ICJK
Chinese Journal of Information Fusion
http://dx.doi.org/10.62762/CJIF.2024.740709

RESEARCH ARTICLE

Robust Distributed State Estimation in Power Systems: A Multi-Estimator Data Fusion Approach to Counteract Cyber-Attacks

Shiyu Jin[1], **Wen Yang**[1,*], **Hongbo Yuan**[1], **Wenjie Ding**[1], **Han Wu**[1] **and Jie Wang**[1]

[1] Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China

Abstract

Cyber security in power systems has become increasingly critical with the rise of network attacks such as Denial-of-Service (DoS) attacks and False Data Injection (FDI) attacks. These threats can severely compromise the integrity and reliability of state estimation, which are fundamental to the operation and control of power systems. In this manuscript, an estimation algorithm based on the fusion of information from multiple estimators is proposed to ensure that state estimation at critical buses can function properly in case of attacks. Our approach leverages a network of estimators that can dynamically adjust to maintain system stability and accuracy. Furthermore, a new detector is adopted based on Kullback-Leibler divergence to detect linear FDI attacks. To address stealthy attacks that may evade detection, we propose a novel weighting scheme that reduces the impact of attacks on estimation results. Numerical experiments demonstrate the effectiveness and accuracy of our proposed estimation algorithm under cyber attacks.

Keywords: state estimation, smart grid, data fusion, Kullback-Leibler divergence, cyber attack.

1 Introduction

State estimation, as an important backbone of smart grid, providing critical data essential for the operation and surveillance of power systems. Yet, with the proliferation of intelligent devices and communication networks, the risk of cyber threats has correspondingly increased. Attackers can employ diverse cyber-attack methods to disrupt the functioning of state estimation, thereby impacting the stable operation of the system. The two most prevalent forms of cyber attacks are DoS attacks and FDI attacks. DoS attacks aim to disrupt the communication channels, preventing the transmission of data between sensors and estimators. FDI attackers replace the measurements with designed false data, resulting in incorrect state estimations. Both types of attack have the potential to result in significant consequences [2–6].

Academic Editor:
Yulong Huang

Submitted: 11 November 2024
Accepted: 29 December 2024
Published: 30 December 2024

Vol. 1, **No.** 3, 2024.
10.62762/CJIF.2024.740709

***Corresponding author:**
✉ Wen Yang
weny@ecust.edu.cn

Citation
Jin, S., Yang, W., Yuan, H., Ding, W., Wu, H. & Wang, J. (2024). Robust Distributed State Estimation in Power Systems: A Multi-Estimator Data Fusion Approach to Counteract Cyber-Attacks. *Chinese Journal of Information Fusion*, 1(3), 212–225.

© 2024 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

Recently, numerous studies have been conducted on cyber attacks within power systems. Traditional state estimation methods are based on static estimation using the least squares approach. To detect cyber attacks in the system under static estimation, researchers in [7] have explored how to enhance the robustness of power system state estimation against stealthy FDI attacks. The authors proposed a method that combines data preprocessing with post-processing of state estimates to reduce the likelihood of successful attacks by adversaries. An optimization-based approach was presented in [8] to maximize the impact of attacks, and the manuscript discussed how to mitigate these attacks by adjusting system parameters. A probabilistic approach is employed in [9] to analyze and defend against FDI attacks. The researchers introduced a detection algorithm based on a probabilistic model, aimed at enhancing the power system's resilience against such attacks. Moving target denfence (MTD) has emerged as an effective strategy for detecting FDI attacks within the static state estimation of power systems. Defenders increase the error introduced by the attack vector by altering the system's topology. Comprehensive analyses have been conducted in [10–14], defining both complete and incomplete MTD and designing robust denfence algorithms. Reference [15] takes economic factors into account, and an optimal defense strategy is presented by integrating game-theoretic methods. Additionally, detection methods based on machine learning have recently gained widespread research attention, playing a significant role in attack detection [16, 17].

With the continuous development of smart grids, the static estimation, which is computationally simple and updates at a slower frequency, no longer meets the demands of modern power systems. Dynamic estimation based on the Kalman filter is gradually becoming the mainstream in state estimation [18]. Dynamic state estimation in power systems, augmented by high-sampling and high-precision measurements from Phasor Measurement Units (PMUs), effectively enhances the detection of cyber attacks within the system. Reference [19] introduces an Extended Kalman Particle Filter-based approach for dynamic state estimation in power systems. By constructing the importance sampling density function within the particle filter using the Extended Kalman Filter, it effectively addresses the particle degeneracy issue, achieving high-precision state estimation. References [20] and [21] further refine the Kalman filter within the context of dynamic estimation, significantly improving the system's robustness. The authors derive and calculate the range of attack vectors for three types of attacks that can successfully destabilize the system, and determine the range of failure for the chi-squared detector against FDI attacks in [22].

The methods described above are capable of detecting cyber attacks within a system and initiating alarms, with the resumption of normal state estimation operations contingent upon the resolution of detected anomalies. However, the operation of power systems is critically important, and even brief periods of maintenance can lead to substantial economic losses. Furthermore, as the capabilities of attackers advance, there has been a surge in research on stealth FDI attacks [23, 24]. These meticulously designed attack vectors can evade detection while inflicting the maximum possible damage on the system. Consequently, there is an urgent requirement for estimation algorithms that can sustain the normal functioning of power systems under attacks and significantly reduce the impact of such attacks. It is evident that traditional estimation methods, which rely on a single estimator, are inadequate for achieving this objective. In this manuscript, we introduce an innovative approach by combining information-fusion-based distributed algorithms with dynamic power system estimation to address the current challenges. Information fusion, a cutting-edge technology, is particularly effective in mitigating the effects of data loss and the introduction of false data [25–27]. We introduce a novel multi-estimator-based distributed estimation methodology, which is designed to effectively diminish the repercussions of data loss and the infiltration of false data. Furthermore, we have developed a weighting strategy grounded in KL-divergence principles, which has proven to be instrumental in diminishing the effects of covert attacks.

The main contributions of our research are as follows:

1. We have designed a state estimation algorithm that ensures the normal operation of state estimation at critical buses under cyber attacks. Additionally, by incorporating KL-divergence detectors on each estimator to detect linear FDI attacks, the integrity of state estimation is effectively safeguarded.

2. In response to stealthy attacks that can evade detection, we propose a novel weighting strategy. This strategy assigns lower weights to estimation

results that are significantly affected by noise and attacks, while higher weights are given to those less affected, thereby effectively reducing the interference of noise and stealthy attacks and enhancing the accuracy of estimation.

3. We demonstrate that the proposed algorithm is superior in accuracy and robustness compared to traditional algorithms when subjected to DoS attacks and FDI attacks by numerical experiments.

The structure of this manuscript is organized as follow: Section 2 provides a concise introduce about the system model and related theories. Section 3 presents the model and estimation algorithm proposed in this manuscript. Section 4 consists of numerical experiments and analysis of the results. Section 5 presents the conclusion of this manuscript.

2 System Model

2.1 State-space model

Power system state estimation can be categorized into two primary methods: DC (Direct Current) estimation and AC (Alternating Current) estimation.The state variables in AC estimation encompass both the phase angle and the voltage magnitude, providing a comprehensive representation of the system's state.In contrast, DC estimation, a simplified version, includes only the voltage magnitude, omitting the phase angle.In this manuscript, we focus primarily on the more prevalent AC estimation approach due to its comprehensiveness and applicability in practical scenarios.Similar to the work presented in [18], the state signal obtained in real-time by sensors can be considered as a discrete-time function concerning the voltage amplitude A_v and the phase angle $(\theta + \phi)$, denoted as :

$$V(t) = A_v \cos(\omega t + \phi) \tag{1}$$

By expanding the trigonometric function in Eq.1, we can derive the following equation:

$$V(t) = A_v \cos(\omega t + \phi) - A_v \sin(\omega t + \phi) \tag{2}$$

Assuming that the voltage frequency ω of the system's buses remains constant over time, and considering only the voltage amplitude and phase angle as variables in the state space, we define the system's state as $x_1 = A_v \cos(\omega t)$ and $x_2 = A_v \sin(\omega t)$. The state signal $V(t)$ acquired by the sensor can be expressed as:

$$V(t) = x_1 \cos(\omega t) - x_2 \sin(\omega t) \tag{3}$$

Assuming there are no additional delays in the system and taking into account the process noise and measurement noise in the calculation, the state equation and measurement equation for the system's buses are:

$$x(t+1) = Ax(t) + w_0(t) \tag{4a}$$
$$y(t) = Cx(t) + w_i(t) \tag{4b}$$

where the state vector $x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}^T$, the system matrix $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and the measurement matrix $C = \begin{bmatrix} \cos(\omega t) \\ -\sin(\omega t) \end{bmatrix}$. $w_0(t)$ and $w_i(t)$ represent the system's process noise and measurement noise, respectively. In power systems, the process noise $w_0(t)$ is small enough and can be neglected during estimation. The measurement noise $w_i(t)$ is assumed to be zero-mean, independently and identically distributed Gaussian noise with a standard deviation of σ and independent of the initial conditions of the system and the process noise.

Based on the state and measurement equations presented, the control center can perform optimal estimation of the system state using the Kalman filter. The estimation process of the Kalman filter follows the formula shown below:

$$x(t) = Ax(t-1) \tag{5a}$$
$$P(t) = AP(t-1)A^T \tag{5b}$$
$$K(t) = P(t-1)C^T(CP(t-1)C^T + W_i)^{-1} \tag{5c}$$
$$\hat{P}(t) = (AP(t-1)A^T)^{-1} + C^T W_i^{-1} C \tag{5d}$$
$$\hat{x}(t) = Ax(t) + K(y(t) - CAx(t-1)) \tag{5e}$$

where $x(t)$ represents the estimated state vector $x(t)$ at time t, and $P(t)$ denotes the covariance matrix of the estimated state at time t.$K(t)$ represents the Kalman gain and $z(t) = (y(t) - CAx(t-1))$ is defined as the innovation of the system. Through the iterative updates, we can obtain the state prediction value at time t with the information at time $(t-1)$, which contains the voltage amplitude and phase angle of the buses.

2.2 Attack model

In this section, we would like to model prevalent cyber threats within power system networks. We mainly focuses on DoS attacks, linear FDI attacks

targeting single estimator systems, and stochastic stealth attacks targeting multi-estimaor systems. We begin our analysis with the most fundamental form of DoS attack. The DoS attack, which is an aggressive maneuver designed to impede the control center's ability to retrieve data from sensors. This disruption is orchestrated by adversaries who either sever communication channels or inundate the network with an excessive deluge of data packets, consequently compromising bandwidth and thwarting the transmission of essential data[3, 4]. In this manuscript, the DoS attack on estimator i is modeled as a Bernoulli variable $\gamma_i \sim \mathcal{B}(1, p)$, implying that the occurrence of an attack is a stochastic event that can be described by a Bernoulli distribution. The Bernoulli distribution is a discrete probability distribution with only two possible outcomes: $\gamma_i = 0$ (the attack occurs) and $\gamma_i = 1$ (the attack does not occur).In the context of DoS attacks, the probability of fail attack is denoted by p, and the probability of successful attack is $1 - p$.

$$\gamma_i(t) = \begin{cases} 0 & \text{if an attack occurs at time } t \\ 1 & \text{if no attack occurs at time } t \end{cases}$$

We assume that the attacker's assault is exerted during the process where the sensor transmits the innovation z to the estimator. Assuming that the i_{th} sensor is under attack, all subsequent subscripts i in the following text refer to estimator i. Consequently, the innovation received by the estimator can be represented as:

$$\hat{z}_i(t) = \gamma_i(t) * z_i(t) \tag{6}$$

When the attack is successful, $\gamma_i(t) = 0$, indicating that the estimator is unable to receive the innovation transmitted from the sensor. Conversely, when the attack fails, the innovation transmitted to the estimator remains unaffected. So that we have completed the modeling of the DoS attack.

Next, we consider linear FDI attacks targeting single-estimator systems. Similar to the mathematical model used in man-in-the-middle attacks [5, 6], we assume that the attacker has complete knowledge of the system's physical model and possesses the capability to access and alter measurements. Specifically, the attacker can arbitrarily modify the innovation z_i obtained by the estimator. Consequently, the attack strategy against estimator i can be defined as:

$$\tilde{z}_i(t) = f_k(z_i(t)) \tag{7}$$

Regarding the non-linear function f_k, it is challenging to analyze its statistical properties, which complicates the determination of system performance and the effectiveness of attacks. Additionally, linear transformations of data do not alter the type of statistical distribution of the data, which enables attackers to deceive detectors that rely on distribution properties. Furthermore, in real-world power systems, random linear attacks may be more feasible and cost-effective to implement. Therefore, we only focus on FDI attacks under the assumption of linear functions [24].

$$\hat{z}_i(t) = T_i \cdot z_i(t) + b_i \tag{8}$$

where T_i is an arbitrary attack matrix and b_i is a constant independent of z_i.

In light of the preceding discussion, we now turn our attention to stochastic stealth attacks targeting multiple estimators. The linear FDI attacks strategy mentioned earlier impose demanding requirements on the attackers, necessitating capabilities that are not feasible to replicate across multiple estimators simultaneously. Additionally, the multi-estimator system significantly increases the complexity of information, which renders the attack methods applied to single estimators ineffective or less potent. To maximize the impact of attacks within a system equipped with multiple estimators, a stochastic stealthy attack strategy based on maximum attack probability has been proposed in [25]:

$$\hat{z}_i(t) = z_i(t) + c_i\zeta_i(t) \tag{9}$$

where c_i represents if there is an attack present in the communication channel of estimator i.$P(c_i = 1) = p$, representing the attack being applied to estimator i and $P(c_i = 0) = 1 - p$, indicating that estimator i is not under attack. The attack signal $\zeta_i \sim \mathcal{N}(0, \sigma_\zeta)$ is a Gaussian distribution that is independent of z_i. With the modeling of the three attack methodologies now complete, it is important to note that the strategies discussed are among the simpler to implement, offer effective attack outcomes, and possess a high degree of stealth. In the realm of power systems, there also exist FDI attacks constructed through data-driven approaches and physical-model based methods. However, these alternatives present various challenges: some are not suitable for dynamic estimation, others demand extensive datasets, and some could be too demanding for attackers. Furthermore, certain methods can disrupt the statistical properties of data, making them more susceptible to detection by common detectors, such as those based on KL-divergence. For these

reasons, they are not within the scope of the present discussion.

2.3 Detection model

We now proceed to discuss the detection model within the system. The extensive wireless sensor networks in smart grids offer ample opportunities for attackers to launch attacks. Consequently, it is imperative to have a detector at the controller end to scrutinize the acquired data for any anomalies or signs of compromise. In the realm of dynamic estimation within smart grids, detectors based on the Kullback-Leibler (KL) divergence have demonstrated remarkable efficacy in detecting cyber attacks. KL-divergence is a crucial concept used to quantify the differences between two probability distributions, which can measure the degree of difference between an actual distribution and another expected distribution. Its definition follows:

$$D(\tilde{\gamma}_k \| \gamma_k) = \int \log \frac{f_{\tilde{\gamma}_k}(\xi_k)}{f_{\gamma_k}(\xi_k)} f_{\tilde{\gamma}_k \| \gamma_k}(\xi_k) d\xi_k \tag{10}$$

$$D(\tilde{\gamma}_k \ \| \ \gamma_k) \leq \delta$$

where $f_{\tilde{\gamma}_k}$ and f_{γ_k} are the probability density function of random sequences $\tilde{\gamma}_k$ and γ_k.It can be observed that $D(\tilde{\gamma}_k \ \| \ \gamma_k) = 0$ if and only if $f_{\tilde{\gamma}_k} = f_{\gamma_k}$, and the K-L divergence is generally not symmetric, ie., $D(\tilde{\gamma}_k \| \gamma_k) \neq D(\gamma_k \| \tilde{\gamma}_k)$ [28]. When $D(\tilde{\gamma}_k \| \gamma_k) \leq \delta$, no anomalies are detected by the sensors, and the data acquired by the estimator is considered normal.When $D(\tilde{\gamma}_k \| \gamma_k) > \delta$, the sensors trigger an alarm, indicating that the data requires inspection. It is necessary to troubleshoot and mitigate any faults or stop any ongoing attacks before resuming normal operation.

Remark 2.1 *Considering the persistent operational nature of power systems, which are vast and complex, the acquisition of extensive data required for analysis is readily achievable. Based on historical data, we can derive the probability density function of the real innovation.*

3 Main Result

3.1 Multi-estimator based estimation

In this section, we present our main results, beginning with the distribution approach based on multi-estimator information fusion. When anomalies occur within the system, state estimation relying on single estimator must be stopped to address the issues before resuming operations. However, the measurement data from certain critical buses are essential for the whole system, and even brief interruptions can lead to significant losses. Therefore, this manuscript is dedicated to devising a novel estimation strategy that ensures the system's continuous operation despite the presence of faults or under attack. It is evident that a single estimator is inadequate for the task of state estimation mentioned above. Therefore, we contemplate employing an approach that integrates information from multiple estimators to achieve this objective. Dynamic estimation based on the fusion of information from multiple estimators has become a widely applied method for interference-resistant estimation in recent years. Since the estimators are independent of each other and the attacker's capabilities are limited, an attack on a single estimator cannot affect the entire state estimation process. Utilizing an estimation approach that fuses information at critical buses can effectively ensure that the system continues to operate normally even when attacks are detected.

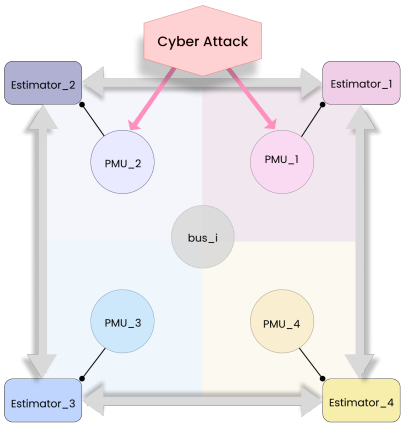


Figure 1. Schematic of multi-estimator based state estimation.

First, we need to select key buses based on economic considerations and the degree of information redundancy[29], and deploy multiple estimators at these critical buses. The structure of the estimator network at the key buses is shown in Figure 1. Each estimator includes a PMU for independently collecting data, a Kalman filter for estimating the state, and communication equipment for transmitting data. Each estimator operates independently, processing data and generating results that are subsequently subjected to a verification procedure. If the results are deemed normal, they are incorporated into subsequent computational steps. However, if any anomalies are detected, the communication of the respective estimator is immediately severed, and an alarm is triggered to alert system operators. By combining

the estimation results from neighbor estimators, the estimated state vector $\hat{x}_i(t)$ at time t and estimated covariance matrix $\hat{P}_i(t)$ by estimator e_i can be obtained as follows:

$$\hat{x}_i(t) = \sum_{j \in \mathcal{N}_i} \lambda_{ij}(t) w_{ij}(t) \hat{x}_{ij}(t) \tag{11a}$$

$$\hat{P}_i(t) = \sum_{j \in \mathcal{N}_i} \lambda_{ij}(t) w_{ij}(t) \hat{P}_{ij}(t) \tag{11b}$$

where N_i represents the set of estimators that can exchange information with estimator e_i, including e_i itself. The variable $\lambda_{ij}(t)$ denotes the detection outcome of the detector in estimator e_j at time t. If the detection is normal at that moment, $\lambda_{ij}(t) = 1$; if estimator e_j is abnormal at that moment, its communication network is severed by the detector, and λ_{ij} will remain 0 until the anomaly is resolved. The notation $\hat{x}_{ij}(t)$ and $\hat{P}_{ij}(t)$ represent respectively the estimation result and covariance matrixz received by estimator e_i from estimator e_j.The convergence of this distributed method has been demonstrated in [30].The weight $w_{ij}(t)$ indicates the influence of the results obtained by estimator e_j within estimator e_i; For the time being, all estimation results are assigned equal weight.

$$w_{ij} = \frac{1}{\sum \lambda_{ij}(t)} \tag{12}$$

A multitude of strategies have been proposed to counteract FDI attacks in sensor networks such as the correntropy-based method [31] and partial consensus method [32] . However, with the constraints on computational resources and bandwidth at buses within power systems, the feasibility of implementing highly sophisticated methods is limited. Consequently, we have adopted a more straightforward weighted approach, which is better suited to the operational realities of power system environments. We will make improvements based on arithmetic and bandwidth constraints in next subsection.

Subsequent numerical experiments have demonstrated that our methodology is capable of sustaining the regular functioning of crucial buses within the system, even in the scene of DoS and FDI attacks."

Remark 3.1 *Despite the robustness against interference and the high estimation precision of state estimation methods that leverage multiple estimators, the prohibitive costs associated with PMUs and the constraints on computational resources preclude their universal application across all buses in power systems.Additionally, the number of estimators installed at each bus should not be excessive; ideally, the best choice based on practical considerations is to install 3-4 sets. In [29], an installation strategy for PMUs is proposed that takes into account the correlation of measurements, enabling the strategic placement of PMUs at critical buses to utilize the methodologies proposed in this manuscript.*

3.2 KL-divergence based weighting strategy

In the event of cyber attacks, the multi-estimator based data fusion approach is adept at sustaining the system's normalcy even amidst anomalous conditions.Nevertheless, with the advancement in attackers' capabilities, the stealthiness and destructive potential of these attacks have escalated.As delineated in [23] and [24] two stealthy FDI attack models are presented, which not only evade detection by KL-divergence detectors but also inflict substantial damage on the system. When confronted with such stealth attacks, the aforementioned method falls short in reducing the influence imposed by these threats.

Prior to implementing the novel weighting strategy, it is essential to determine the differences between the actual innovation probability distribution under cyber attacks and the prior probability distribution of the innovation.

Assumption 3.1 *Considering the complex information within power systems and the capabilities of potential attackers. In this manuscript assumes that no more than one type of cyber attack will occur simultaneously within the system., which means an attacker can only execute a single type of attack on the system at any given time.*

3.2.1 DoS attack

We begin by analyzing the KL-divergence between $\hat{z}_i(t)$ and $z_i(t)$ under the conditions of DoS attack. As previously mentioned, $z_i(t)$ is a Gaussian variable with mean 0 and standard deviation σ, its probability density function can be expressed as:

$$f_{z_i}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \tag{13}$$

where $\hat{z}_i(t)$ is the product of Bernoulli distribution $\gamma_i(t)$ and $z_i(t)$ with the probability density function:

$$f_{\hat{z}_i}(x) = (1-p) \cdot \delta(x) + p \cdot \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \tag{14}$$

where $\delta(x)$ is a Dirac delta function representing the probability of $\hat{z}_i = 0$. Based on the probability density

functions we can obtain:

$$D_{KL}\left(f_{\hat{z}_i}||f_{z_i}\right)=\int_{-\infty}^{\infty}\left[(1-p)\delta(x)+p\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{x^2}{2\sigma^2}}\right]*\log\frac{(1-p)\delta(x)+p\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{x^2}{2\sigma^2}}}{\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{x^2}{2\sigma^2}}}dx \tag{15}$$

Since $\hat{z}_i$ is a mixture distribution, Eq.15 takes into account the contributions from both the Dirac delta function and the Gaussian distribution. However, the integral involves the logarithm of the Dirac delta function, which is undefined at zero, necessitating an alternative approach to analyze the divergence between $f_{\hat{z}_i}(x)$ and $f_{z_i}(x)$. By analyzing the composition of $\hat{z}_i$ we notice that the difference arises mainly from the uncertainty of γ_i. Hence, the information entropy of γ_i serves as a pertinent indicator to quantify the degree of influence on the innovation. The information entropy of a random variable P can be obtained through the following formula:

$$H(P)=-\sum_{i=1}^{n}p_i\log p_i \tag{16}$$

where γ_i is a Bernoulli random variable with probability p, its information entropy can be expressed as:

$$H(\zeta_i)=-p\log p-(1-p)\log(1-p) \tag{17}$$

According to the preceding discussion, it becomes evident that the divergence in probability distributions between $\hat{z}_i(t)$ and $z_i(t)$ under DoS attacks is solely contingent upon the capabilities of the attacker. When there exist an attack, each estimator is subjected to an attack that makes $(1-p)$ maximal, rendering the KL-divergence-based weighted approach equivalent to one with equal weighting. Therefore, in subsequent experimental results, we will focus exclusively on the distinction between estimates derived from multi-estimator data fusion and those from single estimator.

3.2.2 *Linear FDI attack against single estimator*

Next, we consider a linear attack targeting single estimator, where the attacker constructs an attack vector by performing linear operations on Estimator i. Since linear operations on a Gaussian distribution do not alter its probability distribution, $\hat{z}_i$ remains a Gaussian distribution with mean b and variance $T^2\sigma^2$. According to [33, 34], we can define b and $T^2\sigma^2$ as $\mu_{\hat{z}_i}$ and $\sigma_{\hat{z}_i}$, the KL-divergence between $\hat{z}_i$ and z_i as:

$$D_{KL}\left(f_{\hat{z}_i}||f_{z_i}\right)=-\frac{1}{2}\log\frac{\sigma_{\hat{z}_i}^2}{\sigma_{z_i}^2}+\frac{\sigma_{z_i}^2}{2\sigma_{\hat{z}_i}^2}+\frac{(\mu_{\hat{z}_i}-\mu_{z_i})^2}{2\sigma_{\hat{z}_i}^2}-\frac{1}{2} \tag{18}$$

The above equation indicates that as long as we obtain the parameters of the Gaussian distributions, we can obtain the required KL-divergence. However, although we can easily obtain the probability distribution of z_i, we still cannot directly obtain the distribution of $\hat{z}_i$. To obtain the KL-divergence, we need sufficient data to analyze its probability distribution. Therefore, before employing the new weighting strategy, we require a period of data collection to gather information, and state estimation can only proceed once the results are stable.

3.2.3 *Stochastic Stealth FDI Attacks Against Multiple Estimators*

Finally, let us consider the stochastic stealth attack targeting multiple estimators. From the perspective of attackers, we must consider a multi-estimator system as a complex network where information exchange is pervasive. Each estimator's covariance matrix and state updates are influenced by the data obtained from neighboring estimators, which means that an attack on one estimator can have indirect effects on others through the information sharing network.

When analyzing attacks on multiple estimators, it is crucial to account for the interconnectedness and the potential for compounded impacts of an attack across the system. The challenge for the attacker is to craft an attack strategy that exploits the system's inherent dependencies and information exchange mechanisms to remain undetected while still achieving the attack objectives.

However, as the defender, we cannot obtain the opponents' attack strategy and can only determine whether there is an attack on the corresponding estimator through the detector. Since the design process of the attack vector involves linear operations on the Gaussian distribution, the innovation $\hat{z}_i$ after being attacked still conforms to the Gaussian distribution with mean 0 and variance $\sigma^2+\sigma_\zeta^2$, and its KL-divergence with z_i can still be calculated using Equation 18.

In conclusion, we can derive the following insights: Under DoS attacks, the detection and weighting methods based on KL-divergence are not particularly effective, with estimation results

closely resembling those of the Multi-estimators based method.Additionally, the innovation $\hat{z}_i$ in both types of FDI attacks conforms to a Gaussian distribution, and their KL-divergence with z_i can be obtained through Equation 18.

3.2.4 KL-divergence based weighting strategy

In this manuscript, we introduce a novel weighting strategy based on KL-divergence. Since KL-divergence is adept at characterizing the degree of difference between two probability distributions, it is highly suitable for assessing the extent to which an estimator is compromised by an attack. Consequently, we can apply varying weights to the estimation results based on the level of attack, thereby mitigating the impact of the attack.

Specifically, we computed the KL divergence between the actual innovation probability distribution and the prior innovation probability distribution for each estimator to analyze the extent to which the estimation results were affected by attacks. Results with larger KL divergences were assigned higher weights, while those with lower divergences received lower weights.

$$w_{ij}(k) = \frac{\alpha_{ij}(t) f(D_{ij}(t))}{\sum_{j=1}^{n} \alpha_{ij}(t) f(D_{ij}(t))} \tag{19}$$

In equation 19, $\alpha_{ij}(t)$ represents the detection result of the K-L divergence detector on estimator e_j.If the detector passes the test, $\alpha_{ij}(t)$ is 1; otherwise, it is 0. $D_{ij}(t)$ denotes the K-L divergence between the actual noise and the normal noise on estimator e_j. When both $\lambda_{ij}(t)$ and $\alpha_{ij}(t)$ are 1, there is no anomaly on estimator e_j. [30] demands that $f(x)$ is a continuous non-negative and strictly decreasing function, which in this manuscript is defined as $1/x$. The obtained result $\hat{x}_{ij}(t)$ and the K-L divergence can be transmitted to the estimators with which it can communicate, and information can be obtained from these estimators. Then, using this information, the weights for each state estimation value are calculated, which in turn are used to compute the final estimation result.

4 Numerical Experiments

In this section, we conducted numerical experiments using Matlab to evaluate the dynamic estimation based on Kalman Filtering, multi-estimator based estimation and the novel algorithm with KL-divergence based weighting strategy (Abbreviated as KL-divergence based estimation in the subsequent text). Initially, we provide the following clarifications regarding the data used in the experiments:

In this manuscript, the primary objective of the proposed method is to safeguard critical buses within the power grid, mitigate the interference from noise and cyber attacks, and ensure the normal operation of the power system, with data from these key buses being acquired exclusively by PMUs. According to [16], we have established the following provisions for all PMUs: it is assumed that all PMUs installed in the system are of the same model with identical preset sampling frequencies and cycle periods. The amplitude A_v of the voltage signal in the power system is set to 1, the phase angle ϕ is 0, and the sampling frequency is 60Hz, and the sampling period is 1800Hz, which means the signal is sampled 1800 times per second, with 30 sampling points existing within each signal period. Sampling time is set to $0.1s$.Furthermore, in accordance with the guidelines in [35, 36], independent and identically distributed Gaussian noise with a Signal-to-Noise Ratio (SNR) of 70 dB is applied to each PMU. When employing the multi-estimator based algorithm, considering the redundancy of information and economic factors, we have installed three estimators at each critical bus. Each estimator comprises a PMU, a Kalman filter, and a KL-divergence detector.

4.1 Kalman Filter

First we conducted a test on the Kalman Filter(KF) estimation. The system's initial parameters are set as follows: $x_1(0) = 0$, $x_2(0) = 0$, and the covariance matrix P is set to the identity matrix (these initial conditions were maintained consistent throughout the subsequent experiments). Matlab function $randn()$ is used to produce normally distributed noise. We define the sinusoidal voltage signal with noise as the input and the resulting signal from the state estimation is taken as the output. The experimental results are presented in Figure 2. The red curve denotes the input signal, while the blue one indicates the output. It can be seen that the output curve from the state estimation closely matches the input signal, which sufficiently meets the typical requirements of the power system.

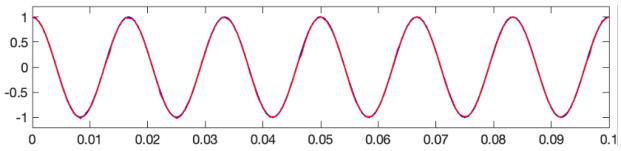


Figure 2. Kalman Filter estimation when there is no attack.

4.2 Estimation under DoS attack

Subsequently, we consider the state estimation under DoS attack. The attacker applies the attack in a manner that maximizes their attacking capability, which means that each estimator is subject to an attack with equal probability. As mentioned before, the difference between the probability distributions only related to the probability of each estimator being attacked. Consequently, in such circumstances, there is no distinction between two different weighting methods. Therefore we only focus on the discrepancies between KF estimation and multi-estimator based estimation.

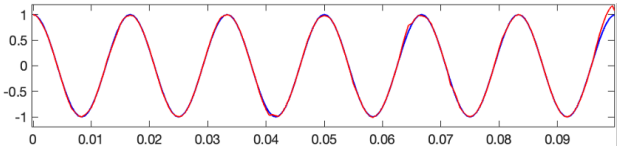


Figure 3. Kalman filter estimation under DoS attack.

When an attacker is unable to target all estimators within a system, multi-estimator based estimation invariably outperforms KF estimation. The advantage is apparent because there are estimators within the system that remain unaffected by the attacks, which can offer data compensation for those estimators that are under attack during the estimation process, thereby reducing the attack's influence. Consequently, in our experiments, we assume that all estimators are subjected to the attacker's assault with an equal probability of $1-p$. Referring to [16], we select $1-p=0.6$ as the probability of a successful attack. Upon a successful attack, the communication channels transmitting data will be severed, rendering estimators incapable of receiving measurements from the sensors.

The results obtained from the KF estimator are depicted in Figure 3. The experimental outcomes reveal that the KF estimation exhibits noticeable errors, demonstrating the impact of data loss on state estimation. The results of the Multi-estimators estimation are presented in Figure 4. Even when all estimators are under attack, the output signal from the state estimation closely resembles the input signal, which is significantly superior to the KF estimation. The Multi-estimator based estimation has a probability of only $(1-p)^3$ for complete data loss, whereas the single estimator has a probability of p, thus being more markedly affected by DoS attack.

Experiments have demonstrated that in the presence of DoS attacks within the system, Multi-estimator based estimation exhibits superior robustness, yielding more precise estimation results .In next subsection we will consider the performance of different estimation methods when confronted with FDI attacks.

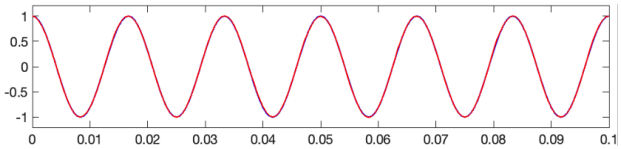


Figure 4. Multi-estimators based estimation under DoS attack.

4.3 Estimation under Linear FDI attack

In this subsection we simulate the linear FDI attack targeting single estimator. Initially, we test an attack that triggers the detector alarm, which means the FDI attack does not possess stealthiness. When the detection result exceeds the threshold, the detector status turns to abnormal, and the communication channel transmitting information from the corresponding estimator is severed. The estimated state of the bus will be provided by other estimators. Furthermore, obtaining the KL-divergence requires sufficient data to determine the probability distribution, which is easily obtainable in power systems. We reset the sampling time to 1s, with the first 0.9 s dedicated to data collection, and estimation of the state commences from 0.9 second. We apply an attack on Estimator 1, and according to Equation 8, we set T_i to 1.7 and the constant b_i to 0.08. Under this simple attack, the detector will trigger an alarm, while the other estimators will not be affected by the attack's influence. The state of the detector at 0.9s is abnormal. The results from three different estimators are presented in Figure 5.

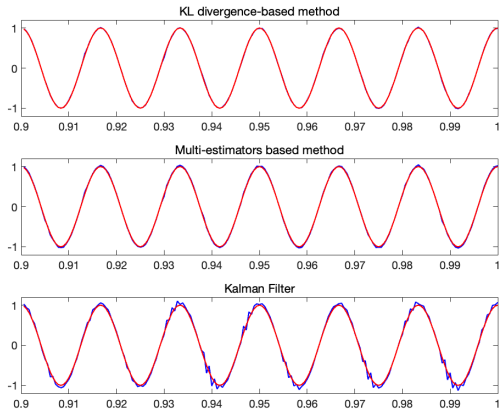


Figure 5. Comparison of three estimation methods under linear FDI attack.

The experimental outcomes clearly demonstrate that the KF estimator exhibits the least favorable

performance. This deficiency stems from the absence of extra estimators within its system to counteract the effects of the attack on single estimator. Multi-estimator based method yields estimation results that markedly outperform those of the KF estimator. This enhancement is attributed to the presence of two estimators within the system that are impervious to the attack. Despite equal weighting of the estimation states from all three estimators, the two uncompromisable estimators contribute precise data, thereby substantially diminishing the detrimental effects of the FDI attack.

The estimation method based on KL-divergence yields the best results, which is quite understandable. At the beginning of state estimation, the attacked estimator is marked as abnormal, its communication channel is severed, and the results it yields no longer impact the entire system; the remaining state estimation is accomplished solely by the unaffected estimators. In other words, the detector can effectively block FDI attacks that do not possess stealthiness, and the system will remain unaffected by such attacks. This experiment only serves to demonstrate the effectiveness of the KL-divergence detector, but it does not indicate the advantages of the weighted strategy. We will proceed to illustrate the superiority of the new estimation method through stealthy attacks.

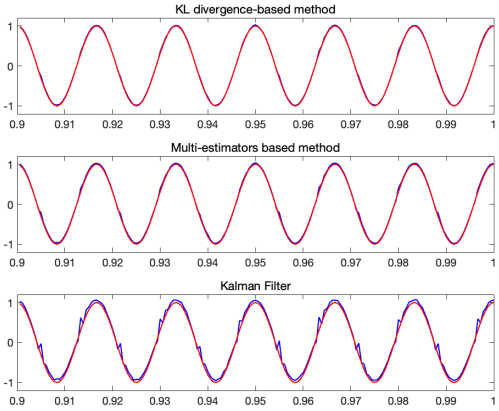


Figure 6. Comparison of three estimation methods under stealth linear FDI attack.

Next we take the stealth FDI attack into consideration. According to [24], we can obtain the attack parameters that yield the most effective results without being detected. We reset parameter T_i to 1.3 and b_i to 0.06, which will have the greatest impact on the estimator while maintaining stealth. The attack is still applied to Estimator 1.The experimental results are shown in Figure 6.

The estimation performance of the KF estimator remains the poorest, with its output signal being affected to a similar extent as the one in Figure 5, which indicates that the modified FDI attack not only has stealth characteristics but also achieves significant disruptive effects. The Multi-estimator based method yields better results than the KF estimator but falls short compared to the KL-divergence based method. However, due to the stealthiness of the attack in this experiment, the detector fails to trigger an alarm and sever the communication channel of Estimator 1.Consequently, the KL divergence based method cannot produce a signal entirely unaffected by the attack as seen in Figure 5.It can only rely on the weighted strategy to assign a lower weight to the more severely affected estimation results, thereby reducing the estimation error.

To better demonstrate the advantages of the new weighting strategy, we compare the absolute errors between the results obtained from the KL-divergence based method and the Multi-estimator based method with the input signal. The errors $|e_i|$ can be obtained by: $|e_i| = |\hat{z}_i - z_i|$.The comparison results are presented in Figure 7.

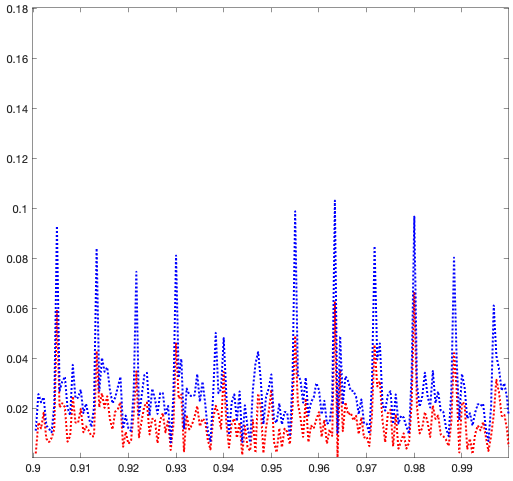


Figure 7. Comparison of estimation errors under linear FDI attacks with different weighting strategy.

In Figure 8, the horizontal axis represents time, and the vertical axis represents the absolute value of the estimation error. Blue curve represents the error of the Multi-estimators based method, and the red one represents the error of the KL-divergence based method. It is evident that for the majority of the time, the blue curve is above the red curve, indicating that the method employing the new weighting strategy

yields better estimation results.

The outcomes illustrated in Figures 5 and 6 indicate that in the presence of undetectable stealthy attacks within the system, the novel weighting strategy effectively enhances the estimation's robustness and precision. Despite the detector's inability to trigger an alarm or sever the communication channels, this strategy mitigates the influence of the attacked estimation results by apportioning varying weights. Consequently, it elevates the significance of the unaffected estimation outcomes, bolstering the system's resilience against such stealth attack.

4.4 Estimation under Stochastic Stealth FDI attack

Finally, we will test the system's estimation performance under Stochastic Stealth FDI attack. According to Equation 9, we set the intensity of ζ_i to three times the level of the system noise. Referring to reference [23], we set p to 0.6, which that the probability of each estimator under attack is $p = 0.6$. When an estimator is attacked, a stronger Gaussian noise is superimposed on the innovation z_i.The output signals estimated by three different methods are displayed in Figure 8:

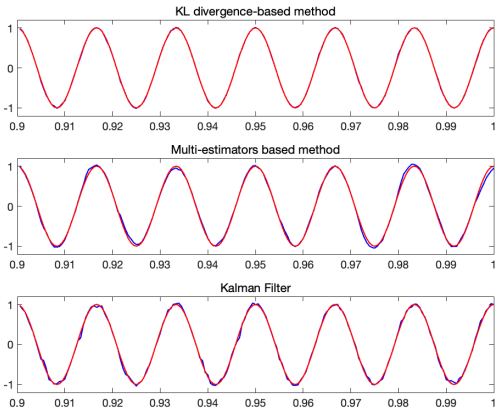


Figure 8. Comparison of three estimation methods under stochastic stealthy FDI attack.

Unlike the previous experimental results, in this experiment, the estimation effect of the KF estimator is not significantly worse than that of the Multi-estimators based method. Upon reviewing the experimental data, we analyzed the cause of this outcome: when attacking all estimators with a probability of 0.6, two estimators in the Multi-estimators based method were attacked. With two estimators simultaneously under attack, the single normal estimation result could not offset the influence of the two abnormal results, leading to an estimation accuracy similar to that of the KF estimation. In contrast to these two methods, the results obtained by the KL-divergence based method were largely unaffected by the attacks, as the abnormal results were assigned a sufficiently small weight, while the normal results had a higher weight, which dominated in the final outcome. Therefore, as long as there are estimators in the system that are not under attack, the estimation method employing the new weighting strategy will maintain a high level of estimation accuracy. As mentioned earlier, the attacker's capabilities are greatly limited, and it is essentially impossible to launch simultaneous attacks on all estimators in the system (usually 3 to 4).Thus, the methods proposed in this manuscript essentially meet the needs of state estimation in power systems.

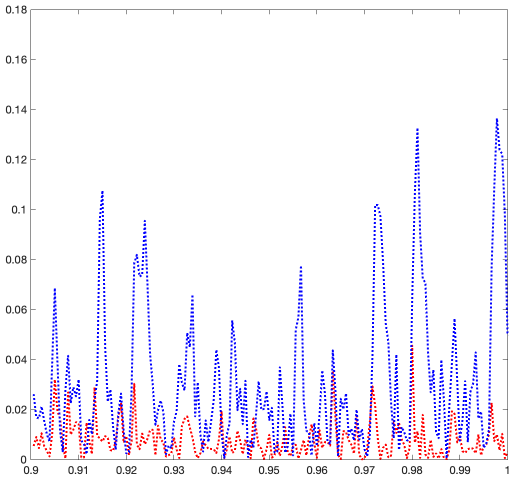


Figure 9. Comparison of estimation errors under stochastic stealth FDI attacks with different weighting strategy.

Similar to the previous subsection, in this experiment, we again compared the estimation errors of two methods. The results are displayed in Figure 9, where blue still represents the Multi-estimators based method and red one represents the KL-divergence based method. It is evident that the blue curve is significantly higher than the red one, which indicates that the new weighting strategy yields a smaller estimation error and higher precision.

It is noticed that the Figure 9 reveals a representative phenomenon: when the estimation errors of both methods are relatively small, the difference in height between the two curves is not significant. However, when the blue curve rises prominently, the difference in height between the curves becomes markedly evident. The explanation for this phenomenon is that the noise

added to the estimators follows a normal distribution with a mean of zero so that the intensity of the attack on the innovation z_i varies at different time. Although the new weighting strategy assigns higher weights to the correct results, it does not fully demonstrate its advantage when the attack is weak, leading to minimal differences between the two curves. In contrast, when the attack is strong, the new method reduces the weight of the abnormal results sufficiently, effectively mitigating the impact of the attack, which results in a significant difference between the two curves.

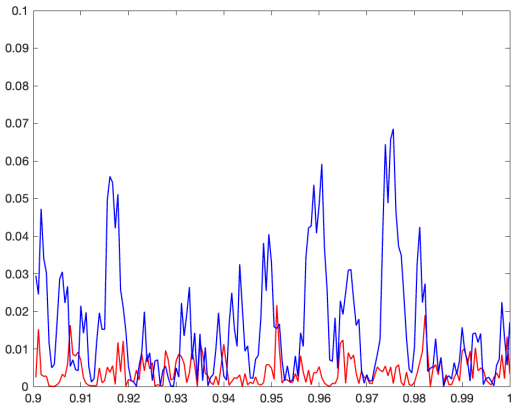


Figure 10. Comparison of estimation errors under different mitigation attack algorithms.

Furthermore, to demonstrate the superiority of the approach outlined in our manuscript, we have conducted comparative experiments between the algorithm presented in our work and the method described in [30]. The results of these experiments are depicted in Figure 10, where the red line corresponds to the KL divergence-based method. The experimental findings indicate that, in the vast majority of instances, our method provides more precise estimation outcomes. This is readily understandable, as a meticulously crafted attack vector does not significantly alter the covariance but substantially affects the KL divergence of the innovation. Consequently, our method outperforms in such scenarios.

Through the experiments conducted in the four subsections above, we have demonstrated that our method can effectively maintain the normal operation of state estimation under no attack, DoS attacks, regular FDI attacks, and stealthy FDI attacks.Additionally, we have proven the superiority of the new weighting strategy in terms of robustness and estimation accuracy when facing attacks.

5 Conclusion

This manuscripts introduces an estimation algorithm based on the fusion of data from estimators to address the state estimation problem at critical buses in power systems. By deploying multiple estimators at key buses and incorporating a KL divergence-based detector, the proposed algorithm can effectively detect linear FDI attacks and maintain the normal operation of power systems under both DoS and FDI attacks. Furthermore, to mitigate the impact of undetectable stealthy attacks, a novel weighting strategy is employed to reduce the influence of noise and attacks on the estimation results. The robustness and superiority of the proposed algorithm are demonstrated through numerical experiments.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported in part by the National Key R&D Program of China under Grant 2023YFF1204805; in part by the National Natural Science Foundation of China under Grant 62336005 and Grant 62122026; in part by the Projects Sponsored by the Programme of Introducing Talents of Discipline to Universities (the 111 Project) under Grant B17017; and in part by the Shuguang Program supported by Shanghai Education Development Foundation and Shanghai Municipal Education Commission.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in engineering*, 102647. [CrossRef]

[2] Li, F., Yan, X., Xie, Y., Sang, Z., & Yuan, X. (2019, October). A review of cyber-attack methods in cyber-physical power system. In *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)* (pp. 1335-1339). IEEE. [CrossRef]

[3] Irfan, M., Sadighian, A., Tanveer, A., Al-Naimi, S. J., & Oligeri, G. (2023). False data injection attacks in smart grids: State of the art and way forward. *arXiv preprint arXiv:2308.10268*. [CrossRef]

[4] Reda, H. T., Anwar, A., & Mahmood, A. (2022). Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. *Renewable and Sustainable Energy Reviews, 163*, 112423. [CrossRef]

[5] Musleh, A. S., Chen, G., & Dong, Z. Y. (2019). A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid, 11*(3), 2218-2234. [CrossRef]

[6] Husnoo, M. A., Anwar, A., Hosseinzadeh, N., Islam, S. N., Mahmood, A. N., & Doss, R. (2023). False data injection threats in active distribution systems: A comprehensive survey. *Future Generation Computer Systems, 140*, 344-364. [CrossRef]

[7] Salehghaffari, H., & Khorrami, F. (2018, February). Resilient power grid state estimation under false data injection attacks. In *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference* (*ISGT*) (pp. 1-5). IEEE. [CrossRef]

[8] Jafari, M., Rahman, M. A., & Paudyal, S. (2022). Optimal false data injection attacks against power system frequency stability. *IEEE Transactions on Smart Grid, 14*(2), 1276-1288. [CrossRef]

[9] Tian, M., Dong, Z., & Wang, X. (2021). Analysis of false data injection attacks in power systems: A dynamic Bayesian game-theoretic approach. *ISA transactions, 115*, 108-123. [CrossRef]

[10] Zhang, Z., Deng, R., Cheng, P., & Chow, M. Y. (2021). Strategic protection against FDI attacks with moving target defense in power grids. *IEEE Transactions on Control of Network Systems, 9*(1), 245-256. [CrossRef]

[11] Liu, B., & Wu, H. (2020). Optimal D-FACTS placement in moving target defense against false data injection attacks. *IEEE Transactions on Smart Grid, 11*(5), 4345-4357. [CrossRef]

[12] Xu, W., Jaimoukha, I. M., & Teng, F. (2022). Robust moving target defence against false data injection attacks in power grids. *IEEE Transactions on Information Forensics and Security, 18*, 29-40. [CrossRef]

[13] Liu, M., Zhao, C., Zhang, Z., & Deng, R. (2022). Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems. *IEEE Transactions on Power Systems, 37*(6), 4732-4746. [CrossRef]

[14] Lakshminarayana, S., Belmega, E. V., & Poor, H. V. (2021). Moving-target defense against cyber-physical attacks in power grids via game theory. *IEEE Transactions on Smart Grid, 12*(6), 5244-5257. [CrossRef]

[15] Shafei, H., Farhangi, M., Aguilera, R. P., & Alhelou, H. H. (2024). A Novel Cyber-Attack Detection and Mitigation for Coupled Power and Information Networks in Microgrids Using Distributed Sliding Mode Unknown Input Observer. *IEEE Transactions on Smart Grid*. [CrossRef]

[16] Garza, L., & Mandal, P. (2023, October). Detection and Classification of False Data Injection Attacks in Power Grids Using Machine Learning and Hyperparameter Optimization Methods. In *2023 IEEE Industry Applications Society Annual Meeting* (*IAS*) (pp. 1-8). IEEE. [CrossRef]

[17] Kumar, A., Saxena, N., & Choi, B. J. (2021, January). Machine learning algorithm for detection of false data injection attack in power system. In *2021 International Conference on Information Networking* (*ICOIN*) (pp. 385-390). IEEE. [CrossRef]

[18] Tebianian, H., & Jeyasurya, B. (2013, August). Dynamic state estimation in power systems using Kalman filters. In *2013 IEEE electrical power & energy conference* (pp. 1-5). IEEE. [CrossRef]

[19] Li, C., & Zhang, J. (2023, October). Dynamic State Estimation of Power Systems Based on Extended Kalman Particle Filter. In *2023 3rd International Conference on Intelligent Power and Systems* (*ICIPS*) (pp. 638-644). IEEE. [CrossRef]

[20] Zhu, M., Liu, H., & Bi, T. (2021, July). Dynamic State Estimation of Power System Based on a Robust H-infinity Cubature Kalman Filter. In *2021 IEEE Power & Energy Society General Meeting* (*PESGM*) (pp. 1-5). IEEE. [CrossRef]

[21] Zhao, J., & Mili, L. (2017). Robust unscented Kalman filter for power system dynamic state estimation with unknown noise statistics. *IEEE Transactions on Smart Grid, 10*(2), 1215-1224. [CrossRef]

[22] Zhang, Z., & Feng, X. (2023, July). Performance Analysis of Chi-square Detection for False Data Injection Attack. In *2023 3rd International Conference on Electrical Engineering and Mechatronics Technology* (*ICEEMT*) (pp. 560-564). IEEE. [CrossRef]

[23] Ye, D., & Wang, J. (2019, May). False data injection attack design in multi-sensor systems based on KL divergence theory. In *2019 IEEE 8th Data Driven Control and Learning Systems Conference* (*DDCLS*) (pp. 333-337). IEEE. [CrossRef]

[24] Guo, Z., Shi, D., Johansson, K. H., & Shi, L. (2018). Worst-case stealthy innovation-based linear attack on remote state estimation. *Automatica, 89*, 117-124. [CrossRef]

[25] Hu, K., Li, L., Tao, X., Velásquez, J. D., & Delaney, P. (2023). Information fusion in crime event analysis: A decade survey on data, features and models. *Information Fusion, 100*, 101904. [CrossRef]

[26] Li, T., Liang, H., Xiao, B., Pan, Q., & He, Y. (2023). Finite mixture modeling in time series: A survey of Bayesian filters and fusion approaches. *Information Fusion, 98*, 101827. [CrossRef]

[27] Hu, L., Zhang, J., Zhang, J., Cheng, S., Wang, Y., Zhang, W., & Yu, N. (2025). Security analysis and adaptive

false data injection against multi-sensor fusion localization for autonomous driving. *Information Fusion*, *117*, 102822. [CrossRef]

[28] Bhalla, V., & Prajapat, G. P. (2024, June). Proficiency Analysis of Unscented Kalman Filter for Bad Data Detection During State Estimation. In *2024 IEEE 3rd International Conference on Electrical Power and Energy Systems (ICEPES)* (pp. 1-5). IEEE. [CrossRef]

[29] Yang, Q., Min, R., An, D., Yu, W., & Yang, X. (2016, March). Towards optimal pmu placement against data integrity attacks in smart grid. In *2016 Annual Conference on Information Science and Systems (CISS)* (pp. 54-58). IEEE. [CrossRef]

[30] Hao, J., & Zhang, Y. (2020, December). Consensus Kalman filtering for sensor networks based on FDI attack detection. In *2020 16th International Conference on Control, Automation, Robotics and Vision (ICARCV)* (pp. 160-165). IEEE. [CrossRef]

[31] Li, T., Song, Y., Song, E., & Fan, H. (2024). Arithmetic average density fusion-Part I: Some statistic and information-theoretic results. *Information Fusion*, *104*, 102199. [CrossRef]

[32] Wang, G., Zhu, Z., Yang, C., Ma, L., Dai, W., & Chen, X. (2024). Distributed Multi-Kernel Maximum Correntropy State-Constrained Kalman Filter Under Deception Attacks. *IEEE Transactions on Network Science and Engineering*. [CrossRef]

[33] Li, T., Corchado, J. M., & Sun, S. (2018). Partial consensus and conservative fusion of Gaussian mixtures for distributed PHD fusion. *IEEE Transactions on Aerospace and Electronic Systems*, *55*(5), 2150-2163. [CrossRef]

[34] Yang, H., Li, T., Yan, J., & Elvira, V. (2024). Hierarchical Average Fusion With GM-PHD Filters Against FDI and DoS Attacks. *IEEE Signal Processing Letters*. [CrossRef]

[35] Bi, T., Liu, H., Zhang, D., & Yang, Q. (2012, July). The PMU dynamic performance evaluation and the comparison of PMU standards. In *2012 IEEE Power and Energy Society General Meeting* (pp. 1-5). IEEE. [CrossRef]

[36] IEEE. (2013). IEEE guide for synchronization, calibration, testing, and installation of phasor measurement units (PMUs) for power system protection and control (IEEE Std C37.242-2013, pp. 1–107). [CrossRef]



Shiyu Jin received the B.S.degree in electrical engineering and automation from East China University of Science and Technology, Shanghai, China, in 2021, where he is currently pursuing the Ph.D.degree in control science and engineering.His research interest include state estimation, smart grid, privacy-preserving and cyber security. (Email: shiyu_jin12138@163.com)



Wen Yang received the B.S.degree in mineral engineering and the M.S.degree in control theory and control engineering from Central South University, Hunan, China, in 2002 and 2005, respectively, and the Ph.D.degree in control theory and control engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009.

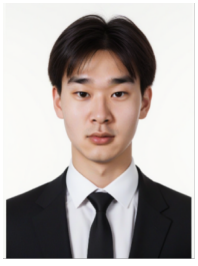
She was a Visiting Student with the University of California at Los Angeles.CA.USA, from 2007 to 2008.She is currently a Professor with the East China University of Science and Technology (ECUST).Her research interests include information fusion, state estimation, network security, coordinated control, complex networks, and reinforcement learning.(Email:weny@ecust.edu.cn)



Hongbo Yuan received the B.S.degree in automation from Hefei University of Science and Technology, Hefei, China, in 2021.He is currently pursuing the Ph.D.degree in control science and engineering with the East China University of Science and Technology, Shanghai, China.His research interests include distributed state estimation, cyber security and information fusion.(Email: Y20210081@mail.ecust.edu.cn)



Wenjie Ding is currently a postdoctoral researcher at East China University of Science and Technology, where he obtained his Ph.D.in 2024.His research interests include state estimation, information fusion, and information security.(Email: 15216780036@163.com)



Han Wu received the B.S.degree in 2023 from the East China University of Science and Technology, Shanghai, China, where he is currently working toward the M.S.degree in control science and engineering. His research interests include state estimation, internet of vehicles and cyber-physical system security. (Email:Y30230986@mail.ecust.edu.cn)



Jie Wang received the M.Sc.degree in Mathematical from Liaocheng University, Liaocheng, China, in 2023.He is currently pursuing the Ph.D.degree in control science and engineering with the School of Information Science and Engineering, East China University of Science and Technology, Shanghai, China. His research interests include state estimation, network security, information fusion and privacy-preserving. (Email: wj951007@163.com)