electronics

MDPI

Article

A Fusion Adaptive Cubature Kalman Filter Approach for False Data Injection Attack Detection of DC Microgrids

Po Wu [1], Jiangnan Zhang [1], Shengyao Luo [2], Yanlou Song [1], Jiawei Zhang [2] and Yi Wang [2,*]

[1] State Grid Henan Electric Power Research Institute, Zhengzhou 450052, China; wupo@ha.sgcc.com.cn (P.W.); zhangjiangnan@ha.sgcc.com.cn (J.Z.); songyanlou@ha.sgcc.com.cn (Y.S.)
[2] School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China; luosy@gs.zzu.edu.cn (S.L.); zjw20221820@gs.zzu.edu.cn (J.Z.)
* Correspondence: yiwang@zzu.edu.cn

Abstract: With the widespread application of information technology in microgrids, microgrids are evolving into a class of power cyber–physical systems (CPSs) that are deeply integrated with physical and information systems. Due to the high dependence of microgrids' distributed cooperative control on real-time communication and system state information, they are increasingly susceptible to false data injection attacks (FDIAs). To deal with this issue, in this paper, a novel false data injection attack detection method for direct-current microgrids (DC MGs) was proposed, based on fusion adaptive cubature Kalman filter (FACKF) approach. Firstly, a DC MG model with false data injection attack is established, and the system under attack is analyzed. Subsequently, an FACKF approach is proposed to detect attacks, capable of accurately identifying the attacks on the DC MG and determining the measurement units injected with false data. Finally, simulation validations were conducted under various DC MG model conditions. The extensive simulation results demonstrate that the proposed method surpasses traditional CKF detection methods in accuracy and effectiveness across different conditions.

Keywords: DC MG; FDIA; fusion adaptive CKF algorithm; attack detection

Citation: Wu, P.; Zhang, J.; Luo, S.; Song, Y.; Zhang, J.; Wang, Y. A Fusion Adaptive Cubature Kalman Filter Approach for False Data Injection Attack Detection of DC Microgrids. *Electronics* **2024**, *13*, 1612. https://doi.org/10.3390/electronics13091612

Academic Editor: Yannis Papaefstathiou

Received: 13 March 2024
Revised: 16 April 2024
Accepted: 20 April 2024
Published: 23 April 2024

1. Introduction

With new energy technologies rapidly advancing and energy policies gradually adapting, the integration of distributed energy resources and the construction of the energy internet have become significant trends in global energy development. Direct-current microgrids (DC MGs), with their efficiency, flexibility, and reliability, play a crucial role in facilitating the access to distributed energy and accelerating the development of the energy internet [1–5]. However, as typical examples of cyber–physical systems (CPSs), the open, distributed, and networked characteristics of nonlinear DC-MG systems require extensive data exchange and information processing in communication and collaboration processes, leading to increased security risks such as data tampering and attacks [6–9]. These attacks can compromise the accurate estimation of the DC MG's state, and inaccurate state assessments can lead to incorrect monitoring decisions. Therefore, in-depth research into the secure operation of DC MGs to ensure their stability and reliability is of significant importance for promoting the development of distributed energy systems and the construction of the energy internet.

In general, a false data injection attack (FDIA) is a prevalent attack that disrupts the normal operation of a system by tampering with its data. This can cause the system to crash or malfunction. In the case of DC MGs, FDIAs can result in voltage fluctuations, load imbalances, and other issues that significantly impact the system's stability and reliability. Therefore, detecting and preventing FDIAs effectively is one of the crucial issues in the field of DC MG research [10–14]. Currently, FDIA detection methods are mainly classified into two categories: model-based and data-based detection methods [15–17]. Model-based

detection methods determine whether it contains false data attack injection by calculating the residual difference between the actual output of the process and the output predicted based on the mathematical model. References [18,19] have received attention for their robustness to model uncertainties and disturbances due to the unknown input observer (UIO) approach to decouple FDIA and perturbation for attack detection. In addition, reference [20] proposed a false attack detection algorithm based on the cubature Kalman filter for detecting attack injections in nonlinear systems. Reference [21] proposed a square root maximum correlation entropy volume Kalman filter with adaptive kernel width for estimating continuous discrete nonlinear dynamic systems with non-Gaussian non-zero mean noise. In references [22,23], the detection problem was treated as an augmented and generalized state space system. The cubature Kalman filter (CKF) and unscented Kalman filter (UKF) were employed to estimate the sensor states. The main drawback of detection schemes based on system models is the requirement for system parameters and models. These parameters are not constant and can be subject to slight uncertainties and fluctuations, which can impact the effectiveness of the detection.

In comparison, the advantage of data-driven detection schemes is their independence from system parameters. These schemes only require the design of a model and training the model using historical data, thereby avoiding the negative impact caused by minor fluctuations in system parameters. Reference [24] employed multilayer perceptron (MLP) neural networks for fault detection and learning vector quantization (LVQ) classification for fault diagnosis. References [25,26] used long short-term memory (LSTM) neural networks and deep convolutional neural network (DCNN) deep learning techniques to improve detection efficiency. Reference [27] proposed a data-driven state estimation method based on data fusion techniques to obtain the optimal estimate, which significantly improved detection accuracy. The drawback of these data-driven fault detection methods is the requirement for a large amount of data, and during the training process, overfitting may occur, making them unsuitable for online implementation.

Although the aforementioned literature provides some effective attack detection strategies, there are still certain limitations. The literature [18–27] primarily focuses on studying whether the system contains false data injection, rather than considering the specific unit of attack injection [28]. This lack of consideration makes it difficult to achieve accurate detection of false data attacks. To address this issue, a false data injection attack detection method based on a fusion adaptive cubature Kalman filter is proposed. The method consists of multiple local units and an information fusion module, which detects attacks by evaluating the estimation results of each local unit. It not only achieves accurate detection of false data injection attacks but also identifies the specific units targeted by the attack through the magnitude of local residuals, enabling the isolation of faulty units. During the information fusion process, after detecting and isolating the corresponding measurements and estimates, the method is able to obtain the correct system estimation. The proposed method is more accurate and effective than the traditional cubature Kalman filter detection method under different working conditions.

The rest of this paper is organized as follows: Section 2 introduces the DC MG models. Section 3 discusses the FACKF algorithm in detail. Section 4 presents simulations to evaluate the proposed algorithm. Finally, Section 5 provides concluding remarks and future perspectives.

2. DC MG Model

2.1. DC MG Structure

Microgrids are classified into three main categories based on the distribution method: DC, AC, and AC-DC hybrid. Among them, the DC microgrid is a small power system that uses DC current for energy transmission and distribution. It mainly consists of DC sources, DC loads, DC centralized controllers, DC grids, and energy storage devices. Figure 1 shows a detailed and simplified diagram of the DC microgrid system structure.

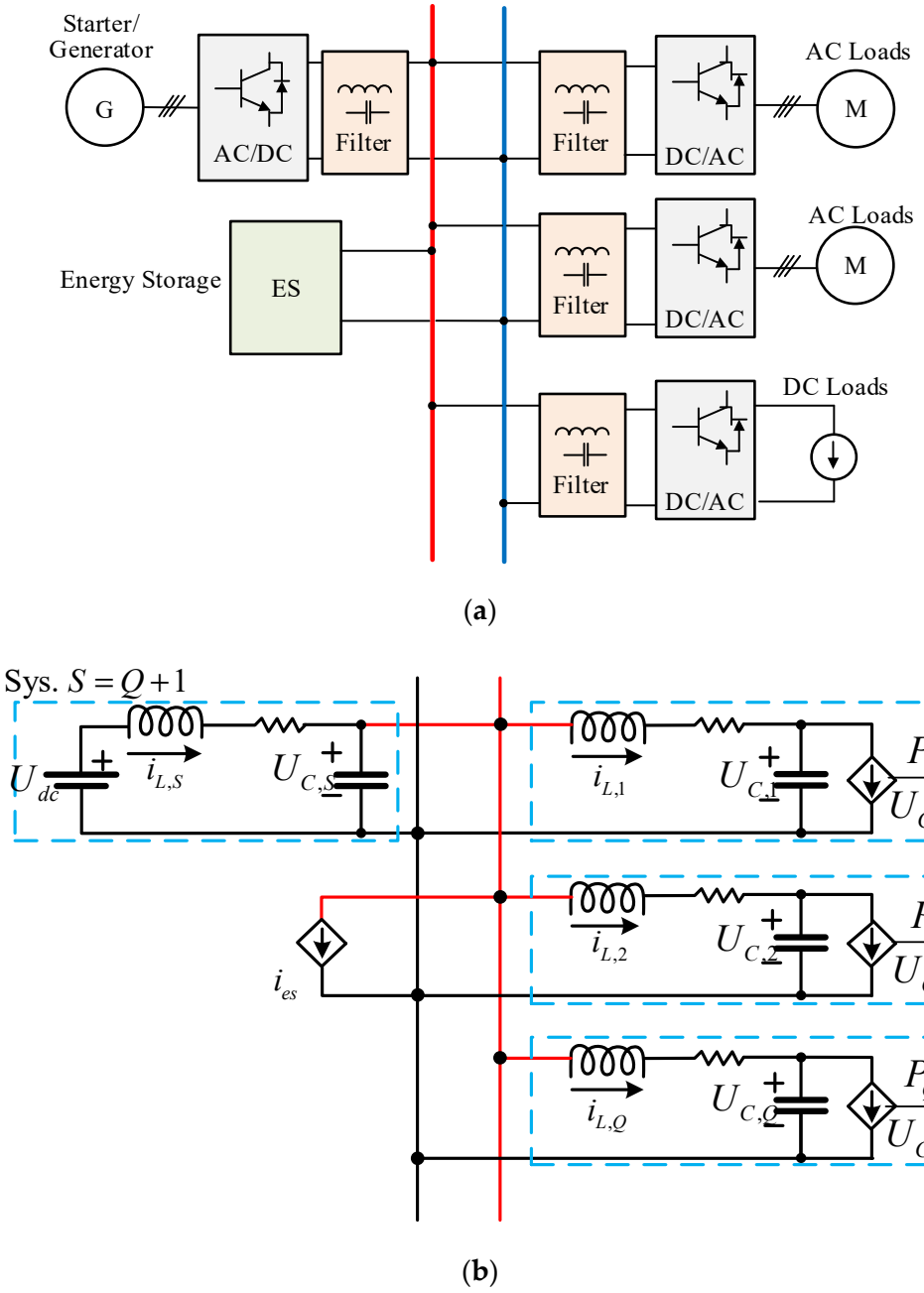


Figure 1. DC MG system structure diagram. (**a**) Detailed system structure of DC MG. (**b**) Simplified system structure of DC MG.

Figure 1a shows an islanded DC microgrid comprising an energy storage system (ESS), a DC source (consisting of a generator and power electronics), and nonlinear loads. Typically, DC and AC loads are connected to the microgrid via tightly regulated converters and inverters. If the loads are connected to the microgrid using multiple power converters and inverters to maintain constant power, they are considered constant power loads (CPLs).

2.2. DC MG Model

To simplify the analysis, Figure 1b presents a simplified model of the DC MG. It is evident that the structure can be decoupled into multiple CPLs and an ESS. Assuming a coordinated variation near the operating point and letting the energy storage current serve as the control input, the nonlinear equation of state of the whole DC MG is shown below:

$$\dot{\boldsymbol{x}}(t) = \mathrm{A}\boldsymbol{x}(t) + \mathrm{DH}(\boldsymbol{x}(t)) + B_{es}\overset{\sim}{\boldsymbol{i}}_{\boldsymbol{es}}(t) + B_{\mathrm{s}}U_{dc} \tag{1}$$

where $\boldsymbol{x}(t)$ indicates the state quantity of the system. $\boldsymbol{x}(t) = \left[\boldsymbol{x}_1^T(t)\cdots\boldsymbol{x}_n^T(t)\boldsymbol{x}_s^T(t)\right]^T$; $\boldsymbol{x_n}(t) = \begin{bmatrix}\boldsymbol{i_{L,n}} & \boldsymbol{U_{C,n}}\end{bmatrix}^T$. $\boldsymbol{i}_{L,n}$ and $\boldsymbol{U_{C,n}}$ denote the inductor current and capacitor voltage in the n-th CPL, respectively. $\boldsymbol{x}_s(t) = \left[\boldsymbol{i}_{L,s}\ \boldsymbol{U}_{C,s}\right]^T$; $\boldsymbol{i}_{L,s}$ and $\boldsymbol{U}_{C,s}$ are the inductor current and capacitor voltage in the ESS. $\dot{\boldsymbol{x}}(t)$ represents the integral of $\boldsymbol{x}(t)$ with respect to the time; DH is the transfer matrix of the perturbation caused by the current fluctuation of the n-th CPL; U_{dc} means the voltage of the storage power supply; B_{s} is the coupling matrix between U_{dc} and the system; $\overset{\sim}{\boldsymbol{i}}_{es}(t)$ is the injected power, which can stabilize the DC MG and improve the robustness of the closed-loop system to disturbances and temporary faults; B_{es} is the coupling matrix. In general, the DC MG model can be expressed as

$$\begin{cases}\boldsymbol{x}_{k+1} = f(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{w}_k \\ \boldsymbol{y}_k = h(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{v}_k\end{cases} \tag{2}$$

where $\boldsymbol{x}_{k+1}$ represents the state vector at moment $k+1$; $\boldsymbol{y}_k$ indicates the measurement output vector at moment k; $f(\boldsymbol{x}_k, \boldsymbol{u}_k)$ and $h(\boldsymbol{x}_k, \boldsymbol{u}_k)$ are the nonlinear functions; $\boldsymbol{u}_k$ means the control input matrix; $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are the system and measurement noise, respectively, both of which are Gaussian white noise.

2.3. DC MG Model with FDIA

FDIA is a type of cyber attack that involves injecting false data into real information. This attack typically occurs when the attacker lacks knowledge of system parameters or previous data. A sophisticated FDIA can cause system instability, posing a serious threat to network security. Therefore, real-time and accurate detection of false data is essential to maintain system stability.

The DC MG model in Equation (2) states that the injection of FDIA into the system will cause interference and alter the measurement information. Therefore, the DC MG measurement equation model with false data injection can be expressed by

$$\boldsymbol{y}_k = h(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{v}_k + f_{k,\varphi}\gamma \tag{3}$$

$$f_{k,\varphi} = \begin{cases}1, & k \geq \varphi \\ 0, & k < \varphi\end{cases} \tag{4}$$

where γ is the type and extent of the false data attack; k denotes the moment of system operation; $f_{k,\varphi}$ and φ are the location of the fault and the moment of the fault, respectively.

3. FDIA Detection Based on an FACKF

3.1. Fusion Adaptive CKF Approach

To implement an effective detection of false data injection in sensors, this section proposes a nonlinear detection method based on the FACKF algorithm. The method comprises local filters and an information fusion module. The local filters perform adaptive cubature estimation on individual parts of the overall unit, and the information fusion module combines the state estimates of all the local filters to obtain a global estimate. Attacks are detected during the information fusion process based on the residuals of the local units, and the sensors injected by the attacks are localized. The computational burden is distributed across various local filters in this structure, rather than the main filter. This approach can enhance the accuracy and reliability of the decision while also reducing the impact of noise by combining the local filters and sharing information. Figure 2 illustrates the FACKF framework.

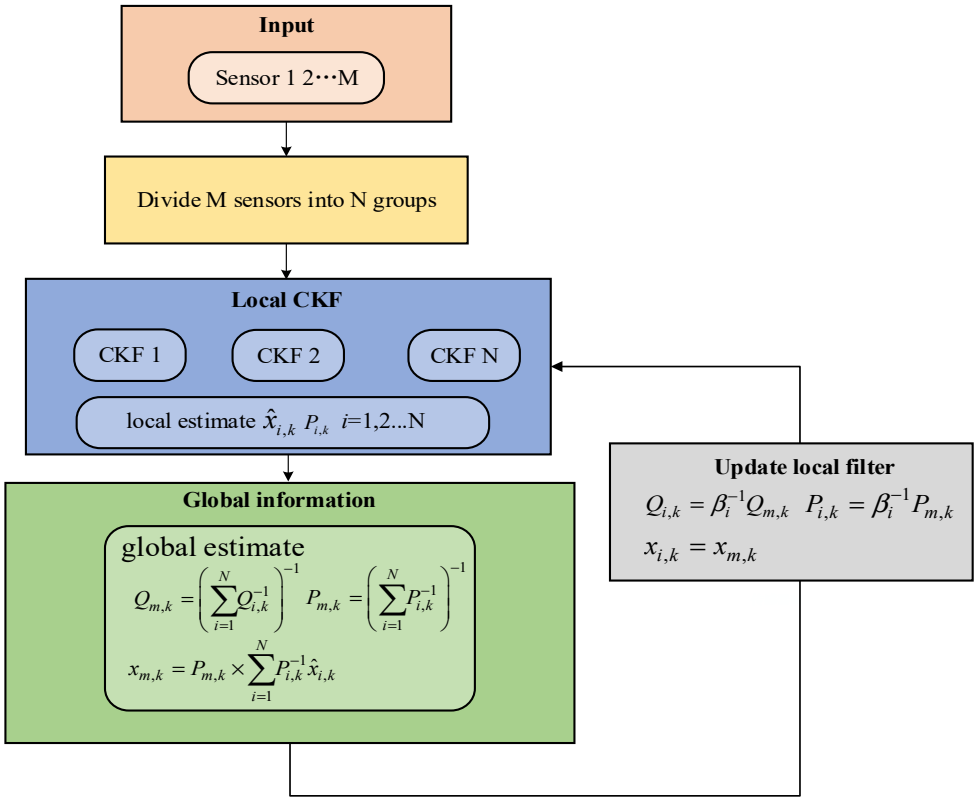


Figure 2. The framework of the FACKF.

Figure 2 illustrates the three main stages of the FACKF. Firstly, M sensors are grouped into N local units, each containing M − 1 sensor values. Secondly, each local unit performs adaptive CKF estimation to obtain a local estimate, $\hat{\boldsymbol{x}}_{i,k}$, and performs information fusion to obtain the global estimate, $\boldsymbol{x}_{m,k}$. Finally, the global estimate is sent back to the local filters and each local filter is updated. The global state estimates, $\boldsymbol{x}_{m,k}$ and $\boldsymbol{P}_{m,k}$, are determined by information fusion and sent to the local units for updating. The information distribution factor (β_i) of the i-th local filter is used to weight the localization. If all local filters have the same weight, 1/N is the number of localization. The nonlinear equations in fusion adaptive CKF describe the localized sensor system.

$$\begin{aligned} \boldsymbol{x}_{k+1} &= f(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{w}_k \\ \boldsymbol{y}_{i,k} &= h_i(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{v}_{i,k} \end{aligned} \tag{5}$$

$$\begin{cases} \boldsymbol{Q}_k = E\left[\boldsymbol{w}_k \boldsymbol{w}_k^T\right] \\ \boldsymbol{R}_{i,k} = E\left[\boldsymbol{v}_{i,k} \boldsymbol{v}_{i,k}^T\right] \end{cases} \tag{6}$$

where $\boldsymbol{x}_{k+1}$ represents the state vector and $\boldsymbol{y}_{i,k}$ indicates the measurement output vector of the i-th local sensor; $f(\boldsymbol{x}_k, \boldsymbol{u}_k)$ and $h_i(\boldsymbol{x}_k, \boldsymbol{u}_k)$ are the system function and measurement function, respectively; $\boldsymbol{w}_k$ is the system noise at the time instant, k; $\boldsymbol{v}_{i,k}$ represents the measurement noise at moment k, and both are Gaussian white noise; $\boldsymbol{Q}_k$ and $\boldsymbol{R}_{i,k}$ are the corresponding covariance matrices, respectively.

The implementation steps for the FACKF method are as follows:

Step 1: Firstly, initialize the initial values of the parameter states and the initial covariance matrix.

Step 2: Generate $2n + 2$ cubature points:

$$\boldsymbol{x}_{i,j,k-1} = \sqrt{\boldsymbol{P}_{i,k-1}}\zeta_i + \hat{\boldsymbol{x}}_{i,k-1},\ i = 1, \cdots, 2n+2 \tag{7}$$

where $\boldsymbol{x}_{i,j,k-1}$ is the i-th cubature point at moment $k-1$ calculated for the j-th local unit, $\hat{\boldsymbol{x}}_{i,k-1}$ is the estimated value at moment $k-1$ for the local unit, ζ_i is the matrix of cubature points, and $\boldsymbol{P}_{i,k-1}$ is the estimated covariance at moment $k-1$ for the i-th local unit.

Step 3: The local CKF is updated in time and measurements, and the estimated state of the CKF for the first local unit is

$$\hat{\boldsymbol{x}}_{i,k|k-1} = \frac{1}{2n}\sum_{j=0}^{2n+2} f\left(\boldsymbol{x}_{i,j,k-1}, \boldsymbol{u}_{i,k-1}\right) \tag{8}$$

$$\boldsymbol{P}_{i,x_{ik|k-1}} = \frac{1}{2n}\sum_{j=0}^{2n+2}\left[\boldsymbol{x}_{i,j,k|k-1} - \hat{\boldsymbol{x}}_{i,k|k-1}\right] \times \left[\boldsymbol{x}_{i,j,k|k-1} - \hat{\boldsymbol{x}}_{i,k|k-1}\right]^T + \boldsymbol{Q}_{i,k-1} \tag{9}$$

$$\hat{\boldsymbol{y}}_{i,j,k|k-1} = \frac{1}{2n}\sum_{j=0}^{2n+2} h\left(\boldsymbol{x}_{i,j,k-1}, \boldsymbol{u}_{i,k-1}\right) \tag{10}$$

where $\boldsymbol{x}_{i,j,k-1}, \boldsymbol{u}_{i,k-1}$ are, respectively, the cubature points of the generated state and control variables; $\hat{\boldsymbol{x}}_{i,k|k-1}$ and $\boldsymbol{P}_{i,x_{ik|k-1}}$ are the a priori estimates of the state quantities and the a priori covariance matrices of the state quantities at the k-th moment in the i-th local unit, which are obtained by averaging over the individual $2n+2$ cubature points; $\hat{\boldsymbol{y}}_{i,j,k|k-1}$ is the estimate of the a priori quantities at the k-th moment of the i-th local unit.

Step 4: Construct adaptive factors and perform correction of the covariance matrix.

To improve the adaptivity and robustness of the CKF algorithm, its filtering performance is enhanced by correcting the covariance matrix online through the construction of an adaptive factor. The main steps can be expressed as

$$\boldsymbol{e}_k = \boldsymbol{y}_{i,k} - \hat{\boldsymbol{y}}_{i,j,k|k-1} \tag{11}$$

$$\Delta\boldsymbol{e} = \boldsymbol{e}_k \boldsymbol{e}_k^T \tag{12}$$

$$\eta_k = \begin{cases} 1 & tr(\Delta\boldsymbol{e}) \le tr(\boldsymbol{P}_{i,y_{i,k}}) \\ \dfrac{tr(\boldsymbol{P}_{i,y_{i,k}})}{tr(\Delta\boldsymbol{e})} & tr(\Delta\boldsymbol{e}) > tr(\boldsymbol{P}_{i,y_{i,k}}) \end{cases} \tag{13}$$

where $\boldsymbol{e_k}$ represents the innovation vector, $\Delta\boldsymbol{e}$ denotes the innovation vector matrix, and η_k is the adaptive factor.

Based on the constructed adaptive factor, the self-covariance matrix and cross-covariance matrix are dynamically adjusted through online correction.

Self-covariance matrix correction:

$$\boldsymbol{P}_{i,y_i,k} = \eta_k\left[\frac{1}{2n}\sum_{j=0}^{2n}(\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1}) \times (\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1})^T\right] + \boldsymbol{R}_{i,k} \tag{14}$$

Cross-covariance matrix correction:

$$\boldsymbol{P}_{i,x_{i,k},y_{i,k}} = \eta_k\left[\frac{1}{2n}\sum_{j=0}^{2n}(\boldsymbol{x}_{i,j,k|k-1} - \hat{\boldsymbol{x}}_{i,k|k-1}) \times (\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1})^T\right] \tag{15}$$

The local cubature Kalman filter gain ($K_{i,k}$) at the current moment is then calculated to obtain the a posteriori estimate, $\hat{x}_{i,k}$:

$$K_{i,k} = \boldsymbol{P}_{i,x_{i,k},y_{i,k}} \boldsymbol{P}_{i,y_{i,k}}{}^{-1} \tag{16}$$

$$\hat{\boldsymbol{x}}_{i,k} = \hat{\boldsymbol{x}}_{i,k|k-1} + K_{i,k}\left(\boldsymbol{y}_{i,k} - \hat{\boldsymbol{y}}_{i,j,k|k-1}\right) \tag{17}$$

$$\boldsymbol{P}_{i,k} = \boldsymbol{P}_{i,x_{ik|k-1}} - K_{i,k}\boldsymbol{P}_{i,y_{i,k}}K_{i,k}^T \tag{18}$$

where $\boldsymbol{P}_{i,x_{i,k},y_{i,k}}$ and $\boldsymbol{P}_{i,y_{i,k}}$ are, respectively, the self-covariance matrix and the mutual covariance matrix at moment k of the i-th local unit; $K_{i,k}$ and $\hat{\boldsymbol{x}}_{i,k}$ are the Kalman gain and a

posteriori estimates of the i-th local unit, respectively; and $\boldsymbol{P}_{i,x_{i,k}}$ is the updated estimated covariance matrix.

Step 5: The estimates of all local state vectors ($\hat{\boldsymbol{x}}_{i,k}$), the state error covariance ($\boldsymbol{P}_{i,k}$), and the process noise covariance ($\boldsymbol{Q}_{i,k}$) of the local CKF are integrated into the information fusion to obtain the global estimate:

$$\begin{cases} \boldsymbol{P}_{m,k} = \left(\sum_{i=1}^{N} \boldsymbol{P}_{i,k}^{-1}\right)^{-1} \\ \boldsymbol{Q}_{m,k} = \left(\sum_{i=1}^{N} \boldsymbol{Q}_{i,k}^{-1}\right)^{-1} \\ \boldsymbol{x}_{m,k} = \boldsymbol{P}_{m,k} \times \sum_{i=1}^{N} \boldsymbol{P}_{i,k}^{-1} \hat{\boldsymbol{x}}_{i,k} \end{cases} \tag{19}$$

where $\boldsymbol{P}_{m,k}$ and $\boldsymbol{Q}_{m,k}$ are the overall state error covariance and process noise covariance obtained by fusing the N local unit estimates, respectively; $\boldsymbol{x}_{m,k}$ is the overall estimate.

Step 6: The global estimates from Step 4 are assigned to each local unit, and the local units use them as previous information in the next step, returning state estimates, state error covariance, and process noise for the first local filter CKF.

$$\begin{cases} \boldsymbol{Q}_{i,k} = \beta_i^{-1} \boldsymbol{Q}_{m,k} \\ \boldsymbol{P}_{i,k} = \beta_i^{-1} \boldsymbol{P}_{m,k} \\ \boldsymbol{x}_{i,k} = \boldsymbol{x}_{m,k} \end{cases} \tag{20}$$

where $\boldsymbol{Q}_{i,k}$ and $\boldsymbol{P}_{i,k}$ are the process noise and state error covariances returned to each local estimator; $\boldsymbol{x}_{i,k}$ is the state estimate returned as the current estimate of the local unit; β_i is the information distribution factor of the i-th local filter and $\sum_{i=1}^{N} \beta_i^{-1} = 1$.

3.2. False Data Injection Attack Detection Based on FACKF

Traditional false data injection detection is based on a single residual size judgement, which is unable to effectively detect the unit of false data injection. When false data are injected, they will quickly spread to other locations and affect the overall system, and the estimated values of other parameters will be affected and deviate from the true values over time, resulting in the final estimation results deviating from the true values. In order to accurately detect the attack and determine the attack injection unit to achieve accurate and reliable state estimation, the state variance (V_k) and local state residual ($r_{i,k}$) are defined:

$$V_k = \left[(\boldsymbol{y}_k - h(\boldsymbol{x}_{m,k}, \boldsymbol{u}_k))^{\mathrm{T}} (\boldsymbol{y}_k - h(\boldsymbol{x}_{m,k}, \boldsymbol{u}_k)) \right]^{\frac{1}{2}} \tag{21}$$

$$r_{i,k} = \left[(\hat{\boldsymbol{x}}_{i,k} - \boldsymbol{x}_{m,k})^{\mathrm{T}} (\hat{\boldsymbol{x}}_{i,k} - \boldsymbol{x}_{m,k}) \right]^{\frac{1}{2}} \tag{22}$$

The state variance, V_k, determines whether a sensor experiences FDIA, while the residual, $r_{i,k}$, identifies the specific measurement unit in which attack injection occurs in FDIA detection. In the absence of FDIA, the locally estimated states of the local adaptive CKF are close to their true values, with V_k and $r_{i,k}$ approaching 0. When false attack injection occurs in a measurement unit, only one local unit is correct. In this case, the state estimate, $x_{m,k}$, is inaccurate and close to the fault estimate. Based on the maximum value of $r_{i,k}$, it is possible to diagnose which local unit is correct, while the measurements from the excluded sensors originating from that local unit are considered incorrect. The steps of the FACKF are summarized in Algorithm 1.

Algorithm 1: Fusion Adaptive Cubature Kalman Filter

1: Generate local measurements.
2: Initialize the parameters X_0, P_0 of each local.
3: Calculate cubature points:

$$\boldsymbol{x}_{i,j,k-1} = \sqrt{\boldsymbol{P}_{i,k-1}}\zeta_i + \hat{\boldsymbol{x}}_{i,k-1};$$

4: Perform time and measurement updates for each local CKF:

$$\boldsymbol{P}_{i,y_i,k} = \eta_k[\frac{1}{2n}\sum_{j=0}^{2n}\left(\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1}\right) \times \left(\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1}\right)^T] + \boldsymbol{R}_{i,k}$$

$$\boldsymbol{P}_{i,x_{i,k},y_{i,k}} = \eta_k[\frac{1}{2n}\sum_{j=0}^{2n}\left(\boldsymbol{x}_{i,j,k|k-1} - \hat{\boldsymbol{x}}_{i,k|k-1}\right) \times \left(\boldsymbol{y}_{i,j,k|k-1} - \hat{\boldsymbol{y}}_{i,j,k|k-1}\right)^T]$$

$$\hat{\boldsymbol{x}}_{i,k} = \hat{\boldsymbol{x}}_{i,k|k-1} + K_{i,k}\left(\boldsymbol{y}_{i,k} - \hat{\boldsymbol{y}}_{i,j,k|k-1}\right)$$

5: Calculate global estimation:

$$\boldsymbol{Q}_{m,k} = \left(\sum_{i=1}^{N} Q_{i,k}^{-1}\right)^{-1}, \boldsymbol{P}_{m,k} = \left(\sum_{i=1}^{N} \boldsymbol{P}_{i,k}^{-1}\right)^{-1};$$

$$x_{m,k} = \boldsymbol{P}_{m,k} \times \sum_{i=1}^{N} \boldsymbol{P}_{i,k}^{-1}\hat{x}_{i,k};$$

6: Calculate state variance and residual of locals:

$$\boldsymbol{V}_{j,k} = \frac{1}{N}\sum\nolimits_{i=1}^{N}\left(\hat{\boldsymbol{x}}_{i,k}^{(j)} - \frac{1}{N}\sum_{i=1}^{N}\hat{\boldsymbol{x}}_{i,k}^{(j)}\right);$$

$$r_{i,k} = \left[\left(\hat{\boldsymbol{x}}_{i,k} - \boldsymbol{x}_{m,k}\right)^T\left(\hat{\boldsymbol{x}}_{i,k} - \boldsymbol{x}_{m,k}\right)\right]^{\frac{1}{2}};$$

7: Compare state variance with threshold. If it is larger than the threshold, go to 9 and alarm a faulty situation. Otherwise, go to 11.
8: Evaluate the residual value and determine the faulty sensor based on correct locals.
9: Eliminate faulty locals and calculate the global estimates based on healthy locals.
10: Assign global estimates to locals, update them, and come back to 3.

$$\boldsymbol{Q}_{i,k} = \beta_i^{-1}\boldsymbol{Q}_{m,k}, \boldsymbol{P}_{i,k} = \beta_i^{-1}\boldsymbol{P}_{m,k}, \boldsymbol{x}_{i,k} = \boldsymbol{x}_{m,k}$$

4. Simulation Results

In order to prove the validity of the proposed FACKF method, a DC microgrid system is set up under different working conditions, and the estimation performance of a DC microgrid under normal operating conditions and the detection and robustness estimation ability of a fake data attack injection scenario are, respectively, compared and analyzed. Through this series of comparative experiments, not only can the FACKF method demonstrate high estimation accuracy under normal operating conditions, but it can also validate its excellent detection efficiency and robustness when faced with security threats. This fully proves the practical value and effectiveness of the method in ensuring the stable operation and security protection of DC microgrids.

4.1. Test Systems

Case 1: A CPL source and a DC source are set up in the DC microgrid. In the absence of network attacks, the CKF and FACKF are, respectively, used for state estimation to evaluate the estimation accuracy of the two algorithms in the presence of noise.

Case 2: On the basis of Case 1, the case of false data injection attack is considered; the traditional residual detection method and the FACKF method proposed in this paper are used to detect the false data injection attack.

Case 3: The DC grid unit is extended to 2 CPL, and the false data injection attack is set to test the validity of the detection algorithm considering multiple CPL.

Case 4: The computational efficiency of the conventional CKF and the proposed FACKF is investigated.

In order to accurately simulate the field measurements measured by the PMUs, additional noise is added to the simulated data. It is worth pointing out that all the discussed methods were executed in MATLAB R2021b on a PC with Intel Core CPU E5-11400H, 4.5 GHz, and 16 GB memory.

Furthermore, for the purpose of conducting a quantitative analysis and comparison of various methods' performance, the performance metric known as root mean square deviation (RMSD) is used to comprehensively assess the effectiveness of the CKF and FACKF. It is defined as follows:

$$RMSD = \sqrt{\frac{\sum_{k=1}^{n} (\hat{\boldsymbol{x}}_k - \boldsymbol{x}_k)^2}{n}} \tag{23}$$

where k represents the time instant, $\boldsymbol{x}$ denotes the state variable, n represents the number of time steps, $\hat{\boldsymbol{x}}_k$ represents the estimated value of the state variable, and $\boldsymbol{x}_k$ signifies the true value.

4.2. Case 1: Comparison of Estimation Accuracy

To compare the estimated performance of the two in the absence of an attack, consider a CPL and a source. The system variables are $\boldsymbol{X} = [i_{L1}, v_{c1}, i_{Ls}, v_{cs}]$, the system parameters are given in Table 1, and the initial conditions of the DC microgrid are chosen as follows: $\boldsymbol{X_0} = [1.5, 200, 1.5, 200]$. The initial conditions of the Kalman filter are as follows: $\hat{\boldsymbol{x}}_{0|0} = [1, 200, 1, 200]$. The initial covariance is $10^{-6}\boldsymbol{I}_{2\times2}$; the standard deviation of the system and measurement noise is $10^{-8}\boldsymbol{I}_{2\times2}$.

Table 1. The parameters of DC MG system with a CPL.

$r_{L,1} = 1.1\ \Omega$	$L_1 = 39.5$ mH	$C_1 = 500\ \mu$F	$P_1 = 300$ W
$r_s = 1\ \Omega$	$L_s = 17$ mH	$C_S = 550\ \mu$F	$V_{dc} = 200$ V

In order to study the performance of the proposed FACKF algorithm for the attack-free injection case, we assume that all state measurements are available. Therefore, we consider four local variables (M = 4), each consisting of measurements from three sensors, as follows:

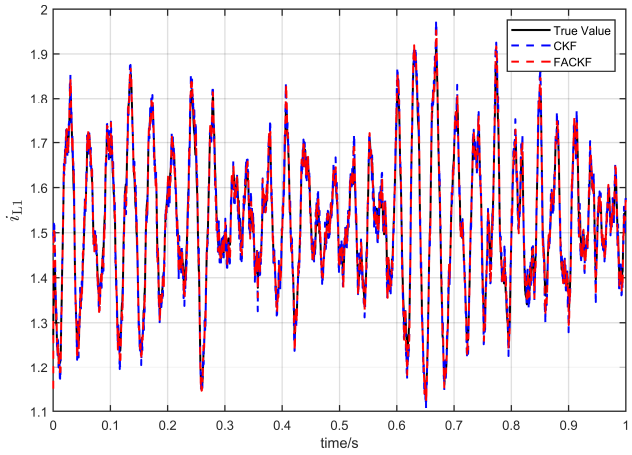
$$y_1 = [v_{c1}, i_{Ls}, v_{cs}],\ y_2 = [i_{L1}, i_{Ls}, v_{cs}]\ y_3 = [v_{c1}, i_{L1}, v_{cs}]\ y_4 = [v_{c1}, i_{Ls}, i_{L1}] \tag{24}$$

The CKF and the FACKF proposed in this paper are applied to estimate the system state for comparison, respectively, and the estimation results are shown in Figure 3.

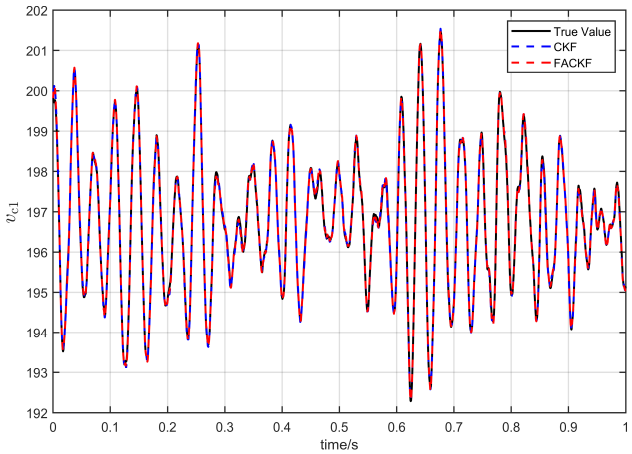
From the test results, it can be seen that without FDIA, both the traditional CKF method and the FACKF method proposed in this paper can accurately track the operating state of the DC microgrid system with good dynamic performance, and the state estimation accuracy of the two methods can satisfy the system monitoring requirements.

The results of the root mean square error (RMSE), root mean square deviation (RMSD), and constant norm-2 error (E_{n2}) calculated for both the traditional CKF method and the FACKF method are shown in Table 2. From the results in Table 2, it can be seen that the RMSEs of both the traditional CKF method and the FACKF method are smaller, which is consistent with the results presented in Figure 3; i.e., both the CKF method and the proposed method have higher tracking accuracy without spurious data injection. It can

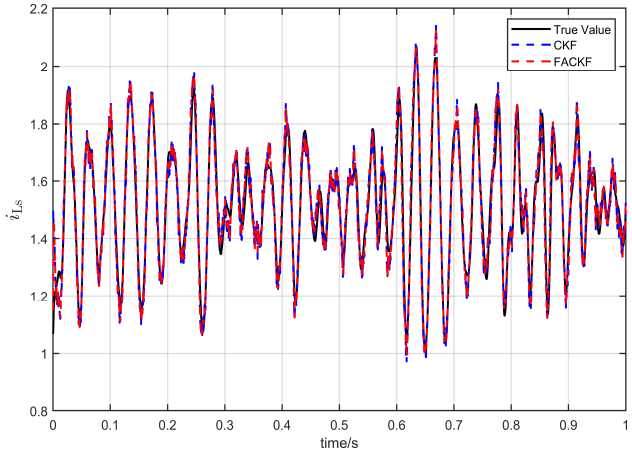
also be found that the RMSE, RMSD, and E_{n2} of each state component of the proposed partitioned FACKF method are slightly smaller than that of the traditional CKF method, compared to the traditional CKF method, and this result indicates that the proposed FACKF method has a higher state estimation accuracy, which is attributed to its use of the distributed estimation strategy.



(**a**)

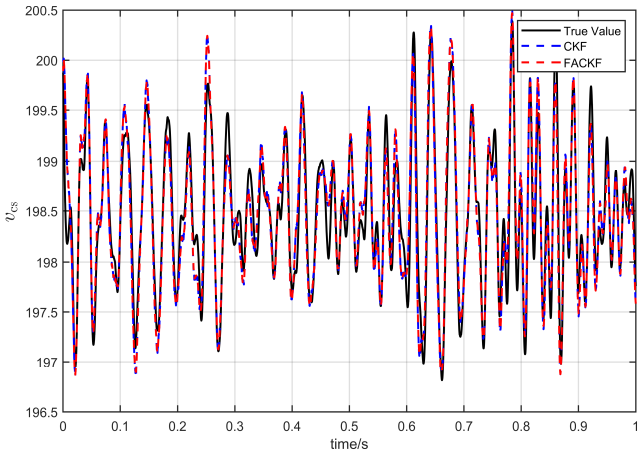


(**b**)



(**c**)

Figure 3. *Cont.*



(**d**)

Figure 3. Estimated results of the two algorithms in the no-attack case. (**a**) Estimation results of two methods for the state variable i_{L1}. (**b**) Estimation results of two methods for the state variable v_{c1}. (**c**) Estimation results of two methods for the state variable $i_{L\,1}$. (**d**) Estimation results of two methods for the state variable v_{cs}.

Table 2. Comparison between different methods.

State	Method	RMSE	RMSD	E_{n2}
i_{L1}	CKF	0.0099	0.0741	0.0357
	Proposed method	0.0108	0.0712	0.0302
v_{c1}	CKF	0.0142	0.0624	0.0421
	Proposed method	0.0120	0.0584	0.0367
i_{Ls}	CKF	0.0142	0.0725	0.0483
	Proposed method	0.0097	0.0676	0.0321
v_{cs}	CKF	0.0129	0.0863	0.0546
	Proposed method	0.0099	0.0825	0.0474

4.3. Case 2: Single CPL DC MG System

In the case of a single attack, in order to verify the detection and localization ability of the fusion CKF method proposed in this paper for false data attacks, an attack is set up on v_{c1} based on case 1. The traditional residual detection method and the partitioned fusion CKF method proposed in this paper are used to detect the system false data injection attack, respectively.

As can be seen from Figure 4, under the false attack injection, the residual difference increases significantly. Although the system can be detected by FDIA at this time, the specific location of FDIA injection cannot be determined. The results of the system using the conventional residual method are shown in Figure 5, where the residual values are the normalized data with no units.

It can be seen from Figure 5 that the state variance amplitude of the proposed FACKF method increases significantly when 0.3 s $\leq$ t $\leq$ 0.5 s, and FDIA can be judged to exist in the DC microgrid. When the voltage state is attacked, it has a larger value than other local residuals, because there is no measurement information containing attacks in the second local unit. In conclusion, the FACKF method proposed in this paper can not only achieve accurate detection of false data injection, but also locate the injected specific measurement unit.

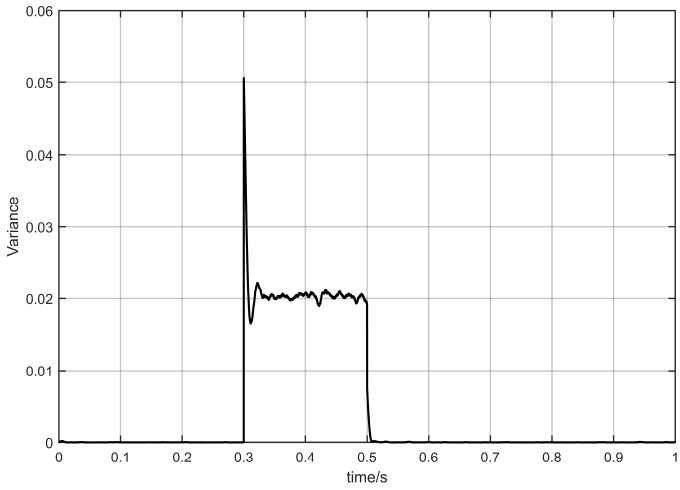


Figure 4. Traditional residual method detects the system.

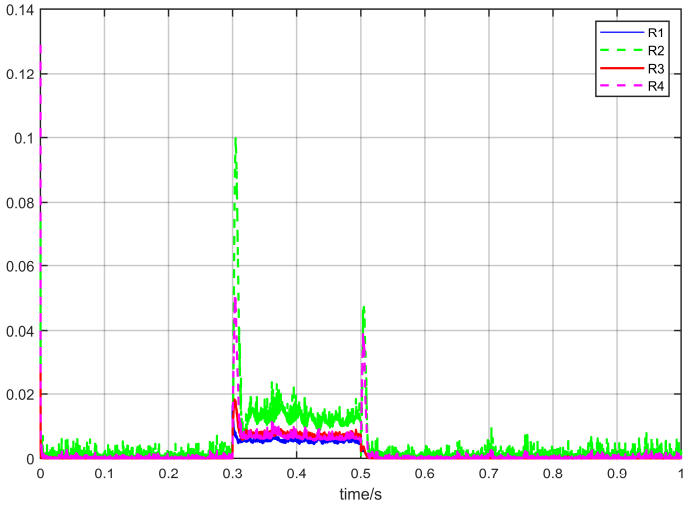


Figure 5. Based on fusion CKF residual detection.

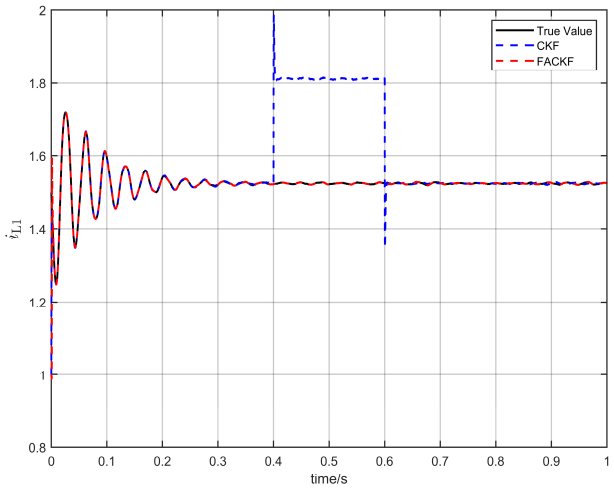
4.4. Case 3: Effectiveness of the FACKF under Multiple CPLs

To validate the effectiveness of the FACKF method under multiple CPL scenarios, the model is extended to include 2 CPLs, and false data injection is employed to detect the system. Setting $\boldsymbol{P}_{i,0}$ as $10^{-6}\boldsymbol{I}_{6\times6}$, $\boldsymbol{Q}_{i,k}$ as $10^{-6}\boldsymbol{I}_{5\times5}$, and $\boldsymbol{R}_{i,k}$ as $10^{-6}\boldsymbol{I}_{5\times5}$, an attack is initiated by injecting false data into $\boldsymbol{v}_{c1}$, starting at 0.4. In the attack scenario, we compare the state estimation results of the proposed method in this paper and the CKF.

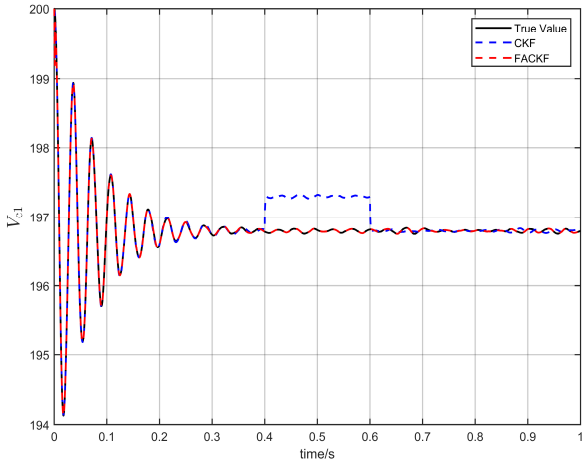
From Figure 6, it can be seen that under attack conditions, the system state estimation of the traditional CKF starts to deviate and gradually moves away from the true values. This is primarily due to erroneous data progressively influencing the system's state. However, the method proposed in this paper is capable of accurately detecting FDIA and identifying the affected measurement units. Upon detecting FDIA, this method isolates the injected unit and uses correct estimates from unaffected local units for overall estimation. As a result, this approach not only precisely tracks the operating state of the DC microgrid system but also demonstrates excellent dynamic performance.

Table 3 shows the comparison of various estimation metrics in the case of an attack. It can be clearly seen that once a network attack occurs, the RMSE, RAMD, and E_{n2} of the CKF are significantly larger than those of the FACKF, which is due to the fact that the traditional CKF design framework does not take into account the effect of attacks. Therefore, once an attack occurs, the estimation results of the CKF will be disturbed and seriously deviate from the real value or even regress. Compared with the traditional CKF,

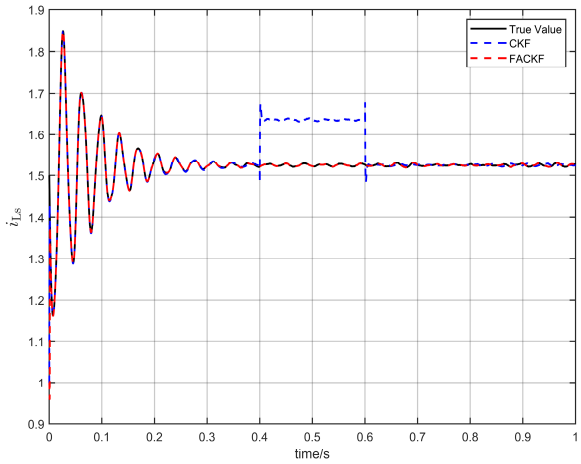
the proposed FACKF method can isolate the attack-induced bias and thus obtain better estimation performance. These results validate the effectiveness and excellent performance of the proposed FACKF method.



(**a**)

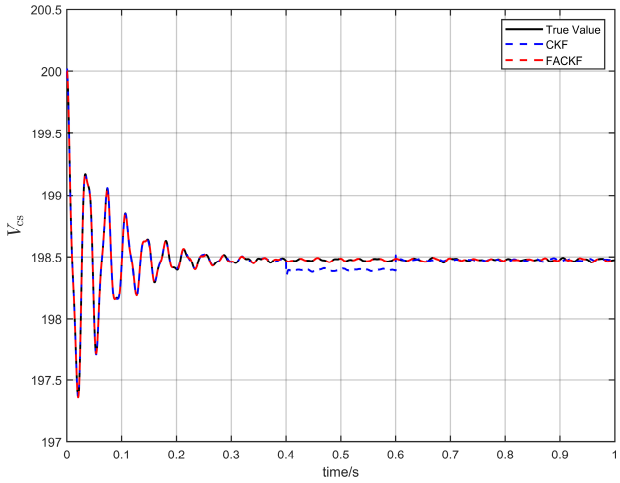


(**b**)



(**c**)

Figure 6. *Cont.*



(**d**)

Figure 6. Comparison of state estimation results for FACKF and CKF under attack. (**a**) Comparison of estimation results for i_{L1}. (**b**) Comparison of estimation results for V_{c1}. (**c**) Comparison of estimation results for i_{Ls}. (**d**) Comparison of estimation results for V_{cs}.

Table 3. Comparison between different methods under attack.

State	Method	RMSE	RMSD	E_{n2}
i_{L1}	CKF	0.1437	0.3524	0.2417
	Proposed method	0.0112	0.0693	0.0321
V_{c1}	CKF	0.1120	0.4351	0.3442
	Proposed method	0.0105	0.0542	0.0402
i_{Ls}	CKF	0.1406	0.3346	0.3157
	Proposed method	0.0120	0.0443	0.0297
V_{cs}	CKF	0.2598	0.4887	0.4021
	Proposed method	0.0139	0.0632	0.0214

4.5. Case 4: Computational Efficiency Test

In order to meet the requirements of various real-time applications in energy management systems (EMSs), dynamic estimation in DC microgrids needs to be not only accurate but also computationally efficient. This section aims to validate the feasibility of the proposed FACKF method for adapting to the sampling rate of 30–60 samples per second from PMUs, ensuring its suitability for real-time applications. By conducting tests on the computation time of the FACKF method and the traditional CKF method under different conditions, the computation times of both algorithms are shown in Figure 7.

The results demonstrate that although the FACKF method has a slightly longer computation time compared to the traditional CKF method, this difference is primarily due to the introduction of more complex formulas in the state estimation process of the FACKF. However, it is worth noting that the average computation time for both methods is significantly lower than the PMU sampling rate. This indicates that the FACKF method can meet the real-time requirements while maintaining accurate synchronous estimation capabilities. Furthermore, despite involving more complex computational steps, the additional computation time of the FACKF method has minimal impact on performance in practical applications, effectively meeting the real-time processing requirements of the EMS in DC microgrids. Therefore, the proposed FACKF method not only demonstrates superior estimation accuracy but also confirms its practicality and efficiency in fast, dynamic environments. It provides a reliable technical solution for energy management in DC microgrids.

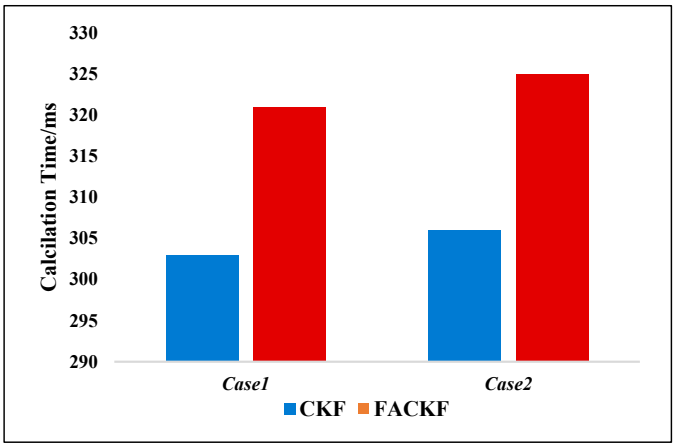


Figure 7. The comparison of computation times.

5. Conclusions

In the safe operation of a DC microgrid, real-time and accurate state estimation is crucial. To address this requirement, this paper introduces a novel method using fusion adaptive cubature Kalman filter (FACKF) technology, aiming to effectively detect and precisely locate the source of false data injection attacks. Through the analysis of experimental results, several conclusions can be drawn:

(1) The FACKF method proposed in this study can effectively detect false data injection attacks and accurately identify the attacked injection units, enhancing the system's protection against malicious attacks.
(2) After applying this research method, once an attack is identified, isolating the attacked unit and replacing the overall estimate with the correct local estimate can significantly enhance the robustness of the estimation process, thereby improving the stability and reliability of the system.
(3) The method proposed in this study exhibits low computational complexity. It not only effectively detects and locates attacks but also accurately estimates the system state under attack conditions, further ensuring the safe operation of the DC microgrid.

Although the FACKF method significantly enhances the system's protection against fake data injection attacks, its performance will vary with different attack modes and intensification. For the future work, we put forward the following suggestions: (1) adjust the algorithm to improve the adaptability to various attack scenarios and system configurations and (2) consider introducing advanced data analysis and machine learning techniques to improve the sensitivity of attack detection.

Author Contributions: P.W. and J.Z. (Jiangnan Zhang) were responsible for methodology, simulation, and validation. P.W. conducted the analysis and wrote the paper. Conceptualization was handled by S.L. and J.Z. (Jiangnan Zhang); resource management by S.L. and Y.S.; data curation by P.W. and Y.S.; original draft preparation by S.L. and J.Z. (Jiawei Zhang); review and editing by Y.W.; visualization by J.Z. (Jiangnan Zhang) and J.Z. (Jiawei Zhang); supervision by Y.W.; project management by J.Z. (Jiangnan Zhang); and funding acquisition by Y.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Science and Technology Project of State Grid Henan Electric Power Company under Grant 521702230004, the National Natural Science Foundation of China under Grant 62203395, in part by the China Postdoctoral Science Foundation under Grant 2023TQ0306, and in part by the Postdoctoral Research Project of Henan Province under Grant 202101011.

Data Availability Statement: Data are contained within the article.

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

References

1. Ansari, S.; Zhang, J.; Singh, R.E. A review of stabilization methods for DCMG with CPL, the role of bandwidth limits and droop control. *Prot. Control Mod. Power Syst.* **2022**, *7*, 12–19. [CrossRef]
2. Liu, B.; Li, H.; Zhang, H.; Han, M. A reactive power injection algorithm for improving the microgrid operational reliability. *Electronics* **2023**, *12*, 2932. [CrossRef]
3. Jiang, X.; Liu, W.; Yan, G.; Shao, H.; Zhang, L.; Wen, Y. Research on load carrying capacity evaluation of main grid with multiple DC feeds. *J. Electr. Power Sci. Technol.* **2023**, *38*, 216–225.
4. Liu, J.; Zhang, L.; Zhao, B.; Li, X. Online dynamic black start strategy for multi-power microgrid with energy storage. *Distrib. Util.* **2023**, *40*, 13–20.
5. Jasim, A.M.; Jasim, B.H.; Neagu, B.-C.; Alhasnawi, B.N. Coordination vontrol of a hybrid AC/DC smart microgrid with online fault detection, diagnostics, and localization using artificial neural networks. *Electronics* **2023**, *12*, 187. [CrossRef]
6. Fu, Y.; Zhang, Y.; Tian, S.; Shen, J.; Li, H.; Geng, F. State estimation method of active distribution network resisting multi-point false data attack. *Smart Power* **2023**, *51*, 69–76+83.
7. Xie, W.; Han, M.; Cao, W.; Guerrero, J.M.; Vasquez, J.C. Virtual resistance trade off design for DCMG grid-forming converters considering static-and large-signal dynamic constraints. *IEEE Trans. Power Electron.* **2020**, *36*, 5582–5593. [CrossRef]
8. Zhang, J.; Wu, Z.; Lu, X.; Wang, C. Research on coordinated control strategy of "optical storage direct and flexible" system considering DC power spring. *Distrib. Util.* **2023**, *40*, 82–92.
9. Yi, R. Research on the defense mechanism based on FDIA in smart grid. *Front. Comput. Intell. Syst.* **2022**, *2*, 84–88. [CrossRef]
10. Madichetty, S.; Mishra, S. Cyber attack detection and correction mechanisms in a distributed DC microgrid. *IEEE Trans. Power Electron.* **2021**, *37*, 1476–1485.
11. Dehghani, M.; Niknam, T.; Ghiasi, M.; Bayati, N.; Savaghebi, M. Cyber-attack detection in DC microgrids based on deep machine learning and wavelet singular values approach. *Electronics* **2021**, *10*, 1914. [CrossRef]
12. Huang, C.; Hong, M.; Fu, S. Distributed state estimation of active distribution network considering false data injection attack. *Electr. Power Eng. Technol.* **2022**, *41*, 22–31.
13. Xie, Y.; Yan, X.; Sang, Z.; Yang, X.; Ying, M.; Zhou, Y. Fake data injection attack method for hybrid AC-DC systems. *Electr. Power Eng. Technol.* **2022**, *41*, 165–172.
14. Xia, Y.S.; Wang, Y.; Zhou, L.; Fan, R.S. False data injection attack detection method based on improved generative adversarial network. *Electr. Power Constr.* **2022**, *43*, 58–65.
15. Wang, B.; Peng, X.; Jiang, M.; Liu, D. Real-time fault detection for UAV based on model acceleration engine. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 9505–9516. [CrossRef]
16. Bhandari, G.; Lyth, A.; Shalaginov, A.; Grønli, T.-M. Distributed deep neural-network-based middleware for cyber-attacks detection in smart IoT ecosystem: A novel framework and performance evaluation approach. *Electronics* **2023**, *12*, 298. [CrossRef]
17. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
18. Yang, J.; Zhu, F.; Wang, X.; Bu, X. Robust sliding-mode observer-based sensor fault estimation, actuator fault detection and isolation for uncertain nonlinear systems. *Int. J. Control Autom. Syst.* **2015**, *13*, 1037–1046. [CrossRef]
19. Liu, M.; Zhao, C.; Deng, R.; Cheng, P.; Chen, J. False data injection attacks and the distributed countermeasure in DC microgrids. *IEEE Trans. Control Netw. Syst.* **2022**, *9*, 1962–1974. [CrossRef]
20. Yan, L.; Zhang, Y.; Xiao, B.; Xia, Y.; Fu, M. Fault detection for nonlinear systems with unreliable measurements based on hierarchy cubature Kalman filter. *Can. J. Chem. Eng.* **2018**, *96*, 497–506. [CrossRef]
21. Wang, Y.; Liu, D. Maximum correntropy cubature Kalman filter and smoother for continuous-discrete nonlinear systems with non-Gaussian noises. *ISA Trans.* **2023**, *137*, 436–445. [CrossRef] [PubMed]
22. El Sayed, W.; Abd El Geliel, M.; Lotfy, A. Fault diagnosis of PMSG stator inter-turn fault using extended Kalman filter and unscented Kalman filter. *Energies* **2020**, *13*, 2972. [CrossRef]
23. Wang, S.; Zhang, W.; Sun, Y.; Trivedi, A.; Chung, C.; Srinivasan, D. Wind Power Forecasting in the presence of data scarcity: A very short-term conditional probabilistic modeling framework. *Energy* **2024**, *291*, 130305. [CrossRef]
24. Tang, H.; Tang, Y.; Su, Y.; Feng, W.; Wang, B.; Chen, P.; Zuo, D. Feature extraction of multi-sensors for early bearing fault diagnosis using deep learning based on minimum unscented kalman filter. *Eng. Appl. Artif. Intell.* **2024**, *127*, 107138. [CrossRef]
25. Yang, J.; Guo, Y.; Zhao, W. Long short-term memory neural network based fault detection and isolation for electro-mechanical actuators. *Neurocomputing* **2019**, *360*, 85–96. [CrossRef]
26. Ma, Y.; Li, C.; Cao, Z.; Pan, L.; Yang, C.; Yang, Z. Robust dynamic state estimation method of power system based on data fusion technology. *Smart Power* **2023**, *51*, 78–84.

27. Vafamand, A.; Moshiri, B.; Vafamand, N. Fusing unscented Kalman filter to detect and isolate sensor faults in DC microgrids with CPLs. *IEEE Trans. Instrum. Meas.* **2021**, *71*, 1–8. [CrossRef]
28. Shao, S.; Yan, R.; Lu, Y.; Wang, P.; Gao, R.X. DCNN-based multi-signal induction motor fault diagnosis. *IEEE Trans. Instrum. Meas.* **2019**, *69*, 2658–2669. [CrossRef]