016.2532347.
98. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios. *IEEE Trans. Smart Grid* **2017**, *10*, 1704–1712. https://doi.org/10.1109/tsg.2017.2776325.
99. Zhou, T.; Xiahou, K.; Zhang, L.; Wu, Q.H. Real-Time Detection of Cyber-Physical False Data Injection Attacks on Power Systems. *IEEE Trans. Ind. Informatics* **2020**, *17*, 6810–6819. https://doi.org/10.1109/tii.2020.3048386.
100. Ding M, Li X, Zhang J. Impact of cyber attacks on SCADA systems on the reliability of power systems. Power System Protection and Control, 2018, 46(11): 37-45.
101. Zhang, Y.; Wang, L.; Xiang, Y. Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems. *IEEE Trans. Smart Grid* **2015**, *7*, 669–683. https://doi.org/10.1109/tsg.2015.2439693.
102. Risbud, P.; Gatsis, N.; Taha, A. Vulnerability Analysis of Smart Grids to GPS Spoofing. *IEEE Trans. Smart Grid* **2018**, *10*, 3535–3548. https://doi.org/10.1109/tsg.2018.2830118.
103. Pradhan P, Nagananda K, Venkitasubramaniam P, et al. GPS spoofing attack characterization and detection in smart grids[C]//2016 IEEE Conference on Communications and Network Security (CNS). IEEE, 2016: 391-395.
104. Barreto, S.; Pignati, M.; Dan, G.; Le Boudec, J.-Y.; Paolone, M. Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation. *IEEE Trans. Smart Grid* **2016**, *9*, 3530–3542. https://doi.org/10.1109/tsg.2016.2634124.
105. Boyaci, O.; Narimani, M.R.; Davis, K.R.; Ismail, M.; Overbye, T.J.; Serpedin, E. Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids Using Graph Neural Networks. *IEEE Trans. Smart Grid* **2021**, *13*, 807–819. https://doi.org/10.1109/tsg.2021.3117977.
106. Chen Y, Qi D, Li Z, et al. Distributed cooperative control of microgrids under false data injection attacks. Automation of Electric Power Systems, 2021, 45(5): 97-103.
107. Zhao, J.; Zhang, G.; La Scala, M.; Dong, Z.Y.; Chen, C.; Wang, J. Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks. *IEEE Trans. Smart Grid* **2015**, *8*, 1580–1590. https://doi.org/10.1109/tsg.2015.2492827.
108. Manandhar K, Cao X, Hu F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter.IEEE transactions on control of network systems, 2014, 1(4):370-379.
109. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. https://doi.org/10.1109/tsg.2015.2495133.
110. Bo, X.; Qu, Z.; Liu, Y.; Dong, Y.; Zhang, Z.; Cui, M. Review of active defense methods against power CPS false data injection attacks from the multiple spatiotemporal perspective. *Energy Rep.* **2022**, *8*, 11235–11248. https://doi.org/10.1016/j.egyr.2022.08.236.
111. Musleh A S, Chen G, Dong Z. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Transactions on Smart Grid, 2019, 11(3): 2218-2234.
112. Xu, C.; Abur, A. A Massively Parallel Framework for Very Large Scale Linear State Estimation. *IEEE Trans. Power Syst.* **2017**, *33*, 4407–4413. https://doi.org/10.1109/tpwrs.2017.2788360.
113. Chakhchoukh, Y.; Ishii, H. Enhancing Robustness to Cyber-Attacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. *IEEE Trans. Power Syst.* **2016**, *31*, 4395–4405. https://doi.org/10.1109/tpwrs.2015.2503736.
114. Fan, Y.; Zhang, Z.; Trinkle, M.; Dimitrovski, A.D.; Bin Song, J.; Li, H. A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids. *IEEE Trans. Smart Grid* **2014**, *6*, 2659–2668. https://doi.org/10.1109/tsg.2014.2346088.

 doi:10.20944/preprints202501.2043.v1

115. Duan, J.; Zeng, W.; Chow, M.-Y. Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack. *IEEE Trans. Smart Grid* **2016**, *9*, 3543–3552. https://doi.org/10.1109/tsg.2016.2633943.
116. Cao, G.; Gu, W.; Lou, G.; Sheng, W.; Liu, K. Distributed synchronous detection for false data injection attack in cyber-physical microgrids. *Int. J. Electr. Power Energy Syst.* **2022**, *137*. https://doi.org/10.1016/j.ijepes.2021.107788.
117. Lei, W.; Pang, Z.; Wen, H.; Hou, W.; Han, W. FDI Attack Detection at the Edge of Smart Grids Based on Classification of Predicted Residuals. *IEEE Trans. Ind. Informatics* **2022**, *18*, 9302–9311. https://doi.org/10.1109/tii.2022.3174159.
118. Lukicheva I, Pozo D, Kulikov A. Cyberattack detection in intelligent grids using non-linear filtering[C]//2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2018: 1-6.
119. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control. *IEEE Trans. Smart Grid* **2018**, *10*, 2158–2169. https://doi.org/10.1109/tsg.2018.2790704.
120. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter. *IEEE Trans. Control. Netw. Syst.* **2014**, *1*, 370–379. https://doi.org/10.1109/tcns.2014.2357531.
121. Kurt M N, Yılmaz Y, Wang X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Transactions on Information Forensics and Security, 2018, 14(2): 498-513.
122. Chakhchoukh, Y.; Lei, H.; Johnson, B.K. Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation. *IEEE Trans. Power Syst.* **2019**, *35*, 1188–1197. https://doi.org/10.1109/tpwrs.2019.2939192.
123. Li, X.; Wang, Z.; Zhang, C.; Du, D.; Fei, M. A Novel Dynamic Watermarking-Based EKF Detection Method for FDIAs in Smart Grid. *Ieee/caa J. Autom. Sin.* **2022**, *9*, 1319–1322. https://doi.org/10.1109/jas.2022.105704.
124. Qu, Z.; Bo, X.; Yu, T.; Liu, Y.; Dong, Y.; Kan, Z.; Wang, L.; Li, Y. Active and passive hybrid detection method for power CPS false data injection attacks with improved AKF and GRU-CNN. *IET Renew. Power Gener.* **2022**, *16*, 1490–1508. https://doi.org/10.1049/rpg2.12432.
125. Drayer, E.; Routtenberg, T. Detection of False Data Injection Attacks in Smart Grids Based on Graph Signal Processing. *IEEE Syst. J.* **2019**, *14*, 1886–1896. https://doi.org/10.1109/jsyst.2019.2927469.
126. Hasnat, A.; Rahnamay-Naeini, M. A Graph Signal Processing Framework for Detecting and Locating Cyber and Physical Stresses in Smart Grids. *IEEE Trans. Smart Grid* **2022**, *13*, 3688–3699. https://doi.org/10.1109/tsg.2022.3177154.
127. Moslemi, R.; Mesbahi, A.; Velni, J.M. A Fast, Decentralized Covariance Selection-Based Approach to Detect Cyber Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2017**, *9*, 4930–4941. https://doi.org/10.1109/tsg.2017.2675960.
128. Boyaci, O.; Umunnakwe, A.; Sahu, A.; Narimani, M.R.; Ismail, M.; Davis, K.R.; Serpedin, E. Graph Neural Networks Based Detection of Stealth False Data Injection Attacks in Smart Grids. *IEEE Syst. J.* **2021**, *16*, 2946–2957. https://doi.org/10.1109/jsyst.2021.3109082.
129. Jorjani, M.; Seifi, H.; Varjani, A.Y. A Graph Theory-Based Approach to Detect False Data Injection Attacks in Power System AC State Estimation. *IEEE Trans. Ind. Informatics* **2020**, *17*, 2465–2475. https://doi.org/10.1109/tii.2020.2999571.
130. Chakrabarty, S.; Sikdar, B. Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems. *IEEE Trans. Power Syst.* **2020**, *36*, 271–280. https://doi.org/10.1109/tpwrs.2020.3008184.
131. Li, X.; Hedman, K.W. Enhancing Power System Cyber-Security With Systematic Two-Stage Detection Strategy. *IEEE Trans. Power Syst.* **2020**, *35*, 1549–1561. https://doi.org/10.1109/TPWRS.2019.2942333.
132. Ameli, A.; Hooshyar, A.; El-Saadany, E.F. Development of a Cyber-Resilient Line Current Differential Relay. *IEEE Trans. Ind. Informatics* **2018**, *15*, 305–318. https://doi.org/10.1109/tii.2018.2831198.
133. Pal, S.; Sikdar, B.; Chow, J.H. Classification and Detection of PMU Data Manipulation Attacks Using Transmission Line Parameters. *IEEE Trans. Smart Grid* **2017**, *9*, 5057–5066. https://doi.org/10.1109/tsg.2017.2679122.

134. Anwar, A.; Mahmood, A.N.; Tari, Z. Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid. *Inf. Syst.* **2015**, *53*, 201–212. https://doi.org/10.1016/j.is.2014.12.001.
135. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Tajik, E.; Padmanaban, S.; Aliev, H. Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. *IEEE Access* **2021**, *9*, 16488–16507. https://doi.org/10.1109/access.2021.3051300.
136. Huang, K.; Xiang, Z.; Deng, W.; Yang, C.; Wang, Z. False Data Injection Attacks Detection in Smart Grid: A Structural Sparse Matrix Separation Method. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2545–2558. https://doi.org/10.1109/tnse.2021.3098738.
137. Huang, Y.; Tang, J.; Cheng, Y.; Li, H.; Campbell, K.A.; Han, Z. Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis. *IEEE Syst. J.* **2014**, *10*, 532–543. https://doi.org/10.1109/jsyst.2014.2323266.
138. Yang Y Z, Liu W X, Li C Z, et al. A review of FDIA detection methods for power SCADA systems. Proceedings of the Chinese Society of Electrical Engineering, 2023, 43(22): 8602-8622.
139. Dou, C.; Wu, D.; Yue, D.; Jin, B.; Xu, S. A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM. *CSEE J. Power Energy Syst.* **2020**, *8*, 1697–1707. https://doi.org/10.17775/cseejpes.2019.00670.
140. Adhikari, U.; Morris, T.H.; Pan, S. Applying Non-Nested Generalized Exemplars Classification for Cyber-Power Event and Intrusion Detection. *IEEE Trans. Smart Grid* **2016**, *9*, 3928–3941. https://doi.org/10.1109/tsg.2016.2642787.
141. Farajzadeh-Zanjani, M.; Hallaji, E.; Razavi-Far, R.; Saif, M.; Parvania, M. Adversarial Semi-Supervised Learning for Diagnosing Faults and Attacks in Power Grids. *IEEE Trans. Smart Grid* **2021**, *12*, 3468–3478. https://doi.org/10.1109/tsg.2021.3061395.
142. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Physical Syst. Theory Appl.* **2017**, *2*, 161–171. https://doi.org/10.1049/iet-cps.2017.0013.
143. Lin, W.-T.; Chen, G.; Huang, Y. Incentive edge-based federated learning for false data injection attack detection on power grid state estimation: A novel mechanism design approach. *Appl. Energy* **2022**, *314*. https://doi.org/10.1016/j.apenergy.2022.118828.
144. Han, Y.; Feng, H.; Li, K.; Zhao, Q. False data injection attacks detection with modified temporal multi-graph convolutional network in smart grids. *Comput. Secur.* **2022**, *124*. https://doi.org/10.1016/j.cose.2022.103016.
145. Reda, H.T.; Anwar, A.; Mahmood, A.; Chilamkurti, N. Data-driven Approach for State Prediction and Detection of False Data Injection Attacks in Smart Grid. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 455–467. https://doi.org/10.35833/mpce.2020.000827.
146. Wang, S.; Bi, S.; Zhang, Y.-J.A. Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach. *IEEE Internet Things J.* **2020**, *7*, 8218–8227. https://doi.org/10.1109/jiot.2020.2983911.
147. Wu, T.; Xue, W.; Wang, H.; Chung, C.Y.; Wang, G.; Peng, J.; Yang, Q. Extreme Learning Machine-Based State Reconstruction for Automatic Attack Filtering in Cyber Physical Power System. *IEEE Trans. Ind. Informatics* **2020**, *17*, 1892–1904. https://doi.org/10.1109/tii.2020.2984315.
148. Nudell, T.R.; Nabavi, S.; Chakrabortty, A. A Real-Time Attack Localization Algorithm for Large Power System Networks Using Graph-Theoretic Techniques. *IEEE Trans. Smart Grid* **2015**, *6*, 2551–2559. https://doi.org/10.1109/tsg.2015.2406571.
149. Mukherjee, D. A novel strategy for locational detection of false data injection attack. *Sustain. Energy, Grids Networks* **2022**, *31*. https://doi.org/10.1016/j.segan.2022.100702.
150. Li, Y.; Wang, Y. Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system. **2019**, *105*, 101705. https://doi.org/10.1016/j.sysarc.2019.101705.
151. Mallikarjunaswamy S, Sharmila N, Siddesh G K, et al. A Novel Architecture for Cluster Based False Data Injection Attack Detection and Location Identification in Smart Grid[C]//Advances in Thermofluids and Renewable Energy: Select Proceedings of TFRE 2020. Springer Singapore, 2022: 599-611.

152. Huang, X.; Qin, Z.; Xie, M.; Liu, H.; Meng, L. Defense of Massive False Data Injection Attack via Sparse Attack Points Considering Uncertain Topological Changes. *J. Mod. Power Syst. Clean Energy* **2022**, *10*, 1588–1598. https://doi.org/10.35833/mpce.2020.000686.
153. Cao Y, Song Sr H D, Zhang Sr T, et al. Research on location detection method of power network false data injection based on FCN-GRU[C]//2nd International Conference on Mechanical, Electronics, and Electrical and Automation Control (METMS 2022). SPIE, 2022, 12244: 1242-1247.
154. Luo, X.; Li, Y.; Wang, X.; Guan, X. Interval Observer-Based Detection and Localization Against False Data Injection Attack in Smart Grids. *IEEE Internet Things J.* **2020**, *8*, 657–671. https://doi.org/10.1109/jiot.2020.3005926.
155. Liu X, Li Z, Li Z. Optimal protection strategy against false data injection attacks in power systems. IEEE Transactions on Smart Grid, 2016, 8(4): 1802-1810.
156. Hao, J.; Piechocki, R.J.; Kaleshi, D.; Chin, W.H.; Fan, Z. Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids. *IEEE Trans. Ind. Informatics* **2015**, *11*, 1–12. https://doi.org/10.1109/tii.2015.2475695.
157. Yi, N.; Wang, Q.; Yan, L.; Tang, Y.; Xu, J. A multi-stage game model for the false data injection attack from attacker's perspective. *Sustain. Energy, Grids Networks* **2021**, *28*. https://doi.org/10.1016/j.segan.2021.100541.
158. Zhang, H.; Liu, B.; Liu, X.; Pahwa, A.; Wu, H. Voltage Stability Constrained Moving Target Defense Against Net Load Redistribution Attacks. *IEEE Trans. Smart Grid* **2022**, *13*, 3748–3759. https://doi.org/10.1109/tsg.2022.3170839.
159. Liu, B.; Wu, H. Optimal D-FACTS Placement in Moving Target Defense Against False Data Injection Attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 4345–4357. https://doi.org/10.1109/tsg.2020.2977207.
160. Li, Y.; Wang, Y.; Hu, S. Online Generative Adversary Network Based Measurement Recovery in False Data Injection Attacks: A Cyber-Physical Approach. *IEEE Trans. Ind. Informatics* **2019**, *16*, 2031–2043. https://doi.org/10.1109/tii.2019.2921106.
161. Liu X, Wu Z. Research on online defense against stealthy malicious data injection attacks in smart grids. Proceedings of the Chinese Society of Electrical Engineering, 2020, 40(8): 2546-2559.
162. Chen B, Xiahou K, Li M. Research on a data-driven framework for defending against false data injection attacks in power systems. Electric Measurement & Instrumentation, 2024, 61(12): 10-16.