electronics

MDPI

Review

The Information Security Issues of Distributed Economic Dispatch for New Generation Power Systems—Present Situation and Forecast

Jian Le, **Hongke Lang ***, **Jing Wang**, **Weihao Wang** and **Guangyi Luo**

School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China; lej01@tsinghua.org.cn (J.L.)
* Correspondence: langhk@whu.edu.cn

Abstract: With the large scale and high proportion of distributed generation connected to the power grid, the distributed economic dispatch system has attracted more attention because of its significant advantages. However, the distributed economic dispatch system faces more serious information security issues due to the variation of communication topology. Therefore, the purpose of this paper is to review the information security issues that may occur in the distributed economic dispatch system and the defense measures. By summarizing the existing literature on information security issues and defense measures, it can be found that the current research focuses on the cyber-side defense for information security, and lacks consideration of the cyber-physical coupling characteristics. Additionally, the separate cyber-side defense measures still have a defense blind spot and cannot respond in a timely manner to the physical-side actions caused by information security issues. Finally, the establishment of the information security issues model and the construction of the integrated security defense system are discussed from the perspective of the power cyber-physical system. This research will be helpful in the construction of the security defense system for information issues in distributed economic dispatch systems.

Keywords: power cyber-physical system; distributed economic dispatch; information security; external cyber-attack; internal malicious behavior

check for updates

Citation: Le, J.; Lang, H.; Wang, J.; Wang, W.; Luo, G. The Information Security Issues of Distributed Economic Dispatch for New Generation Power Systems—Present Situation and Forecast. *Electronics* **2024**, *13*, 2680. https://doi.org/10.3390/electronics13142680

Academic Editor: Ahmed Abu-Siada

Received: 13 June 2024
Revised: 2 July 2024
Accepted: 6 July 2024
Published: 9 July 2024

1. Introduction

The new generation power system takes wind, solar, and other new energies as mainstays while fossil fuels will serve as supplements, and the proportion of new energy sources is gradually increasing. Meanwhile, smart meters, distributed generation inverters, and other intelligent terminals will be widely integrated into the new generation power system. These characteristics contribute to promoting the cleanliness, flexibility, digitization, and intelligence of the power system [1]. A large number of geographically dispersed distributed generations (DGs), such as photovoltaic, wind power and energy storage, access the power system [2]. Therefore, it is crucial to design an efficient economic dispatch strategy. Under the premise of satisfying the system power quality and safe operation, the active power among each DG is rationally distributed to minimize the economic cost of system operation.

Depending on the structure, the economic dispatch system can be divided into the centralized model and the distributed model. The centralized economic dispatch system has advantages such as simplicity and efficient operation. When the number of DGs is larger, the centralized economic dispatch system has poor reliability and robustness, high construction and maintenance costs, heavy computational burden on the dispatch center, and the inability to meet the "plug-and-play" needs for DGs. Therefore, the requirements of stable control and optimized operation of the system can no longer be met [3,4]. Compared with the centralized economic dispatch system, the distributed economic dispatch system has the characteristics of decentralization, higher reliability and scalability, smaller communication burden, and greater robustness and privacy. The DGs in the distributed economic dispatch system can make decisions independently, perform necessary information interaction with others through the communication network, and cooperate with each other to complete the economic dispatch task. In the distributed economic dispatch system, the topology of the communication network changes from the star shape in the centralized mode to an arbitrary connected graph. Intelligent agents cooperate with each other to complete the tasks of information collection, processing, computation, and decision [5,6].

Although the distributed economic dispatch system has many of the advantages described above, the large scale and complexity of the system make it imperative to consider security issues. Currently there are two new types of security issues in the distributed economic dispatch system, namely cyber-attacks conducted by attackers external to the system and malicious behaviors initiated by internal members of the system. First of all, the local communication network topology of the distributed economic dispatch system is no longer a single star topology, and its variation provides wider space conditions for the implementation of cyber-attacks from the external environment [7,8]. At the same time, the solution of distributed economic dispatch problems usually needs to be completed through an iterative process, which provides wider time conditions for attackers to implement cyber-attacks. Once one or more nodes in the system suffer from cyber-attacks, the false information will quickly spread to all nodes, preventing the distributed economic dispatch system from running in the optimal state, and even causing system instability. In addition, the prerequisite for the successful implementation of distributed economic dispatch is that each participant is "honest" and trusts and cooperates with each other. However, each individual involved in the power system economic dispatch has independent control and decision-making power in the distributed mode. Therefore, a small number of individuals may carry out malicious behaviors to gain more economic benefits, which destroys the optimal operating state of the system and damages the overall economic benefits of the system [9].

If there is no security protection mechanism in the system, it may fail to achieve the goal of economic dispatch, result in data loss and heavy economic losses, and even cause system instability due to cyber-attacks or malicious behaviors. Therefore, based on collecting and summarizing the existing literature and research, this paper comprehensively reviews information security issues in distributed economic dispatch. It covers the types, hazards, and preventive measures of information security issues, and suggests areas for future research. The work of this paper will provide some guidance for the subsequent design of the distributed integrated security and economic dispatch strategy of the new generation power system.

The structure of this paper is as follows: In Section 2, two typical information security issues, namely external cyber-attacks and internal malicious behavior, are introduced and qualitatively evaluated. Furthermore, the countermeasures of external cyber-attacks and internal malicious behaviors are summarized in Sections 3 and 4, respectively. Finally, based on the current research situation, the model building of information issues and the security defense system are discussed in Section 5.

2. Information Security Issues in Distributed Economic Dispatch Systems

The three elements of power system information security objectives are confidentiality, integrity, and availability, or "CIA" for short [10]. From the perspective of breaking or violating the three elements of security, the information security issues of economic dispatch in the new generation power system will arise from both internal and external sources of the system [11]. Figure 1 shows the information security issues of the distributed economic dispatch system. Data acquisition equipment, mainly using phasor measurement units (PMUs), collects voltage and current data from the power distribution network and DGs, calculates active and reactive power, and uploads the data to communication networks. Based on the uploaded power and other data information, the designed distributed economic dispatch strategy calculates output commands for DGs and adjusts their output through control equipment. Similar to existing cyber-physical systems (CPSs), the external information security concerns mainly arise from a series of attacks targeting communication networks and PMUs. Furthermore, the internal information security issues are specific to distributed economic dispatch systems and are caused by the malicious behavior of selfish nodes within the system.

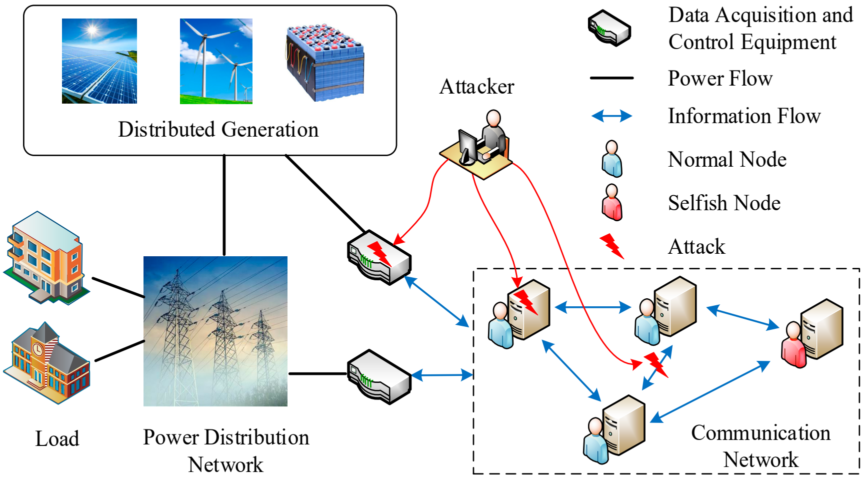


Figure 1. Information security issues of the distributed economic dispatch system.

2.1. *External Cyber-Attacks*

External network attacks mainly target physical equipment and communication networks. As a crucial piece of data acquisition equipment, PMU data directly impact the operational effectiveness of system monitoring, early warning, protection, and dispatch control. Cyber-attacks causing abnormal PMU data include false data injection (FDI) attack and time synchronization (TS) attack [12]. According to the different means of attack on communication networks, the attacks can be divided into information attacks and communication attacks. Information attacks are usually implemented on the cyber side to manipulate the transmitted information, and for FDI attack and replay attack [13,14]. Communication attacks usually target communication links or channels to disrupt communication to affect system information interaction, and the denial of service (DoS) attack is the most important type of communication attack.

2.1.1. TS Attack

PMUs digitize voltage and current sampled signals from voltage transformers and current transformers using analog-to-digital converters [15,16]. These signals are processed by phasor computation modules and synchronized with GPS to generate phasor measurement data with timestamps. PMUs synchronize time using civilian GPS, which does not require authentication, making them vulnerable to a GPS spoofing attack, also known as a TS attack. The attacker first emits interference signals to disrupt GPS receivers, preventing them from receiving accurate GPS information. They then spoof incorrect GPS signals to the receivers, altering the time signal of PMUs and introducing errors in phase angle measurements. Synchronized measurement data under TS attack can be represented as follows [12]:

$$z_t^{\mathrm{TS}} = e^{j\Delta\theta_t} z_t \tag{1}$$

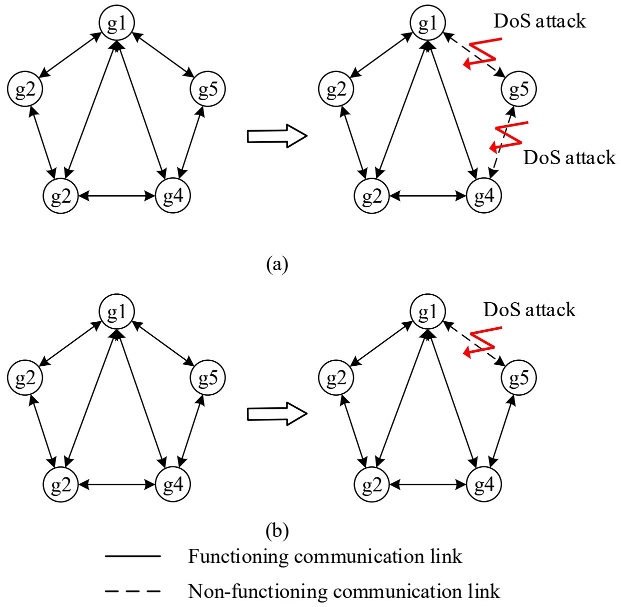
$$\Delta\theta_t = 2\pi f \Delta t_{att} \tag{2}$$

where z_t is the normal phasor measurement data at time t for the PMU; z_t^{TS} is the phasor measurement data for the PMU at time t under TS attack; $\Delta\theta_t$ represents the phase shift caused by the TS attack at time t for the PMU; Δt_{att} represents the time deviation caused by the TS attack at time t for the PMU; f is the frequency of the power system.

The phase shift caused by a TS attack directly alters measurements such as active power, which affects the decisions in distributed economic dispatch and increases the operating costs of the power system. Furthermore, measurement data under TS attack may affect system state estimation and dispatch controls, potentially leading to cascading failures or widespread blackout incidents. TS attack can compromise data integrity without physical network access, and current GPS receivers have difficulty detecting false GPS signals [17–19].

2.1.2. DoS Attack

In a DoS attack, the attacker sends a large number of invalid messages to the neighboring nodes to block the communication link and disrupt the normal transmission of information in the communication network. The effect of a DoS attack on a communication network is equivalent to the loss of data packets, which results in the failure of information transmission between nodes. The communication link with data packet loss can be considered as disconnected, so the topology of a communication network subjected to DoS attack is changed from a fixed topology to a time-varying one [20,21]. Due to the randomness of DoS attack, the attack may occur at any communication time and on any communication link. The communication topology of the system after a DoS attack will have two types, as shown in Figure 2 [22].


g1
g2
g5
g2
g4
DoS attack
DoS attack
Functioning communication link
Non-functioning communication link

(a)

(b)

Figure 2. Influence of the DoS attack on the communication network topology. (**a**) Unconnected graph; (**b**) connected graph.

In Figure 2a, the attacker concentrates resources to block all the communication links of a node so that it cannot communicate normally with its neighboring nodes. The node is isolated in the communication network, and the system communication network topology becomes an unconnected graph. In Figure 2b, the attacker performs information blocking only on one or more communication links of a node. However, the node still maintains communication with some of its neighbors and the system communication network topology remains connected.

2.1.3. FDI Attack

In an FDI attack, the attacker injects predetermined false data into PMU measurement data [23] or communication data in communication networks [24], thereby compromising data integrity and authenticity. The system makes dispatch decisions based on PMU measurement data and communication data. Therefore, the false data directly affect the dispatch or state estimation of the system, leading to deviations from the economically optimal state. This will result in increased operational costs or economic losses and may even lead to serious power incidents.

A stealthy attack is a common well-coordinated and designed malicious FDI attack [25], whose attack signals can bypass protection mechanisms such as bad data detection without triggering alarms. Furthermore, it will usually cause the system to operate in a non-optimal state, resulting in economic losses. Stealthy attacks can be categorized into offline and online forms [26]. The former injects false data into the consensus formation process of distributed algorithms, which usually does not destroy the convergence of the algorithms. However, it will lead to the imbalance of supply and demand power and the decrease in the consensus efficiency of distributed algorithms, and will also cause the distributed system to deviate from the optimal operating point. The latter injects false data into the cost parameters of power generation, which can increase the operating cost of the power system while maintaining the balance of supply and demand power.

2.1.4. Replay Attack

A replay attack compromises data integrity by maliciously intercepting and then retransmitting data [27]. In a replay attack, the attacker first intercepts and records the normal transmission data and then selects some of the normal data to transmit to the neighbor nodes in the form of data duplication or data delay [28]. A replay attack allows the attacker to obtain the system data so as to grasp the system operation status, which destroys the closure of the system. In addition, a replay attack will cause some nodes to receive incorrect information, which will degrade the system performance and even cause a loss of stability.

2.2. Internal Malicious Behaviors

The internal information security issues of distributed economic dispatch systems arise from the malicious behaviors of some nodes participating in economic dispatch to gain more economic benefits, and can be categorized into deception behavior and fraud behavior.

2.2.1. Deception Behavior

Deception behavior is similar to external deception attack, but performed by selfish nodes within the system. Depending on the scale, the deception behavior can be performed by a single individual [29] or by multiple cooperating individuals [30]. In single individual deception, a single selfish node injects random data to interfere with the distributed algorithm. The node sends misleading messages to the neighbor nodes to influence the consensus process of the distributed system, and affects the operation of the system to converge to the desired target value of the selfish node. Therefore, single individual deception destroys the optimal economic operation of the system and benefits the selfish node. In multi-individual cooperative deception, multiple selfish nodes cooperate to launch deception behaviors to their neighboring nodes, dragging all the common nodes to the operating state of the selfish nodes, causing greater economic losses in the system.

2.2.2. Fraud Behavior

Fraud behavior is the behavior of selfish nodes that participate in distributed algorithms by falsely modifying their information to gain benefits. Depending on the modification of the selfish node's information, the fraud behavior can be classified into constraint fraud behavior [31] and cost fraud behavior [32]. In constraint fraud behavior, selfish nodes use false constraints when their neighbor nodes participate in the distributed algorithm, and the rest of the nodes optimize their objective function by considering their original constraints. The selfish nodes use false constraints to make the system to run in their own profitable operating state by reducing their own cost function. Cost fraud behavior is a false modification of the true cost function by the selfish nodes, resulting in a coordination process that is more favorable to their self-interest.

Overall, internal malicious behaviors are implemented by internal selfish nodes to improve their own economic interests. Therefore, the behaviors only decrease the overall economic efficiency of the system and generally do not affect other aspects of system performance.

2.3. Impact Assessment of Information Security Issues

Based on the above analysis, Table 1 synthesizes the characteristics of various types of information security issues in distributed economic dispatch systems.

Table 1. Characteristics of the information security issues.

Information Security Issues	Type	Means	Purpose
External cyber-attack	TS attack	Tampering with data timestamps	Destroying information integrity
	DoS attack	Communication interruption	Disrupting communication availability
	FDI attack	Injecting false data	Destroying information integrity
	Replay attack	Tampering with real-time data	Destroying information integrity
Internal malicious behavior	Deception behavior	Injecting false data	Undermining system economy
	Fraud behavior	Tampering with one's own information	Undermining system economy

This paper qualitatively evaluates the impact of external attacks using six indicators: communication availability, information integrity, data confidentiality, system economy, destructiveness, and stealthiness of the attack, as shown in Figure 3. A TS attack is extremely stealthy and destroys data integrity by spoofing incorrect GPS signals to the GPS receivers in PMUs and tampering with timestamps. A DoS attack affects the information communication by disrupting the communication channel, causing certain damage and economic loss to the system. An FDI attack in deception attacks has a high degree of stealthiness and destructiveness by intercepting the communication information and injecting false information, causing the system to operate in non-optimal conditions, and resulting in economic loss to the system. A replay attack in deception attacks also has a high degree of stealth and attacks in real time through the means of communication data duplication or delay, resulting in the degradation of the system performance and a certain amount of economic loss.

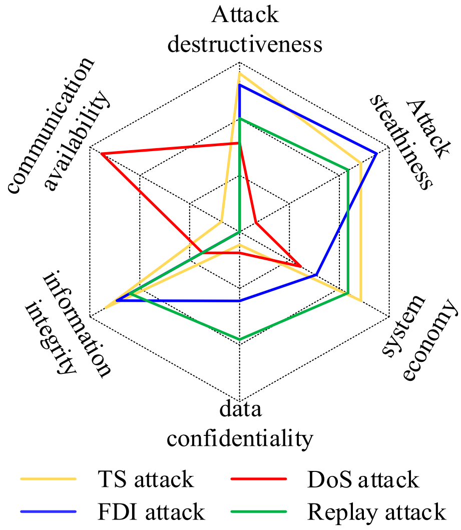


Figure 3. Evaluation of external cyber-attacks.

Internal malicious behaviors, which are dishonest behaviors performed by internal malicious nodes in order to improve their own economic interests, only reduce the overall economic benefit of the system and do not cause any other impact.

3. Countermeasures for External Cyber-Attack

In this paper, the strategies to respond to external cyber-attacks on the system are categorized into pre-attack prevention, detection during the attack, and suppression during the attack, which can be analyzed according to the different defense stages [33].

3.1. Pre-Attack Prevention

Some of the more researched pre-attack prevention methods include communication authentication, data encryption, and secure communication mechanisms based on emerging technologies, as shown in Figure 4.

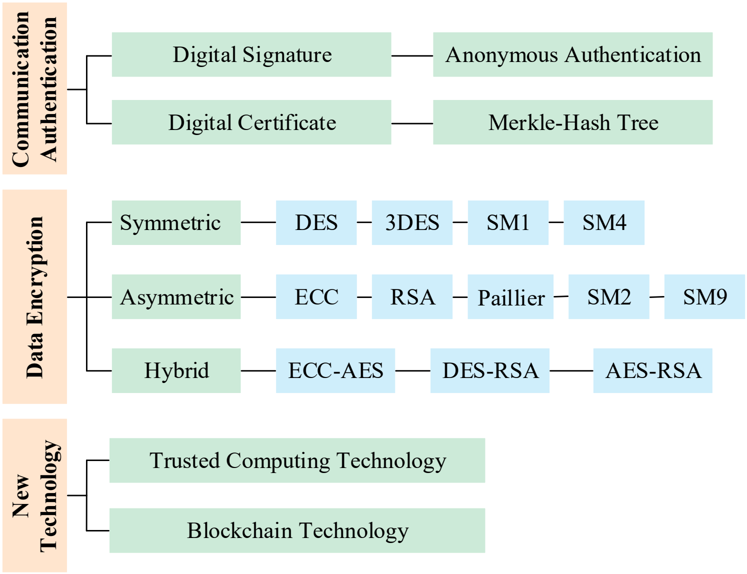


Figure 4. Pre-attack prevention methods for external cyber-attacks.

Communication authentication: Communication authentication verifies the identity of the communicating parties and confirms whether the communication information is complete or modified. At present, digital signature technology [34,35], digital certificates [36], and anonymous authentication technology [37] are widely used, which can effectively prevent many types of attacks. In addition, communication authentication based on the hash tree has also been promoted and applied. Ref. [38] proposes an authentication scheme based on the Merkle hash tree, which has low operational cost and computational complexity, and can effectively defend against FDI attack and replay attack. Ref. [39] proposed a trusted sensing foundation based on hash message authentication, encrypting measurement data in PMUs to effectively prevent attackers from conducting an FDI attack.

Data encryption: In order to ensure the integrity and confidentiality of data, information is usually encrypted by specific means before it is transmitted. Currently, there are two main types of encryption algorithms: symmetric encryption algorithms and asymmetric encryption algorithms. The former is single key encryption, which means that the same key is used for both the encryption process and the decryption process. The commonly used symmetric encryption algorithms are the data encryption standard (DES) [40], the triple data encryption standard (3DES) [41], the advanced encryption standard (AES) [42], and cryptography algorithms SM1 and SM4 formulated by China's National Commercial Cryptography Management Office. The asymmetric encryption algorithms are public key encryptions, where the public key and secret key exist in pairs; the public key is publicly released and the secret key is held by the user. Asymmetric encryption algorithms include elliptic curve cryptography (ECC) [43,44], Rivest–Shamir–Adleman (RSA) [45], the Paillier cryptosystem [46], and cryptography algorithms SM2 and SM9 formulated by China's National Commercial Cryptography Management Office. In addition, in order to improve the speed of communication encryption and decryption while ensuring the security of communication information, researchers have started to try to combine multiple encryption algorithms to improve the performance, such as ECC-AES encryption algorithms [47], improved DES-RSA hybrid encryption algorithms [48], and AES-RSA hybrid [49] encryption algorithms.

Secure communication mechanisms based on new technologies: In addition to communication authentication and data encryption, two traditional means to prevent external attacks, new information security technologies represented by trusted computing technology [50] and blockchain technology [51], are also gradually applied to prevent information attacks in power systems. Based on trusted computing technology, the trusted communication channel is established between communication nodes to achieve trusted identity authentication of the communication nodes, which can ensure the integrity and trustworthiness of communication data and prevent tampering by cyber-attackers [52]. Blockchain technology has the characteristics of decentralization, data security and trustworthiness, non-tampering, and programmability, which can provide reliable technical support for power system communication [53].

3.2. Detection during Attack

According to the different operation mechanisms, the more researched and applied attack detection methods mainly include signature-based detection, anomaly-based detection, and hybrid detection [54,55], as shown in Figure 5.

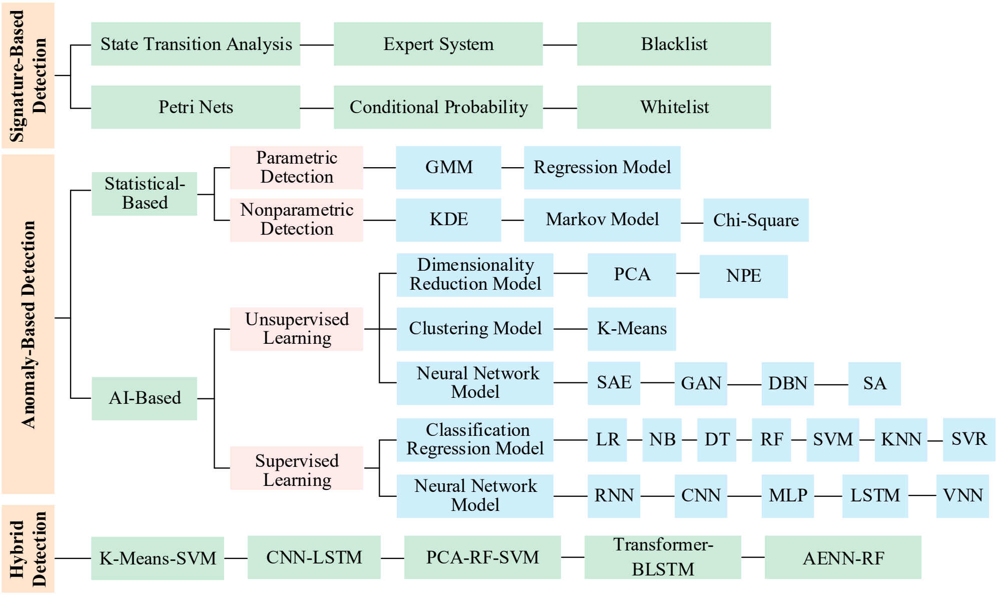


Figure 5. Detection methods for external cyber-attacks.

3.2.1. Signature-Based Detection

This type of detection is mainly applied to known or previously experienced attack methods and attack types. It is usually necessary to first build a database of attack behavior signatures, and then compare the real-time data with the signature database to detect attacks. Currently, the main attack detection methods based on this mechanism are the following:

State transition analysis [56,57]: This method is based on a state transition diagram, where each attack behavior is defined by its initial state, attack state, and the conditions for transition between states. These state transitions are represented in a state transition diagram and integrated into the detection model, where the state transition conditions are the signatures of different attacks.

Expert system [58]: The conclusions are drawn from known attacks based on the expert experience and translated into fixed rules or conditions. When any one of the conditions is met, an attack is proven to have occurred and the type of the attack is identified.

Petri nets [59,60]: Petri nets are used to represent the initial state, attack state, and state transition features under attack behaviors, and are integrated into the model to judge the occurrence of the attack behavior based on whether the state transition conditions are satisfied or not.

Conditional probability [61]: For each attack behavior, a corresponding sequence of events is established, and then the probability of the attack occurring is inferred according to Bayes theorem.

Blacklist and whitelist [62,63]: By creating a blacklist based on known attack behaviors, any attack behavior that exists in the blacklist will be detected. Conversely, by creating a whitelist based on legitimate behaviors, the detection information is verified and any behavior that does not exist in the whitelist will trigger the alarm.

A signature-based detection mechanism can effectively detect known attacks with high detection accuracy and low error rates. However, the disadvantage is that it cannot detect the attack types that are not in the signature database, and this type of detection mechanism tends to fail when the attacker slightly changes the attack signatures. Therefore, this detection mechanism needs to periodically update the signature database.

3.2.2. Anomaly-Based Detection

Anomaly-based detection is based on the normal state of the constructed system. When the real-time operational data deviate significantly from the normal state or exceed the predefined threshold, the system is considered to have abnormal behavior, indicating that it is suffering from an attack. Anomaly-based detection methods are mainly divided into two categories: statistical-based methods and artificial intelligence-based (AI-based) methods.

The core idea of statistical-based methods is to use statistical methods to build a statistically generative model. In the model, data with probability values below a threshold are considered anomalous, indicating that a cyber-attack has occurred. This class of method can be further categorized into two subclasses: parametric and nonparametric detection methods [64]. Parametric detection methods assume a basic distribution model of the data and estimate the parameters of the distribution model based on empirical data. Representative methods of parametric detection include the Gaussian mixture model (GMM) [65] and the regression model [66]. Nonparametric detection methods do not rely on any distribution model, and the main methods include the Markov model [67,68] and kernel density estimation (KDE) [69]. Ref. [70] proposed a modified state estimator based on Kalman filtering and designed a chi-square-based detection method to detect FDI attacks on PMUs by integrating attacked estimation information with undamaged measurement information. Statistical-based detection mechanisms are easy to implement and have a fast detection speed after the model is constructed. However, the detection accuracy is highly dependent on empirical data and model assumptions, and insufficient empirical data are likely to lead to erroneous detection results.

AI-based detection methods extract the abnormal state when the attacks occur through machine learning, and distinguish the normal state from the abnormal state caused by the attacks through classification or clustering algorithms. AI-based detection methods can be further categorized into two subclasses: supervised learning and unsupervised learning.

Unsupervised learning utilizes unlabeled data to obtain unknown feature relationships between data through model training, and can be categorized into the dimensionality reduction model, clustering model, and neural network model according to the different learning methods. Principal component analysis (PCA) can reduce the dimensionality of high-dimensional data, remove noise and unimportant features, and effectively separate normal and abnormal data without losing important information, so it is often used for data processing before machine learning training [71]. However, PCA is a linear dimensionality reduction and cannot realize nonlinear dimensionality reduction. The neighborhood preserving embedding (NPE) algorithm not only achieves linear and nonlinear dimensionality reduction, but also has better detection results than PCA [72]. Compared with the dimensionality reduction model, the K-means clustering method [73] reduces the computational complexity, is easy to implement, and has better performance in attack detection. With the development of the smart grid, the amount of power system data will be explosive and characterized by a nonlinear structure, data imbalance, and missing data. Therefore, it will be difficult for traditional methods to improve the detection ability. As a result, unsupervised neural network models such as sparse autoencoders (SAEs) [74], generative adversarial networks (GANs) [75], deep belief networks (DBNs) [76], and stacked autoencoders (SAs) [77] are gradually being applied to solve these issues.

Supervised learning detection methods use labeled data to train the model and obtain the optimal relationship model among the known features in the data, and usually provide better detection performance compared to unsupervised learning detection methods. Usually, supervised learning can be categorized into classification and regression models, and neural network models. Among the classification and regression models, logistic regression (LR), the K-nearest neighbor (KNN) algorithm, naive Bayes (NB), decision tree (DT), support vector machine (SVM), and random forest (RF) are widely used [78–82]. Ref. [83] utilized a support vector regressor (SVR) to extract an affine relationship within PMUs, for verifying FDI attack on PUM measurement data and identifying injected false data. In general, detection methods based on DT have the highest accuracy and correctness. The KNN algorithm and SVM show high accuracy in small-sample data but have high computational complexity. LR is simple to compute and easy to implement, and is effective for binary classification problems. NB has low data quality requirements and is insensitive to missing data. RF has a high level of resistance to overfitting. With the increasing requirements for computational power and the development of neural network models, researchers have gradually applied neural network models such as the recurrent neural network (RNN) [84], convolutional neural network (CNN) [85], long short-term memory (LSTM) neural network [86], multi-layer perceptron (MLP) [87,88], and vector neural network (VNN) [12] to detect attacks on PMUs and communication networks. Compared with traditional machine classification and regression detection algorithms, neural network-based detection models have powerful nonlinear feature extraction capabilities and better detection and identification results.

Overall, artificial intelligence-based detection methods are able to adjust the model in time according to the changes in data information and have high detection accuracy, but they incur a high cost by consuming a large amount of resources, and may not be able to provide accurate detection results when there are insufficient sample data.

3.2.3. Hybrid Detection

Hybrid detection methods combine two or more of the above detection strategies. By combining multiple detection mechanisms, the accuracy of attack detection can be improved. When signature-based strategies are used in conjunction with anomaly-based techniques, the hybrid system can detect intruders attempting to modify attack signatures stored in the model database [89]. To improve the system performance, several fusion methods and techniques are sometimes adopted to integrate detection models. Ref. [73] significantly reduces the time complexity and improves the detection accuracy by combining K-means clustering and SVM. Ref. [90] uses PAC for data dimensionality reduction and then detects attacks through a hybrid RF-SVM classification model. Ref. [91] used a hybrid CNN-LSTM attack detection model with particle swarm optimization to detect anomalous data in PMUs and determine the type of attack, combining the advantages of both neural network models. Ref. [92] proposed a transformer-bidirectional long short-term memory (BLSTM) attack detection model to detect phase shifts in PMU measurement data caused by TS attack. Ref. [93] proposed a model and dual data-driven TA attack detection mechanism, which included two model threshold-based detection methods and detection using an autoencoder neural network (AENN) and RF, and demonstrated good detection performance against TS attack. Combining different approaches can make the detection system more robust, but the detection results are not always optimal. In fact, developing hybrid detection systems from different approaches that can interoperate effectively is a challenging task.

3.2.4. Comparison of Detection Methods

A comparison of the three methods, signature-based detection, anomaly-based detection, and hybrid detection, is shown in the Table 2. The false positive rate represents the probability that the detection model will consider normal data as attack data; the false negative rate represents the probability that the detection model will consider attack data as normal data.

Table 2. Performance comparison of classification detection methods.

Metrics	Signature-Based Detection	Anomaly-Based Detection	Hybrid Detection
Complexity	Low	Medium	High
Detection Accuracy	High	Medium	High
False Positive Rate	Very low	High	Low
False Negative Rate	Medium	High	Low
False Alarm Rate	Low	High	Medium
Implementation Cost	Low	Medium	High

3.3. Suppression during Attack

Currently, there are several methods to mitigate the impact of cyber-attacks:

Attack vector removal: Attack vector removal refers to removing the attack-injected portion of the attacked measure values and restoring the measure data to its original state to mitigate the impact of data integrity attacks [33]. Ref. [94] used a matrix decomposition technique to decompose the communication information matrix into a low-rank measure value matrix and a sparse attack matrix, and the actual measure matrix is obtained after removing the attack matrix. In addition, some neural network algorithms have been applied to recover communication data during attacks. CNN [95], GAN [96], and the denoising autoencoder (DAE) [97] can eliminate the biases caused by attacks and recover the communication values affected by FDI attack.

Designing compensators. Designing compensators is a common and straightforward method used to mitigate DoS attack by compensating for lost data to protect the communication channel [98]. Ref. [99] established model-free predictive compensation to predictively compensate for the problem of communication data loss caused by DoS attack by obtaining the supply–demand imbalance power. Ref. [100] designed a CNN-LSTM hybrid deep neural network compensator, which can effectively solve the problem of data loss due to DoS attack.

4. Countermeasures for Internal Malicious Behavior

Currently, research on power system information security issues mainly focuses on external network attacks, while research on selfish nodes implementing malicious behaviors in distributed economic dispatch scenarios is relatively rare. Countermeasures for internal malicious behaviors usually include detection and prevention.

4.1. Detection of Internal Malicious Behavior

According to the different mechanisms, the current malicious behavior detection methods mainly include two categories: trust management and AI-based.

In the trust management detection mechanism, the nodes in the system repeatedly interact with each other and get information to evaluate the reputation of the nodes. The nodes then distinguish between normal nodes and malicious nodes and ensure that only trusted nodes can participate in network communication [101]. With the widespread application of blockchain technology, many researchers have also combined the blockchain with trust management. Reputation values are stored in the blockchain, which ensures the invariance, decentralization, and availability of data [102,103].

AI-based detection mechanisms: In the field of network information intrusion detection, neural network models have been very popular for identifying and classifying anomalous behavior. Ref. [104] proposed three online detection and localization strategies for malicious nodes based on neural network models with a temporal difference, spatial difference, and frequency difference, which showed significant detection and localization performance. Based on the CNN technique, Refs. [29,105] implement the detection and localization of internal malicious nodes in a gossip-based distributed projected gradient algorithm.

4.2. Prevention for Internal Malicious Behavior

The currently recognized effective means of preventing and controlling malicious behavior by selfish nodes is the application of resilient distributed algorithms. The algorithms isolate selfish nodes in the communication network or ignore their communication data, while normal nodes maintain communication with each other and continue to execute the distributed algorithms. Ref. [106] proposes a resilient distributed algorithm based on trusted nodes, which achieves consensus among normal and trusted nodes after excluding selfish nodes. This idea of completely removing malicious information was then further extended to a family of algorithms known as mean subsequence reduced (MSR) algorithms [107]. The idea of this class of method is that a normal node ranks the information values received from all its neighbors in order of magnitude. The normal nodes then remove the F largest and F smallest values (F represents the estimated upper bound of nodes performing malicious behavior), and use only the remaining information to update their own state.

The method is likely to discard some normal information, resulting in slower system convergence. To overcome this problem, the weighted MSR (W-MSR) [108] algorithm and event-based MSR (E-MSR) [109] algorithm have been successively proposed. The former calculates the weighted average of the filtered valid information, and the latter achieves resilient consensus by reducing the frequency of information exchange between nodes through event-triggered mechanisms. Both algorithms can effectively reduce the impact of the malicious behavior of the selfish nodes on the convergence speed of the distributed algorithm and the economy of the system.

5. Prospects for Information Security Measure Methods in Distributed Economic Dispatch Systems

The current research on information security lacks consideration of the cyber-physical coupling characteristics, and single cyber-side defense measures still have a defense blind spot and cannot promptly respond to the physical-side actions. Therefore, cyber-physical coupling needs to be considered in subsequent research. Combined with previous analysis, this section discusses two aspects: information security issues models and the integrated security defense system.

5.1. Information Security Issues Model

The basis for solving the internal and external information security issues in distributed economic dispatch systems is to construct the dynamics model of the system in distributed control mode, and further integrate the external cyber-attack model and internal malicious behavior model from the perspective of the power CPS.

5.1.1. New Generation Power System CPS Model

The new generation power system CPS combines power information technology with the power physical system, where the power flow and information flow coexist and influence each other. The continuous dynamic behavior of the power system is coupled with the discrete dynamic behavior of the information system to improve the control and operation performance of the power system. However, because of the high level of cyber-physical coupling, the information security issues may lead to cascading failure reaction of the power system, thus affecting the safe and stable operation of the system. Therefore, the construction of a CPS model adapted to the new generation power system is the basis and premise of the prevention and control of information security issues.

At present, the research on the construction of the power CPS model mainly focuses on traditional centralized control systems, and lacks research on the power system under distributed control. Constructing a new generation power system CPS model is crucial for preventing and controlling information security problems in power systems under distributed control. This involves considering changes in real-time physical and communication topology, the mutual conversion of power and information flows, as well as the cyber-physical interaction process.

In this paper, the active distribution network model [110] is combined with a distributed economic dispatch strategy [111] to propose a preliminary distributed economic dispatch model system that considers the cyber-physical coupling. The model is formulated as follows:

$$\begin{bmatrix} \dot{\boldsymbol{\lambda}} \\ \dot{\boldsymbol{x}}_{\mathrm{DG}} \end{bmatrix} = \begin{bmatrix} \boldsymbol{C}_{\lambda} & \boldsymbol{A}_{\lambda} \\ \boldsymbol{C}_{\mathrm{DG}} & \boldsymbol{A}_{\mathrm{DG}} \end{bmatrix} \begin{bmatrix} \boldsymbol{\lambda} \\ \boldsymbol{x}_{\mathrm{DG}} \end{bmatrix} + \begin{bmatrix} \boldsymbol{B}_{\lambda} \\ \boldsymbol{B}_{\mathrm{DG}} \end{bmatrix} \boldsymbol{u}_{dq} \tag{3}$$

where $\boldsymbol{A}_{\lambda} = (-\boldsymbol{L}_{B1}\boldsymbol{A}_{P}\boldsymbol{S}_{i} + \boldsymbol{F}_{i})\boldsymbol{M}$; $\boldsymbol{B}_{\lambda} = -\boldsymbol{L}_{B1}\boldsymbol{A}_{P}\boldsymbol{S}_{u} + \boldsymbol{F}_{u}$; $\boldsymbol{C}_{\lambda} = \boldsymbol{L}_{B2}$; $\boldsymbol{L}_{B1} = \mathrm{diag}\{0, \boldsymbol{L} + \boldsymbol{D}\}$. $\boldsymbol{x}_{\mathrm{DG}}$ is the state variable of the DG control model; $\boldsymbol{\lambda}$ is the incremental cost of power generation by the DG; $\boldsymbol{u}_{dq}$ denotes the dq-axis component of the grid-connected voltage of the DG; $\boldsymbol{A}_{\mathrm{DG}}$ and $\boldsymbol{B}_{\mathrm{DG}}$ are constant matrices related to the parameters of the DG control model; $\boldsymbol{C}_{\mathrm{DG}}$ is related to the parameters of the DG control model and to the power-cost function of the DG; $\boldsymbol{M}$ is a constant transformation matrix; $\boldsymbol{L}$ and $\boldsymbol{D}$ are the Laplacian matrix and degree matrix of communication topology of the nodes except the leader node, respectively; $\boldsymbol{L}_{B2}$ is the degree matrix of the communication topology of the leader node with other nodes; $\boldsymbol{A}_{p}$ is related to the power-cost function of the DG; $\boldsymbol{S}_{i}$, $\boldsymbol{S}_{u}$, $\boldsymbol{S}_{i}$, and $\boldsymbol{F}_{u}$ are related to the active power emitted by the DG.

The most important communication data in the distributed economic dispatch system are the incremental cost of generation of each DG, the change in which affects the control of the DGs in the system. The following analysis preliminarily examines the impact of information security issues on the system in conjunction with the distributed economic dispatch model shown in Equation (3). The DoS attack blocks the communication link and prevents normal communication, resulting in a change in the communication topology. The parameters of the matrices $\boldsymbol{L}$, $\boldsymbol{D}$, and $\boldsymbol{L}_{B2}$ in the model that are related to the communication topology are affected. The FDI attack and replay attack cause the active power of DGs to deviate from the economic optimum by tampering with the incremental cost $\boldsymbol{\lambda}$ of the communication transmission. Therefore, the matrices $\boldsymbol{A}_{\lambda}$ and $\boldsymbol{B}_{\lambda}$ are changed by the FDI attack and replay attack. Similarly, the deception behavior tampers with the incremental cost $\boldsymbol{\lambda}$ of the communication transmission, so that $\boldsymbol{A}_{\lambda}$ and $\boldsymbol{B}_{\lambda}$ are changed by deception behavior. Fraud behavior involves a spurious modification of the cost function, which affects $\boldsymbol{C}_{\mathrm{DG}}$ and $\boldsymbol{A}_{p}$ in the model. Further research is needed to understand the impact of external cyber-attacks and internal malicious behaviors on the stability and convergence of the distributed economic dispatch system. This can be achieved by establishing mathematical models and integrating them with the distributed economic dispatch model.

5.1.2. External Cyber-Attack Model

The current research of cyber-attack models usually separates the information system from the physical system. Therefore, the complete attack and response process of the cyber-attack is divided into two phases: information invasion of the information system, and impact analysis and control of the physical system. This leads to the corresponding defense measures only for a single information or physical level. The cyber-attack based on the new generation power system CPS has new characteristics. It contributes to the construction of the cyber-physical hybrid model of the cyber-attack that considers the cyber-physical coupling and clearly studies the relationship between the information attack and the physical response. In addition, the subjective behaviors of the attackers will significantly increase the randomness of cyber-attacks, making cyber-attacks more difficult to detect and their effect more difficult to control. Therefore, by introducing the knowledge of game theory, such as offensive and defensive games, human intention is considered as a factor in the modeling of cyber-attacks.

5.1.3. Internal Malicious Behaviors Model

Internal malicious behaviors with extremely stealth are difficult to manage and defend in the distributed economic dispatch system. The behaviors hide malicious data in a large amount of normal data in order to seek benefits and destroy the economic operation of the system. Processing historical data and extracting the characteristics of malicious behaviors implied in the data, and using the portrait method to portray the malicious behavior pattern, can improve the accuracy of judging the malicious behaviors of the internal members in the distributed economic dispatch system. Similarly, the implementation of malicious behavior is accompanied by human intention and psychological fluctuations. The behavioral performance and psychological state of the implementer of malicious behaviors can be inferred from game theory and a psychological perspective. The possibility of the occurrence and development of malicious behavior can be judged.

5.2. Integrated Security Defense System

The current defense measures for information security issues mainly focus on cyber-side detection and suppression. In the future, it will be necessary to design corresponding defense measures based on the information security issues model from the perspective of the new generation power system CPS. Additionally, constructing the distributed economic dispatch information security issues defense system is crucial.

5.2.1. Secure Measurement Technology Based on PMU

The GPS timing and communication methods of PMUs have information security risks, and their measurement and communication data are vulnerable to TS attack and FDI attack, respectively. The measurement data provided by PMUs serve as a critical foundation for power system state estimation, situational awareness, and dispatch control. Any anomalies in the data caused by attacks can lead to erroneous system decisions, ultimately threatening the security and stability of the power system. To ensure reliable support for economic dispatch in the power system, it is imperative to establish secure measurement technology based on PMUs. Firstly, at the active defense level, the system should be made more resistant to attacks by improving physical devices. This includes developing secure cryptographic chips to encrypt the communication of measurement data and enhancing the anti-interference capability of GPS signal receivers. Secondly, the detection and recovery from attacks are paramount, constituting a critical step in mitigating PMU information security risks. A deep analysis needs to be conducted of the time synchronization deviation characteristics and specific effects on phasor measurement and communication caused by the TS attack and FDI attack. Based on these attack characteristics, it should fully utilize PMU measurement data to develop local detection and recovery methods based on temporal features, and integrate system topology and parameter information to establish regional detection and recovery methods based on data spatio-temporal correlations.

5.2.2. Defense Technology Support Base on Blockchain

The rapid development of information security technology, represented by trusted computing technology and blockchain technology, provides a new solution to address the information security of the distributed economic dispatch system. In particular, blockchain technology is well suited to the characteristics of the new generation power system, as shown below. The decentralized characteristics of the blockchain correspond to the distribution characteristics of power sources and loads in the new power system. The new power system in the future will be dominated by DGs such as wind power and photovoltaic power. Blockchain technology ensures data integrity through encryption algorithms, which provides a degree of prevention against cyber-attacks. Each block is timestamped and arranged chronologically in a chain structure to ensure data traceability, which can prevent the malicious behaviors of selfish nodes that intentionally transmit false information. Node information transmission adopts consensus algorithms, such as the PoW algorithm, for attack detection and security strategy decisions to resist external cyber-attacks. The blockchain provides a script code system and supports the application and development of various scenarios, and smart contracts can be written according to the actual application requirements.

Therefore, combining the specific application of the distributed economic dispatch of the new generation power system, key blockchain technologies can be integrated into various aspects of information security defense by taking it as a unified underlying technology platform. This includes the following five aspects: the construction of a node identity registration and authentication system, the construction of a communication data encryption and verification system, the design of a node punishment and incentive mechanism, the compilation of a distributed economic dispatch smart contract, and the research into new defense methods based on consensus mechanisms. These defensive means of realizing information security protection against external cyber-attacks and internal malicious behavior are the next research direction to focus on.

5.2.3. Cyber-Physical Cooperative Defense System

Due to the deep cyber-physical coupling of the power CPS, the information security issues on the cyber side and the stable operation status on the physical side are closely related and mutually interacting. Separate security defense measures on the cyber side cannot respond to failures or damages on the physical side, while real-time measurement information on the physical side affects communication and decision-making on the cyber side. Defense measures based on the cyber side are relatively mature. However, there are also shortcomings such as high real-time information requirements, inability to simultaneously achieve high accuracy and low leakage rates in detection, and suppression measures only targeting specific information security issues.

The cyber-physical cooperative defense in power systems can include attack detection and identification, security risk assessment of the power CPS, security strategy decision-making, and consensus. However, the following issues also need to be considered: (1) Data heterogeneity and balance. In the power CPS, there is a coexistence of continuous physical data and discrete information data, with significant differences in real-time and temporal characteristics. Additionally, most of the data represent normal power system operations, and there is a lack of relevant data for information security issues and defense. (2) Rational utilization of information and physical resources. The physical side possesses defense resources such as manpower, technology, and equipment. By optimizing the allocation of physical defense resources and coordinating with cyber-side security defense technologies, the defense effectiveness can be maximized.

Therefore, the construction of a cyber-physical cooperative defense system for the power system is worthy of attention in the future. This needs to make full use of the characteristics of interdependence and support between information and physics in the power system and coordinate the allocation of defense resources.

6. Conclusions

This paper provides a thorough review of the information security problems of the distributed economic dispatch system and its protective measures. Four kinds of external network attacks and two kinds of internal malicious behaviors are introduced. This paper emphatically summarizes the three-phase defense measures of prevention, detection, and suppression for external network attacks, and the detection and prevention measures for internal malicious behaviors. Most of the existing studies have failed to analyze the impact of information security issues on DGs and power systems, and the designed defense measures only focus on the information layer without considering the cyber-physical coupling of the power system. Therefore, future research on information security issues of the distributed economic dispatch system can be mainly approached from the following two directions. Firstly, it is necessary to consider the characteristics of cyber-physical coupling to establish an information security issues model and analyze the impact on the performance of the distributed economic dispatch system. The second aspect is to design the security defense system. This includes the development of secure measurement technology based on PMUs and cyber-physical collaborative defense strategies integrating new information security technologies such as the blockchain. This article aims to review the current research status of information security issues and provide guidance for future studies.

Author Contributions: Conceptualization, J.L. and H.L.; methodology, J.L.; formal analysis, H.L. and J.W.; investigation, W.W. and G.L.; resources, H.L. and J.W.; data curation, H.L., J.W., W.W. and G.L.; writing—original draft preparation, J.L. and H.L.; writing—review and editing, H.L. and G.L.; visualization, J.W.; supervision, W.W.; project administration, J.L.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China, grant number 2022YFF0610601.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DGs	Distributed generations
PMUs	Phasor measurement units
CPS	Cyber-physical systems
TS	Time synchronization
DoS	Denial of service
FDI	False data injection
DES	Data encryption standard
3DES	Triple data encryption standard
AES	Advanced encryption standard
ECC	Elliptic curve cryptography
RSA	Rivest–Shamir–Adleman
GMM	Gaussian mixture model
KDE	Kernel density estimation
PCA	Principal component analysis
NPE	Neighborhood preserving embedding
SAE	Sparse autoencoder
GAN	Generative adversarial network
SA	Stacked autoencoder
DBN	Deep belief network
LR	Logistic regression
KNN	K-nearest neighbor
NB	Naive Bayes
DT	Decision tree
SVM	Support vector machine
RF	Random forest
SVR	Support vector regressor
RNN	Recurrent neural network
CNN	Convolutional neural network
LSTM	Long short-term memory
MLP	Multi-layer perceptron

VNN	Vector neural network
BLSTM	Bidirectional long short-term memory
AENN	Autoencoder neural network
DAE	Denoising autoencoder
MSR	Mean subsequence reduced
W-MSR	Weighted mean subsequence reduced
E-MSR	Event-based mean subsequence reduced

References

1. Hang, B.; Liu, X.; Yu, Z.; Wang, W.; Jin, Q.; Li, W. Review on artificial intelligence-based network attack detection in power systems. *High Volt. Eng.* **2022**, *48*, 4413–4426.
2. Wen, G.; Yu, X.; Liu, Z. Recent progress on the study of distributed economic dispatch in smart grid: An overview. *Front. Inf. Technol. Electron. Eng.* **2021**, *22*, 25–39. [CrossRef]
3. Peng, Y.; Jiang, W.; Wei, X.; Pan, J.; Kong, X.; Yang, Z. Microgrid optimal dispatch based on distributed economic model predictive control algorithm. *Energies* **2023**, *16*, 4658. [CrossRef]
4. Le, J.; Zhou, Q.; Zhao, L.; Wang, Y. Overview of distributed economic dispatch methods for power system based on consensus algorithm. *Electr. Power Autom. Equip.* **2020**, *40*, 44–54.
5. Tu, H.; Du, Y.; Yu, H.; Meena, S.; Lu, X.; Lukic, S. Distributed economic dispatch for microgrids tracking ramp power commands. *IEEE Trans. Smart Grid* **2023**, *14*, 94–111. [CrossRef]
6. Liu, L.; Song, H.; Piao, X.; Wang, S.; Qu, Y. Data protection of distributed economic dispatch based on blockchain. *Electr. Power Inf. Commun. Technol.* **2022**, *20*, 44–52.
7. Li, P.; Liu, Y.; Xin, H.; Jiang, X. A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4343–4352. [CrossRef]
8. Sharma, D.D.; Singh, S.N.; Lin, J.; Lin, J.; Foruzan, E. Agent-based distributed control schemes for distributed energy storage systems under cyber attacks. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 307–318. [CrossRef]
9. Le, J.; Zhou, Q.; Zhao, L.; You, M. Fully distributed economic dispatch of active distribution network considering individual cheating. *Proc. CSEE* **2020**, *40*, 5445–5454.
10. Tang, Y.; Chen, Q.; Li, M.; Wang, Q.; Ni, M.; Liang, Y. Overview on cyber-attacks against cyber physical power system. *Autom. Electr. Power Syst.* **2016**, *40*, 59–69.
11. Liu, X.; Cui, Y.; Xu, D. Performance optimization for low voltage power line communication. *Electr. Power Autom. Equip.* **2017**, *37*, 30–42.
12. Huang, R.; Li, Y. False phasor data detection under time synchronization attacks: A neural network approach. *IEEE Trans. Smart Grid* **2022**, *13*, 4828–4836. [CrossRef]
13. He, W.; Gao, X.; Zhong, W.; Qian, F. Secure impulsive synchronization control of multi-agent systems under deception attacks. *Inf. Sci.* **2018**, *459*, 354–368. [CrossRef]
14. Pang, Z.; Liu, G. Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Trans. Control Syst. Technol.* **2012**, *20*, 1334–1342. [CrossRef]
15. Zadsar, M.; Ghafouri, M.; Ameli, A.; Moussa, B. Preventing time-synchronization attacks on synchrophasor measurements of wide-area damping controllers. *IEEE Trans. Instrum. Meas.* **2023**, *72*, 1–14. [CrossRef]
16. Xu, F.; Xue, A.; Chang, N.; Kong, H.; Xu, J. Research status and prospects of detection, correction and recovery for abnormal synchrophasor data in power system. *Proc. CSEE* **2021**, *41*, 6869–6885.
17. Almas, M.S.; Vanfretti, L.; Singh, R.S.; Jonsdottir, G.M. Vulnerability of synchrophasor-based WAMPAC applications to time synchronization spoofing. *IEEE Trans. Smart Grid* **2018**, *9*, 4601–4612. [CrossRef]
18. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153. [CrossRef]
19. Xue, A.; Xu, F.; Chow, J.H.; Leng, S.; Kong, H.; Xu, J.; Bi, T. Data-driven detection for GPS spoofing attack using phasor measurements in smart grid. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106883. [CrossRef]
20. Wang, Y.; Zhang, M.; Song, K.; Li, T.; Zhang, N. An optimal DoS attack strategy disturbing the distributed economic dispatch of microgrid. *Complexity* **2021**, *11*, 1–16. [CrossRef]
21. Zhang, Y.; Xie, X.; Fu, W.; Chen, X.; Hu, S.; Zhang, L.; Xia, Y. An optimal combining attack strategy against economic dispatch of integrated energy system. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 246–250. [CrossRef]
22. Huang, B.; Zhan, F.; Zhang, T.; Yang, C. An optimal DoS attack strategy against the economic dispatch for electric-thermal integrated energy system. *Proc. CSEE* **2020**, *40*, 6839–6854.
23. Liu, X.; Che, L.; Gao, K.; Li, Z. Power system intra-interval operational security under false data injection attacks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4997–5008. [CrossRef]
24. Zhang, W.; He, X. Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem. *Int. J. Electr. Power Energy Syst.* **2018**, *103*, 233–246. [CrossRef]
25. Siu, J.Y.; Kumar, N.; Panda, S.K. Command authentication using multiagent system for attacks on the economic dispatch problem. *IEEE Trans. Ind. Appl.* **2022**, *58*, 4381–4393. [CrossRef]

26. Zhao, C.; He, J.; Cheng, P.; Chen, J. Analysis of consensus-based distributed economic dispatch under stealthy attacks. *IEEE Trans. Ind. Electron.* **2016**, *64*, 5107–5117. [CrossRef]
27. Yassaie, N.; Hallajiyan, M.; Sharifi, I.; Talebi, H.A. Resilient control of multi-microgrids against false data injection attack. *ISA Trans.* **2021**, *110*, 238–246. [CrossRef]
28. Xu, W.; Kurths, J.; Wen, G.; Wen, G.; Yu, X. Resilient event-triggered control strategies for second-order consensus. *IEEE Trans. Autom. Control* **2022**, *67*, 4226–4233. [CrossRef]
29. Wu, S.X.; Li, G.; Zhang, S.; Lin, X. Detection of insider attacks in distributed projected sub-gradient algorithms. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 1099–1111. [CrossRef]
30. Gentz, R.; Wu, S.X.; Wai, H.T.; Scaglione, A.; Leshem, A. Data injection attacks in randomized gossiping. *IEEE Trans. Signal Inf. Process. Netw.* **2016**, *2*, 523–538. [CrossRef]
31. Maestre, J.M.; Velarde, P.; Ishii, H.; Negenborn, R.R. Scenario-based defense mechanism against vulnerabilities in Lagrange-based DMPC. *Control Eng. Pract.* **2021**, *114*, 104879. [CrossRef]
32. Velarde, P.; Maestre, J.M.; Ishii, H.; Negenborn, R.R. Vulnerabilities in Lagrange-based distributed model predictive control. *Optim. Control Appl. Methods* **2017**, *39*, 601–621. [CrossRef]
33. Peng, S.; Sun, M.; Zhang, Z.; Deng, R.; Cheng, P. Application of machine learning in cyber security of cyber-physical power system. *Electr. Power Autom. Equip.* **2022**, *46*, 200–215.
34. Shukla, S.; Thakur, S.; Breslin, J.G. Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 261–266.
35. Manickam, S.; Kesavaraja, D. Secure multi server authentication system using elliptic curve digital signature. In Proceedings of the International Conference on Circuit, Power and Computing Technologies, Nagercoil, India, 18–19 March 2016; pp. 1–4.
36. Verma, U.K.; Kumar, S.; Sinha, D. A secure and efficient certificate based authentication protocol for MANET. In Proceedings of the International Conference on Circuit, Power and Computing Technologies, Nagercoil, India, 18–19 March 2016; pp. 1–7.
37. Tanveer, M.; Khan, A.U.; Shah, H.; Alkhayyat, A.; Chaudhry, S.A.; Ahmad, M. ARAP-SG: Anonymous and reliable authentication protocol for smart grids. *IEEE Access* **2021**, *9*, 143366–143377. [CrossRef]
38. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Syst. J.* **2014**, *8*, 655–663. [CrossRef]
39. Mazloomzadeh, A.; Mohammed, O.A.; Zonouzsaman, S. Empirical development of a trusted sensing base for power system infrastructures. *IEEE Trans. Smart Grid* **2015**, *6*, 2454–2463. [CrossRef]
40. Cui, A.; Zhao, H.; Zhang, X.; Zhao, B.; Li, Z. Power system real time data encryption system based on DES algorithm. In Proceedings of the 13th International Conference on Measuring Technology and Mechatronics Automation, Beihai, China, 16–17 January 2021; pp. 220–228.
41. Hong, W.; Sheng, W.; Qing, Z.; Jian, Z. Research on data encryption of network communication based on big data. In Proceedings of the International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, Fuzhou, China, 12–14 June 2020; pp. 129–131.
42. Ramesh, A.; Suruliandi, A. Performance analysis of encryption algorithms for Information Security. In Proceedings of the International Conference on Circuits, Power and Computing Technologies, Nagercoil, India, 20–21 March 2013; pp. 840–844.
43. Dua, A.; Dutta, A. A study of applications based on elliptic curve cryptography. In Proceedings of the 3rd International Conference on Trends in Electronics and Informatics, Tirunelveli, India, 23–25 April 2019; pp. 249–254.
44. Vahedi, E.; Baya, M.; Pakravan, M.R.; Rref, M.R. A secure ECC-based privacy preserving data aggregation scheme for smart grids. *Comput. Netw.* **2017**, *129*, 28–36. [CrossRef]
45. Sharmam, M.; Choudhary, V.; Bhatia, R.S.; Malik, S.; Raina, A.; Khandelwal, H. Leveraging the power of quantum computing for breaking RSA encryption. *Cyber-Phys. Syst.* **2021**, *7*, 73–92. [CrossRef]
46. Qu, B.; Wang, Z.; Shen, B.; Dong, H.; Zhang, X. Secure particle filtering with Paillier encryption–decryption scheme: Application to multi-machine power grids. *IEEE Trans. Smart Grid* **2024**, *15*, 863–873. [CrossRef]
47. Yu, M.; Zhu, L.; Rao, Y.; Yi, Y.; Liu, J. Research on fast encryption method for smart energy management system in smart gird. In Proceedings of the International Conference on Communications, Information System and Computer Engineering, Kuala Lumpur, Malaysia, 3–5 July 2020; pp. 76–80.
48. Deng, J.; Kang, H. Hybrid encryption scheme for secure storage of smart grid data. In Proceedings of the Smart Grid and Internet of Things-4th EAI International Conference, TaiChung, Taiwan, 5–6 December 2020; pp. 135–156.
49. Jin, L.; He, J.; Zhao, W.; Pang, J.; Lv, J.; Cheng, L. Design of electricity market big data analysis system based on hybrid encryption and secure transmission. In Proceedings of the 4th International Electrical and Energy Conference, Wuhan, China, 28–30 May 2021; pp. 1–6.
50. Paverd, A.; Martin, A.; Brown, I. Privacy-enhanced bi-directional communication in the Smart Grid using trusted computing. In Proceedings of the International Conference on Smart Grid Communications, Venice, Italy, 3–6 November 2014; pp. 872–877.
51. Cao, J.; Chen, X.; Li, E.; Xing, H.; Zhang, J.; Mu, G.; Miao, C.; Xu, C. Design of identity authentication scheme in smart grid based on blockchain. In Proceedings of the 4th International Conference on Frontiers Technology of Information and Computer, Qingdao, China, 2–4 December 2022; pp. 1093–1100.

52. Gong, G.; Gao, S.; Lu, J.; Zhang, B.; Liu, R.; Wu, Q.; Su, C.; Chen, Z. Study on secure trusted protection architecture for prefecture-level regional energy internet. *Proc. CSEE* **2018**, *38*, 2861–2873 + 3137.
53. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z. Distributed blockchain-based data protection framework for modern power systems against cyber-attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 3162–3173. [CrossRef]
54. Raja, D.J.S.; Sriranjani, R.; Parvathy, A.; Hemavathi, N. A review on distributed denial of service attack in smart grid. In Proceedings of the 7th International Conference on Communication and Electronics Systems, Coimbatore, India, 22–24 June 2022; pp. 812–819.
55. Kaur, P.; Kumar, M.; Bhandari, A. A review of detection approaches for distributed denial of service attacks. *Syst. Sci. Control Eng.* **2017**, *5*, 301–320. [CrossRef]
56. Wang, J.; Phan, R.C.-W.; Whitley, J.N.; Parish, D.J. Augmented attack tree modeling of distributed denial of services and tree-based attack detection method. In Proceedings of the 10th IEEE International Conference on Computer and Information Technology, West Yorkshire, UK, 29 June–1 July 2010; pp. 1009–1014.
57. Mitchell, R.; Chen, I.-R. Behavior-rule based intrusion detection systems for safety critical smart grid applications. *IEEE Trans. Smart Grid* **2013**, *4*, 1254–1263. [CrossRef]
58. Aneetha, A.S.; Indhu, T.S.; Bose, S. Hybrid network intrusion detection system using expert rule-based approach. In Proceedings of the 2nd International Conference on Computational Science, Engineering and Information, Coimbatore, India, 26–28 October 2012; pp. 47–51.
59. Cao, H.; Shi, J.; Zhang, J.; Jing, H. Attack detection technology of electricity consumption information collection system based on fuzzy Petri net. *Electron. Des. Eng.* **2022**, *30*, 105–108 + 119.
60. Deng, Z.; Lv, J.; Jiang, D.; An, Y.; Song, C. A defense model of information system for colored Petri net under DoS attack. *Electr. Power Inf. Commun. Technol.* **2020**, *18*, 44–49.
61. Han, K.; Duan, Y.; Jin, R.; Ma, Z.; Wang, H.; Wu, W.; Wang, B.; Cai, X. Attack detection method based on Bayesian hypothesis testing principle in CPS. *Procedia Comput. Sci.* **2021**, *178*, 474–480. [CrossRef]
62. Cai, X. Research on Cyber-Physical Collaborative Defense Methods for Cyber-Attacks against Power Systems. Master's Thesis, Southeast University, Nanjing, China, 2021.
63. Sen, Ö.; Velde, D.V.D.; Lühman, M.; Sprünken, F.; Hacker, I.; Ulbig, A.; Andres, M.; Henze, M. On specification-based cyber-attack detection in smart grids. *Energy Inform.* **2022**, *5*, 23. [CrossRef]
64. Wang, H.; Bah, M.J.; Hammad, M. Progress in outlier detection techniques: A survey. *IEEE Access* **2019**, *7*, 107964–108000. [CrossRef]
65. Yang, X.; Zhao, P.; Zhang, X.; Lin, J.; Yu, W. A gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid. In Proceedings of the 25th International Conference on Computer Communication and Networks, Waikoloa, HI, USA, 1–4 August 2016; pp. 1–9.
66. Chen, Y.; Hayawi, K.; Zhao, Q.; Mou, J.; Yang, L.; Tang, J.; Li, Q.; Wen, H. Vector auto-regression-based false data injection attack detection method in edge computing environment. *Sensors* **2022**, *22*, 6789. [CrossRef]
67. Ntalampiras, S. Automatic identification of integrity attacks in cyber-physical systems. *Expert Syst. Appl.* **2016**, *58*, 164–173. [CrossRef]
68. Yuan, L.; Deng, S.; Xie, X. Attack detection based on alternating direction multiplier method for distributed state estimation in smart grid. In Proceedings of the China Automation Congress, Xiamen, China, 25–27 November 2022; pp. 264–269.
69. Mosatafa, M.; Karim, A.; Behnam, M.-I.; Amjad, A.M.; Shalmani, M.E.; Arjamnd, A. Anomaly detection in the distribution grid: A nonparametric approach. In Proceedings of the International Conference on Smart Energy Systems and Technologies, Istanbul, Turkey, 7–9 September 2020; pp. 1–6.
70. Cheng, Z.; Ren, H.; Qin, J.; Lu, R. Security analysis for dynamic state estimation of power systems with measurement delays. *IEEE Trans. Cybern.* **2023**, *53*, 2087–2096. [CrossRef]
71. Waghmare, S.; Kazi, F.; Singh, N. Data driven approach to attack detection in a cyber-physical smart grid system. In Proceedings of the Indian Control Conference, Guwahati, India, 4–6 January 2017; pp. 271–276.
72. Zeng, J.; Li, P.; Gao, L.; Shen, X. Detection of false data injection attacks in smart grids based on time neighbor preserving embedding (TNPE). *J. Saf. Sci. Technol.* **2021**, *17*, 124–129.
73. Rose, T.; Kifayat, K.; Abbas, S.; Asim, M. A hybrid anomaly-based intrusion detection system to improve time complexity in the Internet of Energy environment. *J. Parallel Distrib. Comput.* **2020**, *145*, 124–139. [CrossRef]
74. Wang, W.; Ren, Z.; Sun, Y.; Pan, D.; Liu, Z. False data injection attack detection on transmission line using wavelet and sparse auto-encoder. *Adv. Technol. Electr. Eng. Energy* **2022**, *41*, 51–59.
75. Xia, Y.; Wang, Y.; Zhou, L.; Fan, R. False Data injection attack detection method based on improved generative adversarial network. *Electr. Power Constr.* **2022**, *41*, 51–59.
76. Guo, F.; Yi, X.; Xu, B.; Dong, H.; Zhang, W. Stealthy FDI attack detection based on deep belief network and transfer learning. *Control Decis.* **2022**, *37*, 913–921.
77. Chen, L.; Gu, S.; Wang, Y.; Yang, Y.; Li, Y. Stacked autoencoder framework of false data injection attack detection in smart grid. *Math. Probl. Eng.* **2021**, *2021*, 2014345. [CrossRef]
78. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 1773–1786. [CrossRef]

79. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Adefemi Alimi, K.O. Empirical comparison of machine learning algorithms for mitigating power systems intrusion attacks. In Proceedings of the International Symposium on Networks, Computers and Communications, Montreal, QC, Canada, 20–22 October 2020; pp. 1–5.
80. Knesek, K.; Wlazlo, P.; Huang, H.; Sahu, A.; Goulart, A.; Davis, K. Detecting attacks on synchrophasor protocol using machine learning algorithms. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 102–107.
81. Wei, X.; Aman, M.N.; Sikdar, B. Exploiting correlation among gps signals to detect gps spoofing in power grids. *IEEE Trans. Ind. Appl.* **2022**, *58*, 697–708. [CrossRef]
82. Meriaux, E.; Koehler, D.; Islam, M.Z.; Vokkarane, V.; Lin, Y. Performance comparison of machine learning methods in DDoS attack detection in smart grids. In Proceedings of the IEEE MIT Undergraduate Research Technology Conference, Cambridge, MA, USA, 30 September–2 October 2022; pp. 1–5.
83. Khare, G.; Mohapatra, A.; Singh, S.N. A Real-Time Approach for Detection and Correction of False Data in PMU Measurements. *Electr. Power Syst. Res.* **2021**, *191*, 106866. [CrossRef]
84. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access* **2022**, *8*, 77572–77586. [CrossRef]
85. Li, Y.; Zeng, J. Detection method of false data injection attack on power grid based on improved convolutional neural network. *Autom. Electr. Power Syst.* **2019**, *43*, 97–104. [CrossRef]
86. Chen, L.; Liu, N. False data injection attack and its detection method for interactive Demand response. *Autom. Electr. Power Syst.* **2021**, *45*, 15–23.
87. Paul, S.; Kundu, R.K. A bagging MLP-based autoencoder for detection of false data injection attack in smart grid. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, New Orleans, LA, USA, 24–28 April 2022; pp. 1–5.
88. Orouji, N.; Mosavi, M.R.; Martín, D. A lightweight and real-time hardware architecture for interference detection and mitigation of time synchronization attacks based on MLP neural networks. *IEEE Access* **2021**, *9*, 142938–142949. [CrossRef]
89. Suhag, A.; Daniel, A. Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDoS) assault and defense. *J. Cyber Secur. Technol.* **2022**, *7*, 21–51. [CrossRef]
90. Aribisala, A.; Khan, M.S.; Husari, G. Machine learning algorithms and their applications in classifying cyber-attacks on a smart gird network. In Proceedings of the 12th Annual Information Technology, Electronics and Mobile Communication Conference, Vancouver, BC, Canada, 27–30 October 2021; pp. 0063–0069.
91. Bitirgen, K.; Filik, Ü.B. A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. *Int. J. Crit. Infrastruct. Prot.* **2023**, *40*, 100582. [CrossRef]
92. Almutairy, F.; Scekic, L.; Matar, M.; Elmoudi, R.; Wshah, S. Detection and mitigation of GPS Spoofing Attacks on Phasor Measurement Units using deep learning. *Int. J. Electr. Power Energy Syst.* **2023**, *151*, 109160. [CrossRef]
93. Shereen, E.; Dán, G. Model-based and data-driven detectors for time synchronization attacks against PMUs. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 169–179. [CrossRef]
94. Hao, J.; Piechocki, R.J.; Kaleshi, D.; Chin, W.H.; Fan, Z. Sparse malicious false data injection attacks and defense mechanisms in smart grids. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1–12. [CrossRef]
95. Ge, Q.; Jiao, C. Mitigating the impacts of false data injection attacks in smart grids using deep convolutional neural network s. In Proceedings of the 10th International Conference on Electronics Information and Emergency Communication, Beijing, China, 17–19 July 2020; pp. 174–177.
96. Li, Y.; Wang, Y.; Hu, S. Online generative adversary network-based measurement recovery in false data injection attacks: A cyber-physical approach. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2031–2043. [CrossRef]
97. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Mitigating the impacts of covert cyber-attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders. *Energies* **2019**, *12*, 3091. [CrossRef]
98. Li, X.; Li, W.; Du, D.; Sun, Q.; Fei, M.R. Dynamic state estimation of smart grid based on UKF under denial of service attacks. *Acta Autom. Sin.* **2019**, *45*, 120–131.
99. Li, Y.; Huang, W.; Sun, B.; Zhang, X.; Xue, Y. Optimal energy management in micro-grid based on distributed event-triggered consensus predictive compensation under DoS attack. *Mod. Electr. Power* **2021**, *38*, 178–186.
100. Xu, X.; Sun, J.; Wang, C.; Zou, B. A novel hybrid CNN-LSTM compensation model against DoS attacks in power system state estimation. *Neural Process. Lett.* **2022**, *54*, 1597–1621. [CrossRef]
101. Li, W.; Wang, Y.; Li, J. A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. *Int. J. Inf. Secur.* **2023**, *22*, 1219–1230. [CrossRef]
102. Singh, J.; Sinha, A.; Goli, P.; Subramanian, V.; Shukla, S.K.; Vyas, O.P. Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology. *Int. J. Inf. Secur.* **2022**, *21*, 527–546. [CrossRef]
103. Meng, W.; Li, W.; Yang, L.T.; Li, P. Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *Int. J. Inf. Secur.* **2020**, *19*, 279–290. [CrossRef]
104. Li, G.; Wu, S.X.; Zhang, S.; Li, Q. Neural networks-aided insider attack detection for the average consensus algorithm. *IEEE Access* **2020**, *8*, 51871–51883. [CrossRef]

105. Li, G.; Wu, S.X.; Zhang, S.; Li, Q. Detect insider attacks using cnn in decentralized optimization. In Proceedings of the International Conference on Acoustics, Speech and Signal Processing, Barcelona, Spain, 4–8 May 2020; pp. 8758–8762.
106. Zhao, C.; He, J.; Wang, Q. Resilient distributed optimization algorithm against adversarial attacks. *IEEE Trans. Autom. Control* **2020**, *65*, 4308–4315. [CrossRef]
107. Dibaji, S.M.; Ishii, H. Consensus of second-order multi-agent systems in the presence of locally bounded faults. *Syst. Control Lett.* **2018**, *79*, 23–29. [CrossRef]
108. Leblanc, H.J.; Zhang, H.; Koutsoukos, X.; Sundaram, S. Resilient asymptotic consensus in robust networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 766–781. [CrossRef]
109. Wang, Y.; Ishii, H. Resilient consensus through event-based communication. *IEEE Trans. Control Netw. Syst.* **2022**, *7*, 471–482. [CrossRef]
110. Zhao, L. *Research on Distributed Control Strategy of Active Distribution Network Considering Time Delay*; Wuhan University: Wuhan, China, 2022.
111. Le, J.; Qi, G.; Zhao, L.; Liao, X. Time-delay stability analysis of an active distribution network adopting a distributed economic dispatch strategy. *Power Syst. Prot. Control* **2022**, *50*, 75–87.

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