Detection of False Data Injection Attacks in Microgrids Based on IGWO-CKF Algorithm

Wei Luo, Minglei Xie, Jinfeng Wang, Yuanzhe Zhu, Wanlin Du, Weizhong Chen, and Qinlong Hu

Abstract—**With the widespread application of information technology in power systems, microgrids have gradually evolved into Cyber Physical Power Systems that integrate power networks and physical systems. However, it increases the risk of false data injection attacks (FDIA) in the microgrids because their distributed cooperative control relies on real-time communication and system state information. To address this trouble, an Improved Grey Wolf Optimized Cubature Kalman Filter (IGWO-CKF) algorithm is proposed in this paper for the FDIA detection in microgrids. Specifically, a microgrid model that contains multiple levels false data attacks is firstly established. Then, by introducing Improved Grey Wolf Optimizer into Cubature Kalman Filter, a new IGWO-CKF is proposed to enhance the accuracy of attack detection in microgrids and overcome the poor performance defect of traditional Cubature Kalman Filter (CKF) in handling highly nonlinear systems. Finally, simulations are conducted on the WECC 9-bus system and the New England 39-bus system, which demonstrate the effectiveness and practicality the proposed method.**

Index Terms—**Microgrids; CPPSs; FDIA; IGWO-CKF**

I. INTRODUCTION

With the widespread application of information control technology in the power systems, microgrids have gradually evolved into Cyber Physical Power Systems (CPPSs) [1]. The communication environment of CPPSs makes its information network more vulnerable to network attacks, and pose a serious threat to the security and stability of the system [2]. False Data Injection Attacks (FDIA) which disrupt the integrity of power system data by tampering with measurement data, seriously affects the accuracy of system state estimation, and potentially leads to incorrect decision-making by control centers [3,4], and even causes large-scale blackouts. Therefore, how to effectively detect FDIA has become an urgent issue of smart grid.

The existing methods for FDIA detection are mainly classified into three categories: statistical analysis-based, machine learning-based, and state estimation-based methods [5]. The statistical analysis-based methods detect deviations between measurement data and actual states by residual analysis. In [6], the Measurement Error Residual Similarity (MERS) is proposed to effectively improve FDIA detection accuracy and reduce false positive rates. In [7], a Generalized Likelihood Ratio Test (GLRT) is proposed to statistically analyze measurement data and identify anomalies caused by FDIA. Principal Component Analysis (PCA) and Canonical Correlation Analysis (CCA) methods are investigated in [8], which shows that CCA performs better than PCA for FDIA detection. Second, machine learning-based methods utilize deep learning architectures to detect FDIA. In [9], a deep learning model is designed by combining traditional methods for real-time detection of both structured and unstructured attacks. In [10], the application of machine learning in FDIA detection is discussed to address class imbalance issues in datasets by using feature selection and oversampling. Support Vector Machine (SVM) and Artificial Neural Network (ANN) are employed to classify attacks based on normal and attack data features. In addition, other machine learning technique such as Convolkutional Neural Networks (CNN) is also applied to enhance detection efficiency [11,12].

In contrast, due to state estimation-based methods analyzing grid state variables (e.g., voltage magnitude and phase angle) through physical models and effectively identifying abnormal states in the system, they have unique advantages of stronger sensitivity to dynamic changes in the system, which can more accurately distinguish between normal fluctuations and attack behavior. In [13], a method based on dynamic-static parallel state estimation is proposed to identify FDIA in real-time. When the system is affected by FDIA, the reduced correlation in parallel time series effectively reveals potential FDIA. By combining the Unscented Kalman Filter (UKF) with the Weighted Least Squares (WLS) algorithm in real-time, [14] detects the differences between estimated values to identify FDIA. [15] establishes a DC MG model with FDIAs and analyzes the system under attack. By reviewing the FDIA detection limitations of traditional residual methods and Kalman filter-based detectors in noisy and complex networks, an attack magnitude planning strategy is introduced in [16] to exploit noise tolerance and bypass residual detection. In [17],

Manuscript received November 17, 2024; revised May 6, 2025.

This work was supported by the China Southern Power Grid Project under grant 031400KC23120011.

Wei Luo is a senior engineer in the Meizhou Power Supply Bureau of Guangdong Power Grid, Guangdong Power Grid Corporation, Meizhou 514021, China (email: lwgd86@126.com).

Minglei Xie is a senior engineer in the Southern Power Grid Scientific Research Institute Company of Limited Liability, Guangzhou 510080, China (email: xieminglei@126.com).

Jinfeng Wang is a senior engineer with the rank of a professor in the Guangdong Electric Power Research Institute, Guangzhou 518118, China (email: jfwang@163.com).

Yuanzhe Zhu is a senior engineer in the Southern Power Grid Energy Development Research Institute Company of Limited Liability, Guangzhou 511458 (email: szzhouyong1975@126.com).

Wanlin Du is an engineer in the Guangdong Electric Power Research Institute, Guangzhou 518118, China (e-mail: dwlgd@126.com).

Weizhong Chen is a senior engineer in the Meizhou Power Supply Bureau of Guangdong Power Grid, Guangdong Power Grid Corporation, Meizhou 514021, China (e-mail: chenweizhong@126.com).

Qinlong Hu is an engineer in the Hangzhou Lengyue Technology Company of Limited Liability, Hangzhou 310020, China (e-mail: huqinlong@126.com).

a novel outlier detection and state correction strategy is proposed by comparing deviations between EKF and weighted least squares (WLS) against an offline threshold. In [18], the robustness of the Cubature Kalman Filter (CKF) algorithm is enhanced by utilizing a fading factor and integrated an interacting multiple model to achieve hypersonic target tracking. Similarly, the robustness of the CKF algorithm is improved by different attempts in [19-21].

The Kalman Filter (KF) is a common tool for dynamic state estimation, however the classical KF is only applicable to linear systems. As the extension, the Cubature Kalman Filter (CKF) can handle nonlinear systems. However, the CKF suffers from the linearization errors when it is employed to deal with highly nonlinear situations, especially during severe dynamic events like short-circuit faults. It may result in insufficient estimation accuracy. As a result, to compensate for this drawback, this paper proposes an improved Cubature Kalman Filter based on an enhanced Grey Wolf Optimization. The standard Grey Wolf Optimization (GWO) algorithm is prone to local optima and slow convergence. To mitigate these issues, this study incorporates the quasi-oppositional population initialization strategy, nonlinear parameter adjustment, boundary handling strategy, and dynamic weight adjustment to form an Improved Grey Wolf Optimization (IGWO) algorithm. The IGWO-CKF utilizes GWO to adaptively tune the process noise covariance and measurement noise covariance in real-time, thereby it optimizes the Kalman gain to tackle complex False Data Injection Attacks (FDIA) in power systems. Simulation results demonstrate that the proposed method effectively detects FDIA attacks.

II. POWER SYSTEM DYNAMIC MODEL

The power system model reflects the dynamic response of generators under various operating conditions, which provides a foundation for FDIA detection and analysis. Based on a classical generator model, we introduce the dynamic model (1), which is used for state estimation of power systems, and provides a reliable framework to accurately describe the dynamic behavior of power systems.

$$\begin{aligned} \dot{\delta}_i &= \omega_i - \omega_0 \\ \dot{\omega}_i &= \frac{\omega_0}{2H_i}(P_{mi} - P_{Gi} - D(\omega_i - \omega_0)) \end{aligned} \tag{1}$$

where δ_i, ω_i, P_{mi}, P_{Gi} represent the rotor angle, angular speed, mechanical power and output power of generator i, respectively. ω_0 is the synchronous (rated) speed of this generator. D denotes the damping coefficient, and H represents the inertia constant of this generator. The output power of this generator is as:

$$P_{Gi} = E_i \sum_{j=1}^{n} E_j Y_{ij} \cos\left(\delta_i - \delta_j - \theta_{ij}\right) \tag{2}$$

where Y denotes the admittance matrix of a simplified network consisting only of internal generator buses, E is the internal voltage of the generator, and θ is the angle of Y The calculation for Y follows equation (3):

$$Y = Y_{22} - Y_{21} \times Y_{11}^{-1} \times Y_{12} \tag{3}$$

where Y_{11} is the admittance matrix between loads, $Y_{12} = Y_{21}^{T}$ is the admittance matrix between loads and generators, and Y_{22} is the admittance matrix between rotors. The discrete form of equation (1) is shown as:

$$\begin{aligned} \delta_{i,k} &= \delta_{i,k-1} + \omega_0 \times (\omega_{i,k-1} - 1) + \omega_{i,\delta} \\ f(x_k, \mu_k) = \ \omega_{i,k} &= \omega_{i,k-1} + \omega_{i,\omega} + (P_{mi} - P_{Gi,k-1} \\ &\quad - D(\omega_{i,k-1} - 1)) / M + \omega_{i,\omega} \end{aligned} \tag{4}$$

where $\omega_{i,\delta}$ and $\omega_{i,\omega}$ are the process noise associated with state variables δ and ω, respectively, and Δt is the simulation time step. Therefore, the parameters to be predicted are the rotor angle δ and the rotor angular velocity ω.

A nonlinear measurement function is used for dynamic state estimation in power systems, referred to as the measurement model. In the dynamic state estimation of power systems, the active and reactive power obtained from generators are typically used as inputs. The expression for the active power output of a generator is given in equation (2), while the expression for the reactive power output of the generator is represented as:

$$Q_{Gi} = E_i \sum_{j=1}^{n} E_j Y_{ij} \sin(\delta_i - \delta_j - \theta_{ij}) \tag{5}$$

The voltage magnitude and phase angle measurements are given in equation (6).

$$Y_{exp} V_{exp} = \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix} \begin{pmatrix} V\angle\theta \\ \mathrm{E}\angle\theta \end{pmatrix} = \begin{pmatrix} 0 \\ I_G\angle\delta \end{pmatrix} \tag{6}$$

where Y_{exp} represents the extended system matrix. V_{exp} denotes the extended voltage vector, including the internal rotor voltage E and the bus voltage V. I_G is the injected current. From equation (6), the relationship between V and E can be derived as follows:

$$\mathrm{V}\angle\theta = (-Y_{11})^{-1} Y_{22} \mathrm{E}\angle\delta = R_V \mathrm{E}\angle\delta \tag{7}$$

where R_V is the voltage reconstruction matrix. As a result, the dynamic state estimation model and the measurement model is formulated as:

$$X = [\delta^T \quad \omega^T] \tag{8}$$

$$Z = [P_{G_i}^T \quad Q_{G_i}^T \quad V^T \quad \theta^T] \tag{9}$$

III. FDIA MODEL

A. FDIA Introduction

FDIAs can be implemented at multiple levels, which includes measurement unit attacks (A1), communication network attacks (A2), and control device attacks (A3). By manipulating data at these levels, attackers can affect the state estimation of the power system, and cause the system to make incorrect decisions based on erroneous data. In turn, it impacts the stability and security of the power systems. The structure of FDIA targeting microgrids is illustrated in the Fig.1. Data collected by sensors is transmitted through the communication network to the remote terminal unit (RTU) at the information layer. The communication layer is a critical attack point for FDIAs. Attackers can hijack, alter, or forge communication data, passing false measurements to the upper layers and disrupting the normal operation of the

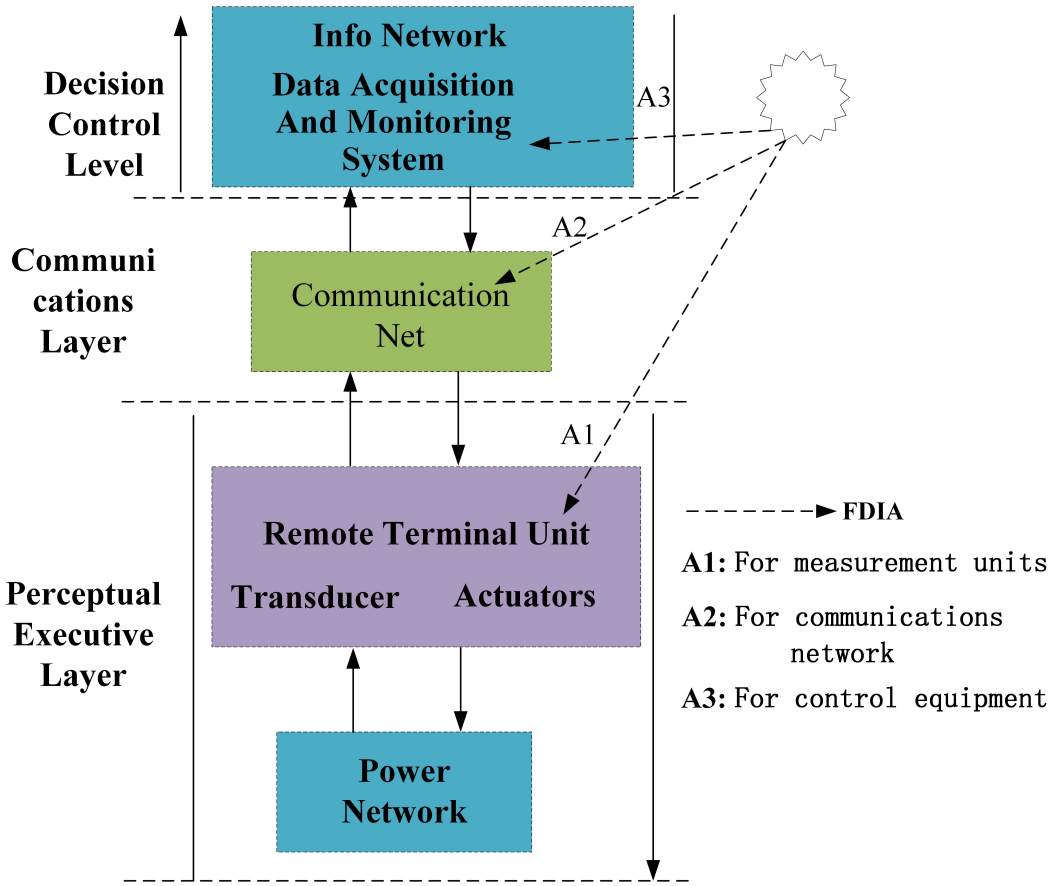

Fig. 1. The FDIA structure in the smart grid

power system. The RTU can also transmit data obtained from the sensing and execution layers to the Supervisory Control and Data Acquisition (SCADA) system. At this level, attackers can directly tamper with the data, inject false measurements (A1), or interfere with system operation by altering network communications (A2). The SCADA system transmits the data from the lower levels to the decision control system, where grid operators and automation systems make decisions. Once attackers successfully inject false data, the decision system may make erroneous optimization decisions (A3) based on these falsified data, and lead to control operation failures that affect grid performance.

To address bad data caused by FDIA, this paper employs the Kalman Filter for prediction, comparing predicted values with actual values to detect FDIA. In power systems, modeling false data injection attacks (FDIA) typically involves tampering with system measurements to alter state estimation results. This paper targets FDIA on sensor data in generator measurement units. To verify the effectiveness of the proposed algorithm under various attack modes, we select measurement values from three generators in the WECC 9-bus system and ten generators in the New England 39-bus system as attack targets. To comprehensively test the algorithm's detection capabilities, this study utilizes three typical FDIA models—pulse attacks, ramp attacks, and random attacks—to simulate different types of malicious interference scenarios.

B. Pulse Attack

A pulse attack is an instantaneous attack where the attacker injects a pulse into the measurement data at a specific moment, attempting to disrupt the system's state estimation over a short period. Its mathematical model is as follows:

$$\begin{cases} X_i(t) = B_i x_i(t) + v_i(t) + s_i, t \notin \tau_a \\ X_i(t) = B_i x_i(t) + v_i(t) + s_i + a_i, t \notin \tau_a \end{cases} \tag{10}$$

In the above equation, $X_i(t)$ represents the original measurement value of the system, and a_i denotes the pulse attack signal, $a_i=[a_{i1},a_{i2},a_{i3}]^T$ The pulse attack can be expressed by the following formula: a_{i1} is the FDIA applied to the rotor angle δ_i in the measurement of the i generator, a_{i2} is the FDIA applied to the rotor speed ω_i of the i generator, a_{i3} is the FDIA applied to the voltage measurement of the i generator, and τ_i represents the duration of the attack.

C. Ramp Attack

A ramp attack is a gradual attack where the attacker increases or decreases the measurement value incrementally from a specific moment, ultimately impacting the state estimation of the system. Its mathematical model is as follows:

$$\begin{cases} X_i(t) = B_i x_i(t) + v_i(t) + s_i, t \notin \tau_a \\ X_i(t) = B_i x_i(t) + v_i(t) + s_i + \lambda_i \times t, t \notin \tau_a \end{cases} \tag{11}$$

where λ_i is the ramp coefficient.

D. Random Attack

A random attack is the attacker injects disturbances into the measurements based on a random distribution. The objective of a random attack is to increase system noise and compromise the accuracy of state estimation. The random

attack can be expressed as follows, where m and n are the upper and lower bounds of the random attack:

$$\begin{cases} X_i(t) = B_i x_i(t) + v_i(t) + s_i, t \notin \tau_a \\ X_i(t) = B_i x_i(t) + v_i(t) + s_i + rank(m,n), t \notin \tau_a \end{cases} \quad (12)$$

The randomness of random attacks makes it difficult for the system to distinguish between normal noise and attack signals using conventional detection methods.

IV. Improved Grey Wolf Optimized Cubature Kalman Filter

A. Standard Cubature Kalman Filter

For a nonlinear discrete-time tracking system with additive noise, the state-space equations are represented as:

$$\begin{aligned} x_k &= f(x_{k-1}) + w_{k-1} \\ z_k &= h(x_k) + v_k \end{aligned} \quad (13)$$

where x_k represents the state vector at time k, and z_k represents the measurement vector at time k. w_{k-1} denotes the process Gaussian white noise with variance Q_{k-1}, and v_k denotes the measurement Gaussian white noise with variance R_k. $f(\cdot)$ and $h(\cdot)$ correspond to the state transition function and measurement function, respectively.

The core task of nonlinear filtering is to obtain the minimum variance estimate of the system state using noisy measurements. The key challenge lies in solving the following integral:

$$I(f) = \int f(x)\exp(-x^T x)dx \quad (14)$$

The core of CKF is to select cubature points using the third-order spherical-radial cubature rule. Specifically, let $x = ry$ and y be the unit directional vectors in a dimensional space. Equation (15) can be decomposed into a dimensional spherical integral and a one-dimensional radial integral in the spherical-radial coordinate system:

$$\begin{aligned} I(f) &= \int_0^\infty \int_{U_n} f(ry) r^{n-1} \exp(-r^2) d\sigma(y) dr \\ &= \int_0^\infty r^{n-1}\exp(-r^2)dr \int_{U_n} f(ry)d\sigma(y) \end{aligned} \quad (15)$$

$$S_n(r) = \int_{U_n} f(ry)d\sigma(y) \approx \sum_{i=1}^{N_y} w_{y,i} f(ry_i) \quad (16)$$

$$R(r) = \int_0^\infty \mathrm{S}(\mathrm{r}) r^{n-1} \mathrm{e}^{-r^2} dr \approx \sum_{j=1}^{N_r} w_{r,j} S(r_j) \quad (17)$$

where $U_n = \{\mathbf{y} \in R^n | \ \mathbf{y}^T\mathbf{y} = 1\}$, Let $d\sigma(y)$ denote the spherical micro-element U_n. In equation (16), $w_f(y) = 1$ represents the spherical integral weight, and $w_f(r) = r^{n-1}\mathrm{e}^{-r^2}$ denotes the radial integral weight. Here, y_i and $w_{y,i}$ correspond to the quadrature points and weights for spherical integration, while r_j and $w_{r,j}$ represent the quadrature points and weights for radial integration. Equation (16) can be expressed as:

$$I(f) \approx \sum_{i=1}^{N_y}\sum_{j=1}^{N_r} w_{y,i} w_{r,j} f(r_j y_i) \quad (18)$$

Applying Equation (19) to Gaussian-weighted integration yields:

$$\int g(x)N(x;0,I)dx = \frac{1}{\sqrt{\pi^n}} \sum_{i=1}^{N_y}\sum_{j=1}^{N_r} w_{y,i} w_{r,j} g(\sqrt{2} r_j y_i) \quad (19)$$

In summary, the third-order spherical-phase radial cubature criterion is formulated as:

$$\begin{aligned} I(g) &= \int \mathrm{g}(x)\exp(-x^{\mathrm{T}}x)dx \approx \\ &\frac{\sqrt{\pi^n}}{2n}\sum_{i=1}^{2n} g\left(\sqrt{\frac{n}{2}[1]_i}\right) = \sum_{i=1}^{2n} \omega_i g(\zeta_i) \end{aligned} \quad (20)$$

where n denotes the state dimension.

$$\xi_i = \sqrt{n}\left[\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} \cdots \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \begin{pmatrix}-1\\0\\0\\0\end{pmatrix} \cdots \begin{pmatrix}0\\0\\0\\-1\end{pmatrix}\right], \ \omega_i = \frac{1}{2n} \quad (21)$$

Based on the aforementioned third-order spherical-phase radial cubature criterion, the computational workflow of the CKF for $x_k \sim N(\hat{x}_k, P_k)$ proceeds as follows:

1. Filter Initialization

The initial state vector $\hat{x}_0$ and error covariance matrix P_0 are defined as:

$$\begin{aligned} \hat{x}_0 &= E[x_0] \\ P_0 &= E[(x_0 - \hat{x}_0)(x_0 - \hat{x}_0)^T] \end{aligned} \quad (22)$$

2. Time Update

Compute cubature points: Replace Cholesky with SVD decomposition to enhance the stability and robustness of the filtering.

$$P_{k|k} = U_k S_k V_k^T \quad (23)$$

$$x_{k,i} = \hat{x}_k + U_k\sqrt{S_k}\xi_i \quad (24)$$

Propagate cubature points:

$$\mathrm{x}_{\mathrm{k+1|k,i}} = \mathrm{f}(\mathrm{x}_{\mathrm{k,i}}) \quad (25)$$

Calculate the one-step state prediction $\hat{x}_{k+1|k}$:

$$\hat{x}_{k+1|k} = \sum_{i=1}^{2n} \omega_i x_{k+1|k,i} \quad (26)$$

$$P_{k+1|k} = \sum_{i=1}^{2n} \omega_i (x_{k+1|k,i} - \hat{x}_{k+1|k})(x_{k+1|k,i} - \hat{x}_{k+1|k})^T + Q_k \quad (27)$$

3. Measurement Update

Compute cubature points:

$$\begin{aligned} P_{k+l|k} &= U_{k+l|k} S_{k+l|k} V_{k+l|k}^T \\ \overline{x}_{k+l|k,i} &= \hat{x}_{k+l|k} + U_{k+l|k}\sqrt{S_{k+l|k}}\xi_i \end{aligned} \quad (28)$$

Propagate cubature points:

$$z_{k+1,i} = h(\overline{x}_{k+1|k,i}) \quad (29)$$

Calculate the one-step measurement prediction:

$$\hat{z}_{k+1} = \sum_{i=1}^{2n} \omega_i z_{k+1,i} \quad (30)$$

Compute the error covariance matrix $P_{k+1|k}^{zz}$ and cross-covariance matrix $P_{k+1|k}^{xz}$:

$$P_{k+1|k}^{zz} = \sum_{i=1}^{2n} \omega_i (z_{k+1,i} - \hat{z}_{k+1})(z_{k+1,i} - \hat{z}_{k+1})^T + R_{k+1} \quad (31)$$

$$P_{k+1|k}^{xz} = \sum_{i=1}^{2n} \omega_i (\overline{x}_{k+1|k,i} - \hat{x}_{k+1|k})(z_{k+1,i} - \hat{z}_{k+1})^T \quad (32)$$

Calculate the gain matrix K_{k+1}:

$$K_{k+1} = P_{k+1|k}^{xz}\left(P_{k+1|k}^{zz}\right)^{-1} \quad (33)$$

Estimate the state at time step k+1:

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(z_{k+1} - \hat{z}_{k+1})$$
$$P_{k+1} = P_{k+1|k} - K_{k+1}P^{zz}_{z_{k+1|k}}K^{T}_{k+1} \quad (34)$$

B. IGWO-CKF Algorithm

The GWO algorithm simulates the social hierarchy and hunting behavior of grey wolf packs to search for optimal solutions. In the algorithm, each wolf's position corresponds to a feasible solution, and the fitness value determines the pyramid-like social hierarchy within the population (Figure 2). The top three wolves with the highest fitness values are designated as α, β, and δ, responsible for tracking and guiding the pack toward prey. The remaining wolves are classified as ω, tasked with encircling and attacking the prey.

The search behavior of grey wolves is modeled as:

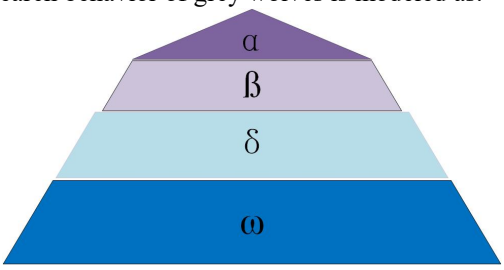

Fig. 2. Social hierarchy of grey wolves

$$X(t+I) = X_p(t) - A \cdot D$$
$$D = \left| C \bullet X_p - X(t) \right| \quad (35)$$

where t denotes the current iteration number, and $X_p(t)$ represents the current prey position. The disturbance factors A and C are calculated as:

$$A = 2a \cdot r_1 - a \quad (36)$$
$$C = 2 \cdot r_2 \quad (37)$$
$$a = 2\left(1 - t / t_{\max}\right) \quad (38)$$

where r_1 and r_2 are random vectors within [0,1], and $t_{\max}$ is the maximum number of iterations.

$$\begin{cases} D_\alpha = \left| C_1 \cdot X_\alpha(t) - X(t) \right| \\ D_\beta = \left| C_2 \cdot X_\beta(t) - X(t) \right| \\ D_\delta = \left| C_3 \cdot X_\delta(t) - X(t) \right| \end{cases} \quad \begin{cases} X_1 = X_\alpha - A_1 \cdot D_\alpha \\ X_2 = X_\beta - A_2 \cdot D_\beta \\ X_3 = X_\delta - A_1 \cdot D_\delta \\ X(t+I) = (X_1 + \\ \quad X_2 + X_3)/3 \end{cases} \quad (39)$$

where X_α, X_β and X_δ denote the positions of the α, β, and δ wolves, respectively, and D_α, D_β and D_δ represent the distances between these elite wolves and the ω wolves.

During the search for the optimal solution (prey position), the α, β, and δ wolves gradually converge toward the prey. For ω wolves, proximity to the three elite wolves implies closer proximity to the prey. The final movement direction and distance of each wolf are calculated using Equation (39).

C. Improved Grey Wolf Optimizer (IGWO)

Process noise during the time update and measurement noise, as critical filtering input parameters in the CKF, significantly influence target tracking accuracy. Measurement noise originates from sensing devices and can be determined based on device specifications, whereas process noise, generated dynamically during target motion, exhibits time-varying characteristics. To enhance the filtering precision of the CKF algorithm, the Grey Wolf Optimizer (GWO) can be employed to dynamically adjust the process noise covariance.

The GWO algorithm has been widely applied to path planning, economic dispatch, optimal control, and other fields due to its structural simplicity, minimal input parameters, and ease of implementation. Many scholars have also proposed improvements to the GWO algorithm. Current advancements primarily focus on three aspects: Initial population generation, Search mechanism refinement, and Algorithm parameter optimization. Building on prior research, this study introduces corresponding improvements to all three components to enhance search speed and achieve global optimality.

1. Good Point Set Initialization Strategy

In the GWO algorithm, the initial positions of the grey wolf population individuals are defined as:

$$X_i = GW_{lb} + rand(GW_{ub} - GW_{lb}) \quad (40)$$

where GW_{lb} and GW_{ub} denote the lower and upper bounds of the grey wolf positions, respectively.

For a two-dimensional grey wolf population, 300 individuals are generated within the interval [0,10]. This limits the GWO algorithm's ability to fully exploit the search space and increases susceptibility to local optima. To address this, the Good Point Set theory is introduced to initialize the grey wolf population. The revised initialization strategy is formulated as:

$$X_i = GW_{lb} + \{Pn(k)\}(GW_{ub} - GW_{lb}) \quad (41)$$

2. Boundary Handling Strategy

In conventional GWO, out-of-bounds individuals are typically clamped to the boundary limits. However, excessive boundary violations lead to positional homogenization among wolves, degrading population diversity and trapping the search in local optima. To preserve diversity, a secondary update rule is applied to reposition boundary-violating individuals:

$$X_{i,new} = \begin{cases} \begin{cases} lb & \omega > 1-\sigma \\ lb + \omega(ub - lb) & \omega < \sigma \end{cases} & X < lb \\ \begin{cases} lb + \omega(ub - lb) & \omega < \sigma \\ ub & \omega > 1-\sigma \end{cases} & X > ub \end{cases} \quad (42)$$

where ω is a uniformly distributed random number in [0,1], and σ is the boundary-handling parameter (set to 0.5 in this study).

3. Nonlinear Convergence Factor Strategy

In the standard GWO, the convergence factor a linearly decreases from 2 to 0 over iterations, which often leads to premature convergence. To balance exploration and exploitation, a nonlinear decay strategy based on an exponential function is proposed:

$$a = a_{\min} - (a_{\max} - a_{\min}) e^{-\left(\frac{2t}{t_{\max}}\right)^4} \quad (43)$$

4. Dynamic Weight Adjustment Strategy

The original GWO updates wolf positions using the arithmetic mean of step sizes toward the α, β, and δ wolves, neglecting their hierarchical dominance in guiding the search. To align with the social hierarchy and accelerate convergence,

a weighted average approach is adopted, where weights are assigned based on the fitness values of the elite wolves:

$$X(t+I)=\frac{1}{3}\sum_{i=1,2,3}\omega_i X_i(t+I)$$
$$\omega_i=\frac{f(X_i(t+I))}{\sum_{i=1,2,3}f(X_i(t+I))} \quad (44)$$

where $f(X_i)(i=1,2,3)$ denote the fitness values of the α, β, δ wolves, respectively, and the weights are calculated as ω_i.

D. Improved Grey Wolf Optimized Cubature Kalman Filter (IGWO-CKF)

The IGWO-CKF optimizes the process noise covariance matrix Q in the CKF using the IGWO algorithm to achieve adaptive parameter tuning. Since Q is a diagonal matrix, the grey wolf positions in the IGWO algorithm are set as the diagonal elements of Q. The iterative optimization process is as follows:

Step 1: Initialize the population size (N), maximum iteration count $t_{\max}$, convergence factor (a) and perturbation factors A and C.

Step 2: Generate the initial population positions using the good point set theory to ensure uniform distribution of grey wolf individuals in the search space. The initial population positions are denoted as $\{X_1, X_2, \cdots, X_N\}$.

Step 3: Select the actual variance of the filter innovation as the fitness function (equation (45)), calculate the fitness values of all grey wolves, and identify the top three elite wolves, whose positions are denoted as X_α, X_β and X_δ.

Step 4: Update the nonlinear convergence factor according to equation (43), and compute the perturbation factors A and C.

Step 5: Update the positions X_k of grey wolf individuals using equations (39) and (44). Handle out-of-bounds individuals and recalculate their fitness values $f(X_k)$.

Step 6: Update the positions and fitness values of α, β and δ wolves.

Step 7: Terminate the iteration if the stopping criteria are met; otherwise, return to Step 4. The optimized diagonal elements of Q, derived from the optimal solution $X_\alpha(t)=[q_1,q_2,q_3,q_4,q_5]$, are used as inputs for the next iteration.

During the IGWO-based optimization of filter noise, a well-designed fitness function guides the overall movement direction of the grey wolf population and serves as an effective termination criterion. The filter innovation, defined as the difference between the actual and predicted measurements, is closely related to Q. Therefore, the fitness function is set as the actual variance of the innovation. A smaller fitness value corresponds to higher target tracking accuracy.

$$l=\min((z_{k+1}-\hat{z}_{k+1})(z_{k+1}-\hat{z}_{k+1})') \quad (45)$$

In the equations: l represents the actual variance of the innovation, z_{k+1} and $\hat{z}_{k+1}$ denote the measured and predicted values at the corresponding time steps, respectively.

V. SIMULATION RESULTS AND ANALYSIS

A. Parameter Settings

Simulations were conducted using the WECC 3-machine 9-bus system and the New England 10-machine 39-bus system in the MATLAB environment to analyze the proposed IGWO-CKF prediction algorithm for detecting FDIA in power cyber-physical systems. The specific parameters are shown in the table below:

TABLE I
WECC 3-machine 9-bus system

Generator	H(p. u)	D(p. u)	X(p. u)
1	23.64	0.0225	0.0608
2	6.4	0.00663	0.1198
3	3.01	0.00265	0.1813

TABLE Π
New England 10-machine 39-bus system

Generator	H(p. u)	D(p. u)	X(p. u)
1	500	0.006	0
2	30.3	0.0697	0
3	35.8	0.0531	0

The WECC 3-machine 9-bus system consists of 3 generators and 3 load points, with total loads of 315 MW and 115 MVar, respectively. The system data, configuration, and inertia constants are listed in Table 1. This system has been widely used in multiple power system stability studies. The New England 10-machine 39-bus system includes 10 generators and 21 load points, with a total load of 6254.2 MW and 1387.1 MVar. In this study, three generators were selected as the research subjects. The system data, configuration, and inertia constants are detailed in Table 2.

B. Performance Analysis of CKF and IGWO-CKF Prediction Algorithms

To validate the proposed algorithm's effectiveness in detecting false data injection attacks, we first tested the performance of CKF and IGWO-CKF in estimating power system states under no FDIA conditions. The measurement targets were the rotor angles and speeds of the generators, and the actual values were compared with the CKF and IGWO-CKF predictions. The simulation results are shown in Figs. 2-5. The study selected three generators from each of the two power systems mentioned above. As observed, both CKF and IGWO-CKF can accurately estimate the system states when no FDIA is presented, which suggests that the proposed algorithm can be further applied for FDIA detection.

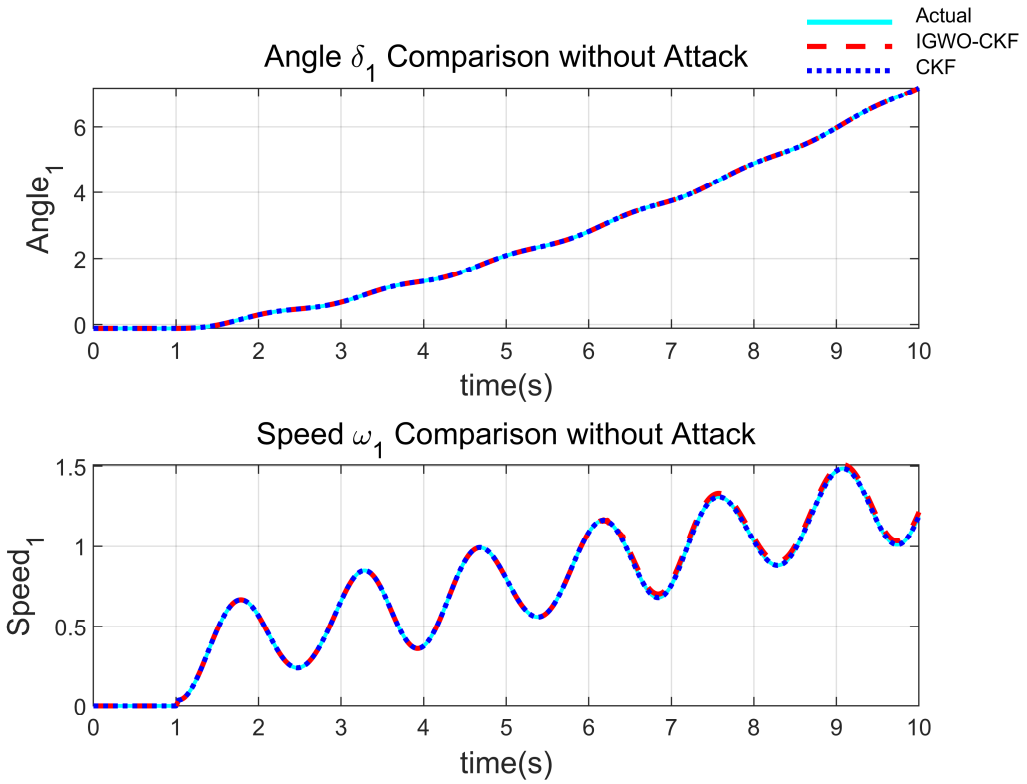

Fig. 3. Estimation of rotor angles and speeds of generator 1 for the WECC 3-machine 9-bus system without FDIA.

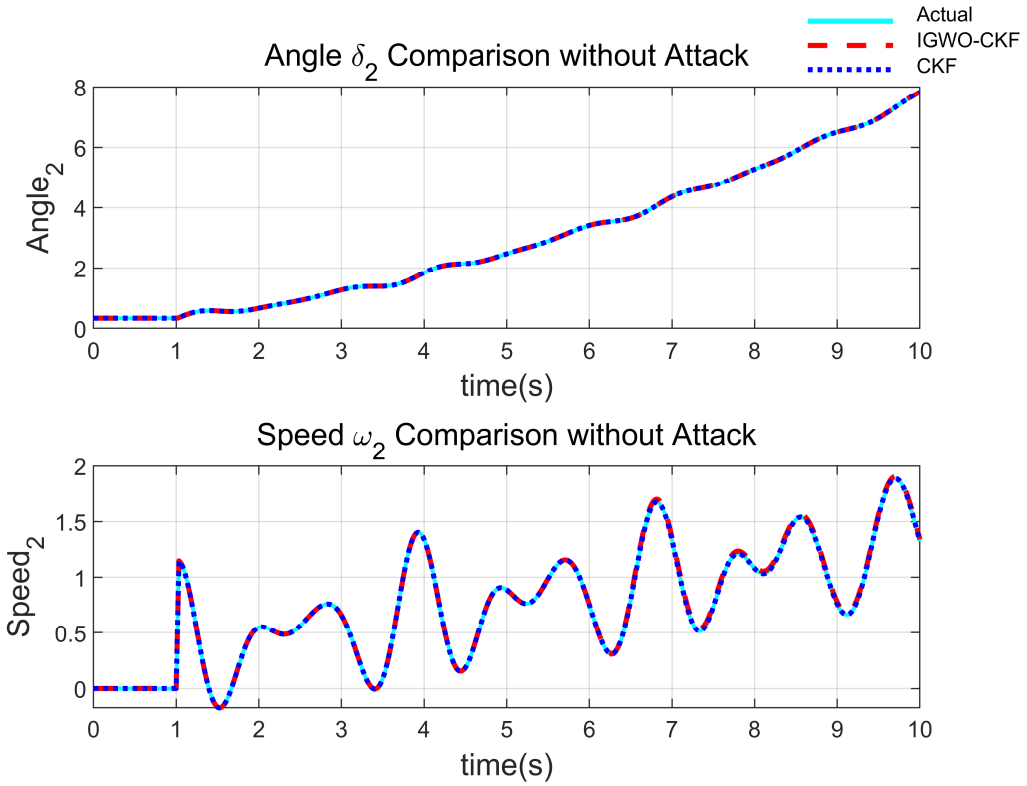

Fig. 4. Estimation of rotor angles and speeds of generator 2 for the WECC 3-machine 9-bus system without FDIA

C. Performance Analysis of CKF and IGWO-CKF Prediction Algorithms

To validate the proposed algorithm's effectiveness in detecting false data injection attacks, we first tested the performance of CKF and IGWO-CKF in estimating power system states under no FDIA conditions. The measurement targets were the rotor angles and speeds of the generators, and the actual values were compared with the CKF and IGWO-CKF predictions. The simulation results are shown in Figs. 2-5. The study selected three generators from each of the two power systems mentioned above. As observed, both CKF and IGWO-CKF can accurately estimate the system states when no FDIA is present, suggesting that the proposed algorithm can be further applied for FDIA detection.

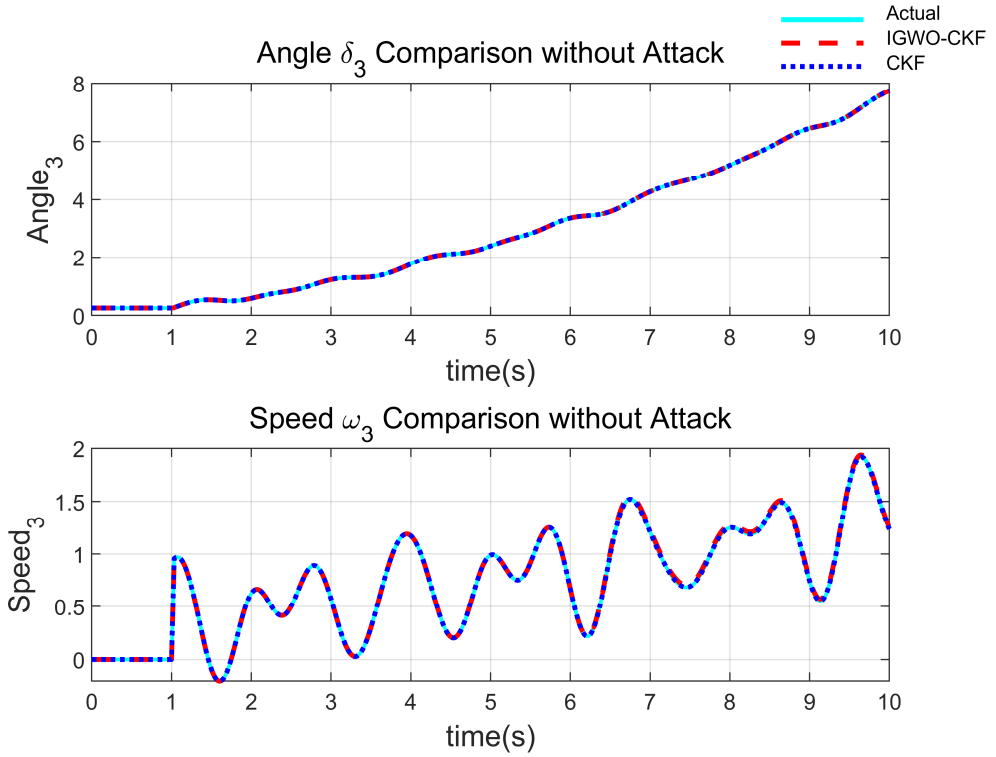

Fig. 5. Estimation of rotor angles and speeds of generator 3 for the New England without FDIA.

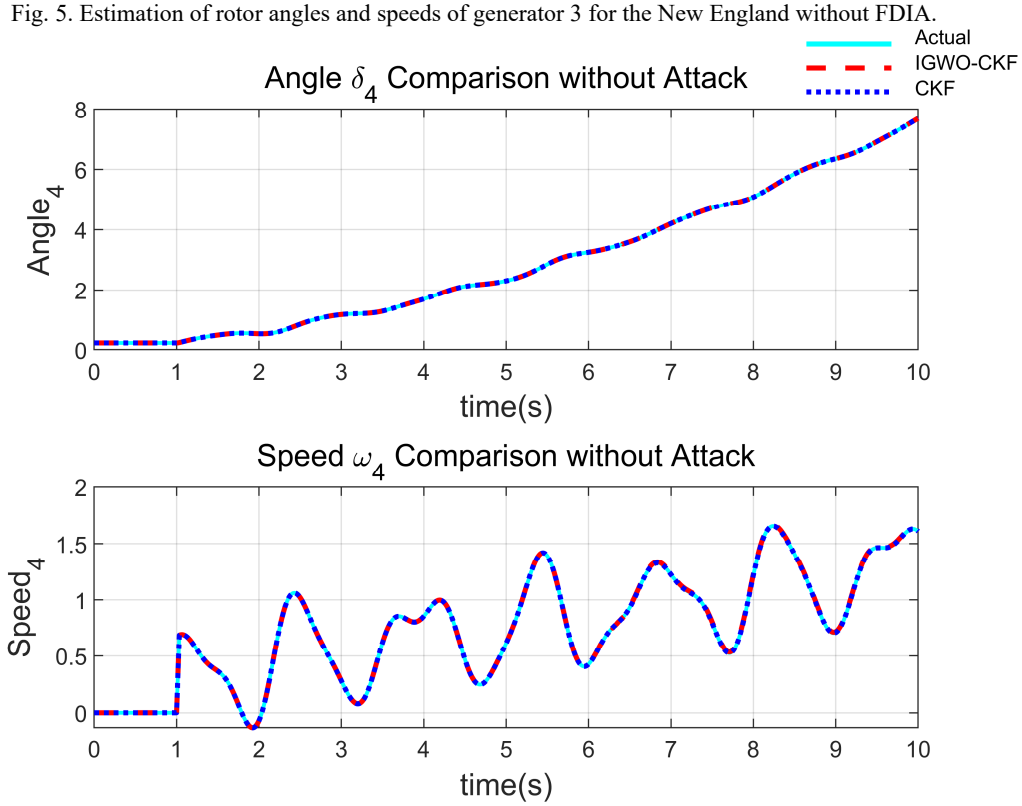

Fig. 6. Estimation of rotor angles and speeds of generator 4 for the New England without FDIA.

D. FDIA Detection and Analysis

When the rotor angles and speeds of the generators are subjected to FDIA, the traditional CKF and the improved IGWO-CKF were used for state estimation, and the simulation results are shown in the figures below.

As shown in Figs. 6 to 9, during the time interval of 6.2 to 6.3 seconds, when the system is subjected to a pulse attack (equation (11)) with an attack magnitude of 0.2, the CKF fails to detect the pulse attack and does not respond. In contrast, the proposed IGWO-CKF estimates values that are very close to the actual ones, reacting swiftly and meeting design requirements. At the 4-second mark, the system experiences a ramp attack (equation (12)) with a magnitude of 0.2, lasting for 4 seconds.

As shown in Figs. 10 to 13, the traditional CKF also fails to detect the ramp attack and does not respond, with results even tending to diverge. On the other hand, the estimates from the proposed IGWO-CKF remain close to the actual values, further validating the algorithm of effectiveness.

Figs. 14 to 17 illustrate that when a random attack (equation (13)) with a magnitude of 0.1 is applied between 5 and 8 seconds, the traditional CKF again fails to detect the attack, shows no response, and its results diverge. In contrast, the IGWO-CKF estimates remain consistent with the actual values, confirming the algorithm's effectiveness in detecting FDIA.

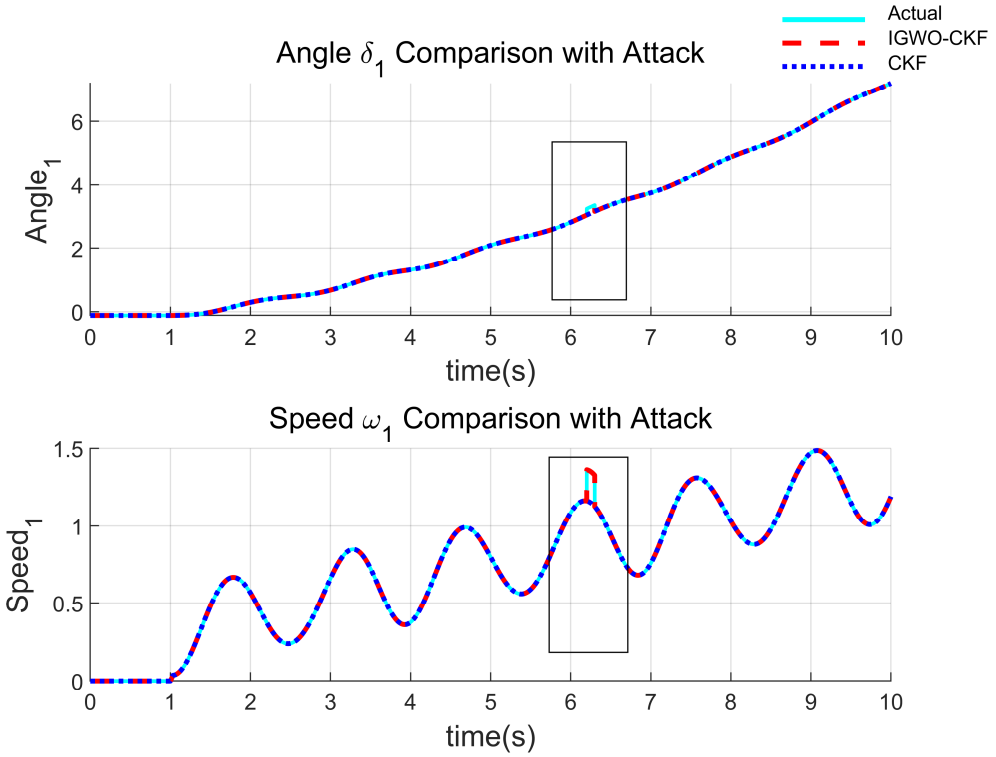

Fig. 7. Actual and estimated state values for Generators 1 under pulse attacks.

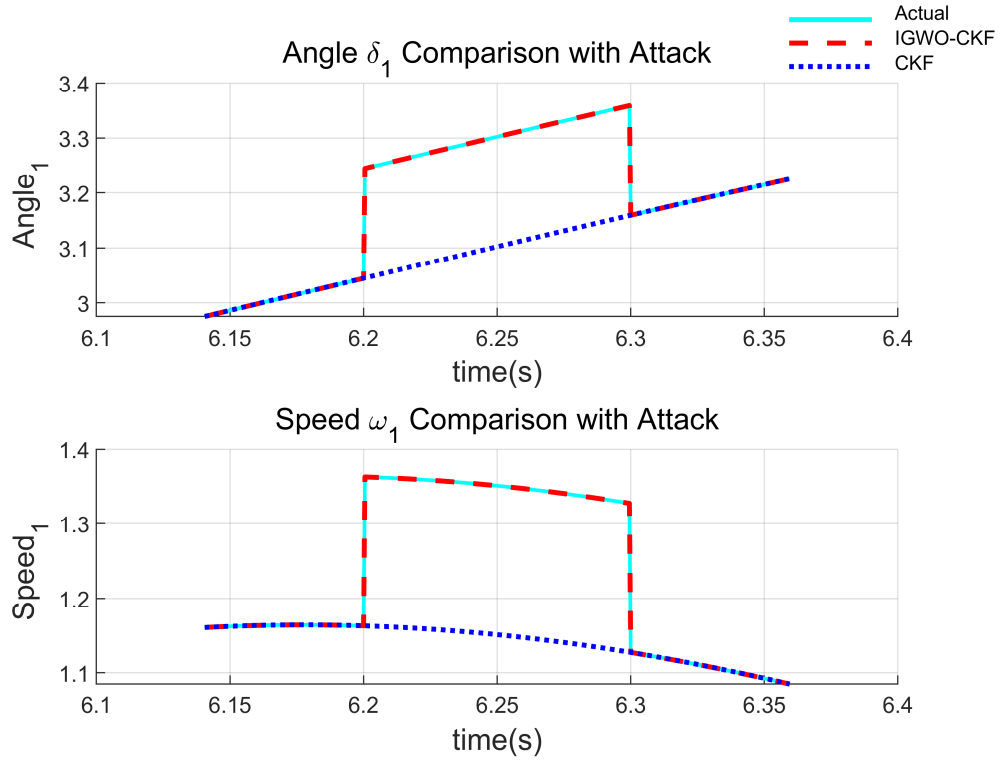

Fig. 8. Magnified view.

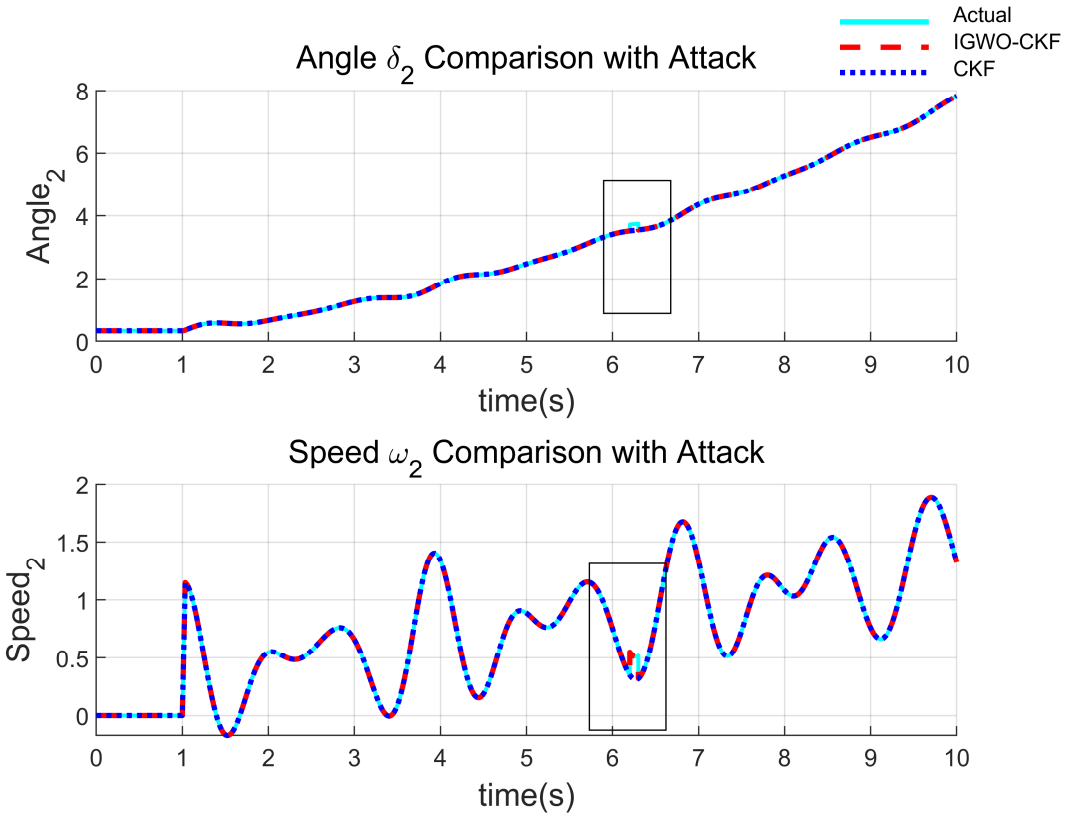

Fig. 9. Actual and estimated state values for Generators 2 under pulse attacks.

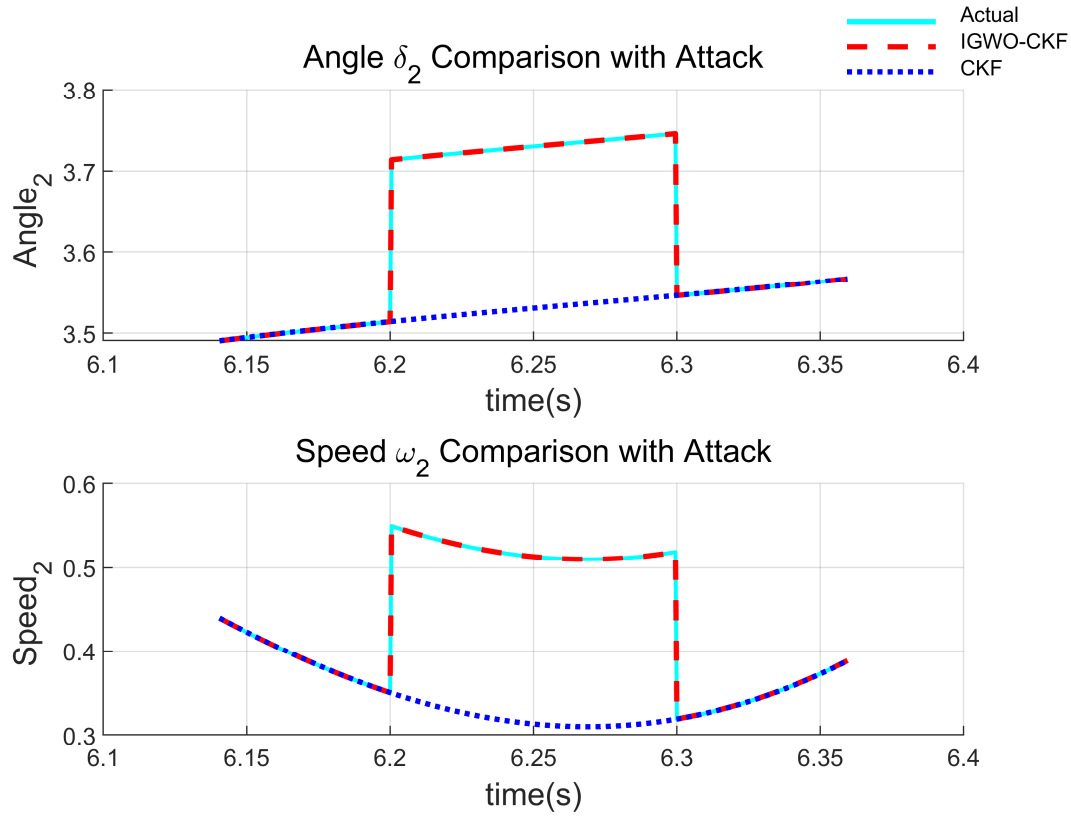

Fig. 10. Magnified view.

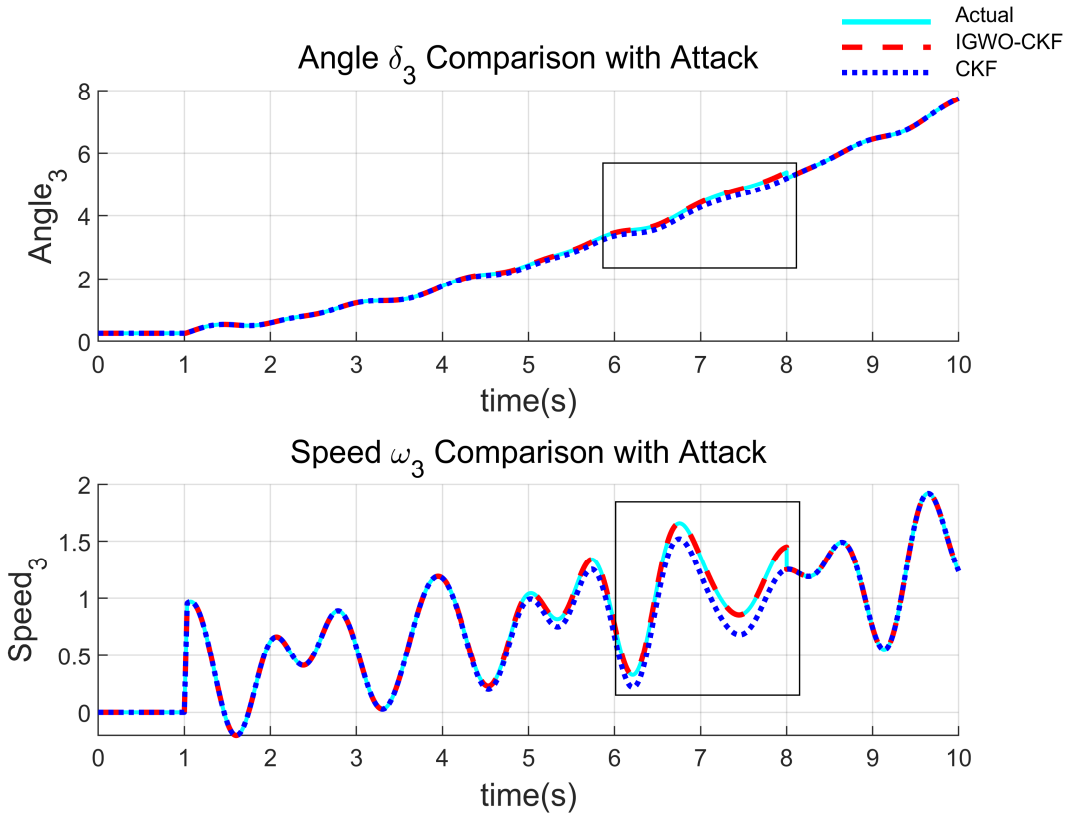

Fig. 11. Actual and estimated state values for Generators 3 under ramp attacks.

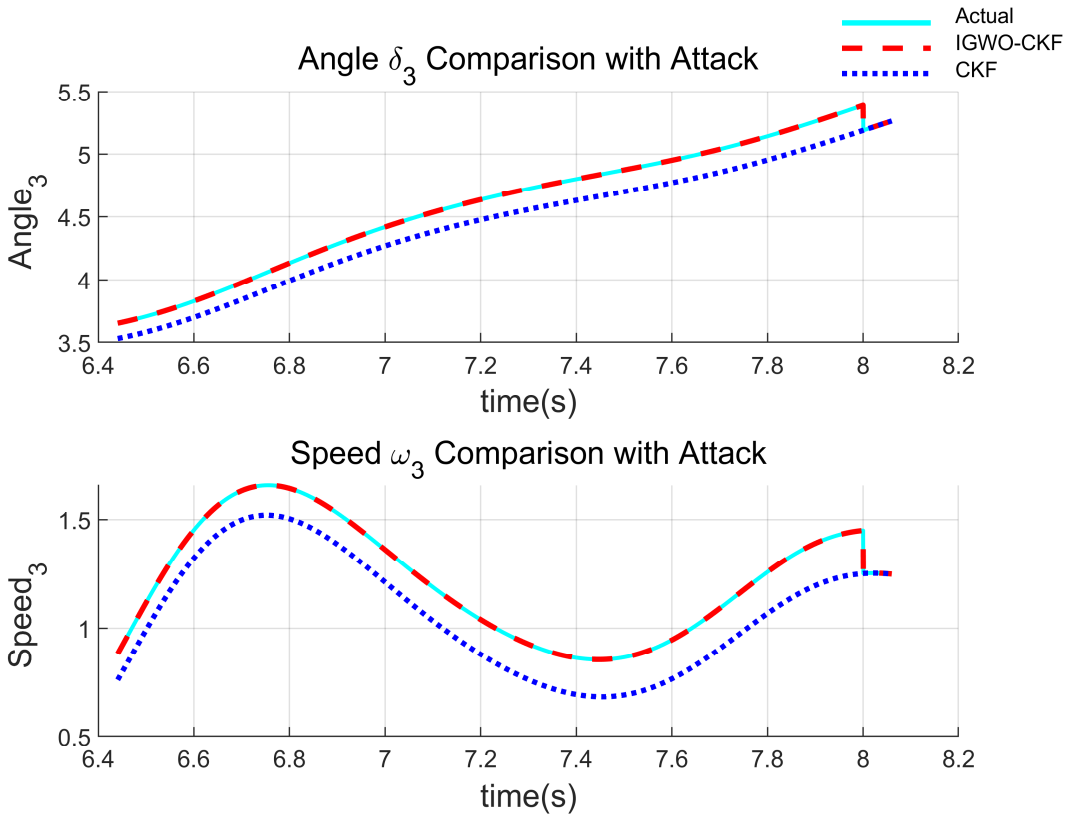

Fig. 12. Magnified view.

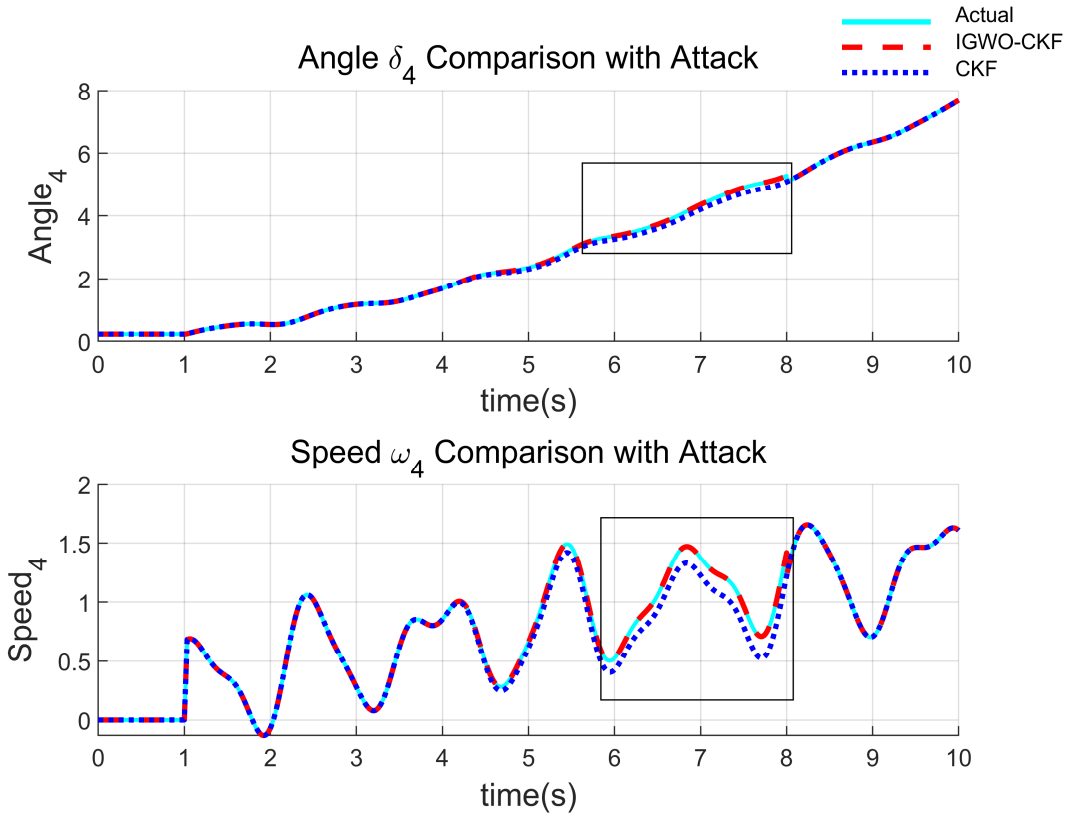

Fig.13. Actual and estimated state values for Generators 4 under ramp attacks.

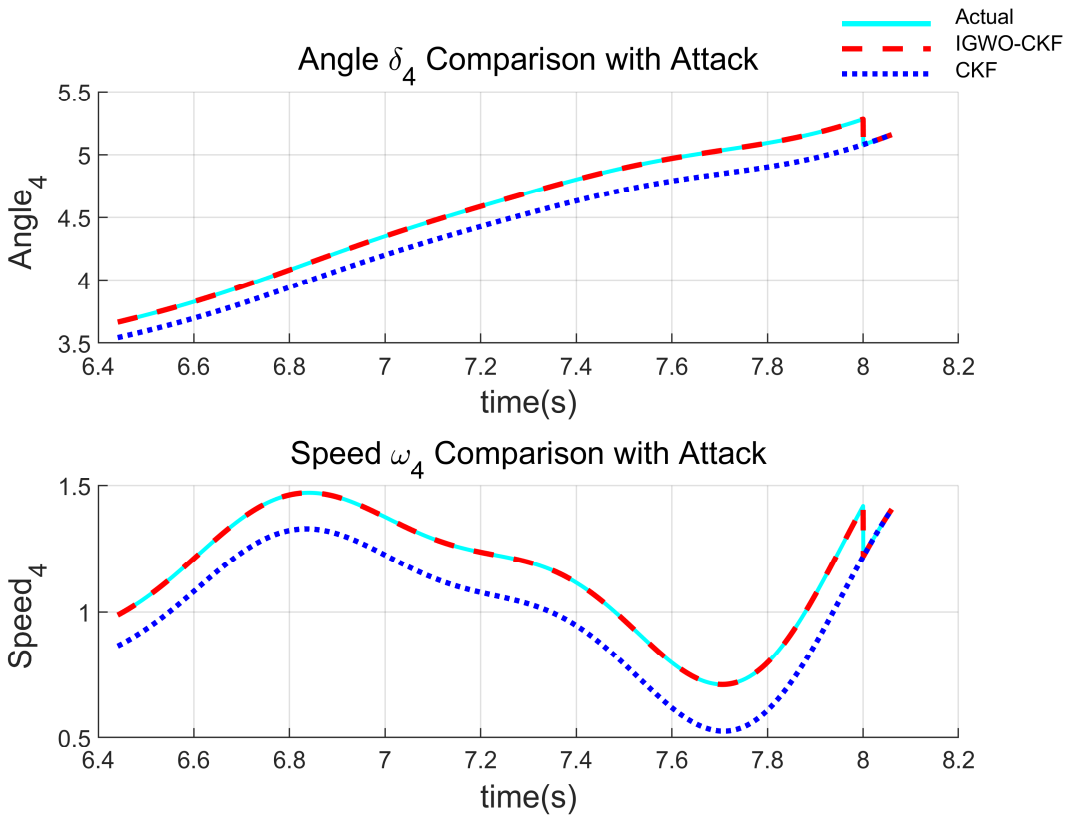

Fig. 14. Magnified view.

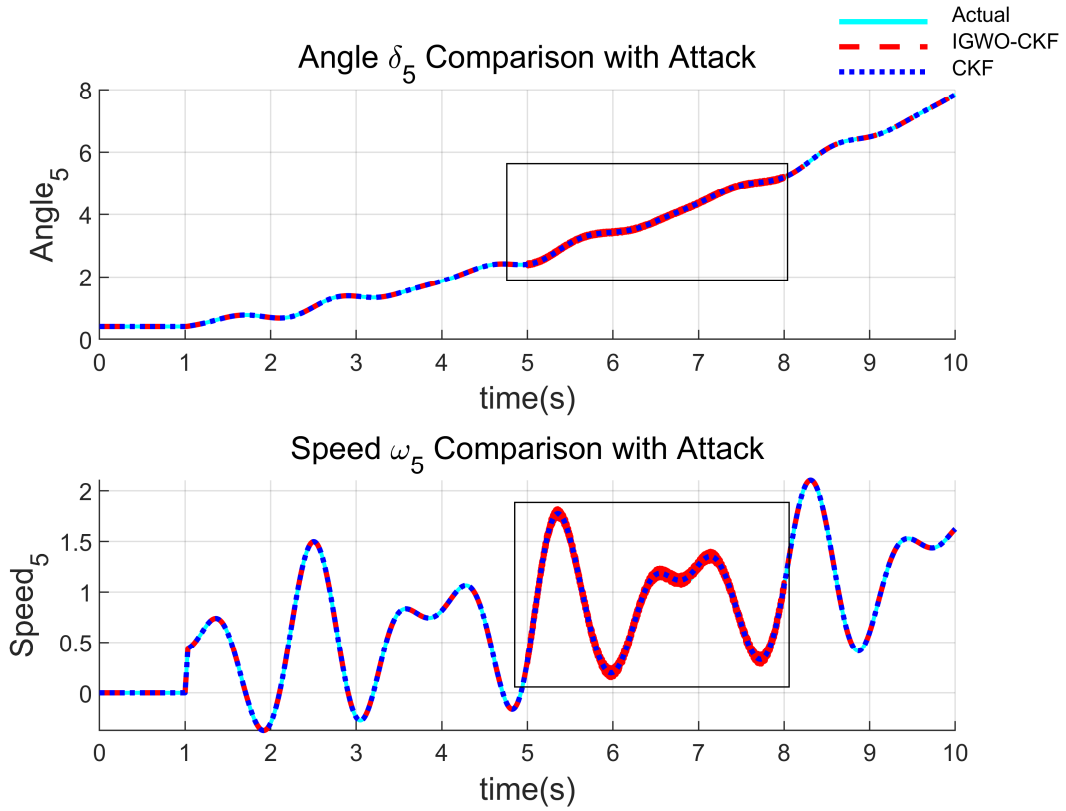

Fig. 15. Actual and estimated state values for Generator 5 under FDIA.

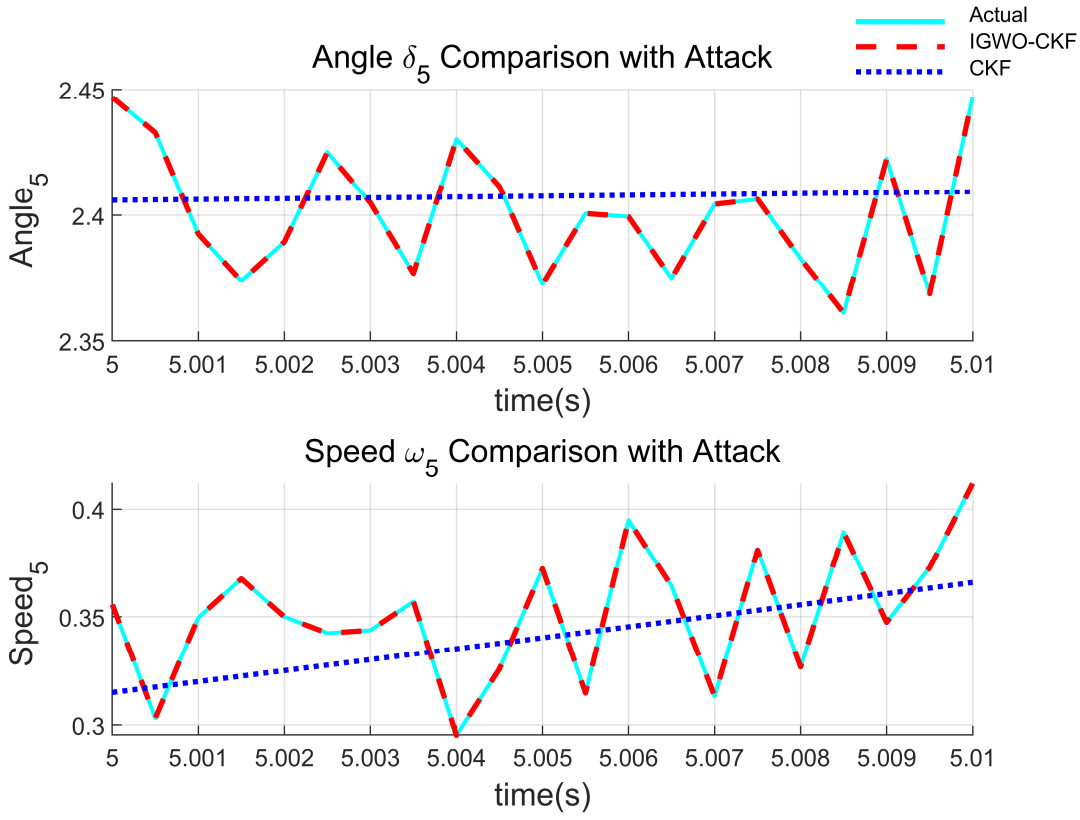

Fig. 16. Magnified view.

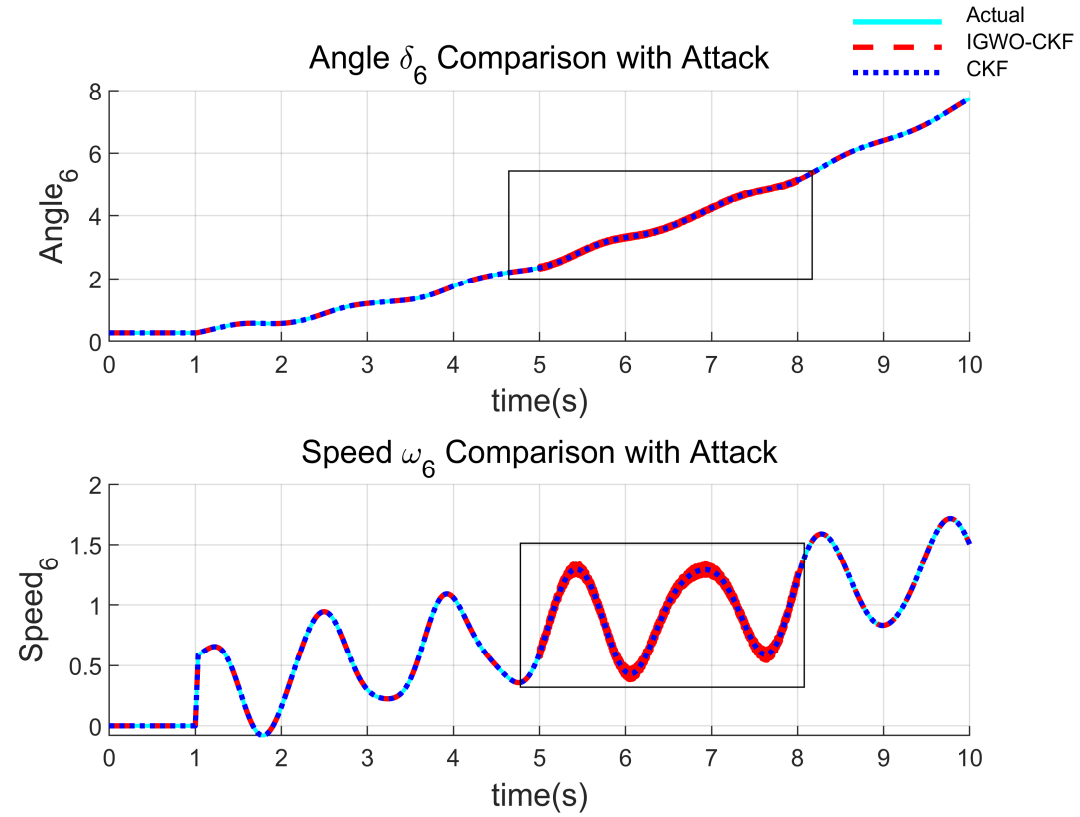

Fig. 17. Actual and estimated state values for Generator 6 under FDIA.

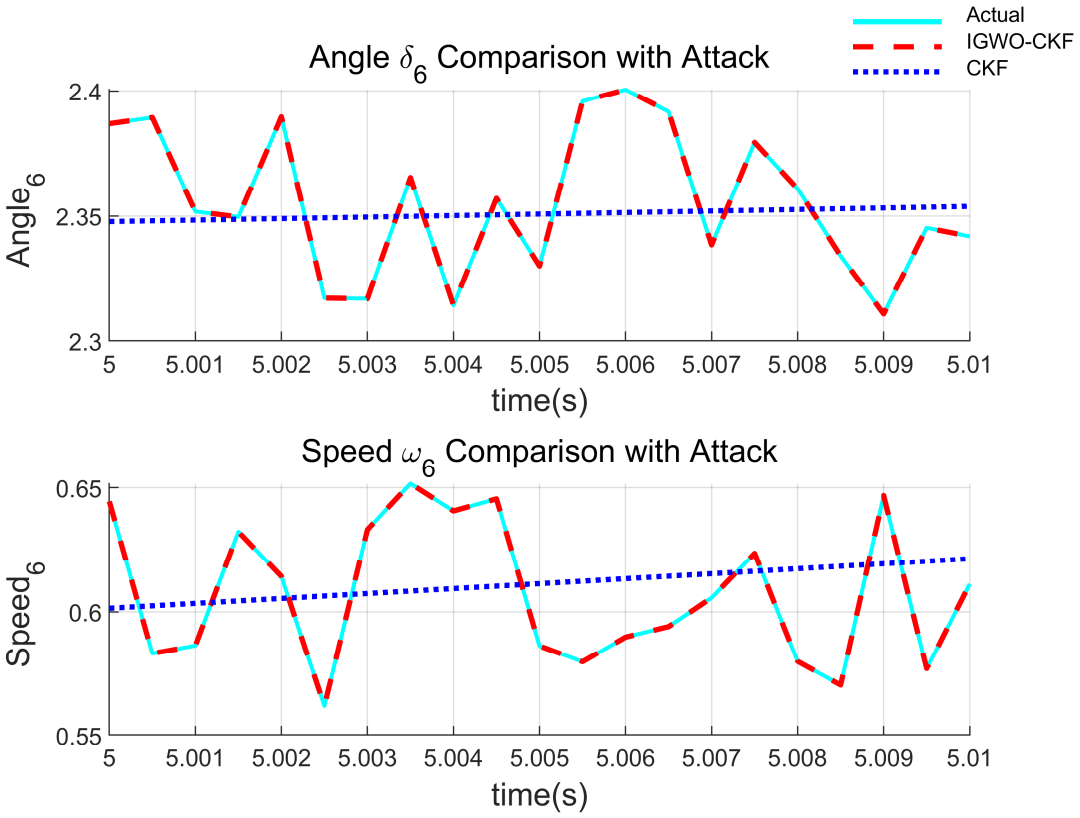

Fig. 18. Magnified view.

VI. Conclusions

This paper has proposed an IGWO-CKF algorithm to effectively address false data injection attacks (FDIA) in microgrids. By introducing Grey Wolf Optimization into Cubature Kalman Filter, the limitations of the traditional CKF in handling highly nonlinear dynamic changes are revealed. Simulation results show that, compared with CKF, the IGWO-CKF can more accurately identify and respond to attacks, thereby it enhances the security and reliability of microgrid systems.The findings provide a theoretical foundation for microgrid security protection and lay the groundwork for further research and practical applications.

References

[1] S. Anand, T. Anan, M. Kumar and A. Suma, "Enhancing smart grid security with SHA-SARIMAX: identifying and restoring corrupted files from FDIA," *IAENG International Journal of Computer Science*, vol. 51, no. 8, pp. 1112-1121, 2024.

[2] H. Moudoud, L. Khoukhi, S. Cherkaoui, "Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT," *IEEE Network*, vol. 35, no. 2, pp. 194-201, 2020.

[3] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, 2022.

[4] M. Bueno and G. Eduardo, "Real-time decentralized control of a hardware-in-the-loop microgrid,"*IAENG International Journal of Computer Science*, vol. 48, no. 3, pp. 653-662, 2021.

[5] T. Yi, T. Chen, Y. Zhu, W. Ge, and Z. Han, "Review on the application of deep learning in network attack detection," *Journal of Network and Computer Applications*, vol. 212, pp. 103580, 2023.

[6] Q. Chen, H. Wu, M. Li and K. Hou, "Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks," *Protection and Control of Modern Power Systems*, vol. 8, no. 2, pp. 1-12, 2023.

[7] B. Zhou, X. Li, T. Zang, Y. Cai, J. Wu, and S. Wang, "The detection of false data injection attack for cyber–physical power systems considering a multi-attack mode," *Applied Sciences*, vol. 13, no. 19, pp. 10596, 2023.

[8] S. Musleh, G. Chen, Z. Dong, C. Wang and S. Chen, "Statistical techniques-based characterization of FDIA in smart grids considering grid contingencies," *2020 International Conference on Smart Grids and Energy Systems (SGES)*, pp. 83-88, 2020.

[9] D. Mukherjee, S. Chakraborty, and S. Ghosh, "Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids," *Electrical Engineering*, vol. 104, no. 1, pp. 259-282, 2022.

[10] A. Kumar, N. Saxena, S. Jung, and B. Choi, "Improving detection of false data injection attacks using machine learning with feature selection and oversampling," *Energies*, vol. 15, no. 1, pp.212, 2021.

[11] T. Yi, T. Chen, Y. Zhu, W. Ge, and Z. Han, "Review on the application of deep learning in network attack detection," *Journal of Network and Computer Applications*, vol. 212, pp. 103580, 2023.

[12] K. Hasan, A. Abdulkadir, S. Islam, R. Gadekallu and N. Safie," A review on machine learning techniques for secured cyber-physical systems in smart grid networks," *Energy Reports*, vol. 11, pp. 1268-1290, 2024.

[13] Q. Pang, S. Han, and Tai. Zhou, "Detection of false data injection attacks in cyber-physical power systems based on ASRUKF and IMC algorithms," *Intelligent Power*, vol. 52, no. 7, pp. 111-118, 2024.

[14] J. Zhang, J. Zhang and Po. Wu, "False data detection in DC microgrids based on integrated cubature kalman filter," *Intelligent Power*, vol. 52, no.3, pp. 87-93, 2024.

[15] P. Wu, J. Zhang, S. Luo, Y. Song, J. Zhang, and Y. Wang, "A fusion adaptive cubature kalman filter approach for false data injection attack detection of DC microgrids," *Electronics*, vol. 13, no. 9, pp. 1612, 2024.

[16] Y. Liu, L. Cheng, "Relentless false data injection attacks against kalman-filter-based detection in smart grid," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 3, pp. 1238-1250, 2022.

[17] P. Hu, W. Gao, Y. Li, X. Guo, F. Hua, and L. Qiao, "Anomaly detection and state correction in smart grid using EKF and data compensation techniques," *IEEE Sensors Journal*, vol. 24, no. 8, pp. 12995-13009, 2024.

[18] S. Samer, E. Song, and D. Niu, "Robust cubature kalman filter for moving-target tracking with missing measurement," *Sensors,* vol. 24, no. 2, pp. 392, 2024.

[19] T. Lu, W. Zhou, S. Tong, "Improved maximum correntropy cubature Kalman and information filters with application to target tracking under non-gaussian noise," *International Journal of Adaptive Control and Signal Processing*, vol. 38, no. 4, pp. 1199-1221, 2024.

[20] Z. Li, X. Yang, L. Li, and H. Chen" Iterated orthogonal simplex cubature kalman filter and its application in target tracking," *Applied Sciences,* vol. 14, no. 1, pp. 392, 2024.

[21] N. Vafamand, R. Razavi-Far, M. Arefi, and M. Saif, "Fuzzy EKF-based intrusion detection and accurate state estimation of interconnected DC MGs with CPLs," *IEEE Transactions on Power Systems*, vol. 38, no. 6, pp. 5245-5256, 2023.

[22] A. Habib, M. Hasan, S. Islam, and L. Alkwai, "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction," *Computers and Electrical Engineering*, vol. 107, pp. 108638, 2023.