Review

Review of False Data Injection Attacks in Power CPS: Challenges, Detection, and Resilience Strategies

Weijia Liu *

Posted Date: 5 May 2025

doi: 10.20944/preprints202505.0166.v1

Keywords: False Data Injection Attacks; Power Cyber-Physical Systems; Attack Detection; Machine Learning; Resilience Strategies; Hybrid Detection Methods

Review

Review of False Data Injection Attacks in Power CPS: Challenges, Detection, and Resilience Strategies

Weijia Liu

School of Electrical Engineering, Shenyang Institute of Engineering, Shenyang, China

Abstract: The increasing integration of Cyber-Physical Systems (CPS) into power grids has significantly enhanced their efficiency and flexibility. However, this integration has also exposed power grids to emerging cyber threats, particularly False Data Injection Attacks (FDIAs), which can disrupt the operation of Power CPS by manipulating system data. This paper reviews the challenges, detection methods, and resilience strategies related to FDIAs in Power CPS. It provides an overview of the types of FDIAs, their impact on system security and stability, and the evolving nature of these attacks. It further examines recent advances in detection techniques, including machine learning, deep learning, and hybrid detection methods, as well as data reconstruction and attack localization strategies. The paper concludes by highlighting future research directions, emphasizing the need for a multi-faceted approach combining technical, regulatory, and operational measures to secure Power CPS against the growing threat of FDIAs.

Keywords: False Data Injection Attacks; Power Cyber-Physical Systems; Attack Detection; Machine Learning; Resilience Strategies; Hybrid Detection Methods

1. Introduction

1.1. Overview of Power CPS and Integration with Modern Technologies

Cyber-Physical Systems (CPS) in the context of power grids represent the convergence of physical power infrastructure with computational and communication technologies [1-3]. These systems leverage advanced sensors, automated control devices, and data analytics to monitor and optimize grid operations in real-time. Power CPS include the integration of smart meters, phasor measurement units (PMUs), distributed energy resources (DERs), and electric vehicles, all connected through a sophisticated network of communication protocols [4]. This interconnection enhances grid efficiency, operational flexibility, and resilience, providing utilities with the ability to manage real-time energy flows, forecast demand, and perform predictive maintenance [5-6].

As the global energy landscape shifts toward renewable energy sources such as solar and wind [7-8], and as demand for electric vehicles and decentralized energy solutions grows [9-10], the role of Power CPS becomes even more crucial. These advancements enable grid operators to integrate intermittent renewable resources, improve load balancing, and enhance the overall flexibility of the grid [11-12]. Power CPS allow for more efficient energy distribution, enhance system reliability, and reduce operational costs by facilitating automation and data-driven decision-making [13].

However, with the integration of modern information and communication technologies (ICT), Power CPS become increasingly vulnerable to cyber threats [14]. While these technologies offer immense benefits in terms of efficiency and resilience, they also open new attack vectors that can compromise the integrity of the power grid [15]. This makes cybersecurity an essential aspect of Power CPS, as any disruption or manipulation of data can have significant consequences on the overall operation of the grid [16-18].

1.2. False Data Injection Attacks in Power Systems: Types and Impact

False Data Injection Attacks (FDIAs) are a class of cyber-attacks specifically targeting the data flows within Power CPS [19-21]. These attacks aim to manipulate system measurements, such as voltage levels, current flows, and frequency, by injecting false or misleading data into the system's state estimation processes [22]. Since Power CPS rely heavily on real-time data to make operational decisions, FDIAs can have far-reaching consequences, making them one of the most dangerous types of cyber threats to power systems [23-25].

The main types of FDIAs in power systems can be categorized into two broad groups:

1) **Measurement Manipulation**: Attackers inject false data into measurement points, such as sensors or meters, to mislead system operators about the state of the grid. These manipulations can cause incorrect estimations of system parameters like voltage angles or power flows, leading to improper grid control actions, such as wrong load dispatching, unnecessary power rerouting, or incorrect fault isolation [26-27].
2) **Control Manipulation**: In more sophisticated attacks, FDIAs target control systems directly, causing incorrect actions in the grid's operational commands [28-29]. For example, attackers could manipulate state estimation results to mislead the automatic control systems into making erroneous decisions, such as triggering circuit breaker operations or rescheduling generation units, which could destabilize the entire grid.

The consequences of such attacks can range from localized faults to large-scale outages. For instance, an attacker may manipulate data to prevent fault detection systems from identifying an ongoing issue, leading to system-wide cascading failures. In more severe cases, FDIAs can cause long-term damage to infrastructure, especially if critical components such as transformers or power lines are forced to operate outside their safe limits [30-32].

1.3. FDIA Impact on Power Grid Security and Stability

The impact of FDIAs on the security and stability of power grids can be devastating, particularly as power grids become more interconnected and automated [33]. A successful FDIA can undermine the integrity of the entire power system, as it can cause miscalculations in grid operation, destabilize power flow, and lead to inefficient use of resources [34-36]. The potential consequences of FDIAs include:

1) **Grid Instability**: FDIAs can disrupt the grid's balance between supply and demand. If the state estimation is compromised, operators might make incorrect decisions that could overload certain sections of the grid, leading to voltage instability, system congestion, or even widespread blackouts [37-38].
2) **Cascading Failures**: Once FDIAs manipulate key grid parameters, the effects can propagate across the system, causing cascading failures [39-40]. For example, incorrect load shedding or generator rescheduling could trigger further system instability, affecting interconnected systems and causing larger outages [41]. These cascading failures can be difficult to control or reverse, especially if the attack is not detected promptly.
3) **Loss of Data Integrity**: In Power CPS, accurate real-time data is essential for ensuring the reliable operation of the grid. FDIAs undermine this data integrity, making it difficult for operators to assess the actual state of the system. This results in incorrect operational decisions, potentially leading to equipment damage or poor resource allocation [42].
4) **Economic Impact**: Beyond technical consequences, FDIAs also carry significant economic risks. Extended outages or grid instability can disrupt industrial operations, leading to production losses and financial damage [43-45]. Additionally, the costs associated with restoring grid stability, including repairs, operational downtime, and regulatory penalties, can be substantial [46].

As the adoption of advanced technologies such as Internet of Things (IoT), machine learning, and smart meters in power systems continues to grow, the risk of FDIAs becomes more pronounced.

These technologies offer enhanced grid performance but also increase the attack surface, making it more difficult to secure the system against sophisticated cyber threats [47-48].

1.4. Motivation for the Review: Identifying Gaps and Future Directions

The rapid advancement of Power CPS and the increasing threat posed by FDIAs highlight the need for a comprehensive understanding of the current research landscape and the challenges in detecting, mitigating, and preventing such attacks [49]. While significant progress has been made in developing detection methods, defense strategies, and resilience mechanisms, several gaps remain in the field. These include:

1) **Detection Accuracy and Speed**: Existing detection methods often suffer from high false-positive rates or long processing times, making it difficult to respond to attacks in real time. More research is needed to develop adaptive, real-time detection systems that can quickly identify and respond to FDIA threats.
2) **Comprehensive Defense Strategies**: Although several mitigation methods have been proposed, many of them are either reactive or only address specific types of FDIAs. A more comprehensive defense approach that combines detection, recovery, and proactive prevention measures is essential.
3) **Integration of Emerging Technologies**: As technologies such as AI, machine learning, and quantum computing evolve, they offer new opportunities for FDIA detection and defense. However, integrating these technologies with existing systems remains a challenge and requires further exploration.
4) **Cross-Domain Security**: Power CPS are highly interconnected with other critical infrastructure, such as communication networks and data centers. Ensuring the security of these interdependent systems is a complex task that requires coordinated research across multiple domains.

This review aims to address these research gaps by providing an overview of the latest developments in FDIA detection, mitigation, and prevention strategies. It will also highlight promising future directions, focusing on the integration of emerging technologies and multi-layered defense approaches to secure Power CPS. Additionally, the review will emphasize the need for continued collaboration between academia, industry, and government agencies to create a comprehensive framework for securing power grids against cyber threats.

2. FDIA Background and Evolution

2.1. Early Detection and Historical Incidents

FDIAs were first conceptualized in the context of power systems in the late 2000s, and since then, significant research has been conducted to understand their potential impact [50-52]. The early detection of FDIAs was limited, mainly because existing power grid monitoring systems were not designed to handle cyber threats. Initial detection methods relied heavily on traditional bad data detection algorithms, which were effective at identifying anomalies, but these methods could not distinguish between legitimate operational discrepancies and malicious data manipulation, especially when attackers injected false data that conformed to the system's constraints [53].

The 2009 discovery of the Stuxnet worm in industrial control systems marked a pivotal moment in cybersecurity for critical infrastructure, including power systems. Although Stuxnet was not an FDIA, it demonstrated the vulnerability of control systems to cyber-attacks, thus highlighting the need for advanced security measures in modern power grids. The worm's ability to manipulate industrial processes without triggering immediate alarms mirrored how FDIAs could infiltrate power CPS by subtly altering system data, making it harder to detect.

In the years that followed, BlackEnergy malware and the 2015 Ukraine power grid attack further illustrated the dangers of FDIAs. During the Ukraine attack, attackers gained control over SCADA (Supervisory Control and Data Acquisition) systems and manipulated the state estimation process, leading to a large-scale blackout that affected over 200,000 people. This incident exposed the real-world threat of FDIAs and showcased their potential for causing widespread grid instability. These early incidents highlighted a key challenge: the inability to detect FDIAs due to the stealthy nature of these attacks, where false data is strategically injected into the system to avoid triggering alarms [54-56].

2.2. Types of FDIAs: Manipulation of Measurement Data, State Estimation, and Control Actions

FDIAs in power systems can be categorized based on their specific targets and objectives, but the most common types include manipulation of measurement data, state estimation, and control actions.

1) **Manipulation of Measurement Data**: The most straightforward form of FDIA involves directly manipulating measurement data obtained from various sensors or devices such as PMUs, Remote Terminal Units (RTUs), and smart meters. These devices continuously collect real-time data from the power grid, including voltage, current, and frequency [57]. By injecting false data into these measurements, attackers can mislead system operators about the actual state of the grid, thereby preventing them from making informed decisions about system operation. Since many bad data detection algorithms rely on discrepancies in the measurements to detect anomalies, attackers can manipulate the measurements in a way that satisfies system constraints, making the false data nearly indistinguishable from legitimate data [58].
2) **State Estimation**: State estimation refers to the process by which grid operators use available measurements to estimate unmeasured states of the system, such as voltage angles and magnitudes [59-60]. Since power system operations are largely governed by these state estimations, manipulating the estimated state of the system can have far-reaching consequences [61]. FDIAs can target state estimation algorithms by injecting false data that causes the estimated states to deviate from their true values. These manipulations can lead to incorrect decisions, such as unnecessary generator rescheduling, misallocation of power, or improper fault isolation. State estimation manipulation is particularly dangerous because it can affect large areas of the grid while remaining undetected [62-64].
3) **Control Actions**: In more advanced FDIA scenarios, attackers target the control actions executed by the grid’s supervisory systems. By manipulating state estimation data, attackers can influence automated control systems that rely on the system’s state information to make real-time decisions, such as load shedding, generation dispatch, or the opening and closing of circuit breakers. These attacks can cause disruptions, such as overloading transformers or generators, unnecessarily isolating parts of the grid, or causing power quality issues. The long-term consequences can be severe, including cascading failures and widespread blackouts, especially if the attacks are left undetected for extended periods [65].

2.3. FDIA Evolution: From Basic Attacks to Sophisticated, Multi-Stage Strategies

Initially, FDIAs were relatively simple, involving direct manipulation of system measurements to mislead state estimation algorithms. However, as detection methods have evolved, so too have the sophistication and complexity of FDIA strategies. Over time, attackers have developed multi-stage, multi-phase attack strategies designed to evade detection and cause more significant damage [66-68].

1) **Basic Attacks**: Early FDIAs were mostly focused on the direct injection of false data into the system’s measurement devices. These attacks targeted weak points in the system where traditional detection algorithms, based on residual analysis, could not identify malicious alterations. The attacks were often limited to small-scale disturbances, such as misreporting voltage or power flows, which could go unnoticed in a system with high levels of data noise or error [69-70].
2) **Advanced Multi-Stage Attacks**: As the grid's security and detection mechanisms have become more sophisticated, attackers have shifted towards more elaborate multi-stage attacks. These attacks may begin with network infiltration, followed by the manipulation of critical control system components [70]. For example, attackers may first gain unauthorized access to communication networks or control centers, then inject false data into sensors or manipulate data

exchanges between devices. Following this, they may exploit vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) systems to alter system behavior, leading to larger-scale failures or cascading blackouts [71-72].

The introduction of advanced persistent threats (APTs), which often involve prolonged, covert operations, has further complicated the detection of these attacks. Attackers can remain inside the system for extended periods, observing system behaviors and refining their attacks to avoid detection. The multi-stage nature of these attacks requires security systems that can detect anomalies not just in real-time data, but across different stages of the attack lifecycle [73].

3) **Targeted and Coordinated Attacks**: The evolution of FDIAs has also seen the rise of coordinated attacks targeting multiple parts of the grid simultaneously. These attacks often leverage collaborative strategies that involve compromising various components of the system, such as attacking both the communication network and the control systems, or manipulating the physical infrastructure to mislead grid operators. In these scenarios, the attacks are not isolated to one component but are distributed across several layers of the system, making them much harder to detect and mitigate [74].

2.4. The Stealthy Nature of FDIAs: Challenges in Detection

One of the most challenging aspects of FDIAs is their stealthy nature. Unlike traditional cyber-attacks that cause immediate disruptions or are easily detectable through signature-based methods, FDIAs are designed to operate without being noticed for long periods. The primary goal of an FDIA is to subtly alter the system’s operational data while avoiding detection by traditional bad data detection systems [75]. This is achieved by injecting false data that aligns with the system’s operational constraints, making it difficult for existing detection methods to distinguish between legitimate data and malicious alterations [76].

1) **Data Conformance to System Constraints**: Attackers often design FDIAs to inject data that conforms to the physical constraints of the system [77-78]. For example, they might manipulate voltage measurements in such a way that they appear valid according to the system's power flow equations. This makes traditional bad data detection techniques, which rely on finding inconsistencies in the data, ineffective against sophisticated FDIAs.
2) **Use of Encryption and Secure Communication Channels**: The increasing use of secure communication protocols, such as encryption, in power CPS further complicates the detection of FDIAs. While encryption enhances the security of data transmission, it also makes it more difficult to inspect and verify the data being exchanged between devices [79]. This presents a challenge for security systems that aim to detect false data or malicious commands within encrypted data streams.
3) **Long Detection Time**: Because FDIAs are typically low-profile and occur over extended periods, detection systems often struggle to identify them in real time. The time window for detecting such attacks is crucial, as even minor delays in detection can allow an attacker to achieve their objectives [80-81]. Moreover, the complexity of modern power systems means that detecting abnormal patterns or inconsistencies requires sophisticated analysis, often involving machine learning and AI-based techniques [82-84].

3. Challenges in FDIA Detection

3.1. Current Detection Techniques: Model-Driven vs. Data-Driven Approaches

The detection of FDIAs in Power CPS has been an area of active research, with two main approaches—model-driven and data-driven—dominating the landscape of FDIA detection. Each approach has its own strengths and weaknesses, and their effectiveness depends on the specific characteristics of the system under scrutiny.

1) **Model-Driven Approaches**: Model-driven detection techniques rely on system models and mathematical formulations to compare measured data against expected data [85]. These approaches typically use state estimation methods, where the system's state is inferred from a set of measurements, and any significant deviation from expected values is flagged as an anomaly. The most common model-driven approach is based on bad data detection (BDD) algorithms, such as Weighted Least Squares (WLS), which checks for discrepancies between measured data and the state estimation model [86-87].

These methods have been effective in detecting FDIAs when the data deviates significantly from the expected results, but they face challenges when dealing with more subtle attacks. Attackers often inject false data that aligns with system constraints, making it difficult for model-driven methods to distinguish between real and manipulated data. Furthermore, the reliance on accurate system models and predefined parameters makes model-driven approaches less adaptable to dynamic changes in the system or to attacks that evolve over time.

2) **Data-Driven Approaches**: Data-driven detection techniques, on the other hand, utilize machine learning (ML) and statistical models to identify anomalies in the system without relying on a pre-existing system model [88]. These methods focus on learning patterns from large datasets to predict normal system behavior, and any deviation from these patterns can indicate an attack. Commonly used data-driven techniques include Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks [89-91].

The advantage of data-driven approaches is their ability to adapt to changing grid conditions and detect complex, subtle attacks that model-driven methods might miss. These methods do not require an explicit system model, making them more flexible and suitable for large, distributed systems. However, data-driven methods require large amounts of training data to perform well and can be sensitive to noise or incomplete data, which is common in real-world power systems.

3) **Hybrid Approaches**: In recent years, hybrid approaches that combine both model-driven and data-driven methods have gained attention [92]. These methods seek to leverage the strengths of both approaches, using state estimation to provide initial detection and machine learning algorithms to refine the results and improve accuracy. Hybrid methods can potentially improve the robustness and adaptability of FDIA detection, particularly in large and complex systems [93].

3.2. Limitations of Existing Methods: Accuracy, Cost, Adaptability

Despite the advancements in detection methods, several challenges remain, particularly in terms of **accuracy**, **cost**, and **adaptability**. These limitations affect the practical deployment of FDIA detection systems in real-world power CPS.

1) **Accuracy**: One of the biggest challenges with existing detection methods is accuracy. Both model-driven and data-driven approaches can suffer from high false-positive rates, where legitimate system variations are flagged as attacks. This is particularly problematic in large-scale systems where normal fluctuations in system performance (e.g., due to load changes or renewable generation variability [94]) can be mistaken for anomalies. Inaccurate detection can lead to unnecessary corrective actions, such as load shedding or rescheduling generation, which could negatively impact grid stability and efficiency [95].

On the other hand, false negatives, where attacks go undetected, are even more dangerous. Attackers can manipulate system data in ways that align with system constraints, making it difficult for detection algorithms to distinguish between normal and malicious behavior [96]. As a result, enhancing the detection sensitivity and reducing the error rates are critical objectives for future research.

2) **Cost**: Many detection methods, particularly those based on state estimation and machine learning, require significant computational resources. Model-driven methods, such as WLS, may involve solving complex optimization problems in real-time, which can be computationally expensive, especially for large-scale power grids. Similarly, data-driven approaches, particularly those based on deep learning, require substantial training data and computing power, which may not be available in all settings [97].

The cost of implementing FDIA detection systems is a significant barrier, particularly for utilities in regions with limited resources. There is a need for more efficient and cost-effective detection methods that balance accuracy with computational feasibility. Edge computing and cloud-based solutions may offer a way to reduce the computational burden by processing data closer to the source or distributing the workload across multiple systems.

3) **Adaptability**: The adaptability of detection systems is another critical issue. Power systems are constantly evolving, with new technologies like smart meters, DERs, and electric vehicles being integrated into the grid. As the grid evolves, the patterns of normal behavior also change, and FDIA detection systems must be able to adapt to these changes [98].

Traditional model-driven methods may struggle with this adaptability since they rely on fixed models and parameters that may become outdated as the system evolves. Data-driven methods, while more flexible, require continuous training on updated data, which can be difficult to manage in real-time systems. Future detection systems must be adaptive, able to update their models or learn new patterns of behavior in response to changes in grid operations and attack strategies.

3.3. Real-Time Detection and Large-Scale Grid Challenges

Real-time detection of FDIAs in large-scale power CPS presents significant challenges due to the complex and dynamic nature of modern grids. Power CPS are highly distributed, with thousands of data points being collected and transmitted continuously [99]. Ensuring that FDIA detection is both accurate and timely is critical, as delays in detecting an attack can result in severe consequences.

1) **Real-Time Detection**: The ability to detect FDIAs in real-time is crucial for minimizing the impact of an attack [100]. Many current detection methods, particularly those based on machine learning, require significant processing time to analyze large datasets and make predictions. This can be a problem in a fast-moving environment like a power grid, where decisions need to be made within seconds to avoid grid instability [101].

Advances in edge computing and distributed processing can help address these challenges by allowing data to be processed closer to the source, reducing latency and enabling faster detection [102]. Additionally, streaming data analysis techniques, such as those used in real-time anomaly detection, can help identify attacks as soon as they occur, enabling immediate countermeasures to be taken [103].

2) **Large-Scale Grid Challenges**: Large-scale grids, especially those with high levels of distributed generation and renewable energy integration, pose unique challenges for FDIA detection [104-106]. These systems generate vast amounts of data, and the interconnectivity between different grid components makes it difficult to identify the source of an attack. Attackers can target multiple points within the grid, injecting false data in ways that affect different parts of the system, making detection and localization [107].

4. Recent Advances in FDIA Detection Techniques

4.1. Machine Learning and AI Approaches: Deep Learning, Ensemble Methods

ML and artificial intelligence (AI) techniques have significantly enhanced the detection of FDIAs in Power CPS. Unlike traditional methods that rely on predefined models and algorithms, AI and ML techniques enable the system to learn from vast amounts of data, making them more adaptable to evolving attack strategies [108-110].

1) **Deep Learning**: Deep learning has emerged as one of the most promising approaches for FDIA detection due to its ability to automatically learn hierarchical features from raw data [111]. In particular, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been successfully applied in FDIA detection. CNNs, for example, are excellent at processing temporal data, such as the time-series data from PMUs and smart meters, allowing them to detect subtle anomalies indicative of FDIAs. RNNs, especially Long Short-Term Memory (LSTM) networks, are effective for modeling the temporal dependencies inherent in power grid measurements, allowing the detection of time-sensitive attacks that evolve gradually [112].

Deep learning models can also process large-scale datasets in real-time, making them well-suited for high-dimensional and time-varying grid data [113]. The ability of deep learning models to improve with more data, while avoiding manual feature engineering, makes them increasingly popular for detecting complex attack patterns that are hard to identify using traditional methods [114].

2) **Ensemble Methods**: Ensemble learning methods, such as Random Forests and Gradient Boosting Machines (GBM), are another significant advancement in FDIA detection [115]. These methods aggregate the predictions from multiple machine learning models to improve the robustness and accuracy of detection. By combining the outputs of several classifiers, ensemble methods reduce the likelihood of errors caused by individual models and can better capture the diversity of attacks [116].

Random Forests, for instance, are particularly effective in handling noisy and incomplete data, which is often encountered in real-world power grid environments. They work by constructing multiple decision trees based on random subsets of the input data, and their collective output provides a more reliable prediction. Similarly, GBM, which builds decision trees sequentially, corrects errors from previous trees and has been found to perform well in detecting FDIAs that involve subtle manipulations of grid data.

These ensemble methods enhance detection accuracy, especially when faced with high-dimensional feature spaces and noisy datasets. By combining different models, ensemble techniques also offer greater resilience against attacks designed to exploit specific weaknesses of individual classifiers [117-118].

4.2. State Estimation Improvements: Robustness and Accuracy

State estimation remains a fundamental component of FDIA detection in power systems, providing critical real-time insights into grid operation. However, traditional state estimation techniques are vulnerable to FDIAs, particularly when attackers inject false data that aligns with system constraints. Recent advancements in state estimation methods focus on improving their robustness and accuracy in the presence of malicious data [119].

1) **Robust State Estimation**: One major area of improvement is the development of **robust state estimation** techniques. These methods are designed to be less sensitive to outliers and anomalies, which are common when FDIAs are present [120]. Huber M-estimators and least absolute deviation (LAD) techniques are examples of robust estimators that prioritize minimizing the impact of large deviations in data, such as those caused by FDIA, while maintaining the accuracy of the overall estimation process [121].

Furthermore, the incorporation of outlier detection mechanisms into state estimation algorithms has become a key trend. These mechanisms help identify measurements that significantly deviate from the expected range, making it easier to spot potential FDIAs. Such techniques often combine statistical methods with machine learning algorithms to improve detection sensitivity [122].

2) **Dynamic and Extended State Estimation**: Modern power systems are dynamic, and state estimation must also account for time-varying conditions [123]. Dynamic state estimation (DSE) methods, which track the state of the system over time, have become more widely used to detect FDIAs in real-time [124]. These techniques consider the grid's operational state as a dynamic process, updating system states and measurements at frequent intervals. The ability to continuously track and update states allows DSE to detect evolving FDIA attacks that span longer durations [125-126].

Extended state estimation methods, which integrate additional measurements and parameters (such as wind generation or demand response data), provide a more comprehensive understanding of the system's state. These methods help in detecting attacks that attempt to exploit specific areas of the grid, such as renewable energy integration, and offer improved accuracy in grid operation [127].

4.3. Hybrid Detection Methods: Combining Model-Based and Data-Driven Approaches

Hybrid detection methods combine the strengths of both **model-based** and **data-driven** approaches to create more effective and adaptive FDIA detection systems [128-130]. Model-based methods rely on predefined system models and assumptions, while data-driven methods use machine learning to learn from historical data and detect anomalous behavior.

1) **Model-Based and Data-Driven Integration**: One promising approach is the integration of state estimation (model-based) with machine learning algorithms (data-driven). For example, residual analysis, commonly used in state estimation, can be combined with machine learning classifiers such as Support Vector Machines (SVMs) or Artificial Neural Networks (ANNs) to improve detection accuracy. In this setup, the state estimation algorithm identifies possible discrepancies, while the machine learning model is used to classify whether those discrepancies are caused by FDIAs or legitimate operational deviations [131].

This hybrid approach leverages the system knowledge inherent in model-based methods and the pattern recognition capabilities of data-driven approaches. The integration allows for better performance in detecting sophisticated, multi-stage attacks that might evade traditional methods [132].

2) **Ensemble Hybrid Approaches**: In some cases, ensemble learning techniques are applied in a hybrid manner, where multiple state estimation models and machine learning classifiers are combined to create a more robust detection system [133-134]. This approach uses ensemble learning to combine the outputs of different models, each of which may be suited to detecting specific types of FDIA, thereby enhancing the overall system's ability to detect a wider variety of attack strategies [135].

The main advantage of hybrid approaches is their flexibility: they can be adapted to different grid configurations and attack scenarios, improving detection capabilities across diverse systems. Furthermore, the combination of model-based and data-driven methods enables these hybrid systems to work efficiently in real-time environments, crucial for preventing large-scale power outages and other grid disruptions [136].

4.4. Case Studies and Real-World Applications

Real-world applications of FDIA detection techniques have demonstrated their effectiveness in securing power CPS. Several case studies have highlighted the practical implementation of detection methods, showcasing how these techniques can be deployed to protect critical infrastructure [137-139].

1) **Case Study: FDIA Detection in a Smart Grid**: In a recent study, researchers deployed an ensemble machine learning model combined with state estimation techniques to detect FDIAs in a smart grid testbed. The system was designed to handle data from both traditional grid components (e.g., transformers and substations) and emerging technologies such as solar panels and electric vehicle charging stations. The ensemble model was able to accurately identify false data injected into the grid by comparing expected measurements with those reported by sensors in real-time [140].
2) **Case Study:** Hybrid Detection in an Urban Distribution Network: Another case study focused on the integration of hybrid detection systems in an urban distribution network. By combining residual-based detection with machine learning algorithms, the system demonstrated a significant improvement in detecting small, targeted attacks that traditional methods failed to identify. This hybrid system was able to identify FDIA events in under 5 seconds, enabling quick corrective actions that prevented grid instability [141].
3) **Real-World Application:** Ukraine Power Grid Attack: The 2015 Ukraine power grid attack provided an opportunity to test the effectiveness of FDIA detection and response strategies in a real-world scenario. Researchers used data from the attack to develop detection methods that could have identified the compromised state estimation systems before widespread power outages occurred. The use of real-time state estimation combined with machine learning algorithms could have significantly reduced the time it took to respond to the attack and isolated the damage to a smaller portion of the grid [142].

5. FDIA Evolution and Impact

5.1. Temporal and Spatial Evolution of FDIAs

The evolution of FDIAs in power CPS has become more sophisticated over time, adapting to the advancements in grid technologies and detection capabilities [143]. The nature of these attacks has transformed from simple data manipulations to complex, multi-phase, and multi-stage strategies that are harder to detect and mitigate.

1) **Temporal Evolution**: Initially, FDIAs were relatively simple and focused on injecting false data into the system to cause short-term disruptions or mislead operators. These attacks were typically reactive, designed to exploit weaknesses in data integrity by introducing false readings from sensors. As detection methods improved, attackers adapted their tactics to evolve into more advanced, long-term attacks [144].

In recent years, FDIAs have become more persistent and subtle, evolving into attacks that remain undetected for longer periods. Attackers can now spend extended periods inside the system, observing its behavior and gradually introducing manipulated data to avoid triggering alarms. This multi-stage evolution allows the attackers to refine their strategies and cause more severe disruptions without being caught early. For example, they may first infiltrate the system, then monitor system behavior, and later inject false data into critical measurements, all while avoiding detection by traditional anomaly detection systems [145-146].

2) **Spatial Evolution**: The spatial evolution of FDIAs refers to how attacks spread across the power grid, potentially affecting multiple components in different areas. Initially, attacks would focus on a limited set of measurements or devices, such as transformers or transmission lines. However, as Power CPS have become more interconnected, attackers have shifted to more distributed strategies, injecting false data into various regions of the grid simultaneously [147].

doi:10.20944/preprints202505.0166.v1

The complexity of modern grids, especially with the integration of renewable energy sources, smart meters, and decentralized energy systems, has made it easier for attackers to target various parts of the grid without being detected. A well-coordinated FDIA can affect different components of the power grid simultaneously—ranging from generation to distribution—leading to cascading failures that are difficult to trace back to their origin. In these cases, the attack is not just localized to one part of the grid but is propagated across the system, causing widespread instability [148].

5.2. Influence of Cyber and Physical Components on Attack Outcomes

FDIAs do not only affect the data or information flows within the system but also interact with the physical components of the power grid. The cyber-physical nature of power CPS makes the outcome of an FDIA highly dependent on the interplay between cyber elements (such as communication networks and control systems) and physical elements (such as generators, transformers, and distribution lines) [149-150].

1) **Cyber Components**: The cyber components of Power CPS, such as communication networks, control centers, and SCADA systems, are crucial for the operation and monitoring of the grid. FDIAs can target these cyber components by disrupting data transmission or manipulating control signals. For example, an attacker might gain access to the control systems, modify state estimation data, or inject false measurements that mislead operators into making incorrect decisions, such as shutting down power plants or rerouting power flows. These attacks can introduce significant errors into the system's operational parameters, leading to performance degradation or catastrophic failures if left unaddressed [151].

As grid communication becomes more digital and reliant on interconnected networks, the vulnerability of cyber components to attacks increases. The use of encrypted communications and network segmentation has been proposed as a means of protecting these components. However, as attackers gain more advanced capabilities, the defense of cyber components requires continuous innovation and adaptation to address emerging threats [152].

2) **Physical Components**: The physical components of the power grid, such as power generators, transformers, circuit breakers, and distribution lines, are directly impacted by the control decisions made based on manipulated data. Once attackers compromise the cyber components and manipulate state estimations, these erroneous signals can result in incorrect control actions, such as triggering the opening or closing of circuit breakers, adjusting generation schedules, or shifting loads. These misjudgments can lead to overloading, overheating, or even physical damage to critical equipment [153].

For instance, if false data leads operators to believe that a transformer is operating within safe limits, the equipment could be exposed to excessive loads, eventually causing overheating or failure. Additionally, incorrect power flow control could result in voltage instability, frequency deviation, or overloading of transmission lines, which could disrupt power supply to large areas.

The combined effect of compromised cyber components and misoperation of physical components underscores the need for integrated security measures that consider both the digital and physical aspects of Power CPS [154-155].

5.3. Impact on System Reliability, Security, and Economic Stability

The consequences of FDIAs on power CPS are profound and wide-reaching, impacting the reliability, safety, and economic stability of the entire power grid. FDIAs can cause both immediate disruptions and long-term instability in power system operations, with cascading effects that extend beyond the grid itself.

1) **System Reliability**: The reliability of a power grid is highly dependent on accurate data and correct decision-making by grid operators. FDIAs undermine this by introducing false data that

leads to faulty decisions, such as improper power flow control or failure to recognize faults. These incorrect decisions can lead to outages, equipment damage, and reduced system resilience [156-157]. In the worst cases, FDIAs can cause system-wide blackouts that take significant time and resources to restore [158].

Modern grids are designed to be resilient and self-healing, with the ability to quickly isolate faults and restore service. However, the presence of undetected FDIAs complicates this process, as false data may mask the presence of real faults or cause the grid to take inappropriate corrective actions. This makes the grid more vulnerable to cascading failures and delays in recovery [159-160].

2) **Security**: The safety implications of FDIAs in power systems cannot be overstated. False data injected into the system can trigger incorrect control actions, such as misoperation of circuit breakers or incorrect load shedding, which can overload critical equipment or lead to unsafe operating conditions [161-162]. For example, failure to isolate a fault or excessive power fluctuations can result in dangerous conditions such as fires, electrical shocks, or explosions. In power plants or substations, these issues can have catastrophic consequences, not only for grid operators but also for surrounding communities.

Furthermore, the compromised data may prevent the grid's fault detection systems from responding to emergency situations, increasing the risk of unsafe conditions. In critical infrastructure, such as nuclear plants or hydroelectric stations, FDIAs can exacerbate existing vulnerabilities, creating life-threatening scenarios if protective mechanisms fail [163].

3) **Economic consequences**: FDIAs can have significant economic impact for utilities, consumers, and industries. The immediate costs of responding to an FDIA, including identifying the attack, isolating compromised components, and recovering from grid instability, can be substantial. Additionally, long-term disruptions to the grid, such as prolonged outages or system inefficiencies, can result in lost productivity, increased operating costs, and decreased confidence in the stability of the energy supply [164].

For large-scale outages, such as those caused by FDIAs targeting control systems, the economic losses can be magnified. In a modern, interconnected economy, industries dependent on consistent power supply, such as manufacturing, healthcare, and telecommunications, can face substantial financial setbacks [165]. Furthermore, the costs of repairing damaged infrastructure and implementing enhanced security measures can add to the financial burden. FDIAs also create uncertainty in energy markets, distorting price signals and potentially leading to market manipulation [166].

6. Mitigation Strategies for FDIAs

Mitigating the impact of FDIAs is critical for ensuring the resilience and reliability of Power CPS [167-169]. As FDIA detection methods have advanced, so have the strategies to mitigate their effects. Mitigation strategies typically focus on data reconstruction, attack localization, countermeasures, and real-time decision support systems [170]. This section outlines these key strategies and their evolution.

6.1. Data Reconstruction Approaches: State-Aware vs. Action-Control Methods

Once FDIAs are detected, the next crucial step is to reconstruct the data and correct any erroneous information injected into the system. The goal of data reconstruction is to recover the system’s state and prevent any harmful effects from the attack, ensuring that the power grid continues to operate optimally.

1) **State-Aware Data Reconstruction**: State-aware reconstruction focuses on estimating the grid’s state after an FDIA is detected by using available data from unaffected sensors and components.

This method relies on the system model, where the state of the grid (such as voltage levels, power flow, and generation schedules) is reconstructed by combining available measurements and the known grid topology. The system uses state estimation algorithms, such as Kalman filtering or Extended Kalman Filters (EKF), to generate the most likely true state of the grid based on the available measurements [171].

The advantage of this method is that it can quickly restore the grid’s operational state without requiring changes to the control system’s setpoints. However, the success of state-aware reconstruction depends on the accuracy of the system model and the availability of sufficient uncorrupted data. If large portions of the system are compromised, state-aware methods may struggle to accurately estimate the grid's state, leading to suboptimal or incorrect operational decisions [172].

2) **Action-Control Data Reconstruction**: **Action-control reconstruction**, on the other hand, focuses on restoring the control actions based on the corrupted state information. Once an FDIA is detected, the attack is isolated, and the system's control actions—such as generator dispatch, load shedding, or power flow adjustment—are corrected. This method does not just estimate the system's state but also corrects the operational decisions made based on the manipulated data [173].

This method is more complex, as it requires a deeper understanding of the control strategies employed by the system. However, it can be more effective in scenarios where the state estimation model alone is insufficient to recover from the effects of an FDIA. Action-control reconstruction ensures that even if false data has been injected, the system will still execute correct control actions that align with the true state of the system [174-175].

6.2. Attack Localization and Minimizing Damage

Attack localization is the process of identifying the specific parts of the power grid that have been affected by an FDIA. Localizing the attack is crucial for minimizing damage and ensuring that the mitigation efforts are focused on the most critical areas of the grid [176-177].

1) **Localization Techniques**: Various localization algorithms are employed to trace the origin of a malicious attack within a power grid. These algorithms typically use residual analysis, graph-based methods, and fault detection techniques to pinpoint discrepancies between expected and actual system states. The grid’s topology is modeled as a graph, with nodes representing the grid’s components (generators, transformers, transmission lines, etc.) and edges representing the connections between them [178]. Anomalies detected in the system can be traced back to specific components by analyzing the residuals or errors introduced by the FDIA [179].

More advanced localization techniques involve the use of machine learning algorithms that learn from historical attack data to identify patterns and anomalies more effectively. These methods can detect subtle signs of attacks that may not be apparent through traditional residual analysis, providing a faster and more accurate means of attack localization [180-181].

2) **Minimizing Damage**: Once the affected components are identified, operators can take localized corrective actions **to** prevent the attack from spreading across the grid. For example, operators can isolate the compromised parts of the grid, reroute power, or adjust load shedding strategies to reduce the impact on grid stability. By containing the attack to a specific region, damage to other parts of the system can be minimized, preserving the overall functionality of the grid [182].

Moreover, attack localization allows for targeted countermeasures, such as applying additional security protocols to the affected components or enhancing data validation checks for sensors in the compromised areas. This targeted approach is more efficient than attempting to apply blanket countermeasures to the entire system [183].

6.3. Developing Robust Countermeasures for Power CPS

To prevent FDIAs and mitigate their impact, it is essential to develop robust countermeasures that can protect both the cyber and physical components of Power CPS. These countermeasures must be designed to prevent, detect, and respond to FDIAs in real time, ensuring that the grid remains resilient in the face of cyber-attacks [184-186].

1) **Data Validation and Integrity Checks**: One of the primary countermeasures for FDIAs is the use of data validation techniques. By constantly validating data from sensors and control systems, any discrepancies between expected and received data can be quickly flagged as potential FDIAs. Redundant data sources, such as backup sensors or data from neighboring systems, can be used to cross-check the integrity of the data and detect any inconsistencies [187]. Additionally, secure communication protocols, such as encryption and authentication, can prevent attackers from injecting false data into the system in the first place.
2) **Multi-Layered Defense Systems**: Another effective countermeasure is the use of multi-layered defense systems. These systems combine various techniques at different levels of the power grid, including physical security, cybersecurity, and system-level monitoring. For instance, at the cyber level, intrusion detection systems (IDS) can monitor network traffic for signs of abnormal activity, while at the physical level, power flow monitoring and automated control systems can be used to detect and isolate faults caused by false data. By applying defense mechanisms at multiple layers, power CPS can better withstand and respond to FDIAs [188].
3) **Resilience and Recovery**: Countermeasures should also include resilience strategies that allow the system to recover quickly from an attack. This can involve the use of automated recovery protocols that restore grid operations after an FDIA has been detected and mitigated. These protocols can automatically reconfigure the grid, reroute power, and restore normal operations without human intervention, reducing recovery times and minimizing the economic impact of an attack [189].

6.4. Advancements in Real-Time Decision Support Systems

The increasing complexity of Power CPS requires advanced real-time decision support systems (DSS) to help operators make informed decisions quickly [190]. These systems integrate various detection, mitigation, and recovery strategies into a cohesive framework, allowing operators to respond to FDIAs in real-time and minimize their impact on the grid.

1) **Real-Time Monitoring and Control**: Real-time monitoring and control systems are designed to provide continuous, up-to-date information about the grid's state. These systems integrate data from various sensors, control devices, and communication networks, allowing operators to monitor system performance and detect any anomalies that may indicate an FDIA. By providing a comprehensive view of the grid's operations, these systems enable operators to make quicker, more accurate decisions during an attack [191].
2) **Automated Response Systems**: In addition to providing real-time data, **automated decision-making** capabilities are increasingly being integrated into decision support systems. These systems use machine learning algorithms to analyze data and make real-time decisions about how to respond to FDIAs. For example, if an attack is detected, the system can automatically isolate the compromised areas, adjust power flows, and trigger corrective actions without operator intervention, reducing response time and preventing further damage to the grid [192].
3) **Predictive Analytics for Preemptive Action**: Predictive analytics is another key feature of modern decision support systems. By analyzing historical data and learning from past attacks, predictive models can forecast potential threats and recommend preemptive actions to mitigate the risk of FDIAs. For instance, if a particular area of the grid is identified as vulnerable to attacks,

the system can suggest additional security measures or deploy countermeasures to strengthen that area before an attack occurs [193].

7. Integration of Cyber and Physical Security in Power CPS

The integration of cyber and physical security in Power CPS is essential for building a robust defense against emerging threats. As power grids become increasingly automated and interconnected with digital communication networks, the boundaries between cyber and physical components are increasingly blurred. Therefore, ensuring the security of both domains is crucial for maintaining the reliability and resilience of power CPS [194]. This section explores the integration of cyber and physical security, the role of advanced communication protocols and architectures, and the potential of emerging technologies such as AI, blockchain, and IoT in strengthening grid security.

7.1. Unified Defense Mechanisms: Cyber and Physical Security Integration

Historically, cyber and physical security were treated as separate domains within Power CPS, with cybersecurity efforts focused on protecting communication networks and digital infrastructure, and physical security efforts aimed at safeguarding equipment like transformers, power lines, and substations. However, the growing convergence of these two domains in modern smart grids has led to the need for unified defense mechanisms that address both cyber and physical threats simultaneously [195].

1) **Cyber-Physical Security Frameworks**: A unified defense strategy integrates cybersecurity and physical security measures, ensuring that both digital and physical assets are protected in a coordinated manner. This framework takes into account the interactions between cyber systems (such as SCADA systems, communication networks, and data storage) and physical systems (such as sensors, generators, and grid controllers). By employing a holistic approach to security, a unified defense mechanism reduces the risk of attack vectors that can exploit vulnerabilities in both domains [196].

For example, in a cyber-physical attack scenario, an attacker might manipulate the data in the SCADA system (cyber) to mislead operators about the state of a physical component, such as a transformer (physical). A unified defense strategy would enable the simultaneous monitoring of both cyber and physical components, ensuring that an anomaly in one domain is promptly detected and corrected by the other. Such integration can enhance early detection, minimize the impact of attacks, and improve recovery time after an incident.

2) **Collaborative Defense Systems**: Collaborative defense systems are gaining traction as a way to integrate cyber and physical security. These systems involve close collaboration between IT and operational technology (OT) teams to ensure that security measures are synchronized across all levels. By sharing threat intelligence, incident reports, and recovery protocols, these teams can act quickly and efficiently when a threat emerges, preventing it from escalating across the grid. Furthermore, collaboration ensures that cybersecurity protocols do not interfere with the safe and reliable operation of the physical infrastructure, and vice versa [197].

7.2. Role of Communication Protocols and Advanced Architectures

Effective communication is vital for the operation of Power CPS, as data transmission between various components (e.g., sensors, meters, generators, control centers) enables real-time decision-making. As cyber threats to communication networks increase, the role of secure communication protocols and advanced system architectures becomes more critical in safeguarding grid operations [198].

1) **Secure Communication Protocols**: One of the primary methods to protect communication in Power CPS is the adoption of secure communication protocols. These protocols help safeguard

the integrity, confidentiality, and authenticity of data transmitted between grid components, reducing the risk of Man-in-the-Middle (MitM) attacks, data manipulation, and unauthorized access. Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption protocols, as well as Virtual Private Networks (VPNs) and Public Key Infrastructure (PKI), are commonly used to secure data exchanges in power CPS [199].

Moreover, the use of quantum-safe encryption is becoming a key area of research, particularly as quantum computing threatens to break traditional encryption methods. Lattice-based encryption and hash-based cryptography are examples of quantum-resistant algorithms that could be integrated into future power grid systems to ensure secure communications in a post-quantum world [200].

2) **Advanced Architectures for Grid Security**: The architecture of the communication network plays a crucial role in securing power CPS. Traditional centralized architectures, where data is routed through a central control unit, are vulnerable to single points of failure, which can be exploited by attackers. To mitigate this, distributed architectures such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are being explored for power CPS. These technologies allow for more flexible and dynamic management of the communication network, enabling quicker detection of attacks and more resilient data routing [201].

Edge computing is another emerging technology that plays a significant role in improving communication security. By processing data closer to the source (at the edge of the network), edge computing reduces the amount of sensitive information that needs to be transmitted over potentially insecure networks, thus minimizing the exposure to cyber threats. This distributed processing capability also improves the speed of decision-making and response times, essential in real-time grid operations [202].

7.3. Future Trends: Leveraging AI, Blockchain, and IoT for Enhanced Security

As the complexity of Power CPS continues to increase, leveraging emerging technologies such as AI, Blockchain, and IoT offers new opportunities for enhancing grid security.

1) **AI**: Artificial intelligence, and particularly ML and deep learning (DL), can significantly enhance the detection and mitigation of FDIAs by automating the analysis of large volumes of data. Machine learning models can be trained to identify subtle patterns of malicious activity in real-time, allowing for quicker detection and response to attacks. Furthermore, reinforcement learning (RL) and adversarial AI can be used to simulate potential attack scenarios, test defense systems, and continuously improve grid resilience [203].

AI can also help optimize the integration of renewable energy sources into the grid by generating operational scenarios [204] and predicting supply fluctuations and ensuring more efficient power dispatch. In terms of security, AI-driven systems can continuously adapt to new threats, making them an essential tool in the ever-evolving landscape of cyber-attacks.

2) **Blockchain for Secure Data Sharing**: Blockchain technology, known for its decentralized and immutable nature, offers a promising solution for securing data exchanges in Power CPS. By using blockchain to verify the authenticity and integrity of data exchanged between different grid components, attackers would be unable to alter or manipulate the data without detection. Smart contracts, which are self-executing contracts with the terms directly written into code, can also be used to automate decision-making processes in grid operations, ensuring that predefined security protocols are followed in response to detected anomalies or attacks [205].

Moreover, blockchain's decentralized nature removes the reliance on a central authority, reducing the risk of single points of failure in the grid's communication network. This makes blockchain an effective tool for enhancing both the security and resilience of power CPS.

3) **IoT for Enhanced Monitoring and Control**: IoT devices, such as smart meters, PMUs, and smart sensors, are increasingly being integrated into power grids to collect real-time data and improve grid management. While IoT devices offer numerous benefits in terms of data collection and operational efficiency, they also introduce new security risks, as these devices can be vulnerable to cyber-attacks.

To address these vulnerabilities, advanced IoT security frameworks are being developed, leveraging encryption, authentication, and access control protocols to protect the devices and the data they generate. Additionally, IoT systems can be integrated with AI and machine learning algorithms to enhance real-time decision-making and improve threat detection at the device level, providing an additional layer of security to the grid [206].

8. Future Directions in FDIA Research

The increasing sophistication of FDIAs in Power CPS has underscored the need for continued innovation in attack modeling, detection techniques, and defense mechanisms. As cyber threats continue to evolve, research in this field must adapt to new challenges and leverage emerging technologies. This section explores the key areas for future research, including identifying gaps in existing methodologies, exploring federated learning and decentralized approaches, leveraging emerging technologies like quantum computing, and developing effective policy and regulatory frameworks.

8.1. Identifying Research Gaps: Attack Modeling, Enhanced Detection, and Efficient Defenses

While substantial progress has been made in detecting and mitigating FDIAs, several gaps remain in research that require further exploration. The complexity and evolving nature of attacks necessitate advanced modeling techniques, more efficient detection systems, and robust defenses.

1) **Advanced Attack Modeling**: One of the critical gaps in FDIA research is the need for advanced attack models that capture the complexities and dynamics of real-world cyber-attacks. Current models tend to simplify the attack scenarios or focus on a limited number of attack types, often overlooking the multi-stage, adaptive nature of modern FDIAs. Future research should focus on developing dynamic, multi-phase attack models that reflect the interactions between cyber and physical components, as well as the evolving tactics of attackers [207].

For example, attackers may initially infiltrate the system through a low-level attack, such as injecting small errors into state estimation, which gradually escalates to more complex attacks targeting control systems. Understanding the lifecycle of these multi-stage attacks can help develop more effective detection and mitigation strategies.

2) **Enhanced Detection Techniques**: Existing detection systems often struggle to balance accuracy and real-time processing in large-scale power CPS. Research should focus on improving detection accuracy while minimizing the computational cost of detection algorithms. Deep learning and reinforcement learning can play a critical role in this, as these techniques can adapt to new attack patterns and improve detection in real-time environments [208-210]. However, these models also require large amounts of data for training, which can be challenging to obtain in power grids.

Additionally, improving detection methods to handle multi-source data and distributed grids is crucial, as the growing number of distributed energy resources and IoT devices introduces new challenges in data integration and anomaly detection.

3) **Efficient Defense Mechanisms**: While several defense techniques have been proposed, there is a need for more efficient defense mechanisms that can quickly detect and mitigate FDIAs without compromising grid performance. Research into multi-layered defense systems, which integrate

detection, recovery, and preventive measures, will be key to achieving resilience in the face of complex and evolving attacks. Furthermore, developing adaptive defense mechanisms that can dynamically respond to new threats in real time will be essential as the grid continues to evolve [211].

8.2. Federated Learning and Decentralized Approaches

As the scale and complexity of Power CPS increase, decentralized approaches and federated learning are becoming promising solutions for improving FDIA detection and resilience.

1) **Federated Learning**: **Federated learning (FL)** allows multiple devices or systems to collaborate on training a machine learning model without sharing their local data [212]. This decentralized approach can be particularly useful for Power CPS, where data privacy and security are paramount. In federated learning, each device or grid component computes local models based on its data, and only model updates are shared with a central server. This method ensures that sensitive data, such as consumer usage patterns or generation profiles, remains local, reducing the risk of data breaches or privacy violations [213].

FL can also enhance the scalability of detection systems. Instead of relying on centralized data processing, which may suffer from bottlenecks or vulnerabilities, FL allows for distributed learning where detection models are continually improved across a network of grid devices. This can lead to more responsive, real-time detection systems that improve as they learn from diverse grid conditions [214].

2) **Decentralized Approaches**: Decentralization is increasingly seen as a way to improve the resilience and robustness of Power CPS. In a decentralized system, the grid's components can operate autonomously, making local decisions based on localized data, without needing to communicate with a central controller. This reduces the risk of a single point of failure and ensures that localized attacks cannot easily propagate throughout the entire system.

Blockchain technology has been explored as a tool to implement decentralized control and secure communication within Power CPS. By using a decentralized ledger, blockchain can ensure the integrity and transparency of data exchanges between grid components, which is crucial for detecting and preventing FDIAs. Additionally, decentralized approaches can help maintain operational continuity if part of the system is compromised, as the unaffected parts can continue to function autonomously [215].

8.3. Emerging Technologies: Quantum Computing and Beyond

Emerging technologies such as quantum computing, blockchain, and IoT offer significant potential to address the challenges of FDIA detection and mitigation. These technologies can provide innovative solutions to the limitations of current approaches and open new avenues for research.

1) **Quantum Computing**: Quantum computing has the potential to revolutionize FDIA detection and mitigation by providing computational power far beyond that of classical computers. Quantum algorithms, such as Shor's algorithm for factoring and Grover's algorithm for searching, could enable faster and more efficient detection of malicious patterns in large datasets. Additionally, quantum-enhanced cryptographic protocols can provide a higher level of security for communications between grid components, making it harder for attackers to manipulate data or gain unauthorized access [216].

However, the practical application of quantum computing in Power CPS is still in its early stages. More research is needed to develop quantum-resistant cryptographic methods and to integrate quantum computing with existing power grid infrastructure. Once implemented, quantum computing could provide significant advancements in real-time anomaly detection and security by solving complex optimization problems that traditional computing methods struggle with.

2) **Blockchain for Security and Transparency**: Blockchain technology can play a key role in securing communication within Power CPS. By providing an immutable and transparent ledger for data transactions, blockchain can help ensure that data exchanges between components are genuine and unaltered. Smart contracts, which automatically execute predefined actions based on conditions met, can also be used to enforce security policies across the grid. For example, smart contracts could automatically initiate recovery procedures in the event of an FDIA, improving response times and minimizing damage.

Furthermore, blockchain can support decentralized authentication and access control mechanisms, ensuring that only authorized components are allowed to exchange data, thus preventing unauthorized data manipulation.

3) **IoT**: The integration of IoT devices in Power CPS—such as smart meters, sensors, and control devices—has greatly enhanced the ability to monitor and control grid operations in real time. However, IoT also introduces new vulnerabilities, as these devices can be targeted by cyber-attacks to manipulate data or disrupt operations. Research into IoT security frameworks will be essential to protect these devices and ensure that they are secure and resilient to FDIAs.

IoT devices, combined with machine learning algorithms, can also enable real-time anomaly detection by continuously monitoring grid conditions and reporting any deviations from normal behavior. This can help detect FDIAs at their inception and trigger countermeasures before they cause significant harm.

8.4. Policy and Regulatory Frameworks for Securing Power CPS

As the threats to Power CPS evolve, so too must the policies and regulatory frameworks that govern their security. Policymakers and regulators must develop comprehensive and standardized guidelines for securing power grids against cyber-attacks, including FDIAs.

1) **Cybersecurity Standards and Regulations**: National and international regulatory bodies, such as the National Institute of Standards and Technology (NIST) and the International Electrotechnical Commission (IEC), have developed cybersecurity frameworks for critical infrastructure, including power systems. These frameworks outline best practices for protecting systems against cyber threats, including FDIAs. Future regulatory frameworks should evolve to address the growing complexity of modern Power CPS and the integration of new technologies such as IoT and AI [217].
2) **Incentives for Cybersecurity Research**: Governments should encourage research funding and public-private partnerships to drive innovations in cybersecurity for Power CPS. By supporting academic and industry-led research on new detection techniques, defense strategies, and resilience frameworks, policymakers can ensure that the security measures implemented are up-to-date and effective in countering the latest threats [218].
3) **International Collaboration**: Since Power CPS often span multiple regions and countries, international collaboration will be essential in securing global energy grids. Shared standards, threat intelligence exchange, and coordinated incident response efforts can help mitigate the risks posed by FDIAs that target interconnected systems. Establishing global cybersecurity policies for Power CPS will enhance overall resilience and ensure a more secure energy future.

9. Conclusions

This review has provided a comprehensive overview of the challenges posed by FDIAs in power cyber-physical systems. The increasing sophistication of FDIAs demands the development of more advanced detection and mitigation techniques, with a particular emphasis on hybrid approaches combining model-driven and data-driven methods. Despite significant advancements in detection accuracy and real-time monitoring, issues such as adaptability, computational cost, and the stealthy nature of attacks remain significant challenges. Future research must focus on enhancing detection systems with adaptive models, integrating emerging technologies like artificial intelligence and quantum computing, and addressing cross-domain security concerns. The adoption of multi-layered defense strategies, alongside robust regulatory frameworks, will be essential for ensuring the long-term security and resilience of Power CPS. Continued collaboration across academia, industry, and government is crucial to overcoming these challenges and securing the power grid from future cyber threats.

References

1. [1] Li B, Lu R, Xiao G. Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems[M]. Springer, 2020.
2. [2] Seshasai B, Koley E, Jena P K, et al. Design of Real-Time False Data Injection Attack on Electricity Market With Limited Sensor Accessibility[J]. IEEE Systems Journal, 2024.
3. [3] Yang H, Zhang W, Liang Z, et al. Parameter-Free False Data Injection Attack Against AC State Estimation: A Canonical Polyadic Decomposition Based Approach[J]. IEEE Transactions on Power Systems, 2024.
4. [4] Qu Z, Zhao T, Zhang Y, et al. Determination Method of Network Risk Propagation Threshold in Power CPS Based on Percolation Theory[J]. Automation of Electric Power Systems, 2020, 44(4): 16-23.
5. [5] Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal-Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
6. [6] Qin B, Liu D. Research Progress and Prospects on Analysis and Control of Power Grid Cyber-Physical Systems[J]. Proceedings of the CSEE, 2020, 40(18): 5816-5826.
7. [7] Li Y, Han M, Yang Z, et al. Coordinating Flexible Demand Response and Renewable Uncertainties for Scheduling of Community Integrated Energy Systems with an Electric Vehicle Charging Station: A Bi-Level Approach[J]. IEEE Transactions on Sustainable Energy, 2021, 12(4): 2321-2331.
8. [8] Chang Z, Wu J, Liang H, et al. A review of Power System False data attack Detection Technology based on Big data[J]. Information, 2024, 15(8): 439.
9. [9] Shang Y, et al. Explainable spatiotemporal multi-task learning for electric vehicle charging demand prediction[J]. Applied Energy, 2025, 384: 125460.
10. [10] Paul B, Sarker A, Abhi S H, et al. Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies[J]. Heliyon, 2024, 10(19): e37980.
11. [11] Cao J, Wang Q, Qu Z, et al. Method for identifying false data injection attacks in power grid based on improved CNN-LSTM[J]. Electrical Engineering, 2025: 1-26.
12. [12] Li Y, Wang C, Li G, et al. Improving operational flexibility of integrated energy system with uncertain renewable generations considering thermal inertia of buildings[J]. Energy Conversion and Management, 2020, 207: 112526.
13. [13] Pannerselvam K, Rajiakodi S. Towards Smarter, Interconnected Futures: The Crucial Role of Data in Cyber-Physical Systems[M]//Intelligent Cyber-Physical Systems for Healthcare Solutions. Springer, Singapore, 2024: 181-194..
14. [14] Qu Z, Dong Y, Qu N, et al. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation[J]. Mathematical Problems in Engineering, 2019, 2019: 2817586.
15. [15] Li Y, Cao J, Xu Y, et al. Deep learning based on Transformer architecture for power system short-term voltage stability assessment with class imbalance[J]. Renewable and Sustainable Energy Reviews, 2024, 189: 113913.
16. [16] Qu Z, Dong Y, Qu N, et al. Quantitative Assessment of Survivability of Power CPS Considering Load Optimization and Reconfiguration[J]. Automation of Electric Power Systems, 2019, 43(6): 15-24.
17. [17] Bo X, Chen X, Li H, et al. Modeling Method for the Coupling Relations of Microgrid Cyber-Physical Systems Driven by Hybrid Spatiotemporal Events[J]. IEEE Access, 2021, 9: 19619-19631.

18. [18] Das S, Wang Z. Enhancing Microgrid Resilience to False Data Injection[C]//2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2024: 147-152.
19. [19] Wang L, Xu P, Qu Z, et al. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link[J]. Frontiers in Energy Research, 2021, 9: 666130.
20. [20] Li T, Zhang L, Wang W. Enhancing Security in Power CPS: Hybrid Solutions for Attack Detection[J]. Journal of Cyber Physical Systems, 2023, 18(9): 1221-1233.
21. [21] Qu Z, Xie Q, Liu Y, et al. Power Cyber-Physical System Risk Area Prediction Using Dependent Markov Chain and Improved Grey Wolf Optimization[J]. IEEE Access, 2020, 8: 82844-82854.
22. [22] Wang T, Sun C, Gu X, et al. Modeling of Power Communication Coupled Networks and Their Vulnerability Analysis[J]. Proceedings of the CSEE, 2018, 38(12): 3556-3567.
23. [23] Zhao J, An K, Wang X. Research on Fast Early Warning of False Data Injection Attack in CPS of Electric Power Communication Network[J]. Journal of Cyber Security and Mobility, 2024: 1331–1356-1331–1356.
24. [24] Chattopadhyay A, Prakash A, Shafique M. Secure Cyber-Physical Systems: Current trends, tools and open research problems[C]//Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. IEEE, 2017: 1104-1109.
25. [25] Bo X, Qu Z, Liu Y, et al. Review of active defense methods against power cps false data injection attacks from the multiple spatiotemporal perspective[J]. Energy Reports, 2022, 8: 11235-11248.
26. [26] Jiang Q, Li B, Liu T, et al. Study of cyber attack's impact on LCC-HVDC system with false data injection[J]. IEEE Transactions on Smart Grid, 2023, 14(4): 3220-3231.
27. [27] Liu Y, Wen M, Wen H, et al. False Data Injection Attacks in Power Distribution Systems Considering the Characteristics of Distributed Photovoltaic[J]. IEEE Transactions on Industrial Informatics, 2024.
28. [28] Guo Q, Xin S, Wang J, et al. Comprehensive Security Assessment of Information-Energy Systems from the Ukraine Blackout Incident[J]. Automation of Electric Power Systems, 2016, 40(5): 145-147.
29. [29] Parizad A, Hatziadoniu C. False data detection in power system under state variables' cyber attacks using information theory[C]//2021 IEEE Power and Energy Conference at Illinois (PECI). IEEE, 2021: 1-8.
30. [30] Kumar R, et al. Schemes and Security Attacks on the Integrity of Cyber-Physical Systems in Energy Systems[J]. Cyber Physical Energy Systems, 2024: 415-444.
31. [31] Hua D, Huang H, Yan P, et al. A Multi-Stage NSGA-III Optimization Model for False Data Injection Attacks in Integrated Power-Hydrogen Cyber-Physical Systems[J]. IET Renewable Power Generation, 2025, 19(1): e70022.
32. [32] Liu Y, Ning P, Reiter M. False Data Injection Attacks against State Estimation in Electric Power Grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 1-16.
33. [33] Qu Z, Zhang Y, Qu N, et al. Method for Quantitative Estimation of the Risk Propagation Threshold in Electric Power CPS Based on Seepage Probability[J]. IEEE Access, 2018, 6: 68813-68823.
34. [34] Jafari M, Rahman M A, Paudyal S. Optimal false data injection attack against load-frequency control in power systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5200-5212.
35. [35] Padhan S, Turuk A K. Design of false data injection attacks and their detection and mitigation in cyber-physical systems[C]//27th International Conference on Advanced Computing and Communications (ADCOM 2022). IET, 2023, 2023: 41-45.
36. [36] Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
37. [37] Zhou T, Xiahou K, Zhang L L, et al. Real-time detection of cyber-physical false data injection attacks on power systems[J]. IEEE Transactions on Industrial Informatics, 2020, 17(10): 6810-6819.
38. [38] Li Y, Zhang S, Li Y. AI-enhanced resilience in power systems: Adversarial deep learning for robust short-term voltage stability assessment under cyber-attacks[J]. Chaos, Solitons & Fractals, 2025, 196: 116406.
39. [39] Wu Z, Zhang W. Microgrid Attack Detection Based on ARO-MKELM[J]. Journal of Metrology, 2024, 45(10): 1444-1452.
40. [40] Weng P, Chen B, Yu L. Fusion Estimation of False Data Injection Attack Signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.

41. [41] Zhang S, et al. A critical review of data-driven transient stability assessment of power systems: principles, prospects and challenges[J]. Energies, 2021, 14(21): 7238.
42. [42] Krawczyk B, Bellinger C, Corizzo B, et al. Undersampling with Support Vectors for Multi-Class Imbalanced Data Classification[C]// 2021 International Joint Conference on Neural Networks (IJCNN), 18-22 July 2021, Shenzhen, China: 1-7.
43. [43] Feng Y, Jia W. Research Status and Prospect of Smart Microgrids Under Network Attack Models[J]. Smart Grid, 2022, 12: 119-125.
44. [44] Li Y, Li Z, Chen L, et al. A false data injection attack method for generator dynamic state estimation[J]. Transactions of China Electrotechnical Society, 2019, 34: 3651-3660.
45. [45] Luo X, He J, Wang X, et al. Topology Optimization for Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
46. [46] Dong Y, et al. Identification of False Data Injection Attacks in Power Grid Based on Oversampling and Cascade Machine Learning[J]. Power System Automation, 2023, 47(8): 179-188.
47. [47] Zeng R, Li Y, Cao Y, et al. Network Attack Detection and Protection Control Technology for Smart Distribution and Consumption Systems: Development and Challenges[J]. Journal of Electrical Engineering, 2023, 18(2): 125-141.
48. [48] Kurt M, Yılmaz Y, Wang X, et al. Distributed Quickest Detection of Cyber-Attacks in Smart Grid[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2015-2030.
49. [49] Zhu J, Huang L, Chen Y. Post-Attack Security Control Strategy for Power Systems Based on Agent Gradient Deep Reinforcement Learning[J]. Power Grid Technology, 2024, 48(10): 4041-4049.
50. [50] Li Y, Li J, Chen L. Dynamic state estimation of synchronous machines based on robust cubature Kalman filter under complex measurement noise conditions[J]. Transactions of china electrotechnical society, 2019, 34(17): 3651-60.
51. [51] Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Power System Automation, 2024, 48(12): 177-191.
52. [52] Fan Q, Liu D, Wang Y, et al. Key Technologies and Progress in the Morphological Evolution of Power Cyber-Physical Systems[J]. Proceedings of the CSEE, 2023, 44(21): 8341-8352.
53. [53] Gong L, Wang X, Tian M, et al. Concept and Advancement of Resilience in Power Cyber-Physical Systems[J]. Power System Protection and Control, 2023, 51(14): 169-187.
54. [54] Liu K, Ma S, Ma O, et al. Security Control of Cyber-Physical Systems Based on Machine Learning[J]. Acta Automatica Sinica, 2021, 47(6): 1273-1283.
55. [55] Xia Y, Wang Y, Zhou L, et al. Detection Method for False Data Injection Attacks Based on Improved Generative Adversarial Networks[J]. Electric Power Construction, 2022, 43(3): 58-65.
56. [56] Wang J, Li Y, Xu T. Modeling of False Data Injection Attacks and Rapid Screening of Vulnerable Lines under Attacks[J]. Electric Power Construction, 2022, 43(1): 104-112.
57. [57] Li Y, Zhang S, et al. PMU measurements-based short-term voltage stability assessment of power systems via deep transfer learning[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 1-11.
58. [58] Shu H, Yang Y, Zhao H, et al. Detection of False Data Injection Attacks in Power Grids Based on Adaptive Weighted Hybrid Prediction[J]. Power Grid Technology, 2024, 49(3): 1246-1256.
59. [59] Yu P, Yang D, Alattas K A, et al. An Observer-based Event Triggered Mechanism for the Detection and Mitigation of FDI Attacks in Deep Brain Stimulation Systems[J]. IEEE Access, 2025.
60. [60] Wang S, Zhao Y, You D, et al. A Survey on Cyber-Physical Systems Attacks in the Framework of Discrete Event Systems[J]. Control and Decision, 2022, 37(8): 1934-1944.
61. [61] Yin H, Liu D, Chen G, et al. Collaborative Network Attack Model and Cross-Space Fault Propagation Mechanism for Virtual Power Plants[J]. Power System Automation, 2023, 47(8): 34-43.
62. [62] Luo X, Pan X, Wang X, et al. False Data Injection Attack Detection in Smart Grids Based on Adaptive Kalman Filtering[J]. Acta Automatica Sinica, 2022, 48(12): 2960-2971.
63. [63] Zhang Y, Cai Z, Li X, et al. Analytical Modeling of traffic Flow in the Substation Communication Network[J]. IEEE Transactions on Power Delivery, 2015, 30(5): 2119-2127.

64. [64] Li Y, Li J, Qi J, et al. Robust Cubature Kalman Filter for Dynamic State Estimation of Synchronous Machines Under Unknown Measurement Noise Statistics[J]. IEEE Access, 2019, 7: 29139-29148.
65. [65] Zhang L, Xu Y, Wu X, et al. Distributed Resilient Control for AC Microgrids to Defend Against False Data Injection Attacks[J]. Power System Automation, 2023, 47(8): 44-52.
66. [66] Wang W, Ren Z, Sun Y, et al. Transmission Grid False Data Detection Method Based on Wavelet-Sparse Autoencoders[J]. Electric Power New Technologies, 2022, 41(1): 51-59.
67. [67] Qu Z, Bo X, Yu T, et al. Active and Passive Hybrid Detection Method for Power CPS False Data Injection Attacks with Improved AKF and GRU-CNN[J]. IET Renewable Power Generation, 2022, 16: 1490-1508. DOI: 10.1049/rpg2.12432.
68. [68] Pang Q, Han S, Zhou T, et al. FDIA Detection in Power Cyber-Physical Systems Based on ASRUKF and IMC Algorithms[J]. Smart Power, 2024, 52(7): 111-118.
69. [69] Shu H, Yang Y, Zhao H, et al. Detection of False Data Injection Attacks in Power Grids Based on Adaptive Weighted Hybrid Prediction[J]. Power Grid Technology, 2024, 49(3): 1246-1256.
70. [70] Yin H, Liu D, Chen G, et al. Collaborative Network Attack Model and Cross-Space Fault Propagation Mechanism for Virtual Power Plants[J]. Power System Automation, 2023, 47(8): 34-43.
71. [71] Luo X, Pan X, Wang X, et al. False Data Injection Attack Detection in Smart Grids Based on Adaptive Kalman Filtering[J]. Acta Automatica Sinica, 2022, 48(12): 2960-2971.
72. [72] Li Y, Zhang S, Li Y, et al. PMU Measurements Based Short-Term Voltage Stability Assessment of Power Systems via Deep Transfer Learning[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 2526111.
73. [73] Zhang L, Xu Y, Wu X, et al. Distributed Resilient Control for AC Microgrids to Defend Against False Data Injection Attacks[J]. Power System Automation, 2023, 47(8): 44-52.
74. [74] Sridhar S, Hahn A, Govindarasu M. Cyber-Physical System Security for the Electric Power Grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.
75. [75] Wang W, Ren Z, Sun Y, et al. Transmission Grid False Data Detection Method Based on Wavelet-Sparse Autoencoders[J]. Electric Power New Technologies, 2022, 41(1): 51-59.
76. [76] Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM-GAB algorithm[J]. Energy Reports, 2022, 8(5): 1156-1164.
77. [77] Yang F, Wang J, Pan Q, et al. Resilient Event-Triggered Control for Cyber-Physical Integrated Power Systems Under Network Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.
78. [78] Chen L, Liu D. Detection Methods for False Data Injection Attacks in Interactive Demand Response[J]. Power System Automation, 2021, 45(3): 15-23.
79. [79] Kou L, Wu J, Zhang F, et al. Image encryption for Offshore wind power based on 2D-LCLM and Zhou Yi Eight Trigrams[J]. International Journal of Bio-Inspired Computation, 2023, 22(1): 53-64.
80. [80] Peng S, Sun M, Zhang Z, et al. Applications of Machine Learning in Cybersecurity for Power Cyber-Physical Systems[J]. Power System Automation, 2022, 46(9): 200-215.
81. [81] Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attacks for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
82. [82] Xia Y, Wang Y, Zhou L, et al. Detection Method for False Data Injection Attacks Based on Improved Generative Adversarial Networks[J]. Electric Power Construction, 2022, 43(3): 58-65.
83. [83] Gallardo C, Burgos-Mellado C, Muñoz-Carpintero D, et al. Reinforcement learning-based false data injection attacks detector for modular multilevel converters[J]. IEEE Transactions on Industrial Electronics, 2023, 71(7): 7927-7937.
84. [84] Yang F, Wang J, Pan Q, et al. Resilient Event-Triggered Control for Cyber-Physical Integrated Power Systems Under Network Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.
85. [85] Chen L, Li Y, Huang M, et al. Robust Dynamic State Estimator of Integrated Energy Systems Based on Natural Gas Partial Differential Equations[J]. IEEE Transactions on Industry Applications, 2022, 58(3): 3303-3312.
86. [86] Wang D, Huang L, Liu J, et al. Defense Strategy for Power Cyber-Physical Systems Against Load False Data Injection Attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.

87. [87] Lu J, Yang C, Du R, et al. False Data Injection Attacks in Power CPS[J]. Intelligent Computer and Applications, 2022, 12(6): 121-126.
88. [88] Yang Y, Guo L, Wang H, et al. Fast Defense Strategy Against False Data Injection Attacks in DC Microgrids Based on Data-Driven Approaches[J]. Electric Power Automation Equipment, 2021, 41(5): 102-110.
89. [89] Guo F, Zheng X, Deng C, et al. Detection and System Recovery Methods for Unbounded False Data Injection Network Attacks in DC Microgrids[J]. Power System Automation, 2023, 47(2): 146-153.
90. [90] Yi N, Xu J, Chen Y, et al. Multi-Stage Low-Cost False Data Injection Attack Methods for Power CPS[J]. Zhejiang Electric Power, 2023, 42(11): 10-21.
91. [91] Yang R, et al. Resilience assessment and improvement for electric power transmission systems against typhoon disasters: a data-model hybrid driven approach[J]. Energy Reports, 2022, 8: 10923-10936.
92. [92] Xia Y, Wang Y, Zhou L, et al. Detection Method for False Data Injection Attacks Based on Improved Generative Adversarial Networks[J]. Electric Power Construction, 2022, 43(3): 58-65.
93. [93] Chen L, Li Y, Cai J, et al. SCKF-LSTM-Based Trajectory Tracking for Electricity–Gas Integrated Energy System[J]. IEEE Transactions on Industrial Informatics, 2025. DOI: 10.1109/TII.2024.3523544
94. [94] Li Y, Wang R, Li Y, et al. Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach[J]. Applied Energy, 2023, 329: 120291.
95. [95] Cui Y, Xu Y, et al. Deep reinforcement learning based optimal energy management of multi-energy microgrids with uncertainties[J]. CSEE Journal of Power and Energy Systems, 2024.
96. [96] Chen F, Shi J, Liu H, et al. Reliability Assessment of Generation-Transmission Systems Considering Load Redistribution Attacks and Vulnerable Line Defenses[J]. Power System Automation, 2022, 46(2): 65-72.
97. [97] Liang G, Weller S, Zhao J, et al. A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 1704-1712.
98. [98] Luo X, He J, Wang X, et al. Topology Optimization for Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
99. [99] Yang Q, Yang J, Ma X. Research on False Data Injection Attacks in Power Systems[J]. Microelectronics & Computer, 2011, 28(12): 175-179.
100. [100] Wei L, Zhang Q. False Data Injection Attack Detection in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
101. [101] Li Y, Yang Z. Application of EOS-ELM with Binary Jaya-Based Feature Selection to Real-Time Transient Stability Assessment Using PMU Data[J]. IEEE Access, 2017, 5: 23092-23101.
102. [102] Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Power System Automation, 2024, 48(12): 177-191.
103. [103] Huang D, Wang Y, Hu A, et al. False Data Injection Attack Detection Combining Unsupervised and Supervised Learning[J]. Electric Power Engineering Technology, 2024, 43(2): 134-141.
104. [104] Zhang Y, Li S, Gu X, et al. Resilience Assessment Method for Backbone Network Considering Malicious Physical Attacks and Secondary Faults[J]. Electric Power Construction, 2023, 44(12): 95-105.
105. [105] Chen J, Rao J, Li W, et al. Detection Method of False Data Injection Attacks on Power Grids Based on Vector Auto-Regression Model[J]. Journal of Electric Power Science and Technology, 2024, 39(3): 1-9.
106. [106] Chen L, Hui X, et al. Dynamic state estimation for integrated natural gas and electric power systems[C]//2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). IEEE, 2021: 397-402.
107. [107] Wang D, Huang L, Liu J, et al. Defense Strategy for Power Cyber-Physical Systems Against Load False Data Injection Attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.
108. [108] Shi Z, et al. Short-term load forecasting based on LS-SVM optimized by bacterial colony chemotaxis algorithm[C]//2009 international conference on information and multimedia technology. IEEE, 2009: 306-309.
109. [109] Fan Q, Liu D, Wang Y, et al. Key Technologies and Progress in the Morphological Evolution of Power Cyber-Physical Systems[J]. Proceedings of the CSEE, 2023, 44(21): 8341-8352.

110. [110] Sun K, Qiu W, Li K, et al. Network Attack Defense Control Strategy for Fast Frequency Response Systems[J]. Chinese Journal of Electrical Engineering, 2021, 41(16): 5476-5485.
111. [111] Chen X, Zhang T, Liu X. False Data Injection Attack Detection and Resilience in Power Grids Using Deep Reinforcement Learning[J]. Energy Reports, 2024, 9: 11260-11274.
112. [112] Syrmakesis A D, Alhelou H H, Hatziargyriou N D. A novel cyberattack-resilient frequency control method for interconnected power systems using SMO-based attack estimation[J]. IEEE Transactions on Power Systems, 2023, 39(4): 5672-5686.
113. [113] Zhang M, Li J, Li Y, et al. Deep learning for short-term voltage stability assessment of power systems[J]. IEEE Access, 2021, 9: 29711-29718.
114. [114] Qu Z, Qu N, Zhou Y, et al. Extraction of Typical Operating Scenarios of New Power System Based on Deep Time Series Aggregation[J]. CAAI Transactions on Intelligence Technology, 2024, 1-17. DOI: 10.1049/cit2.12369.
115. [115] Chen L, Gu S, Wang Y, et al. Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid[J]. Mathematical Problems in Engineering, 2021, 2021(1): 2014345.
116. [116] Zang T, Tong X, Li C, et al. Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks[J]. Energies, 2025, 18(6): 1479.
117. [117] Li Y, Li G, Gu X, et al. Transient stability assessment of power systems based on ensemble OS-ELM[J]. Transactions of China Electrotechnical Society, 2015, 30(14): 412-418.
118. [118] Dehbozorgi, Mohammad Reza, Mohammad Rastegar, and Mohammadreza FM Arani. "False Data Injection Attack Detection and Localization Framework in Power Distribution Systems Using a Novel Ensemble of CNNs and Explainable Artificial Intelligence." IEEE Transactions on Industry Applications (2025). DOI: 10.1109/TIA.2025.3532917
119. [119] 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.
120. [120] Zhang P, Xiong Y, Jian J. Research on False Data Injection Attacks in Smart Grids Based on Multi-Objective Bi-Level Programming[J]. Operations Research and Management, 2023, 32(1): 22.
121. [121] Yuan K, Luo P, Wang G, et al. New Detection Method for Covert Data Attacks in Power Systems Based on Grey Relational Analysis[J]. New Electrical Technology, 2019, 38(1): 17-23.
122. [122] Yang S, Tan B, Guo J. False Data Injection Attack Detection for New Energy Internet Based on Double Markov Chains[J]. Electric Power Automation Equipment, 2021, 41(2): 212-220.
123. [123] Dongmei H, Zhonghui D, Anduo H, et al. Low-Cost Adversarial Stealthy False Data Injection Attack and Detection Method[J]. Power System Technology, 2023, 47(4): 1531-1539.
124. [124] Wu Y, Ru Y, Liu J, et al. Detection of False Data Injection Attacks in Automatic Generation Control Systems Based on Set Member Filtering[J]. Power System Automation, 2022, 46(1): 33-41.
125. [125] Li P, Liu Y, Xin H, et al. Vulnerability Assessment of Distribution Network Cyber-Physical Systems Under Distributed Collaborative Control Mode[J]. Automation of Electric Power Systems, 2018, 42(10): 22-29+59.
126. [126] Li R, Liu S, Yan L. CPS Network Attack Detection Method for New Energy Distribution Networks Based on FP-Growth Algorithm[J]. Telecommunications Science, 2024, 40(11): 103-113.
127. [127] Zhao Z, Shang Y, Qi B, et al. Research on defense strategies for power system frequency stability under false data injection attacks[J]. Applied Energy, 2024, 371: 123711.
128. [128] Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM–GAB algorithm[J]. Energy Reports, 2022, 8: 1156-1164.
129. [129] Zhu H, Xu L, Bao Z, et al. Secure control against multiplicative and additive false data injection attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 92-100.
130. [130] Xie Y, Yan X, Yan Z, et al. Optimization of False Data Injection Attack Strategy for AC-DC Hybrid Power Grids[J]. Electric Power Engineering Technology, 2023, 42(4): 15-24.
131. [131] Li Y, Zhang M, Chen C. A deep-learning intelligent system incorporating data augmentation for short-term voltage stability assessment of power systems[J]. Applied Energy, 2022, 308: 118347.

132. [132] Feng C, Li Y, Xu T. Security Evaluation Method for Distribution Network Cyber-Physical Systems Considering Risk Propagation and Expected Failure Analysis[J]. Science & Technology and Engineering, 2022, 22(23): 10116-10122.
133. [133] Arafah M, Phillips I, Adnane A, et al. Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks[J]. Applied Soft Computing, 2025, 168: 112455.
134. [134] Khalid H, Peng J. Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 697-707.
135. [135] Liu X, Chang P, Sun Q. Detection of False Data Injection Attacks in Power Grids Based on XGBoost and Unscented Kalman Filter Adaptive Hybrid Prediction[J]. Proceedings of the CSEE, 2021, 41(16): 5462-5476.
136. [136] Suan K. Research on False Data Injection Attack Problem in Power CPS State Estimation[D]. Zhejiang University, 2018.
137. [137] Wang T, Sun C, Gu X, et al. Modeling of Power Communication Coupled Networks and Their Vulnerability Analysis[J]. Proceedings of the CSEE, 2018, 38(12): 3556-3567.
138. [138] Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Automation of Electric Power Systems, 2024, 48(12): 177-191.
139. [139] Zhao J, An K, Wang X. Research on Fast Early Warning of False Data Injection Attack in CPS of Electric Power Communication Network[J]. Journal of Cyber Security and Mobility, 2024, 1331-1356.
140. [140] Chattopadhyay A, Prakash A, Shafique M. Secure Cyber-Physical Systems: Current Trends, Tools and Open Research Problems[C]//Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. IEEE, 2017: 1104-1109.
141. [141] Yang Q, Yang J, Ma X. Research on False Data Injection Attacks in Power Systems[J]. Microelectronics & Computer, 2011, 28(12): 175-179.
142. [142] Wang S, Zhao Y, You D, et al. A Survey on Cyber-Physical Systems Attacks in the Framework of Discrete Event Systems[J]. Control and Decision, 2022, 37(8): 1934-1944.
143. [143] Yang S, Sun F, Ren S, et al. Secure Dispatch Strategy for Cyber-Physical Energy Systems under False Data and DoS Attacks[C]//2024 36th Chinese Control and Decision Conference (CCDC). IEEE, 2024: 5056-5060.
144. [144] Cai X, Wang Q, Tai W, et al. Defense Method for False Data Injection Attacks in Power CPS Based on Multi-Stage Game[J]. Electric Power Construction, 2019, (5): 48-54.
145. [145] Zhang Y, Li S, Gu X, et al. Resilience Assessment Method for Backbone Network Considering Malicious Physical Attacks and Secondary Faults[J]. Electric Power Construction, 2023, 44(12): 95-105.
146. [146] Chen J, Rao J, Li W, et al. Detection Method of False Data Injection Attacks on Power Grids Based on Vector Auto-Regression Model[J]. Journal of Electric Power Science and Technology, 2024, 39(3): 1-9.
147. [147] Wang D, Huang L, Liu J, et al. Defense Strategy for Power Cyber-Physical Systems Against Load False Data Injection Attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.
148. [148] Sun K, Qiu W, Li K, et al. Network Attack Defense Control Strategy for Fast Frequency Response Systems[J]. Chinese Journal of Electrical Engineering, 2021, 41(16): 5476-5485.
149. [149] Chen B, Li M. Research on a Data-Driven Framework for Defending Against False Data Injection Attacks in Power Systems[J]. Electric Measurement & Instrumentation, 2024, 61(12): 10-16.
150. [150] 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[J]. Applied Energy, 2023, 333: 120540.
151. [151] Zhang Z, Chen H, Liu B, et al. An effective updating scheme based DETM robust LFC under non-ideal communication network[J]. Automatica, 2024, 167: 111786.
152. [152] Liu Y, Lu Y. Event-Triggered Sliding Mode Control of Direct-Current Microgrid System Under Network Attack[J]. Journal of Electric Power Science and Technology, 2025, 39(6): 212-221.
153. [153] Zheng Y, Mudhangulla S B, Anubi O M. Moving-horizon false data injection attack design against cyber–physical systems[J]. Control Engineering Practice, 2023, 136: 105552.
154. [154] Wu Z, Xu D, Xu J, et al. Key Technologies of Distribution Network State Estimation Under Multiple Cyber-Physical Attacks[J]. Power System Automation, 2024, 48(6): 127-138.

155. [155] Cao K, Li R, Zhang X, et al. Research on Uncertainty for Complex Event Streams in Cyber-Physical Systems[J]. Computer Engineering and Science, 2015, 37(3): 415-421.
156. [156] Feng Y, Jia W. Research Status and Prospect of Smart Microgrids Under Network Attack Models[J]. Smart Grid, 2022, 12: 119-125.
157. [157] Zhang P, Xiong Y, Jian J. Research on False Data Injection Attacks in Smart Grids Based on Multi-Objective Bi-Level Programming[J]. Operations Research and Management, 2023, 32(1): 22.
158. [158] Yuan K, Luo P, Wang G, et al. New Detection Method for Covert Data Attacks in Power Systems Based on Grey Relational Analysis[J]. New Electrical Technology, 2019, 38(1): 17-23.
159. [159] Yang S, Tan B, Guo J. False Data Injection Attack Detection for New Energy Internet Based on Double Markov Chains[J]. Electric Power Automation Equipment, 2021, 41(2): 212-220.
160. [160] Dongmei H, Zhonghui D, Anduo H, et al. Low-Cost Adversarial Stealthy False Data Injection Attack and Detection Method[J]. Power System Technology, 2023, 47(4): 1531-1539.
161. [161] Bo X, Qu Z, Wang L, et al. Active defense research against false data injection attacks of power CPS based on data-driven algorithms[J]. Energies, 2022, 15(19): 7432.
162. [162] Wu Y, Ru Y, Liu J, et al. Detection of False Data Injection Attacks in Automatic Generation Control Systems Based on Set Member Filtering[J]. Power System Automation, 2022, 46(1): 33-41.
163. [163] Li Y, Li Y, Sun Y. Online Static Security Assessment Of Power Systems Based On Lasso Algorithm[J]. Applied Sciences, 2018, 8(9): 1442.
164. [164] Xie Y, Yan X, Yan Z, et al. Optimization of False Data Injection Attack Strategy for AC-DC Hybrid Power Grids[J]. Electric Power Engineering Technology, 2023, 42(4): 15-24.
165. [165] Feng C, Li Y, Xu T. Security Evaluation Method for Distribution Network Cyber-Physical Systems Considering Risk Propagation and Expected Failure Analysis[J]. Science & Technology and Engineering, 2022, 22(23): 10116-10122.
166. [166] Pruengkarn R. Enhancing classification performance by handling noise and imbalanced data with fuzzy classification techniques[D]. Perth, Australia: Murdoch University, 2018.
167. [167] Zhou H, Xu F, Liu X, et al. A Machine Learning Approach for False Data Injection Attack Detection in Power Systems[J]. Journal of Power Systems, 2024, 45(7): 1254-1264.
168. [168] Bai X, Ma Q, Tang Z, et al. A Real-Time False Data Injection Attack Detection Method Using Ensemble Learning[J]. International Journal of Electrical Power & Energy Systems, 2023, 118: 105920.
169. [169] Yang X, et al. Gaussian Mixture Model Uncertainty Modeling for Power Systems Considering Mutual Assistance of Latent Variables[J]. IEEE Transactions on Sustainable Energy, 2024, 1-4. DOI: 10.1109/TSTE.2024.3356259.
170. [170] Li Y, Wei X, Li Y, et al. Detection of false data injection attacks in smart grid: A secure federated deep learning approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862-4872.
171. [171] Shukla S, Thakur S, Hussain S, et al. Identification of false stealthy data injection attacks in smart meters using machine learning and blockchain[C]//International Congress on Blockchain and Applications. Cham: Springer International Publishing, 2022: 398-409.
172. [172] Li X, Wang X, Liu G, et al. Comprehensive Evaluation of False Data Injection Attacks in Power Systems Using a Data-Driven Approach[J]. IEEE Transactions on Industrial Informatics, 2023, 19(4): 2345-2353.
173. [173] Zhang F, Huang Z, Kou L, et al. Data Encryption Based on a 9D Complex Chaotic System with Quaternion for Smart Grid[J]. Chinese Physics B, 2023, 32(1): 010502.
174. [174] Qu Z, Dong Y, Mugemanyi S, et al. Dynamic Exploitation Gaussian Bare-Bones Bat Algorithm for Optimal Reactive Power Dispatch to Improve the Safety and Stability of Power System[J]. IET Renewable Power Generation, 2022, 16: 1401-1424.
175. [175] Fang Z, Zhao D, Chen C, et al. Nonintrusive Appliance Identification with Appliance-Specific Networks[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 3443-3452.
176. [176] Liu Y, Jiang X, Zhang S, et al. Data Integrity Protection in Power CPS: Approaches and Challenges[J]. Journal of Electric Power Engineering, 2022, 50(2): 143-155.
177. [177] Sheng Z, Yao J, Guo L. A Hybrid Detection Framework for Cyber-Attacks in Power Systems[J]. Journal of Electrical Engineering & Technology, 2024, 19(2): 541-550.

178. [178] Qu Z, Dong Y, Li Y, et al. Localization of Dummy Data Injection Attacks in Power Systems Considering Incomplete Topological Information: A Spatio-Temporal Graph Wavelet Convolutional Neural Network Approach[J]. Applied Energy, 2024, 360: 122736.
179. [179] Zhang W, Liang J, Wu T. Survey of Attack Detection and Defense Methods for Smart Grids[J]. Journal of Control and Decision, 2023, 38(10): 2567-2575.
180. [180] Mhapsekar R U, Umrani M I, Faizan M, et al. Building trust in AI-driven decision making for cyber-physical Systems (CPS): A comprehensive review[C]//2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2024: 1-8.
181. [181] Lin W T, Chen G, Zhou X. Privacy-preserving federated learning for detecting false data injection attacks on power system[J]. Electric Power Systems Research, 2024, 229: 110150.
182. [182] Xu S, Lu Y, Wu F. Cyber-Attack Detection and Resilience Strategy in Smart Grids Based on Big Data Analytics[J]. Power System Automation, 2023, 47(12): 1859-1871.
183. [183] Fang Y, Liu Z, Chen D. Hybrid Machine Learning Methods for Cyber-Attack Detection in Power Systems[J]. Journal of Energy Engineering, 2024, 10(2): 134-145.
184. [184] Liu X, Bao Z, Lu D, et al. Modeling of Local False Data Injection Attacks With Reduced Network Information[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686-1696.
185. [185] Xu K, Niu Y. Decentralized attack detection for multi-area power systems via interconnection-decoupled sliding mode observer[J]. International Journal of Robust and Nonlinear Control, 2023, 33(12): 6697-6714.
186. [186] Preeti G, Sanjeev Kumar P. A Blockchain Based Decentralized Application System for Vanet FDIA Detection[C]//International Conference on Computing and Communication Networks. Singapore: Springer Nature Singapore, 2023: 95-119.
187. [187] Tirulo A, Chauhan S. Deep learning for active detection of FDIAs to defend distributed demand response in smart grid[J]. International Journal of Grid and Utility Computing, 2024, 15(6): 572-587.
188. [188] Bai Z, Chen Y, Wei L, et al. Application of AI and ML Techniques in Cybersecurity of Power CPS[J]. Power and Energy Systems, 2024, 46(5): 2267-2278.
189. [189] Li Y, Ma W, Li Y, et al. Enhancing Cyber-Resilience in Integrated Energy System Scheduling with Demand Response Using Deep Reinforcement Learning[J]. Applied Energy, 2025, 379:124831.
190. [190] Syrmakesis A D, Hatziargyriou N D. Cyber resilience methods for smart grids against false data injection attacks: categorization, review and future directions[J]. Frontiers in Smart Grids, 2024, 3: 1397380.
191. [191] Gao S, Zhang H, Wang Z, et al. Data-driven injection attack strategy for linear cyber-physical systems: An input-output data-based approach[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 4082-4095.
192. [192] Wang G, Sun Q, et al. Detection and Mitigation of Coordinated False Data Injection Attacks in Power Grids[J]. Journal of Control Engineering Practice, 2024, 25(7): 347-359.
193. [193] Hu P, Li L. A Review of Cyber-Physical Security in Smart Grids[J]. Information Security Research, 2019, 5(12): 1068.
194. [194] Pei C, Xiao Y, Liang W, et al. Canonical Variate Analysis for Detecting False Data Injection Attacks in Alternating Current State Estimation[J]. IEEE Transactions on Network Science and Engineering, 2024.
195. [195] Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
196. [196] Kausar F, Deo S, Hussain S, et al. Federated Deep Learning Model for False Data Injection Attack Detection in Cyber Physical Power Systems[J]. Energies, 2024, 17(21): 5337
197. [197] Esmalifalak M, Nguyen H, Zheng R, et al. A Stealthy Attack Against Electricity Market Using Independent Component Analysis[J]. IEEE Systems Journal, 2018, 12(1): 297-307.
198. [198] Li W, Fu H, Wu S, et al. RETRACTED: A Kalman Filter-Based Distributed Cyber-Attack Mitigation Strategy for Distributed Generator Units in Meshed DC Microgrids[J]. Energies, 2023, 16(24): 7959
199. [199] Li R, Liu S, Yan L. CPS Network Attack Detection Method for New Energy Distribution Networks Based on FP-Growth Algorithm[J]. Telecommunications Science, 2024, 40(11): 103-113.
200. [200] Bou-Harb E, Ghani N, Erradi A, et al. Passive inference of attacks on CPS communication protocols[J]. Journal of information security and applications, 2018, 43: 110-122.

201. [201] Ezechi C, Akinsolu M O, Sangodoyin A O, et al. Software-defined networking in cyber-physical systems[J]. Cyber Physical System 2.0: Communication and Computational Technologies, 2024: 44.
202. [202] Capogrosso L, Xu S, Fraccaroli E, et al. Learning-Enabled CPS for Edge-Cloud Computing[C]//2024 IEEE 14th International Symposium on Industrial Embedded Systems (SIES). IEEE, 2024: 132-139.
203. [203] Du Y, Chatterjee S, Bhattacharya A, et al. Role of reinforcement learning for risk-based robust control of cyber-physical energy systems[J]. Risk Analysis, 2023, 43(11): 2280-2297.
204. [204] Li Y, Li J, Wang Y. Privacy-preserving spatiotemporal scenario generation of renewable energies: A federated deep generative learning approach[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2310-2320.
205. [205] Ansar S A, Singh A, Aggrawal S, et al. Modernizing CPS with blockchain: Applications, challenges & future directions[C]//2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS). IEEE, 2022: 124-129.
206. [206] Selvi K, Dilip G. Enhancing Cyber-Physical Systems Security: A Review of Deep Learning and Blockchain Integration[C]//2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN). IEEE, 2024: 725-734.
207. [207] Kim K, Youn J, Kim H, et al. State-of-the-Art in Cyber Situational Awareness: A Comprehensive Review and Analysis[J]. KSII Transactions on Internet and Information Systems (TIIS), 2024, 18(5): 1273-1300.
208. [208] Wang Y, et al. Collaborative optimization of multi-microgrids system with shared energy storage based on multi-agent stochastic game and reinforcement learning[J]. Energy, 2023, 280: 128182
209. [209] Liu F, Li Y, Li B, et al. Bitcoin transaction strategy construction based on deep reinforcement learning[J]. Applied Soft Computing, 2021, 113: 107952.
210. [210] Jamshidi S, Amirnia A, Nikanjam A, et al. Enhancing security and energy efficiency of cyber-physical systems using deep reinforcement learning[J]. Procedia Computer Science, 2024, 238: 1074-1079.
211. [211] Li Q, Yang X, Xie X, et al. The data recovery strategy on machine learning against false data injection attacks in power cyber physical systems[J]. Measurement and Control, 2024: 00202940241268444.
212. [212] Li Y, He S, Li Y, et al. Federated multiagent deep reinforcement learning approach via physics-informed reward for multimicrogrid energy management[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(5): 5902-5914.
213. [213] Uddin M R, Rahman R, Nguyen D C. False Data Injection Attack Detection in Edge-based Smart Metering Networks with Federated Learning[J]. arXiv preprint arXiv:2411.01313, 2024.
214. [214] Latif N, Ma W, Ahmad H B. Advancements in securing federated learning with IDS: a comprehensive review of neural networks and feature engineering techniques for malicious client detection[J]. Artificial Intelligence Review, 2025, 58(3): 91.
215. [215] Kumar K, Chakraborty S, Kumar P, et al. Blockchain-Based Defense Mechanisms for Mitigating Unnecessary Islanding in Microgrids Against Cyber-Attack[C]//2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE). IEEE, 2024: 1-4.
216. [216] Wu Z, Liu Y, Liang H. A Quantum Minimum Cut-Set Method for Vulnerable Node Localization Against False Data Injection Attacks[C]//2023 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2023: 147-152.
217. [217] Tan Z, Li Z. Digital twins for sustainable design and management of smart city buildings and municipal infrastructure[J]. Sustainable Energy Technologies and Assessments, 2024, 64: 103682.
218. [218] Wessels M, van den Brink P, Verburgh T, et al. Understanding incentives for cybersecurity investments: Development and application of a typology[J]. Digital Business, 2021, 1(2): 100014.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.