Review

Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions

Kerong Xue *

Posted Date: 23 April 2025

doi: 10.20944/preprints202504.1907.v1

Keywords: False Data Injection Attacks; Power Cyber-Physical Systems; Detection Methods; Machine Learning; Hybrid Defense Strategies; Emerging Technologies

Review

Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions

Kerong Xue

School of Electrical Engineering, Inner Mongolia University of Technology, Hohhot, Inner Mongolia, China

Abstract: False Data Injection Attacks (FDIAs) pose a significant threat to the security and stability of Power Cyber-Physical Systems (CPS). As these systems become more interconnected and automated, the risk of malicious data manipulation has increased, leading to potential grid instability, equipment damage, and large-scale outages. This review provides a comprehensive analysis of recent advancements in FDIA detection, defense mechanisms, and resilience strategies. It examines various detection methods, from traditional state estimation to machine learning-based approaches, and discusses the integration of hybrid techniques for enhanced accuracy. The review also explores emerging technologies such as federated learning, quantum computing, and IoT, highlighting their potential in strengthening FDIA defenses. Additionally, the importance of a multi-faceted approach, combining technical, regulatory, and operational solutions, is emphasized for ensuring the long-term security of power CPS. The review concludes with future research directions focused on dynamic attack modeling, adaptive defense systems, and the integration of emerging technologies to address the evolving landscape of cyber threats.

Keywords: false data injection attacks; power Cyber-Physical Systems; detection methods; machine learning; Hybrid Defense Strategies; emerging technologies

1. Introduction

1.1. Power CPS and Their Integration with Modern Information Technologies

Cyber-Physical Systems (CPS) refer to the integration of physical processes with computational elements, enabling real-time monitoring, control, and optimization [1–3]. In the context of power systems, the increasing integration of information and communication technologies has transformed traditional grids into power Cyber-Physical Systems (Power CPS) [4,5]. These systems incorporate advanced sensors, smart meters, renewable energy sources, electric vehicles, and automated control devices, all interconnected by sophisticated communication networks. The resulting system offers enhanced operational capabilities, such as real-time monitoring, predictive maintenance, and dynamic load management, making power grids more efficient and adaptable [6].

As the world transitions toward more sustainable and resilient energy systems, CPS have become the backbone of modern power grids, supporting the integration of renewable energy sources like wind, solar, and energy storage systems. These advancements provide new opportunities for grid management and optimization, reducing dependency on fossil fuels, and facilitating decentralized energy production. However, the increasing reliance on information and communication technologies (ICT) also opens the door to new vulnerabilities, especially in the face of cyber-attacks. The convergence of the cyber and physical domains in power CPS necessitates the development of robust security measures to prevent and mitigate potential threats [7–9].

 doi:10.20944/preprints202504.1907.v1

1.2. False Data Injection Attacks (FDIAs) in Power Systems

Among the various threats facing Power CPS, FDIAs have emerged as one of the most concerning. FDIAs target the critical measurement and control systems of power grids, where attackers manipulate data to deceive system operators and disrupt the normal operation of the grid [10,11]. These attacks exploit the fact that modern power systems heavily rely on data from measurement devices (e.g., Phasor Measurement Units (PMUs), Remote Terminal Units (RTUs)) to perform state estimation and make control decisions. By injecting false data into these systems, attackers can mislead control centers, resulting in incorrect operational decisions such as improper load dispatch, equipment malfunction, or even large-scale grid instability [12].

The primary challenge of FDIAs lies in their stealthy nature. Unlike other cyber-attacks that cause immediate disruptions, FDIAs can evade traditional bad data detection mechanisms. They are designed to satisfy the system's state estimation constraints, allowing them to remain undetected for extended periods. This covert nature poses a significant risk to the security and stability of power grids, particularly in the face of increasing system complexity and the integration of distributed energy resources.

1.3. FDIA Impact on Power Grid Security and Stability

The impact of FDIAs on the security and stability of power systems can be severe, potentially leading to cascading failures, blackouts, and long-term disruptions [13–15]. The vulnerability of Power CPS to FDIAs underscores the importance of ensuring the integrity and reliability of grid data. Given that these systems are responsible for the safe distribution of electricity to millions of users, compromising their operation can have far-reaching consequences, not only for energy supply but also for public safety and national security.

FDIAs pose a particular threat to the resilience of the grid [16–18]. In addition to the direct consequences of compromised data, FDIAs can hinder the grid's ability to recover from faults or adapt to changes in supply and demand [19]. For example, an attacker could manipulate the system's response to a disturbance, leading to equipment overloads, protection failures, and unnecessary operational costs [20]. Moreover, the increasing reliance on automated systems for grid control means that an FDIA could have a long-lasting and automated effect, making it difficult to contain or reverse the damage once the attack is underway.

Given the growing frequency and sophistication of cyber-attacks on critical infrastructure, addressing FDIAs is vital for safeguarding power systems from emerging cyber threats. Preventing and mitigating the effects of these attacks is crucial to ensuring the secure and stable operation of power CPS, as they represent one of the most significant challenges facing grid operators and cybersecurity experts alike.

1.4. Motivation for the Review: Summarize the Gaps and Challenges in Current Research

This review aims to address the evolving challenge of FDIAs in Power CPS by providing a comprehensive analysis of the current state of research, identifying gaps, and suggesting future directions [21]. While significant progress has been made in developing detection and mitigation strategies for FDIAs, many challenges remain unsolved. First, traditional detection methods, such as residual-based techniques, struggle to detect sophisticated attacks that mimic normal system behavior. The rapid evolution of attack strategies, including the use of dummy data injection (DDIA) and advanced evasion techniques, requires new and adaptive detection approaches [22,23].

Furthermore, much of the existing research focuses on the detection of FDIAs, with limited attention given to the critical area of data reconstruction following an attack. After detecting an FDIA, the ability to reconstruct accurate system states is essential for minimizing the impact of the attack on the system's operation. However, existing methods for data reconstruction are still in their infancy, and their practical applicability in large-scale power grids remains unclear [24].

 doi:10.20944/preprints202504.1907.v1

Additionally, while machine learning and AI have shown promise in improving FDIA detection, these techniques often suffer from issues such as poor interpretability and the need for large amounts of labeled data for training. Moreover, the integration of cyber and physical security measures is still in its early stages, with few studies addressing how to create a unified defense mechanism that combines both domains to protect against FDIAs.

This review aims to fill these gaps by analyzing the latest developments in FDIA detection, mitigation, and reconstruction, while also providing insights into emerging technologies and strategies that could improve the security and resilience of Power CPS. By synthesizing the existing literature and highlighting areas for further investigation, this paper provides a roadmap for future research in the field and contributes to the ongoing effort to secure power systems against increasingly sophisticated cyber-attacks.

2. FDIA Background and Evolution

2.1. Early Detection and Historical Impact in Power Systems

FDIAs emerged as a significant threat to power systems with the increasing integration of cyber-physical systems [25–27]. These attacks exploit vulnerabilities in the information infrastructure of power grids by manipulating data fed into state estimation processes, misguiding the control systems that manage grid operations. The concept of FDIAs was first introduced in the context of power systems in 2009, with researchers showing that attackers could inject false data into power system state estimation, bypassing traditional bad data detection mechanisms. By carefully crafting the injected data to align with system constraints, attackers could mislead the control centers into making erroneous operational decisions without being detected [28].

The early detection of FDIAs posed a substantial challenge because these attacks are designed to mimic normal operational data. Traditional bad data detection mechanisms, which rely on residuals from state estimation models to flag discrepancies, were ineffective against such subtle manipulations. As a result, the attacks went undetected for longer periods, allowing attackers to remain hidden within the system. This posed significant risks to the security, stability, and reliability of power grids. The early realization of the potential impact of FDIAs highlighted the need for advanced detection, prevention, and mitigation strategies, leading to the development of new approaches focused on improving the resilience of power CPS against such attacks [29,30].

2.2. Key Incidents and Relevance to FDIA Research

Several high-profile cyber-attacks on power systems have underscored the importance of FDIA research and the vulnerabilities in modern grid infrastructure [31–33]. Notable incidents include the Stuxnet worm, the BlackEnergy malware, and the 2015 Ukraine blackout, each of which has significantly influenced the research landscape of FDIAs.

1) **Stuxnet (2010)**: The Stuxnet attack is one of the most famous examples of cyber-attacks on critical infrastructure. While primarily focused on Iranian nuclear facilities, Stuxnet demonstrated how cyber-attacks could sabotage industrial control systems (ICS), including power systems. Although Stuxnet was not an FDIA, its tactics and methodology—such as targeting control systems and using sophisticated, stealthy techniques—had direct relevance for FDIA research. It highlighted the potential for cyber-attacks to manipulate sensor data, disrupt operations, and cause physical damage to critical infrastructure.
2) **BlackEnergy (2015)**: The BlackEnergy malware was used in a series of cyber-attacks targeting Ukrainian power grids. This attack demonstrated the potential of cyber threats to cause large-scale power outages by manipulating data flows within power CPS. It showed how a combination of physical attacks on control systems and data manipulation could lead to a blackout. Though not strictly an FDIA in the classic sense, the BlackEnergy attack shares characteristics with FDIAs, such as stealth, coordination, and disruption of normal grid operations.

 doi:10.20944/preprints202504.1907.v1

3) **Ukraine Blackout (2015)**: One of the most significant incidents involving FDIA was the 2015 Ukrainian power grid attack. Hackers used a sophisticated FDIA to manipulate the SCADA systems, leading to the disconnection of critical power transmission lines and causing a widespread power outage that affected over 230,000 people. This attack illustrated the potential scale of damage an FDIA could cause. It also highlighted the increasing sophistication of cyber-attacks, as the attackers used a multi-step process involving both physical and cyber elements to execute the attack, including data manipulation and network infiltration.

These incidents underscored the vulnerabilities of power grids to cyber-attacks, particularly those that involve the manipulation of sensor data and system measurements. They also served as critical turning points in the development of FDIA research, as the need to detect, prevent, and mitigate such attacks became evident to both researchers and power system operators.

2.3. Types of FDIAs and Their Manipulation Techniques

FDIAs can target various aspects of power CPS, each with different consequences depending on the focus of the attack [34]. The primary targets of FDIAs are the measurement data, state estimation algorithms, and control actions that form the backbone of grid operations.

1) **Manipulation of Measurement Data**: FDIAs typically involve the manipulation of data collected by sensors and measurement devices like PMUs and RTUs. These devices collect crucial real-time data, such as voltage, current, power flow, and frequency, which are then transmitted to the control centers for analysis. By injecting false data into this system, attackers can deceive the control center into making incorrect operational decisions, such as failing to recognize faults or misbalancing power distribution [35]. Manipulating measurement data is often the first step in an FDIA, as it directly impacts state estimation and control decisions.
2) **System State Estimation**: State estimation is a critical process in power grids, where the system's operational state (e.g., voltage angles, magnitudes) is inferred from available measurements [36–38]. FDIAs can target this process by injecting false data that satisfies the system's state estimation constraints, thus allowing the attackers to manipulate the estimated system state without being detected. This can lead to the issuance of incorrect control commands, such as altering the power flow, adjusting generator outputs, or misdirecting the grid's response to a disturbance [39].
3) **Control Actions**: Once an attacker has successfully manipulated measurement data and state estimation, they can influence control actions within the grid [40]. These control actions could include load shedding, generator rescheduling, or adjusting power flow in a way that destabilizes the grid. In some cases, attackers may use manipulated data to cause misoperation of critical equipment, such as circuit breakers, transformers, or generators, potentially leading to localized or widespread outages. This is especially concerning in the context of automated or semi-automated grid management, where control systems make decisions based on real-time data and system models [41,42].

2.4. Stealthy and Multi-Stage Nature of FDIAs

One of the defining characteristics of FDIAs is their stealthy and multi-stage nature, which makes them particularly challenging to detect and counter [43,44]. Unlike other types of cyber-attacks that are designed to cause immediate disruptions, FDIAs often operate slowly and covertly, making it difficult for detection systems to identify them in real time.

1) **Stealthiness**: FDIAs are often designed to mimic normal operational data, making them undetectable by traditional bad data detection mechanisms [45]. Attackers carefully craft the false data to satisfy system constraints, such as power flow equations and state estimation models. By doing so, they can bypass detection systems that rely on residuals or discrepancies in the data to flag anomalies. This stealthy nature allows attackers to remain undetected for

 doi:10.20944/preprints202504.1907.v1

extended periods, giving them ample time to manipulate the grid's operations without raising alarms.

2) **Multi-Stage Nature**: FDIAs are often multi-stage attacks that involve several phases. In the initial stages, attackers infiltrate the power grid's communication and control networks, identifying vulnerabilities in measurement devices and control systems. Next, they inject false data into the system, bypassing bad data detection mechanisms. Finally, once the attackers have successfully manipulated the system's state estimation and control actions, they may cause a cascade of failures, such as equipment misoperations or power outages. The multi-stage nature of FDIAs means that they evolve over time, with attackers potentially adjusting their strategies as they learn more about the system's defenses [46].

This gradual and evolving nature of FDIAs presents a significant challenge for detection systems, which must not only identify anomalies in the data but also understand the temporal and spatial evolution of the attack. Current research on FDIA detection and mitigation continues to focus on addressing these challenges, developing adaptive methods that can detect attacks at various stages of their evolution and minimize their impact on the grid.

3. Challenges in FDIA Detection

3.1. Overview of Current Detection Methods

The detection of FDIAs in Power CPS is an ongoing challenge, with several approaches being developed over the years to identify and mitigate such attacks [47–49]. Detection methods can generally be classified into two broad categories: model-driven and data-driven approaches. These methods utilize different strategies and tools to identify malicious data that might have been injected into the power system.

1) **State Estimation-Based Detection Methods**: State estimation plays a pivotal role in power system operation, as it provides the system operators with estimates of unmeasurable system variables, such as voltage magnitudes and phase angles [50,51]. State estimation-based methods are the most traditional approach for detecting FDIAs. These methods rely on comparing measured data with the expected data derived from a system model. If discrepancies (residuals) exceed predefined thresholds, a bad data detection mechanism flags the potential presence of an FDIA. While this method is fast and widely adopted, it struggles to detect sophisticated attacks that align with system constraints, as attackers can inject data that satisfies these constraints without triggering traditional residual-based checks.
2) **Machine Learning Approaches**: Machine learning (ML) techniques have been increasingly applied to FDIA detection due to their ability to analyze large datasets and uncover complex patterns in data [52]. These methods are data-driven, meaning they focus on identifying anomalous behavior without requiring an explicit model of the system. Various ML techniques, such as Support Vector Machines (SVM), Random Forests, and Deep Learning, have been utilized to classify data as normal or attacked based on historical operational data. These methods can be highly effective in detecting subtle anomalies that model-based methods might miss, especially in the presence of large-scale and complex grid systems [53].
    - **Supervised learning** techniques train models using labeled data, where instances of normal and attacked data are clearly identified. The model learns the patterns from this labeled data to predict whether new data points are attacked.
    - **Unsupervised learning** methods, on the other hand, do not require labeled data and are more suited for scenarios where attack labels are unavailable. These methods focus on detecting outliers or patterns that deviate from the normal operating conditions.

Machine learning methods, particularly deep learning, have shown promise in detecting FDIA by learning features from raw data, eliminating the need for manual feature engineering. However,

 doi:10.20944/preprints202504.1907.v1

these methods often require large amounts of data for training, which may not always be available, and can suffer from issues related to model interpretability [54].

3) **Hybrid Methods**: Given the limitations of both state estimation-based and machine learning approaches, hybrid detection strategies have emerged. These methods combine the strengths of model-driven and data-driven techniques to enhance FDIA detection. For instance, integrating machine learning with state estimation can improve the ability to identify sophisticated attacks while also retaining the theoretical underpinnings of system models. Hybrid methods aim to leverage the strengths of both approaches: the interpretability and robustness of model-driven techniques and the flexibility and adaptability of data-driven methods [55].

3.2. Limitations in Existing Detection Approaches

While current FDIA detection methods have contributed significantly to the field, they still face several limitations that hinder their effectiveness, particularly when dealing with real-time detection in large-scale systems [56–58]. The main limitations include:

1) **Low Detection Accuracy**: Despite the advancements in detection methods, the accuracy of FDIA detection remains a critical issue. In state estimation-based methods, the detection thresholds are often predefined based on historical data, and any attack that conforms to these thresholds remains undetected. In the case of machine learning-based methods, the detection accuracy can degrade if the training data is not representative of the system's current operating conditions or if the attack types are not well-represented in the training set. Additionally, the dynamic nature of power systems, especially with the increasing integration of renewable energy sources, makes it difficult for detection algorithms to remain effective across different operating conditions and attack scenarios [59].
2) **High Computational Cost**: Many of the state estimation-based methods, especially those that involve real-time monitoring of grid operations, can be computationally intensive. The need for frequent updates to state estimates, the handling of large datasets, and the requirement for solving optimization problems in real time can place a significant computational burden on detection systems. In machine learning approaches, especially deep learning, the need to train models on large datasets can further increase computational costs. These methods require substantial computational resources, which may not be feasible for deployment in real-time grid operations, particularly in large-scale grids [60].
3) **Poor Adaptability**: One of the key challenges of FDIA detection is the adaptability of existing methods to evolving attack strategies and dynamic grid conditions. Many detection methods are designed to work under specific, predefined assumptions about the grid's operation, such as the types of data being collected or the grid's topology. However, the increasing complexity of modern power grids, along with the evolving sophistication of cyber-attacks, requires detection systems to be highly adaptable. For instance, new attack types, such as Dummy Data Injection Attacks (DDIAs), have emerged, which are even more difficult to detect because the false data injected into the system closely resembles normal measurement data. Existing methods often struggle to adapt to these new types of attacks, leaving gaps in security [61,62].

3.3. Challenges in Integrating Detection Strategies to Enhance Accuracy and Speed

The integration of multiple detection strategies presents an opportunity to improve the accuracy and speed of FDIA detection in power CPS [63–65]. However, this integration also introduces several challenges:

1) **Data Fusion and Synchronization**: Combining different detection methods, such as state estimation and machine learning, requires effective data fusion techniques. In many cases, the data from various sources (e.g., PMUs, RTUs, SCADA systems) may be inconsistent, incomplete, or temporally misaligned. Ensuring that these diverse data streams are properly synchronized

 doi:10.20944/preprints202504.1907.v1

and fused for analysis is a significant challenge. Poor data fusion can lead to inaccurate results, further complicating the detection process [66].

2) **Real-Time Detection**: Power systems operate in real time, and the detection of FDIAs must be fast enough to prevent substantial damage. The integration of multiple detection strategies requires balancing the computational complexity of each method. While more sophisticated methods (such as deep learning) may offer improved detection accuracy, they often come at the cost of processing time. Therefore, achieving real-time detection while maintaining high accuracy is a persistent challenge [67].
3) **Complexity of Combining Model-Driven and Data-Driven Approaches**: Model-driven methods are based on system knowledge and theoretical models of grid behavior, while data-driven methods rely on learning patterns from large datasets. Combining these approaches effectively requires finding ways to leverage the strengths of each without exacerbating the weaknesses. For example, model-driven methods may not be flexible enough to adapt to changing grid conditions, while data-driven methods may lack interpretability. The complexity of integrating these approaches—ensuring that they complement each other and work synergistically—poses a significant challenge [68].
4) **Scalability**: Power systems are growing in complexity and size, particularly with the integration of distributed energy resources, smart meters, and electric vehicles. As the scale of the grid increases, so too does the volume of data that must be processed. Detection systems must be scalable to handle this growth while maintaining detection accuracy and speed. Integrating multiple detection strategies to work efficiently across large-scale systems without overwhelming computational resources remains a key challenge [69,70].

FDIA detection in Power CPS is a complex and multifaceted problem, with various approaches available to address the issue. However, each method faces significant challenges related to accuracy, computational cost, adaptability, and integration [71]. To improve the robustness of FDIA detection systems, researchers must explore novel methods for combining state estimation with machine learning and other advanced techniques. Additionally, the integration of multiple detection strategies must be done carefully, taking into account the trade-offs between accuracy, speed, and scalability. As cyber threats continue to evolve, ongoing research and development will be crucial in designing detection systems that can adapt to new attack methods and provide real-time, effective defense mechanisms for power grids [72].

4. Recent Advances in FDIA Detection Techniques

The field of FDIA detection has witnessed significant advancements in recent years, driven by innovations in machine learning, artificial intelligence, and state estimation methods. These advances aim to enhance the accuracy, robustness, and adaptability of FDIA detection systems in Power CPS [73,74]. This section highlights the recent developments in FDIA detection techniques, focusing on machine learning and AI-based approaches, improvements in state estimation methods, the integration of model-based and data-driven approaches, and case studies showcasing successful implementations.

4.1. Machine Learning and AI-Based Approaches

ML and artificial intelligence (AI) have become central to FDIA detection due to their ability to analyze large volumes of data, uncover hidden patterns, and detect anomalies that may be missed by traditional methods [75–77]. Recent research has focused on leveraging deep learning, ensemble methods, and other AI-enhanced techniques to improve FDIA detection accuracy and adaptability.

1) **Deep Learning**: Deep learning techniques, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown great promise in detecting FDIA in power systems. These networks are capable of learning complex representations of data through multiple layers of abstraction, allowing them to detect subtle changes in grid behavior caused

 doi:10.20944/preprints202504.1907.v1

by FDIAs. For example, CNNs have been used to analyze time-series data from PMUs and identify anomalous patterns indicative of FDIA. Similarly, RNNs, especially Long Short-Term Memory (LSTM) networks, are effective in modeling the temporal dependencies in power system measurements, enabling the detection of FDIA over time [78].

2) **Ensemble Methods**: Ensemble methods combine multiple models to improve prediction accuracy and reduce the likelihood of overfitting. Recent studies have applied ensemble techniques like Random Forests and Gradient Boosting Machines (GBM) for FDIA detection. These methods aggregate the predictions of multiple classifiers to enhance detection robustness. For instance, a Random Forest model can be trained on various features extracted from historical grid data, and its decision trees can be used to classify whether a given set of measurements is likely to have been compromised by FDIA. By combining multiple weak models into a strong predictor, ensemble methods help reduce the impact of noisy or incomplete data on the detection system [79,80].
3) **AI-Enhanced Techniques**: AI techniques, including Reinforcement Learning (RL) and Generative Adversarial Networks (GANs), have been applied to enhance the detection of FDIAs. RL techniques focus on training models to detect FDIAs by optimizing a reward function based on detection performance. In contrast, GANs have been employed in data reconstruction tasks, where they generate realistic measurement data based on normal grid conditions and compare them against actual data to identify discrepancies caused by FDIAs. By employing these advanced AI techniques, researchers aim to create more adaptive and intelligent systems capable of detecting increasingly sophisticated FDIA strategies [81,82].

4.2. State Estimation-Based Methods

State estimation has long been a cornerstone of FDIA detection in power systems. Recent advancements in state estimation methods have improved both the robustness and accuracy of these systems in the presence of malicious data. Traditional state estimation relies on solving power flow equations using available measurements and system models to estimate unmeasured states of the system. However, when FDIAs are introduced, traditional methods often fail to identify the attack due to the stealthy nature of these attacks [83,84].

1) **Robust State Estimation**: Recent work has focused on developing robust state estimation techniques that are less sensitive to false data. These methods incorporate outlier detection and residual-based analysis to flag potential FDIAs more effectively [85]. For example, Weighted Least Squares (WLS) state estimation, which is commonly used in traditional methods, has been modified to handle deviations caused by FDIA by introducing robustness mechanisms. One such improvement is the use of Huber M-estimators, which minimize the impact of large residuals associated with FDIAs while maintaining the robustness of the overall system.
2) **Extended and Dynamic State Estimation**: Traditional state estimation is often static, assuming that the system remains stable over time. However, modern power systems are dynamic, with frequent changes in load, generation, and system topology. As a result, dynamic state estimation (DSE) has gained popularity for FDIA detection. DSE techniques incorporate real-time data updates and time-series analysis, enabling the system to adapt to changes in operational conditions while maintaining detection accuracy. By modeling the system as a dynamic process, DSE methods are better suited for identifying attacks that evolve over time and across different parts of the grid.
3) **Improved Accuracy through Multiple Estimators**: Another recent development is the use of multiple state estimators running in parallel, each with different breakdown points or parameter settings. This approach improves the robustness of the system by enabling the comparison of results across multiple estimation techniques. By cross-checking the results from different estimators, attacks that might evade one method can be detected by others, significantly enhancing detection reliability. For example, combining robust least-squares methods with Kalman Filters allows for more accurate detection of anomalies in dynamic power systems.

 doi:10.20944/preprints202504.1907.v1

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

Given the limitations of relying solely on either model-based or data-driven approaches, hybrid detection methods have been developed to combine the strengths of both. These methods aim to create a more comprehensive and adaptable detection framework that improves the overall accuracy and speed of FDIA detection [86].

1) **Model-Driven and Data-Driven Integration**: Hybrid methods typically involve integrating state estimation (model-driven) with machine learning (data-driven) techniques. For example, SVMs or neural networks (NNs) can be used to analyze the residuals generated by traditional state estimation processes. These methods combine the system's theoretical knowledge (from the state estimator) with the adaptability and pattern recognition capabilities of machine learning, resulting in more robust detection. In one such approach, a model-based state estimator might first identify possible areas of attack, and then a machine learning classifier is employed to validate the detected anomalies and classify them as either normal or caused by an FDIA [87–89].
2) **Dynamic Integration**: Another approach to hybrid detection involves the dynamic integration of model-based and data-driven methods. In this approach, the system continuously updates its models based on real-time data and adapts to changing grid conditions. This technique allows for the detection of evolving attacks over time. For example, a dynamic system might initially use state estimation methods to detect deviations, then switch to machine learning algorithms for further analysis if the detected anomaly is ambiguous. This combination of model-based analysis and machine learning provides a flexible and scalable solution for detecting complex FDIAs [90].
3) **Collaborative Detection Frameworks**: Recent advancements in hybrid detection also include the use of **collaborative detection frameworks** where different components of the grid (e.g., substations, PMUs, control centers) cooperate by sharing data and detection results. This allows the system to detect FDIAs across various levels and locations of the power grid. For instance, in a multi-area detection framework, local detection models at different substations can communicate with each other to validate the detected anomalies and reduce false positives or missed detections [91,92].

4.4. Case Studies in FDIA Detection

1) **Case Study 1: Hybrid Detection System in a Smart Grid**: A recent case study conducted by researchers demonstrated the use of a hybrid detection system combining state estimation and machine learning in a smart grid scenario. The system utilized multi-layer perceptron (MLP) neural networks to classify residuals from a state estimation process, detecting FDIAs in real-time. The study showed that this hybrid approach significantly outperformed traditional state estimation methods in detecting complex attack scenarios, reducing the number of false negatives while maintaining low computational costs [93,94].
2) **Case Study 2: AI-Enhanced Detection in a Transmission Network**: Another case study involved implementing AI-based detection in a large-scale transmission network. The researchers applied deep learning models, specifically **autoencoders**, to identify subtle changes in the system's measurements caused by FDIAs. The results showed that the deep learning model could detect attacks that had previously been undetectable by traditional methods, with the added benefit of the system learning from new attack patterns over time [95].
3) **Case Study 3: Integration of Hybrid Detection in a Microgrid**: In a microgrid environment, researchers tested a hybrid detection framework combining state estimation with ensemble learning algorithms. The hybrid system was able to identify FDIA-related anomalies by evaluating the data from both the system model and historical performance data. The case study highlighted the effectiveness of combining these methods to improve detection accuracy, particularly in decentralized systems with limited connectivity between grid components [96].

 doi:10.20944/preprints202504.1907.v1

5. False Data Injection Attack Evolution and Impact

5.1. Temporal and Spatial Evolution of FDIAs

FDIAs are dynamic, multi-phase attacks that evolve over time and across different spatial regions of a CPS. Understanding the temporal and spatial evolution of FDIAs is crucial for developing effective detection and mitigation strategies [97]. These attacks are not static; they unfold in stages, impacting various parts of the system at different times, and their effects cascade throughout the power grid. The complexity and extended timeline of these attacks make them especially difficult to detect and counter in real time [98].

1) **Temporal Evolution**: The temporal nature of FDIAs refers to how attacks evolve over time. Initially, an attacker may exploit vulnerabilities in the system to gain access to the communication or control network, using techniques such as privilege escalation or system exploitation. In the subsequent phase, the attacker begins injecting false data into the system. These injected data points are carefully crafted to satisfy the system's state estimation constraints, making them undetectable by traditional bad data detection methods. The attack can remain hidden for extended periods, allowing the attacker to gather more system information and refine the attack [99].

   Over time, as the attacker gains more control over the grid, the false data injected into the system starts to mislead operators and control centers. This can result in incorrect operational decisions such as generator rescheduling, faulty load shedding, or equipment misoperation. The longer the attack remains undetected, the more pronounced the cascading effects on system reliability and stability. These cascading effects can range from local disturbances to widespread outages, depending on the size and location of the attack [25,100].
2) **Spatial Evolution**: FDIAs also evolve spatially, affecting different parts of the grid in various ways. For example, an attacker might first target certain substations or measurement points, injecting false data into these areas. Over time, the attack may spread to other parts of the grid, affecting interconnected systems and amplifying its impact. This spatial evolution is particularly concerning in modern grids, where interdependencies between power generation, transmission, and distribution systems are increasing due to the integration of renewable energy sources, smart meters, and distributed energy resources [101,102].

The cascading effects of spatially distributed FDIAs can result in system-wide failures, especially when critical components such as transformers, switches, and voltage regulators are affected. The complexity of these interconnections makes it difficult to pinpoint the source of the attack and assess its full impact on the grid's operation.

5.2. Influence of Physical and Cyber Components on FDIA Outcomes

FDIAs in power CPS are not purely digital attacks; they involve a sophisticated interaction between physical and cyber components of the system [103–105]. Understanding the relationship between these components is crucial for predicting and mitigating the impact of such attacks.

1) **Cyber Components**: The cyber components of power CPS include communication networks, control systems, and data processing units such as Supervisory Control and Data Acquisition (SCADA) systems, PMUs, and RTUs. These systems are responsible for collecting and transmitting operational data, running state estimations, and making real-time control decisions. The integrity of these cyber components is vital for the secure operation of the power grid. When FDIAs target these cyber components, they can manipulate the data being sent to control centers, causing incorrect decisions to be made based on false information [81,106]. For instance, state estimation errors due to falsified data can lead to faulty grid responses, like incorrect load balancing or power flow rerouting, which can destabilize the grid [107].
2) **Physical Components**: Physical components of the grid, such as transformers, substations, transmission lines, and generation units, are directly affected by the control decisions made

 doi:10.20944/preprints202504.1907.v1

based on false data [108]. When FDIAs influence the control systems, the resulting operational decisions can cause stress on the physical infrastructure, potentially leading to equipment overloads, failures, or even damage. For example, a misjudged rescheduling of generation units or a faulty operation of circuit breakers can result in overloads, equipment malfunctions, or short circuits. The physical effects of FDIAs can escalate quickly, causing localized faults to develop into large-scale outages or cascading failures that affect a wide area of the grid [109].

The interaction between cyber and physical components also creates feedback loops. For example, cyber attacks may manipulate physical components, leading to abnormal system behavior, which then generates new data patterns that can be further manipulated by the attacker. These feedback loops complicate the detection and mitigation of FDIAs, as the impact of the attack is not only digital but also physical, affecting system stability and reliability [13,110,111].

5.3. Evolution of FDIA Attack Methods

FDIAs have evolved significantly since their introduction, from basic data manipulation attacks to more sophisticated, multi-domain strategies that involve advanced techniques across both the cyber and physical components of the system [112].

1) **Early FDIA Methods**: Initially, FDIAs involved simple data manipulation, where attackers would inject false measurements into the system, such as fake voltage, current, or power flow readings [113,114]. These attacks would typically target the state estimation process, which relies on accurate data to infer the unmeasured states of the grid. Early FDIAs were relatively straightforward and could be detected using traditional bad data detection methods based on residuals or consistency checks. However, as attackers learned more about power system operations, these methods became increasingly sophisticated [115].
2) **Advanced FDIA Techniques**: Modern FDIAs have become more complex and involve multi-step processes. For example, attackers may first infiltrate the system using techniques such as phishing, social engineering, or exploiting vulnerabilities in the grid's communication network. Once they have gained access, they can manipulate both the data and the physical operations of the grid. Advanced FDIAs can alter system topology, cause misoperations in control systems, or even disrupt the synchronization of power grid operations through attacks on time-stamping or GPS signals used by PMUs. These attacks are designed to remain undetected for extended periods and can cause long-term damage to the grid's stability [116,117].
3) **Multi-Domain Attacks:** In recent years, attackers have shifted towards multi-domain FDIAs, where they simultaneously target both the cyber and physical components of the system. These attacks not only manipulate data but also exploit vulnerabilities in physical devices like circuit breakers, transformers, and smart meters. Multi-domain FDIAs can also involve coordinated attacks that span multiple stages, such as injecting false data, compromising control systems, and manipulating system operations, all while remaining hidden from detection systems. Such attacks require advanced knowledge of the grid's operational dynamics and the ability to manipulate both cyber and physical aspects of the system [118].

5.4. Impact of FDIAs on System Reliability, Safety, and Economic Stability

The potential impact of FDIAs on power CPS is far-reaching, affecting system reliability, safety, and economic stability [119–121]. These attacks can cause a wide range of problems, from localized disruptions to large-scale blackouts that affect entire regions or countries.

1) **Reliability**: FDIAs can significantly undermine the reliability of power systems by creating false perceptions of system stability. As false data is injected into the system, operators may make incorrect decisions regarding load balancing, generation scheduling, or system configuration. These erroneous decisions can cause equipment overloads, frequency instability, or power flow issues, ultimately leading to system failures. When FDIAs are undetected, they can lead to cascading failures, where small faults grow into large-scale outages that are difficult to contain.

 doi:10.20944/preprints202504.1907.v1

2) **Safety**: The safety risks associated with FDIAs are substantial. False data injection can lead to incorrect control actions, such as opening or closing circuit breakers, which could result in equipment damage, fires, or even explosions. Moreover, compromised system operation due to FDIAs can prevent proper fault detection and isolation, leaving the grid vulnerable to further damage. In critical infrastructure such as nuclear or hydroelectric power plants, a compromised control system due to FDIA could lead to catastrophic consequences, including environmental hazards or threats to public safety [122].
3) **Economic Stability**: The economic impact of FDIAs on power systems is significant. Power grid instability caused by FDIA can lead to production downtime, damage to equipment, and unplanned maintenance, all of which incur substantial costs. Additionally, the cost of mitigating an FDIA and restoring normal grid operation can be extremely high, particularly when the attack leads to widespread outages or prolonged periods of instability. In markets that rely on dynamic pricing models, such as energy markets, FDIAs can disrupt price signals and distort market operations, leading to financial losses for both operators and consumers. Furthermore, prolonged disruptions in energy supply can harm economic activities, especially in energy-intensive industries, leading to broader economic repercussions [123–125].

6. Mitigation Strategies for FDIAs

The increasing sophistication of FDIAs in Power CPS necessitates the development of effective mitigation strategies. Once an FDIA is detected, it is crucial not only to counteract the attack but also to minimize its long-term impact on the system [126,127]. This section discusses key mitigation strategies, including data reconstruction approaches, the importance of attack localization, the development of robust countermeasures, and advancements in real-time decision support systems.

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

Once an FDIA is detected in a Power CPS, the next critical step is to reconstruct the affected data and restore the system to its normal operating state [128]. Data reconstruction methods aim to compensate for the false measurements injected by the attacker, ensuring that the system can continue functioning without disruption.

1) **State-Aware Attack Data Reconstruction**: State-aware reconstruction focuses on maintaining the system's state estimation, which is critical for ongoing grid operations. These methods are designed to restore the integrity of the system's state by estimating what the correct measurements should have been, based on the remaining valid data [129,130]. In a typical state-aware reconstruction method, the system uses a model of the grid, along with the remaining uncorrupted measurements, to estimate the most likely state of the grid that would have existed without the attack.
   Advanced state-aware reconstruction methods leverage GANs and Variational Autoencoders (VAEs) to generate data that fits the expected system behavior. For example, GAN-based techniques can learn the underlying distribution of normal grid measurements and use this knowledge to generate reconstructed data that closely aligns with expected system states [82,131]. Wasserstein GANs (WGANs), for instance, can provide more stable and reliable reconstructions, particularly in scenarios where the data distribution is complex or sparse [15,132,133].
   State-aware methods are highly effective when the system's model is well-known and the remaining data is reliable. However, they face challenges when a large portion of the measurement data is compromised or when the system model itself is inaccurate, limiting the effectiveness of these methods.
2) **Action-Control Attack Data Reconstruction**: Action-control reconstruction methods focus on restoring the system's operational control following an FDIA. While state-aware methods restore the system's state, action-control methods aim to repair the control commands that the system

 doi:10.20944/preprints202504.1907.v1

would have issued under normal conditions. These methods typically use data from unaffected parts of the system to estimate and reconstruct the correct control actions, such as load shedding, generator scheduling, or power flow adjustments [134].

For example, an adaptive sliding mode observer can be used to detect discrepancies in control variables, such as feedback from power system controllers, and correct the control signals in real-time. These methods are particularly valuable when the FDIA involves manipulating control systems, as they restore the system's decision-making process and help minimize operational disruptions.

While action-control reconstruction is crucial for preventing the spread of damage through incorrect control actions, it is often more complex and computationally demanding compared to state-aware reconstruction. This is because it requires a detailed understanding of the control systems' dynamics and must ensure that the reconstructed actions do not interfere with normal grid operations.

6.2. The Importance of Attack Localization for Minimizing Damages

Once an FDIA is detected, it is crucial to identify the specific location of the attack within the grid to minimize the impact on the system [135,136]. Attack localization involves pinpointing the compromised measurement points, control systems, or communication networks that have been targeted by the attacker [25,137]. Effective localization helps prioritize mitigation efforts, allowing grid operators to address the most critical areas first and limit the scope of the attack.

1) **Spatial Localization Techniques**: Several techniques have been developed to locate the source of FDIAs within the grid. One approach involves using residual analysis, where the residuals from state estimation are analyzed to determine which measurement points exhibit abnormal behavior. In a large grid, however, this can lead to ambiguities, as multiple measurements may be affected simultaneously, complicating the localization process. Advanced methods such as graph theory-based localization have been applied, where the grid's topology is modeled as a graph, and anomalies in data are traced back to specific nodes or edges in the network [138].
2) **Multi-Sensor Localization**: In large-scale grids, attack localization can be achieved by utilizing multiple sensors and measurement devices spread across the system. Multi-sensor fusion techniques combine data from different sources, such as PMUs, RTUs, and SCADA systems, to identify correlated anomalies and pinpoint the attack's origin. These techniques rely on the spatial and temporal correlations between measurements, and their effectiveness increases as more sensor data becomes available [139].

The ability to localize an FDIA quickly is critical for minimizing its impact. By focusing mitigation efforts on the affected areas, operators can prevent the attack from spreading, reduce operational disruptions, and quickly restore the grid to normal functioning.

6.3. Developing Robust Countermeasures and Defensive Protocols

As FDIAs grow in sophistication, the need for robust countermeasures and defensive protocols for power CPS becomes increasingly critical [140–142]. Developing these countermeasures requires a comprehensive understanding of the attack dynamics and an ability to deploy defense mechanisms that can adapt to changing attack strategies.

1) **Multi-Layered Defense Strategies**: One of the most effective approaches to defending against FDIAs is the use of multi-layered defense strategies. These strategies involve implementing multiple security measures at various levels of the power CPS, including the physical layer, the cyber layer, and the operational layer. For instance, network segmentation can be used to prevent attackers from accessing critical control systems, while encryption can secure communication channels to prevent data manipulation during transmission [143].

Real-time monitoring and intrusion detection systems (IDS) can help identify suspicious activities and isolate compromised parts of the grid. Machine learning-based IDS can be trained

 doi:10.20944/preprints202504.1907.v1

to detect anomalous patterns of data transmission or system behavior, providing a proactive defense against FDIAs [144].

2) **Resilience and Redundancy**: Building resilience into the system is another key aspect of defending against FDIAs. Redundancy at both the data and control levels helps ensure that the system can continue operating even in the presence of an attack. For example, employing redundant data sources can allow the system to cross-check information and identify discrepancies that may signal an attack. Similarly, backup control systems that can take over in the event of an attack can prevent major disruptions to grid operations [145].
3) **Adaptive Defense Protocols**: Modern defense protocols for power CPS should be adaptive, capable of evolving in response to new threats. This can be achieved by using adaptive filtering and dynamic security protocols that can adjust their parameters based on real-time attack patterns. By continuously learning from ongoing attack attempts, these systems can improve their detection capabilities and respond more effectively to future attacks [146,147].

6.4. Real-Time Decision Support to Mitigate FDIA Impact

Incorporating real-time decision support systems into the grid's operational infrastructure is essential for mitigating the impact of FDIAs. These systems help operators make informed decisions by providing real-time insights into the system's state, identifying anomalies, and suggesting appropriate actions to mitigate damage.

1) **Real-Time Monitoring and Control Systems**: Advanced real-time monitoring **systems** that integrate state estimation, data analytics, and machine learning can provide grid operators with immediate feedback about the system's health. These systems continuously assess system performance, identify discrepancies caused by FDIAs, and provide recommendations for corrective actions. Real-time decision support systems are particularly effective in decentralized grids, where decision-making is distributed across multiple control centers [148,149].
2) **Predictive Analytics for Attack Mitigation**: Using predictive analytics, operators can anticipate the potential consequences of an FDIA and take proactive steps to minimize damage. Predictive models can forecast the likely evolution of an attack and suggest mitigation strategies before the attack escalates. For instance, if an attack is detected in a substation, predictive models can estimate the potential impact on adjacent areas and provide recommendations for load re-distribution, generation rescheduling, or circuit breaker activation to prevent cascading failures.
3) **Automated Response Mechanisms**: In some cases, real-time decision support systems can be integrated with automated response mechanisms that trigger corrective actions without human intervention. For example, if an FDIA is detected and localized in a specific part of the grid, the system can automatically initiate load shedding or reroute power to stabilize the affected areas. These automated responses help reduce the time it takes to recover from an attack and prevent further damage to the grid [150].

7. Cyber-Physical Security Integration in Power CPS

The security of power CPS has become a top priority as these systems become increasingly interconnected with advanced communication networks, sensor technologies, and control systems [151]. The traditional separation between cyber and physical security has become insufficient in addressing the complex vulnerabilities inherent in modern grids. To ensure the resilience of power CPS against increasingly sophisticated threats, there is a pressing need for a unified defense approach that integrates both cyber and physical security mechanisms [152,153]. This section explores the importance of such an integrated approach, the role of advanced communication protocols and system architectures, and future trends in cross-domain security, particularly the integration of AI, Blockchain, and the Internet of Things (IoT).

 doi:10.20944/preprints202504.1907.v1

7.1. Need for Unified Cyber and Physical Security Approaches

Power CPS consist of two closely intertwined domains: the cyber domain, which involves data collection, processing, communication, and control; and the physical domain, which includes the actual power grid infrastructure such as power generation units, transmission lines, substations, and transformers [59,154]. Historically, cyber and physical security were treated as separate disciplines, each with its own set of protocols and protective measures. However, this approach has become increasingly inadequate due to the convergence of digital and physical systems, where vulnerabilities in one domain can have cascading effects on the other [155–157].

1) **Cyber-Physical Interaction and Vulnerabilities**: Modern power grids rely heavily on **real-time data** for decision-making, such as measurements of voltage, current, and power flows, which are transmitted across cyber networks to control centers. This data influences physical operations, such as load balancing, power distribution, and fault management. A cyber-attack that manipulates the data or disrupts the communication network can directly affect the physical operation of the grid, causing misoperations of circuit breakers, incorrect load shedding, or equipment overloads. Similarly, physical failures, such as equipment malfunctions or faults in power lines, can result in faulty data being sent to control systems, creating vulnerabilities that attackers can exploit [158].
   The integration of these two domains demands a unified defense strategy that can respond to threats across both cyber and physical layers. A comprehensive security framework must simultaneously protect the cyber infrastructure, such as communication channels and control systems, and the physical assets, such as transformers, generators, and power transmission lines. This unified approach helps ensure that security measures are synchronized, reducing the likelihood of gaps in protection and improving the overall resilience of the system [159].
2) **Challenges in Integration**: One of the key challenges in integrating cyber and physical security lies in the different nature of the threats faced by each domain. Cybersecurity threats often involve data manipulation, unauthorized access, and disruptions in communication, while physical security threats tend to involve equipment failures, physical damage, and operational malfunctions [160]. To address these challenges, a cross-domain defense strategy must facilitate seamless coordination between IT security experts, who focus on the cyber components, and engineers responsible for the physical infrastructure. Furthermore, the implementation of such an integrated defense strategy requires the development of standardized protocols, shared threat intelligence, and unified incident response mechanisms that bridge the gap between these traditionally distinct domains [161].

7.2. Role of Communication Protocols and System Architectures

Effective communication is a cornerstone of Power CPS, as data transmission between measurement devices, control systems, and monitoring centers is essential for real-time decision-making. As cyber threats evolve, the need for robust and secure communication protocols becomes critical in ensuring the resilience of power systems. Advanced communication protocols and system architectures play a key role in reducing vulnerabilities and strengthening the security posture of Power CPS [162].

1) **Secure Communication Protocols**: The integrity and confidentiality of data transmitted across power CPS are crucial for preventing cyber-attacks such as Man-in-the-Middle (MitM) attacks, where attackers intercept or alter data flowing between devices [163]. The adoption of end-to-end encryption protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL), ensures that data transmitted over networks remains confidential and untampered with. Additionally, Public Key Infrastructure (PKI) can be used for authentication and digital signatures, helping to verify the authenticity of devices and data sources within the power grid. More advanced quantum-safe encryption protocols are gaining attention as the development of quantum computing poses a potential threat to traditional encryption methods. Quantum-safe

 doi:10.20944/preprints202504.1907.v1

cryptographic algorithms, such as lattice-based and hash-based techniques, aim to future-proof communication protocols by making them resistant to attacks from quantum computers, which are expected to have the ability to break current encryption schemes.

2) **Resilient Communication Architectures**: Power systems depend on a vast network of interconnected devices, such as PMUs, RTUs, and smart meters, all of which communicate data to control systems. To ensure resilience in the face of cyber threats, it is essential to design robust communication architectures that can withstand attacks and continue to function under adverse conditions. Decentralized communication systems based on blockchain technology and peer-to-peer (P2P) networks are emerging as potential solutions to address single points of failure in centralized systems. These architectures provide greater security and fault tolerance by ensuring that data can be securely shared across multiple nodes, even if some parts of the network are compromised [164].

   Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) are also being explored to increase network flexibility and resilience. These technologies allow for the dynamic allocation of network resources, enabling better network monitoring, traffic management, and the ability to isolate and contain cyber threats as they emerge [165].

7.3. Future Trends in Cross-Domain Security

As the complexity of power CPS increases, so does the need for advanced security measures that can address the evolving threat landscape [166]. Future trends in cross-domain security suggest that integrating AI, Blockchain, and the IoT will play a central role in enhancing the resilience of power grids against both cyber and physical threats.

1) **AI**: AI techniques, particularly machine learning and deep learning, are already being integrated into various aspects of Power CPS security. AI can enhance threat detection by analyzing vast amounts of data from sensors and control systems in real-time, identifying anomalies, and predicting potential cyber-attacks or physical failures. Furthermore, AI can enable autonomous decision-making, where the system can respond to threats automatically without human intervention, reducing response times and mitigating potential damage [167].

   RL and adversarial AI are two promising areas of research for enhancing cyber-physical security. RL can be used to develop adaptive security protocols that learn from previous incidents and continuously improve the defense mechanisms. Adversarial AI can be used to simulate potential attack scenarios, allowing security systems to test their resilience and adapt to new attack strategies before they occur in the real world [168,169].

2) **Blockchain**: Blockchain technology offers a decentralized and tamper-proof method of recording transactions and data exchanges. In Power CPS, blockchain can be used to secure communication between devices, ensuring data integrity and preventing malicious alterations. By using blockchain for secure data logging, system operators can trace the origin of any data or control actions, providing a transparent and auditable record of grid operations. Additionally, smart contracts based on blockchain can automate decision-making processes, ensuring that predefined security protocols are automatically triggered when certain conditions are met, without requiring manual intervention [170,171].

   Blockchain also provides an effective solution for identity and access management (IAM), allowing for secure authentication and authorization of devices, users, and systems within the power grid. This can significantly reduce the risk of unauthorized access to critical infrastructure and mitigate the impact of cyber-attacks [172].

3) **IoT**: The growing deployment of IoT devices in power systems, such as smart meters, sensors, and connected machines, increases the amount of data available for real-time monitoring and decision-making. However, the proliferation of IoT devices also introduces new security risks, as these devices can become entry points for cyber-attacks. To address this, IoT security frameworks that integrate AI and blockchain technologies are being developed to secure the massive networks of interconnected devices [173].

 doi:10.20944/preprints202504.1907.v1

In the future, 5G networks and edge computing will further enhance IoT security by enabling ultra-fast communication and real-time data processing at the edge of the network, closer to the source of the data. This reduces latency, improves system responsiveness, and ensures that data from IoT devices is processed and analyzed securely in real time, without relying solely on central cloud infrastructure.

8. Future Directions in FDIA Research

The detection and mitigation of FDIAs in Power CPS is an evolving field, and ongoing research is essential to keep pace with the increasing complexity and sophistication of these attacks. As power grids become more interconnected and automated, the challenges associated with FDIA detection and defense continue to grow [174,175]. This section explores the future directions of FDIA research, identifying key research gaps, the role of emerging technologies such as federated learning, quantum computing, and the need for robust policy and regulatory frameworks to ensure the security of power CPS.

8.1. Identifying Research Gaps in Attack Models and Detection Methods

1) **Better Attack Models**: One of the primary research gaps in the field of FDIA is the need for more advanced and realistic attack models that reflect the complexities of modern power CPS. Existing models primarily focus on static or simplified representations of FDIA, which do not account for the dynamic and multi-phase nature of real-world attacks. More sophisticated models are needed that can capture the evolving tactics of attackers, the interactions between cyber and physical components, and the cascading effects of FDIAs across large-scale, distributed systems [176].
   Future research should focus on multi-stage attack models, where attacks evolve over time and space, exploiting vulnerabilities in both cyber and physical domains. Additionally, the integration of machine learning into attack modeling could help simulate different types of FDIAs, allowing researchers to understand attack dynamics better and identify potential vulnerabilities before they are exploited.
2) **Enhanced Detection Methods**: Although substantial progress has been made in FDIA detection, there remains a need for more accurate and efficient detection methods. Current detection systems often suffer from high false positive rates and low detection accuracy, especially when dealing with sophisticated, stealthy attacks. Future research should focus on developing adaptive detection methods that can respond to evolving attack strategies in real time [177].
   Combining deep learning and anomaly detection with existing model-based approaches could significantly enhance the detection of subtle attack patterns that are often missed by traditional methods. Moreover, real-time detection remains a challenge, as power systems are large, dynamic, and operate in highly distributed environments. Research should explore edge computing and distributed detection systems to enable real-time, localized attack detection across vast power grid networks.
3) **Efficient Defense Mechanisms**: Another key gap in FDIA research is the need for more efficient defense mechanisms that can prevent, mitigate, and recover from attacks. While traditional state estimation and data reconstruction techniques provide some defense, these methods often fail to address advanced or multi-stage FDIAs. Future research should aim to develop integrated defense systems that combine proactive and reactive measures, ensuring robust security even in the presence of sophisticated attacks [178].
   One promising direction is the development of adaptive defense protocols that dynamically adjust based on the type of attack detected. Additionally, the use of blockchain for securing data exchanges and AI-based resilience mechanisms for real-time attack mitigation could provide more comprehensive defense strategies. These systems could automatically adjust grid operations or trigger recovery processes without manual intervention, reducing response times and preventing further damage.

 doi:10.20944/preprints202504.1907.v1

8.2. Role of Federated Learning and Decentralized Approaches

1) **Federated Learning for Collaborative Defense**: Federated learning (FL) is an emerging technique that allows multiple systems or nodes to collaboratively learn a machine learning model without sharing sensitive data [39,179]. This approach could significantly improve the detection of FDIAs by enabling distributed detection across multiple grid nodes while maintaining privacy and data security. Since power CPS often operate in a decentralized manner with many geographically dispersed devices, FL provides an opportunity to create more robust and scalable detection systems.
   With federated learning, local detection models can be trained on data generated by sensors or control systems at individual grid nodes, and these models can then be aggregated to improve the global model [180,181]. This collaborative approach enables the grid to learn from local attack patterns, improving the overall system's ability to detect a wide range of FDIA strategies. Moreover, FL reduces the need to centralize sensitive data, mitigating the risk of data breaches and ensuring that private grid information remains protected [182–184].
2) **Decentralized Detection and Response**: The adoption of decentralized approaches in FDIA detection and mitigation holds great promise for future research. In a decentralized model, detection systems are distributed across multiple parts of the grid, allowing them to independently identify and respond to attacks. Decentralized systems reduce reliance on a central control center, making the grid more resilient to single points of failure and enabling quicker localized responses to FDIAs [185].
   Blockchain technology could play a key role in enabling secure, decentralized data exchange, enhancing the reliability and trustworthiness of information shared across the grid. By implementing a distributed ledger, blockchain ensures that all communication and data exchanges are secure, transparent, and tamper-proof, which can significantly improve the resilience of decentralized detection and mitigation systems [186].

8.3. Potential of Quantum Computing in FDIA Challenges

As power systems become more complex and cyber threats evolve, **quantum computing** and other emerging technologies offer exciting potential for addressing some of the challenges faced in FDIA detection and mitigation.

1) **Quantum Computing for Enhanced Detection and Security**: Quantum computing holds the promise of significantly enhancing the speed and accuracy of FDIA detection. Quantum algorithms are capable of solving certain computational problems exponentially faster than classical computers, making them highly suitable for real-time detection in large-scale, dynamic power systems. For example, quantum machine learning techniques could accelerate the training and inference processes of FDIA detection models, enabling them to handle the vast amounts of data generated by modern power grids [187]. Additionally, quantum cryptography techniques, such as quantum key distribution (QKD), could strengthen the security of communication channels within power CPS. QKD offers theoretically unbreakable encryption methods, providing a new level of protection against cyber-attacks that aim to intercept or manipulate data [188].
2) **Emerging Technologies for Threat Modeling**: In addition to quantum computing, other emerging technologies, such as edge computing and 5G networks, could significantly enhance the security and resilience of power CPS. Edge computing allows for processing and analyzing data closer to the source, reducing latency and improving real-time attack detection capabilities. This is particularly important in distributed power systems where localized decision-making is critical for preventing cascading failures. 5G networks offer higher bandwidth and lower latency, enabling faster data transmission and more efficient communication between devices within the power grid. The combination of edge computing and 5G networks could enable real-

 doi:10.20944/preprints202504.1907.v1

time, decentralized detection systems that operate autonomously at the edge of the network, reducing the time required to respond to potential FDIAs [189].

8.4. Policy and Regulatory Frameworks for Securing Power CPS

1) **Regulatory Standards for Cybersecurity**: As cyber threats to power systems grow, so does the need for comprehensive policy and regulatory frameworks to guide the security efforts of power grid operators and regulators. International standards, such as NIST Cybersecurity Framework and ISO/IEC 27001, provide guidelines for managing cybersecurity risks in critical infrastructure. Future regulatory frameworks must evolve to address the unique challenges of Power CPS, including the integration of IoT devices, the proliferation of renewable energy sources, and the increasing reliance on automated control systems [190,191].
2) **National and Global Cybersecurity Policies**: Policymakers need to establish national and international agreements for the collaborative defense of power CPS. These frameworks should encourage information sharing, standardized security protocols, and coordinated responses to cyber threats across borders. Governments should also incentivize private-sector investment in cybersecurity technologies and foster collaboration between utility providers, technology companies, and regulatory bodies [192].
3) **Cybersecurity Governance in Smart Grids**: Effective cybersecurity governance in smart grids requires the involvement of both technical experts and policymakers to ensure that security measures align with operational goals. Regulators should mandate regular security audits, threat assessments, and system resilience evaluations to ensure that power CPS are prepared for emerging threats. Furthermore, training and certification programs for grid operators, cybersecurity professionals, and system engineers should be prioritized to build expertise and ensure the readiness of the workforce in managing cybersecurity risks [193].

9. Conclusion

This review highlights significant advancements in False Data Injection Attack (FDIA) detection, defense, and resilience strategies in Power CPS. Research has progressed from basic state estimation methods to more sophisticated AI-based approaches, such as deep learning and ensemble methods, improving detection accuracy. Furthermore, hybrid techniques combining model-based and data-driven approaches have enhanced the system's ability to detect complex attacks.

Despite these advancements, gaps remain in attack modeling, detection accuracy, and the efficiency of defense mechanisms. The integration of emerging technologies, including federated learning, quantum computing, and IoT, promises to strengthen FDIA detection and resilience, while the implementation of multi-layered defense systems is crucial to address both cyber and physical security challenges. A unified approach that combines technical, regulatory, and operational solutions will be essential in ensuring the long-term stability and security of power CPS.

Looking forward, future research should focus on developing dynamic, multi-stage attack models and adaptive defense systems capable of responding in real-time. The integration of emerging technologies such as blockchain, AI, and quantum computing will play a pivotal role in the ongoing efforts to secure power grids against evolving cyber threats. Cross-domain collaboration among researchers, policymakers, and industry stakeholders will be key to developing comprehensive and effective security frameworks for power CPS.

References

1. Tooki O O, Popoola O M. A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems[J]. Renewable Energy Focus, 2024: 100628.

 doi:10.20944/preprints202504.1907.v1

2. Pourmadadkar M, Lezzi M, Corallo A. Cyber Security for Cyber-Physical Systems in Critical Infrastructures: Bibliometrics Analysis and Future Directions[J]. IEEE Transactions on Engineering Management, 2024, 71: 15405-15421.
3. Lin H, Slagell A, Kalbarczyk Z, et al. Runtime Semantic Security Analysis to Detect and Mitigate Control-Related Attacks in Power Grids[J]. IEEE Transactions on Smart Grid, 2016, 9(1): 163-178.
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. 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. 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. 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.
8. 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.
9. Alomari M A, Al-Andoli M N, Ghaleb M, et al. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions[J]. Energies, 2025, 18(1): 141.
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. 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. 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.
13. 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.
14. 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.
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. 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. 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. 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: 1-11.
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. 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.
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. 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. Tian J, Wang B, Li J, et al. Datadriven false data injection attacks against cyber-physical power systems[J]. Computers & Security, 2022, 121: 102836.
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.

 doi:10.20944/preprints202504.1907.v1

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. Manias D M, Saber A M, Radaideh M I, et al. Trends in Smart Grid Cyber-Physical Security: Components, Threats and Solutions[J]. IEEE Access, 2024.
27. Xin S, Guo Q, Sun H, et al. Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems[J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2375-2385.
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. Liu X, Wu Z. Research on Online Defense against Stealthy Data Injection Attacks in Smart Grids[J]. Proceedings of the CSEE, 2020, 40(8): 2546-2558.
30. Kumar R, Singh C, Raju Y, 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. Yu W, Xue Y, Luo J, et al. An UHV Grid Security and Stability Defense System: Considering the Risk of Power System Communication[J]. IEEE Transactions on Smart Grid, 2016, 7(1): 491-500.
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. 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. Liang J, Sankar L, Kosut O. Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation[J]. IEEE Transactions on Power Systems, 2016, 31(5): 3864-3872.
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. Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
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. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
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. Kaur U, Celik Z B, Voyles R M. Robust and energy efficient malware detection for robotic cyber-physical systems[C]//2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS). IEEE, 2022: 314-315.
46. Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attack Research for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
47. 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.

 doi:10.20944/preprints202504.1907.v1

48. Peng D, Dong J, Cai Z, et al. Stability Analysis of Information-Physical Fusion Systems under False Data Injection Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 196-205.
49. Zhang J, Chen J J, Peng K, et al. Multi-objective cost-effective optimization for defending against false data injection attacks in power system operation[J]. Electric Power Systems Research, 2021, 200: 107469.
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. Shen Y, Zhang W, Ni H, et al. Guaranteed Cost Control of Networked Control Systems with DoS Attack and Time-varying Delay[J]. International Journal of Control, Automation and Systems, 2019, 17(4): 811-821.
52. Liang Y, Wang Y, Liu K, et al. Fault Simulation of Distribution Grid CPS Considering Network Information Security[J]. Power System Technology, 2020, 45(1): 235-242.
53. Rawat D, Bajracharya C. Detection of False Data Injection Attacks in Smart Grid Communication Systems[J]. IEEE Signal Processing Letters, 2015, 22(10): 1652-1656.
54. Jokar P, Leung V. Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids[J]. IEEE Transactions on Smart Grid, 2018: 9(3): 1800-1811.
55. Wang Z, Chen Y, Zeng J, et al. Modeling and Reliability Assessment of Microgrid Cyber-Physical Systems for Fully Distributed Control[J]. Power System Technology, 2019, 43(7): 2413-2421.
56. Liang Z, Hong C, Yang Y, et al. Construction and Application of Cyber Attack Simulation Platform for Power Systems[C]//2024 IEEE PES 16th Asia-Pacific Power and Energy Engineering Conference (APPEEC). IEEE, 2024: 1-5.
57. Shi J, Chen B, Yu L. Hidden FDIA Detection Based on Laplacian Eigenmap Learning[J]. Acta Automatica Sinica, 2021, 47(10): 2494-2500.
58. Jin Z, Liu Y, Diao J, et al. Covert False Data Injection Attacks on Remote State Estimation in Cyber-Physical Systems[J]. Acta Automatica Sinica, 2025, 51(2): 1-10.
59. 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.
60. 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.
61. Liu S, Tan Y, Zhao F, et al. Coupled Modeling Method for Power Information Systems[J]. Journal of Power Systems and Automation, 2021, 33(3): 89-93.
62. Pan K, Teixeira A, Cvetkovic M, et al. Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 3044-3056.
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. 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. Yi N, Xu J, Chen Y, et al. Multi-Stage Cyber-Physical Collaborative Topology Attack Method Based on Deep Reinforcement Learning[J]. Electric Power Engineering Technology, 2023, 42(4): 149-158.
66. 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.
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. 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. Cai X, Wang Q, Huang J, et al. Dual-Layer Cyber-Physical Collaborative Emergency Control Method for Power System Network Attacks[J]. Global Energy Interconnection, 2020, 3(6): 560-568.
70. Wang Y, Lin Z, Liang X, et al. On modeling of electrical cyber-physical systems considering cyber security[J]. Frontiers of Information Technology & Electronic Engineering, 2016, 17(5): 465-478.
71. Wu L, Sun K, Chen K, et al. Detection of False Data Attacks in Power Systems Based on CNN-LSSVM[J]. Zhejiang Electric Power, 2024, 43(11): 90.

 doi:10.20944/preprints202504.1907.v1

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. Zhu W, Tang Y, Wei X, et al. Defense Methods Against Adversarial Attacks on Data-Driven Algorithms in Power CPS[J]. Electric Power, 2024, 57(9):32-40.
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. Wang J, Li Y, Xu T. False Data Detection in Smart Grids Based on Extended Kalman Filtering[J]. Smart Power, 2022, 50(3): 50-56.
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. Mohammadpourfard M, Sami A, Seifi A. A statistical unsupervised method against false data injection attacks: A visualization-based approach. Expert Systems With Applications[J]. 2017, 84: 242-261.
78. Wu T, Xue W, Wang H, et al. Extreme Learning Machine-Based State Reconstruction for Automatic Attack Filtering in Cyber Physical Power System[J]. IEEE Transactions on Industrial Informatics, 2021, 17(3): 1892-1904.
79. Wang Z, Chen Y, Liu F, et al. Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning[J]. IEEE Access, 2018, 6: 48785-48796.
80. Chen Y, Huang S, Liu F, et al. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2158-2169.
81. Liu Y, Wang Y. Evolution Mechanism and Active Defense Exploration of Cross-Domain Cascading Failures in New Power Systems[J]. Electric Power, 2022, 55(2): 62-72+81.
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. Hasan M K, et al. A Review on Machine Learning Techniques for Secured Cyber-Physical Systems in Smart Grid Networks[J]. Energy Reports, 2024, 11: 1268-1290.
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. 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. Susuki Y, Koo T, Ebina H, et al. A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance[J]. Proceedings of the IEEE, 2012, 100(1): 225-239.
87. Aluko A, Carpanen R, Dorrell D, et al. Vulnerability Analysis of False Data Injection Attacks on the Frequency Stability of Isolated Microgrids[C]// 2021 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA), 27-29 January 2021, Potchefstroom, South Africa: 1-6.
88. Liu X, Li Z, Shuai Z, et al. Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 1023-1025.
89. Wei L, Zhang Q. Detection of False Data Attacks in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
90. Fu J, Hu B, Xie K, et al. Power System Generation-Transmission Expansion Stochastic Programming for Coordinated Attacks[J]. Automation of Electric Power Systems, 2021, 45(2): 21-29.
91. Sanjab A, Saad W. Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.
92. Chin W, Lee C, Jiang T. Blind False Data Attacks Against AC State Estimation Based on Geometric Approach in Smart Grid Communications[J]. IEEE Transactions on Smart Grid, 2018, 9(6): 6298-6306.
93. 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.
94. 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.

 doi:10.20944/preprints202504.1907.v1

95. Zhu B, Guo Y, Guo C, et al. A Review of Security Assessment and Defense for Power Cyber-Physical Systems Under Information Failure Threats[J]. Power System Protection and Control, 2021, 49(1): 178-187.
96. Zhang Y, Wang L, Xiang Y. Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems[J]. IEEE Transactions on Smart Grid, 2016, 7(2): 669-683.
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. 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. Deng R, Zhuang P, Liang H. CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2420-2430.
100. Jiang X, Zhang J, Harding B, et al. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units[J]. IEEE Transactions on Power Systems, 2013, 28(3): 3253-3262.
101. Risbud P, Gatsis N, Taha A. Vulnerability Analysis of Smart Grids to GPS Spoofing[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.
102. Barreto S, Pignati M, Dán G, et al. Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 3530-3542.
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. Yin H, Liu D, Chen G, et al. Collaborative Network Attack Model and Cross-Space Fault Propagation Mechanism for Virtual Power Plants[J]. Automation of Electric Power Systems, 2023, 47(8): 34-43.
105. Haider M Z, Mali P, Rahman M A, et al. Impact Analysis of False Data Injection Attacks on Automatic Voltage Regulators of Synchronous Generators[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
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. Yang T, Xu Z, Zhao Y, et al. A Review of Attacks and Defense Methods for Digitalized New Power Systems[J]. Automation of Electric Power Systems, 2024, 48(6): 112-126.
108. Ali M, Sun W. Securing Critical Infrastructures: Restoration from Cyber-Physical Attacks in Active Distribution Grids[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
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. He Z, Gao S, Wei X, et al. Research on Attack-Defense Game Model of False Topology Attacks with Branch and Protection Coordination[J]. Power System Technology, 2022, 46(11): 4346-4355.
111. Li X, Yi L, Liu C, et al. Data-Driven Detection of False Data Injection Attacks in Power Systems[J]. Smart Power, 2023, 51(2): 30-37.
112. Weng P, Chen B, Yu L. Fusion Estimation of False Data Injection Attack Signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.
113. Arafat M, Hoque S, Farid D. Cluster-based Under-sampling with Random Forest for Multi-Class Imbalanced Classification[C]// 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 06-08 December 2017, Malabe, Sri Lanka: 1-6.
114. 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.
115. Jain H, Kumar M, Joshi A M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection[J]. Electrical Engineering, 2022, 104(1): 331-346.
116. 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.

 doi:10.20944/preprints202504.1907.v1

117. Long X, Ding Y, et al. Privacy-Preserving Graph Inference Network for Multi-Entity Wind Power Forecast: A Federated Learning Approach[J]. IEEE Transactions on Network Science and Engineering, 2025. DOI: 10.1109/TNSE.2025.3547227
118. Miao B, Wang H, Liu Y J, et al. Adaptive security control against false data injection attacks in cyber-physical systems[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2023, 13(3): 743-751.
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. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
121. Fan X Y, Lin W J. Reachable Set Control for Cyber-Physical Systems with False Data Injection Attacks[C]//2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS). IEEE, 2023: 1-5.
122. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
123. Chen H, Li T, Fan X, et al. Feature selection for imbalanced data based on neighborhood rough sets[J]. Information Sciences, 2019, 483: 1-20.
124. Li J, Li X M, Cheng Z, et al. Event-based secure control for cyber-physical systems against false data injection attacks[J]. Information Sciences, 2024, 679: 121093.
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. Hu Z, Wang Y, Tian X, et al. False Data Injection Attacks Identification for Smart Grids[C]// 2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 29 April 2015-01 May 2015, Beirut, Lebanon: 139-143.
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. 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. 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. Wang D, Guan X, Liu T, et al. Extended Distributed State Estimation: A Detection Method against Tolerable False Data Injection Attacks in Smart Grids[J]. Energies, 2014, 7(3): 1517-1538.
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. Costilla-Enriquez N, Weng Y. Attack power system state estimation by implicitly learning the underlying models[J]. IEEE Transactions on Smart Grid, 2022, 14(1): 649-662.
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. 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. 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. Alsharif G O, Anagnostopoulos C, Marnerides A K. Energy Market Manipulation via False-Data Injection Attacks[J]. IEEE Access, 2025.
137. Guibene K, Messai N, Ayaida M, et al. A data mining-based intrusion detection system for cyber physical power systems[C]//Proceedings of the 18th ACM International Symposium on QoS and Security for Wireless and Mobile Networks. 2022: 55-62.
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.

 doi:10.20944/preprints202504.1907.v1

139. Bonagura V, Panzieri S, Pascucci F, et al. Strategic interaction over age of incorrect information for false data injection in cyber-physical systems[J]. IEEE Transactions on Control of Network Systems, 2024.
140. Zideh M J, Khalghani M R, Solanki S K. An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids[J]. Electric Power Systems Research, 2024, 232: 110407.
141. Hallaji E, Razavi-Far R, Wang M, et al. A stream learning approach for real-time identification of false data injection attacks in cyber-physical power systems[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3934-3945.
142. Fan X, Du L, Duan D. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.
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. Khalid H, Peng J. A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2026-2037.
145. Mosaad N, Abdel-Rahim O, Rahouma W, et al. Identification and Alleviation of False Data Injection within the Cyber Layer of an Enhanced Distributed Secondary Control in DC Islanded Microgrids[J]. IEEE Access, 2025.
146. Lydia M, Prem Kumar G E, Selvakumar A I. Securing the cyber-physical system: A review[J]. Cyber-Physical Systems, 2023, 9(3): 193-223.
147. Zhu S, Chen J. Security metrics and tradeoff of cyber-physical systems subject to false data injection attacks[C]//3rd International Conference on Control Theory and Applications (ICoCTA 2023). IET, 2023, 2023: 141-145.
148. Zhang D, Shi P, Lim C P, et al. Resilient Tracking Control of Cyber-Physical Systems against False Data Injection Attacks and Obstacle Avoidance[J]. IEEE Transactions on Automation Science and Engineering, 2025.
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. 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. Farraj A, Hammad E, Kundur D. A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability[J]. IEEE Transactions on Signal and Information Processing over Networks, 2018, 4(1): 70-81.
152. Chlela M, Mascarella D, Joós G. Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4702-4711.
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. Sun C, Liu D, Li Q. Study on Dynamic Power Flow in Active Distribution Networks Integrated with Cyber-Physical Systems[J]. Proceedings of the CSEE, 2016, 36(6): 1509-1516.
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. Yin Z, Zhang K, Du H, et al. Event-Driven Modeling of Cyber-Physical Systems[J]. Microelectronics & Computer, 2015, 32(12): 126-129.
157. Makedon F, Le Z, Huang H, et al. An event driven framework for assistive CPS environments[J]. ACM Sigbed Review, 2009, 6(2): 1-9.
158. Guibene K, Messai N, Ayaida M, et al. False data injection attack against cyber-physical systems protected by a watermark[C]//GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022: 01-06.
159. Havlíková M, Jirgl M. Reliability Analysis in Man-Machine Systems[C]// 14th International Carpathian Control Conference (ICCC), 26-29 May 2013, Rytro, Poland: 111-116.
160. Chen J, Wang Q, Tang Y, et al. Anomaly Detection Method for Power Cyber-Physical Systems Considering Bilateral Characteristics[J]. Power System Technology, 2022, 46(6): 2339-2348.

 doi:10.20944/preprints202504.1907.v1

161. Fu Y, Chen L, Ma Z, et al. Preventive Control of Power Systems Including Data-Driven Stability Constraints[J]. Proceedings of the CSEE, 2022, 42(15): 5417-5430.
162. Shahriar M H, Rahman M A, Haque N I, et al. DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems[C]//2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2021: 725-734.
163. Ghaderi M, Gheitasi K, Lucia W. A Blended Active Detection Strategy for False Data Injection Attacks in Cyber-Physical Systems[J]. IEEE Transactions on Control of Network Systems, 2021, 8(1): 168-176.
164. Asghari M, Ameli A, Ghafouri M, et al. Optimal Data Aggregation Reconfiguration Scheme to Mitigate Stealthy False Data Injection Attacks in Energy Management Systems[J]. IEEE Transactions on Smart Grid, 2025.
165. Abou El Houda Z, Senhaji Hafid A, Khoukhi L. A novel unsupervised learning method for intrusion detection in software-defined networks[M]//Computational Intelligence in Recent Communication Networks. Cham: Springer International Publishing, 2021: 103-117.
166. Pruengkarn R. Enhancing classification performance by handling noise and imbalanced data with fuzzy classification techniques[D]. Perth, Australia: Murdoch University, 2018.
167. Cui 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: 1-12. DOI: 10.17775/CSEEJPES.2023.05120.
168. Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.
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. 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.
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. Mansour R F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment[J]. Scientific Reports, 2022, 12(1): 12937.
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. 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. 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. Zhong X, xin Li G, Zhng C. False data injection in power smart grid and identification of the most vulnerable bus; a case study 14 IEEE bus network[J]. Energy Reports, 2021, 7: 8476-8484.
177. BaSin D, Cremers C, Kim T, et al. Design, Analysis, and Implementation of ARPKI: an Attack-Resilient Public-Key Infrastructure[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(3): 393-408.
178. Yan K, Liu X, Lu Y, et al. A cyber-physical power system risk assessment model against cyberattacks[J]. IEEE Systems Journal, 2022, 17(2): 2018-2028.
179. Kesici M, Pal B, Yang G. Detection of false data injection attacks in distribution networks: A vertical federated learning approach[J]. IEEE Transactions on Smart Grid, 2024.
180. 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.
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.

 doi:10.20944/preprints202504.1907.v1

182. Keçeci C, Davis K R, Serpedin E. Federated learning based distributed localization of false data injection attacks on smart grids[J]. arXiv preprint arXiv:2306.10420, 2023.
183. 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.
184. 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.
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. 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. 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.
188. Meng J, Hu J, Shi X, et al. Quantum Distributed Event-Triggered Frequency Control for AC Microgrids Under FDIAs[J]. IEEE Transactions on Smart Grid, 2024.
189. Devi K V R, Koithyar A, Lakhanpal S, et al. Edge Computing and 5G Integration for Real-time Analytics in Interoperable Smart Grids[C]//2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC). IEEE, 2023: 419-424.
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. 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. Khalaf M, Ayad A, Kundur D. Protection of power system state estimation against false data injection attacks[C]//2023 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2023: 387-392.
193. Hu P, Li L. A Review of Cyber-Physical Security in Smart Grids[J]. Information Security Research, 2019, 5(12): 1068.