引用格式:常梦言,刘永慧.虚假数据注入攻击下基于容积卡尔曼滤波的电力系统状态估计[J].电力科学与技术学报,2024,39(3):10-18.
Citation:CHANG Mengyan,LIU Yonghui.State estimation of power system based on cubature Kalman filter under false data injection attacks[J].Journal of Electric Power Science and Technology,2024,39(3):10-18.

虚假数据注入攻击下基于容积卡尔曼滤波的电力系统状态估计

常梦言[1],刘永慧[2]
(1.上海电机学院电气学院,上海 201306; 2.上海第二工业大学智能制造与控制工程学院,上海 201209)

摘 要:针对虚假数据注入攻击下系统状态估计的问题,以电力信息物理系统为研究对象,根据发电机三阶模型和自动电压调节器模型,建立电力系统的数学模型。采用指数平滑法预测测量值,通过对比预测值与真实测量值,检测系统是否发生虚假数据注入攻击。若检测结果判定系统遭受虚假数据注入攻击,用预测值替代不良数据输入状态估计算法,实现虚假数据注入攻击下不良数据的恢复。将指数平滑法与容积卡尔曼滤波算法结合,提出一种改进的容积卡尔曼滤波算法对系统进行状态估计。以典型的五机电力系统为例进行仿真,仿真结果表明提出的方法能有效抵御虚假数据对系统状态估计造成的不良影响。

关 键 词:电力信息物理系统;状态估计;容积卡尔曼滤波;虚假数据注入攻击;指数平滑法
DOI:10.19781/j.issn.1673-9140.2024.03.002 **中图分类号**:TP273 **文章编号**:1673-9140(2024)03-0010-09

State estimation of power system based on cubature Kalman filter under false data injection attacks

CHANG Mengyan[1], LIU Yonghui[2]
(1.School of Electrical Engineering, Shanghai Dianji University, Shanghai 201306, China; 2.School of Intelligent Manufacturing and Control Engineering, Shanghai Polytechnic University, Shanghai 201209, China)

Abstract: Aiming at the problem of system state estimation under false data injection attacks, the mathematical model of power system was established according to the third-order model of generator and the model of automatic voltage regulator, taking the cyber-physical power system as the research object. The exponential smoothing method was used to predict the measured value, and by comparing the predicted value with the actual measured value, it detected whether there were false data injection attacks in the system. If the detection results determine that the system being subjected to false data injection attacks, the predicted value is used instead of the bad data input state estimation algorithm to restore corrupted data cansed by these attacks. Combining the exponential smoothing method with the cubature Kalman filter algorithm, an improved cubature Kalman filter algorithm was proposed to estimate the state of the system. Taking a typical five-machine power system as an example, the simulation results show that the proposed method can effectively prevent the adverse effects of false data on system state estimation.

Key words: cyber-physical power system; state estimation; cubature Kalman filter; false data injection attacks; exponential smoothing method

电力信息物理系统(cyber-physical power system, CPPS)通过传感器与通信网络实时地获取电力系统的运行状态[1]。为保障CPPS的安全稳定运行,需要能量管理系统协调各网络节点间的通信,而通

收稿日期:2022-10-17;**修回日期**:2023-06-07
基金项目:国家自然科学基金(61803253)
通信作者:刘永慧(1986—),女,博士,副教授,主要从事电力系统智能控制和切换系统研究;E-mail:liuyh@sspu.edu.cn

信系统和精确的状态量测保证了能量管理系统的可靠性运行。因此，为提高量测数据的准确性，需要对CPPS进行状态估计[2]。

智能电网的高效运行得益于信息通信技术的大量应用，但网络的开放性同时也使系统可能遭受到网络攻击，其中虚假数据注入攻击（false data injection attack，FDIA）是一种可以干扰电力系统状态估计过程的网络攻击[3]。FDIA通过向传感器的测量结果中注入错误向量来影响状态估计的结果，导致电力系统做出错误控制和错误调度，更严重的可能造成大面积停电事故。目前，针对FDIA的检测方法主要分为3类：图论和距离检测法、时间序列预测法、机器学习检测法[4]。对于图论和距离检测法，文献[5]针对FDIA下的五机电力系统，采用最优滤波器和图论，设计了一种分布式动态状态估计方法。文献[6]构造动态降阶观测器，并通过图论将系统分解为多个互联的子系统，从而提出一种基于自适应检测阈值的分布式攻击检测方法。时间序列预测法利用历史数据对电网当前状态进行预测并通过与实际量测值进行比较，检测受攻击的区域[7]。文献[8]提出了一种考虑时间相关性的基于短期状态预测的方法，并基于统计量的测量一致性检验方法，检验预测测量值与实际测量值的一致性。为检测并更新FDIA下的数据，文献[9]提出了将极端梯度提升与无迹卡尔曼滤波结合的虚假数据注入攻击检测方法。对于机器学习检测法，为了降低FDIA绕过不良数据检测机制的风险，文献[10]提出了一种基于数据驱动学习的算法来检测配电系统中不可观测的FDIA。文献[11]提出了一种基于改进卷积神经网络的检测方法，根据数据的空间及时间特性提取特征值，以实时高效地检测FDIA。目前，FDIA下电力系统状态估计的研究主要集中在检测FDIA是否存在、辨识FDIA的位置[12]，而对于FDIA下异常数据恢复的研究却相对较少。电力系统在受到攻击时不但要检测攻击，更要保证在不停机的情况下持续安全生产电能。为保证持续监测电力系统状态估计，将异常数据及时恢复至正常运行状态很有必要[13-15]。

电力系统动态状态估计主要采用卡尔曼滤波方法。文献[16]提出了两阶容错扩展卡尔曼滤波方法，与传统的扩展卡尔曼滤波相比，精度更高。为了克服扩展卡尔曼滤波线性化过程中用到的雅可比矩阵在维度较高时会产生正交项的问题[17]，文献[18]提出了基于无迹卡尔曼滤波的电力系统抗差动态估计，缓解了电力系统受量测信号不良数据的影响。对于无迹卡尔曼滤波具有参数选取难、灵活性不佳等特点[19-21]，文献[22]基于容积卡尔曼滤波（cubature Kalman filter，CKF）提出了一种考虑输入量存在不良数据的发电机的动态状态估计方法，提高了发电机动态状态估计算法的鲁棒性。以上文献考虑电力系统发生物理故障时的状态估计，但现代智能电网除了发生物理故障，还会出现由网络攻击造成的不良数据，因此需研究网络攻击下CPPS的状态估计。

基于以上分析，本文根据发电机三阶模型和自动电压调节器模型建立电力系统数学模型，在检测FDIA的基础上还考虑FDIA下异常数据的恢复。先采用指数平滑法进行量测量预测，检测FDIA，再用指数平滑法得到的预测值更新FDIA下的不良数据，恢复不良数据。最后结合指数平滑法与CKF方法，提出一种改进的容积卡尔曼滤波（improved cubature Kalman filter，ICKF）方法，实现了FDIA下电力系统的状态估计，并通过对比传统的CKF方法，验证所设计方法的有效性。

1　电力系统模型

本文以包含5台同步发电机的电力系统[5]为研究对象，系统的网络拓扑图如图1所示。根据发电机三阶模型和自动电压调节器模型，建立系统的数学模型。

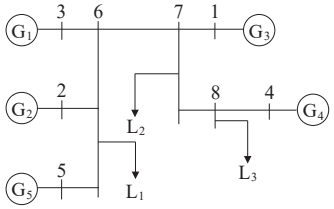


图1　包含5台同步发电机的电力系统

Figure 1　The power system diagram containing five synchronous generators

系统中第i（i=1，2，3，4，5）台同步发电机可表示为

$$\begin{cases}\dfrac{\mathrm{d}\Delta\delta_i}{\mathrm{d}t}=\Delta\omega_i\\ \dfrac{\mathrm{d}\Delta\omega_i}{\mathrm{d}t}=-\dfrac{D_i}{H_i}\Delta\omega_i-\dfrac{\Delta P_{ei}}{H_i}\\ \dfrac{\mathrm{d}\Delta E'_{qi}}{\mathrm{d}t}=-\dfrac{\Delta E'_{qi}}{T'_{doi}}+\dfrac{\Delta E_{fi}}{T'_{doi}}+\dfrac{X_{di}}{T'_{doi}}\Delta I_{di}-\dfrac{X'_{di}}{T'_{doi}}\Delta I_{di}\end{cases}\tag{1}$$

式中，$\Delta\delta_i$为转子运行角和同步转角之差；$\Delta\omega_i$为转子转速与同步转速之差；D_i为阻尼常数；H_i为惯性

常数；T'_{doi}为直轴开路暂态时间常数；ΔE_{fi}为励磁电压偏差；$\Delta E'_{qi}$为交轴暂态电压偏差；E_{fi}为励磁电压；X_{di}为直轴同步电抗；X'_{di}为直轴暂态电抗；I_{di}为直轴电流；ΔI_{di}为直轴电流增量。

自动电压调节器(automatic voltage regulator, AVR)通过控制励磁电流以控制发电机端电压。本文采用如图2所示的二阶传递函数[23]，其动力学方程为

$$\begin{cases}\Delta E_{fi}=b_{0i}z_{1i}+b_{1i}z_{2i}\\ \dfrac{\mathrm{d}z_{1i}}{\mathrm{d}t}=z_{2i}\\ \dfrac{\mathrm{d}z_{2i}}{\mathrm{d}t}=-c_{1i}z_{2i}-c_{0i}z_{1i}+\Delta v_i\end{cases}\tag{2}$$

式中，z_{1i}、z_{2i}为AVR系统的状态变量；Δv_i为系统的控制输入；b_{0i}、b_{1i}为电压控制的传递函数系数；c_{0i}、c_{1i}为励磁系统的传递函数系数。

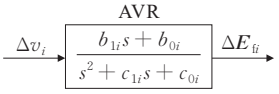


图2 自动电压调节器模型

Figure 2 Automatic voltage regulator model

假设系统有N台发电机，则直轴电流I_{di}和电功率P_{ei}满足[24]：

$$I_{di}=\sum_{j=1}^{N}\Delta E'_{qi}[B_{ij}\cos(\delta_i-\delta_j)-G_{ij}\sin(\delta_i-\delta_j)]\tag{3}$$

$$P_{ei}=E'_{qi}\sum_{j=1}^{N}[B_{ij}\sin(\delta_i-\delta_j)+G_{ij}\cos(\delta_i-\delta_j)]E'_{qj}\tag{4}$$

式(3)～(4)中，N为系统中发电机总数；B_{ij}、G_{ij}为系统网络导纳的虚部和实部，$i,j\in\{1,2,\cdots,N\}$；系统网络导纳矩阵$\boldsymbol{Y}$满足

$$\boldsymbol{Y}=\boldsymbol{Y}_{rr}-\boldsymbol{Y}_{re}\boldsymbol{Y}_{ee}^{-1}\boldsymbol{Y}'_{re}\tag{5}$$

式中，$\boldsymbol{Y}_{rr}$、$\boldsymbol{Y}_{re}$、$\boldsymbol{Y}_{ee}$为$\boldsymbol{Y}$的子矩阵；下标e表示消除节点，r表示保留的节点。

$$\begin{aligned}\boldsymbol{Y}_{rr}=\mathrm{diag}[&Y_{17}+\mathrm{j}B_{17},Y_{26}+\mathrm{j}B_{26},\\&Y_{36}+\mathrm{j}B_{36},Y_{48}+\mathrm{j}B_{48},Y_{56}+\mathrm{j}B_{56}]\end{aligned}\tag{6}$$

$$\boldsymbol{Y}_{re}=\begin{bmatrix}0&-Y_{17}&0\\-Y_{26}&0&0\\-Y_{36}&0&0\\0&0&-Y_{48}\\-Y_{56}&0&0\end{bmatrix}$$

$$\boldsymbol{Y}_{ee}=\begin{bmatrix}Y_{66}&-Y_{67}&0\\-Y_{67}&Y_{77}&-Y_{78}\\0&-Y_{78}&Y_{88}\end{bmatrix}$$

式中，$Y_{17}=1/(R_{17}+\mathrm{j}X_{17})$；$R_{17}$为节点1和节点7之间的互电阻；$X_{17}$、$B_{17}$分别为节点1和节点7之间的电抗和电纳。

将式(3)、(4)进行线性化，直轴电流增量ΔI_{di}和电功率增量ΔP_{ei}满足[5]：

$$\Delta P_{ei}=\begin{bmatrix}\dfrac{\partial P_{ei}}{\partial\delta_i}&\dfrac{\partial P_{ei}}{\partial E'_{qi}}\end{bmatrix}\begin{bmatrix}\Delta\delta_i&\Delta E'_{qi}\end{bmatrix}'\tag{7}$$

$$\Delta I_{di}=\begin{bmatrix}\dfrac{\partial I_{di}}{\partial\delta_i}&\dfrac{\partial I_{di}}{\partial E'_{qi}}\end{bmatrix}\begin{bmatrix}\Delta\delta_i&\Delta E'_{qi}\end{bmatrix}'\tag{8}$$

由式(1)、(2)、(7)、(8)可知，系统的状态方程为

$$\frac{\mathrm{d}\boldsymbol{x}_i}{\mathrm{d}t}=\boldsymbol{A}_i\boldsymbol{x}_i+\boldsymbol{B}_i\boldsymbol{u}_i+\sum_{j\in N_i}\boldsymbol{A}_{ij}\boldsymbol{x}_j\tag{9}$$

式中，状态$\boldsymbol{x}_i=\begin{bmatrix}\Delta\delta_i&\Delta\omega_i&\Delta E'_{qi}&z_{2i}&z_{1i}\end{bmatrix}^{\mathrm{T}}$；输入$\boldsymbol{u}_i=\Delta v_i$；$N_i$表示与第$i$台发电机物理连接的发电机集合；系统参数$\boldsymbol{A}_i$、$\boldsymbol{B}_i$、$\boldsymbol{A}_{ij}$为

$$\boldsymbol{A}_i=\begin{bmatrix}0&1&0&0&0\\-\dfrac{1}{H_i}\dfrac{\partial P_{ei}}{\partial\delta_i}&-\dfrac{D_i}{H_i}&-\dfrac{1}{H_i}\dfrac{\partial P_{ei}}{\partial E'_{qi}}&0&0\\\alpha_i\dfrac{\partial I_{di}}{\partial\delta_i}&0&-\dfrac{1}{T'_{doi}}+\alpha_i\dfrac{\partial I_{di}}{\partial E'_{qi}}&\dfrac{b_{1i}}{T'_{doi}}&\dfrac{b_{0i}}{T'_{doi}}\\0&0&0&-c_{1i}&-c_{0i}\\0&0&0&1&0\end{bmatrix}$$

$$\boldsymbol{A}_{ij}=\begin{bmatrix}0&0&0&0&0\\-\dfrac{1}{H_i}\dfrac{\partial P_{ei}}{\partial\delta_j}&0&-\dfrac{1}{H_i}\dfrac{\partial P_{ei}}{\partial E'_{qj}}&0&0\\\partial_i\dfrac{\partial I_{di}}{\partial\delta_j}&0&-\dfrac{1}{T'_{doi}}+\partial_i\dfrac{\partial I_{di}}{\partial E'_{qj}}&\dfrac{b_{1i}}{T'_{doj}}&\dfrac{b_{0i}}{T'_{doj}}\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}$$

$$\boldsymbol{B}_i=\begin{bmatrix}0&0&0&1&0\end{bmatrix}^{\mathrm{T}}$$

其中，$\partial_i=\dfrac{X_{di}-X'_{di}}{T'_{doi}}$。因此，系统式(9)可进一步表示为

$$\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}\boldsymbol{u}+\boldsymbol{w}\tag{10}$$

式中，$\boldsymbol{x}\in\boldsymbol{R}^{5N\times1}$为状态；$\boldsymbol{u}\in\boldsymbol{R}^{N\times1}$为系统输入；$\boldsymbol{w}\in\boldsymbol{R}^{5N\times1}$为服从$N(0,Q)$的高斯分布的过程噪声；$\boldsymbol{A}\in\boldsymbol{R}^{5N\times5N}$为系统矩阵；$\boldsymbol{B}\in\boldsymbol{R}^{5N\times N}$为输入矩阵，分别表示为

$$\boldsymbol{A}=\begin{bmatrix}\boldsymbol{A}_1&\boldsymbol{A}_{12}&\cdots&\boldsymbol{A}_{1N}\\\boldsymbol{A}_{21}&\boldsymbol{A}_2&\cdots&\boldsymbol{A}_{2N}\\\vdots&\vdots&\ddots&\vdots\\\boldsymbol{A}_{N1}&\boldsymbol{A}_{N2}&\cdots&\boldsymbol{A}_N\end{bmatrix}$$

$$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{B}_1&0&\cdots&0\\0&\boldsymbol{B}_2&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&\boldsymbol{B}_N\end{bmatrix}$$

为了便于分析和设计，采用欧拉法[25]将式(10)写成离散系统：

$$\boldsymbol{x}(t+1)=\boldsymbol{A}_{\mathrm{d}}\boldsymbol{x}(t)+\boldsymbol{B}_{\mathrm{d}}\boldsymbol{u}(t)+\boldsymbol{\omega}(t) \tag{11}$$

式中，$\boldsymbol{A}_{\mathrm{d}}=\boldsymbol{I}+\boldsymbol{A}\Delta t$；$\boldsymbol{B}_{\mathrm{d}}=\boldsymbol{B}\Delta t$，$\Delta t$为采样时间。

第i台发电机的量测方程为

$$\boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i \tag{12}$$

式中，量测值$\boldsymbol{z}_i=[\delta_i\ \ \omega_i\ \ E'_{qi}]^{\mathrm{T}}$，$\delta_i$为第$i$台发电机的转子角度；$\omega_i$为第$i$台发电机的转子转速；$E'_{qi}$为第$i$台发电机的交轴暂态电压；$\boldsymbol{s}_i=[\delta_0\ \ \omega_0\ \ E'_{q0}\ \ 0\ \ 0]^{\mathrm{T}}$；$\delta_0$为发电机的同步转子角度；$\omega_0$为发电机的同步转子转速；$E'_{q0}$为发电机的同步交轴暂态电压；$\boldsymbol{v}_i(t)$为量测噪声；输出矩阵$\boldsymbol{C}_i$表示为

$$\boldsymbol{C}_i=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\end{bmatrix}$$

系统的量测信号为

$$\boldsymbol{z}(t)=\begin{bmatrix}z_1(t)\\z_2(t)\\z_3(t)\\z_4(t)\\z_5(t)\end{bmatrix} \tag{13}$$

2　检测攻击

面向智能电网的FDIA结构如图3所示。

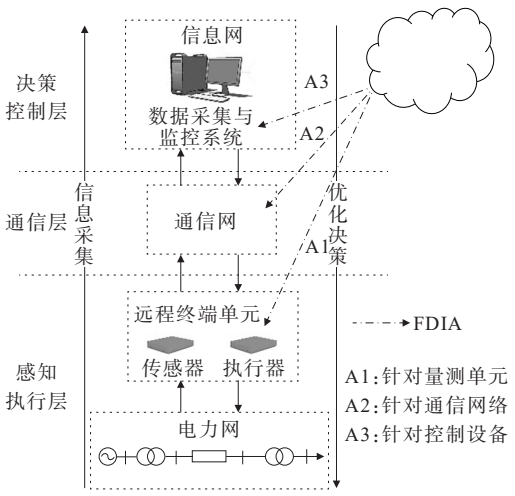


图3　智能电网中FDIA结构

Figure 3　FDIA structure diagram in smart grid

传感器采集的电力系统数据信息经通信网被传输到数据采集与监控中心，控制中心发出的控制命令同样经通信网传输后由执行器传达给电力系统。攻击者可分别针对控制设备、通信网络与量测单元进行攻击。本文考虑将FDIA加在量测单元中传感器测量后的数据上，将导致数据采集与监控系统收到错误的量测信息，直接影响状态估计的结果，造成系统状态估计出现重大偏差[4]。针对FDIA导致的不良数据，本章将采用指数平滑法进行预测，通过对比预测值与真实值检测FDIA。

2.1　FDIA模型

本文考虑对量测单元中传感器量测到的数据进行FDIA，即对5台发电机的量测值进行攻击，为了验证本文所提算法可以有效防御多种FDIA，本文将采用3种FDIA模型，分别为脉冲攻击、斜坡攻击、随机攻击。

1）脉冲攻击。

脉冲攻击在整个攻击持续时间期间将测量值修改为更高或更低值，其数学模型为

$$\begin{cases}\boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i, & t\notin\tau_{\mathrm{a}}\\ \boldsymbol{z}_i(t)=\boldsymbol{C}_i x_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i+\boldsymbol{a}_i, & t\in\tau_{\mathrm{a}}\end{cases} \tag{14}$$

式中，$\boldsymbol{a}_i=[a_{i1}\ \ a_{i2}\ \ a_{i3}]^{\mathrm{T}}$为脉冲攻击向量，$i\in\{1,2,3,4,5\}$，$a_{i1}$表示加在第$i$台发电机量测中转子角度$\delta_i$上的FDIA；$a_{i2}$表示加在第$i$台发电机量测中转子转速$\omega_i$上的FDIA，$a_{i3}$表示加在第$i$台发电机量测中交轴暂态电压$E'_{qi}$上的FDIA；$\tau_{\mathrm{a}}$为攻击者活跃的时间。

2）斜坡攻击。

斜坡攻击通过添加$\lambda_i\times t$来逐渐修改真实测量值，斜坡攻击模型为

$$\begin{cases}\boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i, & t\notin\tau_{\mathrm{a}}\\ \boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i+\lambda_i\times t, & t\in\tau_{\mathrm{a}}\end{cases} \tag{15}$$

式中，λ_i为斜坡系数。

3）随机攻击。

随机攻击将随机值rank(m,n)添加到量测量$\boldsymbol{z}_i(t)$中：

$$\begin{cases}\boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i, & t\notin\tau_{\mathrm{a}}\\ \boldsymbol{z}_i(t)=\boldsymbol{C}_i\boldsymbol{x}_i(t)+\boldsymbol{v}_i(t)+\boldsymbol{s}_i+\mathrm{rank}(m,n), & t\in\tau_{\mathrm{a}}\end{cases} \tag{16}$$

式中，m为随机函数的下界；n为随机函数的上界。

2.2　3次指数平滑法检测FDIA

由于发电机转子动态过程相对缓慢，故本文选取受发电机动态方程约束而不易突变的发电机参数作为状态估计的量测量，根据其不易突变的特性，采用指数平滑法进行量测预测[22]，将发电机真实量测数据与指数平滑预测值之间的误差与判断基准对比，当其误差大于所选定的判断基准时，判定量测数据中加入了FDIA。具体检测过程如下。

首先，将k时刻之前T个时刻的发电机量测值$\tilde{z}_{k-T},\tilde{z}_{k-T+1},\cdots,\tilde{z}_{k-1}$作为观测值输入指数平滑法。然后，给定平滑系数$\alpha\in[0,1]$，3次指数平滑法的计算公式[26]为

$$\begin{cases}S_t^{(1)}=\alpha\tilde{x}_t+(1-\alpha)S_{t-1}^{(1)}\\S_t^{(2)}=\alpha S_t^{(1)}+(1-\alpha)S_{t-1}^{(2)}\\S_t^{(3)}=\alpha S_t^{(2)}+(1-\alpha)S_{t-1}^{(3)}\end{cases}\tag{17}$$

利用$k-1$时刻的3次指数平滑值对k时刻的量测值进行预测：

$$\begin{cases}a_{k-1}=3S_{k-1}^{(1)}-3S_{k-1}^{(2)}+S_{k-1}^{(3)}\\b_{k-1}=\dfrac{\alpha}{2(1-\alpha)^2}[(6-5\alpha)S_{k-1}^{(1)}-(10-\\\qquad 8\alpha)S_{k-1}^{(2)}+(4-3\alpha)S_{k-1}^{(3)}]\\c_{k-1}=\dfrac{\alpha^2}{2(1-\alpha)^2}\left(S_{k-1}^{(1)}-2S_{k-1}^{(2)}+S_{k-1}^{(3)}\right)\\z_k'=a_{k-1}+b_{k-1}+c_{k-1}\end{cases}\tag{18}$$

式中，a_{k-1}、b_{k-1}、c_{k-1}为线性平滑参数；z_k'为k时刻指数平滑发电机量测量预测值。

接下来，通过比较k时刻发电机真实值z_k和预测值z_k'，得到误差值e_k：

$$e_k=|z_k-z_k'|\tag{19}$$

然后，根据误差值e_k判断输入量是否存在不良数据。选择历史时刻e_k的平均值e_{b}作为判别条件，当e_k大于判断基准时，系统存在不良数据，当e_k小于判断基准时，系统无不良数据。平均值e_{b}和判定准则N定义为

$$e_{\mathrm{b}}=\frac{1}{N_{\mathrm{b}}}\sum_{j=1}^{N_{\mathrm{b}}}e_{k-j},e_{k-j}\neq 0\tag{20}$$

$$N=\left|\left\{e_{k,i}\middle|e_{k,i}>k_ie_{\mathrm{b},i}\right\}\right|,k_i\geqslant 1\tag{21}$$

式(20)、(21)中，N_{b}为选取的不为零的历史数据e_k的个数；N为不良数据的个数，为提高灵敏性，当$N\geqslant 2$时，判定输入量存在不良数据[22]。

3 改进的容积卡尔曼滤波

CKF的基本思想是通过高斯加权积分的三阶球面径向容积定律，采用逼近积分项，实现不同方向上的概率性滤波[27]，本节将CKF与3次指数平滑法结合，提出ICKF方法，实现FDIA下电力系统的状态估计。基于ICKF的动态状态估计基本过程包括预测系统状态、FDIA的检测与修正、量测值更新3个步骤。

3.1 预测系统状态

首先，根据球面—径向规则对状态量估计值生成一组等权值容积点，即在文1所选状态变量的周围按估计误差方差阵的平方根矩阵形成一组均匀分布的点[25]。容积点x_{k-1}^i满足：

$$x_{k-1}^i=\hat{x}_{k-1}+\sqrt{P_{k-1}}\,\boldsymbol{\xi}_i,i=1,2,\cdots,2n\tag{22}$$

式中，$\hat{x}_{k-1}$、P_{k-1}分别为$k-1$时刻的状态估计值和估计误差协方差阵；x_{k-1}^i为生成的容积采样点。

容积采样点x_{k-1}^i和第i个采样点相应的权值w_i满足：

$$w_i=\frac{1}{2n}\tag{23}$$

$$\boldsymbol{\xi}=\sqrt{n}\left\{\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}\cdots\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}\begin{bmatrix}-1\\0\\\vdots\\0\end{bmatrix}\begin{bmatrix}0\\-1\\\vdots\\0\end{bmatrix}\cdots\begin{bmatrix}0\\0\\\vdots\\-1\end{bmatrix}\right\}\tag{24}$$

$$\boldsymbol{\xi}_i=\sqrt{n}\,[1]_i,i=1,2,\cdots,2n\tag{25}$$

式中，$[1]_i$为容积点集的第i列。

通过状态方程对容积点进行变换得到$\tilde{\boldsymbol{x}}_{k|k-1}^i$：

$$\tilde{\boldsymbol{x}}_{k|k-1}^i=\boldsymbol{A}_{\mathrm{d}}\boldsymbol{x}_{k-1}^i+\boldsymbol{B}_{\mathrm{d}}\boldsymbol{u}_{k-1}+\boldsymbol{\omega}_{k-1}\tag{26}$$

对$\tilde{\boldsymbol{x}}_{k|k-1}^i$进行加权，得到预测量$\boldsymbol{x}_{k|k-1}$：

$$\boldsymbol{x}_{k|k-1}=\frac{1}{2n}\sum_{i=1}^{2n}\tilde{\boldsymbol{x}}_{k|k-1}^i\tag{27}$$

状态预测值的协方差矩阵$\boldsymbol{P}_{k|k-1}$可表示为

$$\boldsymbol{P}_{k|k-1}=\frac{1}{2n}\sum_{i=1}^{2n}(\tilde{\boldsymbol{x}}_{k|k-1}^i-\boldsymbol{x}_{k|k-1})(\tilde{\boldsymbol{x}}_{k|k-1}^i-\boldsymbol{x}_{k|k-1})^{\mathrm{T}}+\boldsymbol{Q}\tag{28}$$

式中，$\boldsymbol{Q}$为过程噪声协方差阵。

3.2 FDIA检测与修正

将k时刻之前T个历史时刻的发电机量测值输入到指数平滑法中，利用式(17)、(18)计算k时刻指数平滑预测值z_k'。通过式(19)～(21)比较k时刻真实值z_k和预测值z_k'，得到不良数据的个数N。当$n\geqslant 2$时，判定存在不良数据，检测到不良数据后，将3次指数平滑预测值z_k'更新受攻击的真实量测值z_k，将更新后的量测值输入CKF中进行量测值更新。

3.3 更新量测值

更新量测值时，首先在状态预报值周围生成等权值的容积点$\boldsymbol{x}_{k|k-1}^i$：

$$\boldsymbol{x}_{k|k-1}^i=\sqrt{\boldsymbol{P}_{k|k-1}}\,\boldsymbol{\xi}_i+\boldsymbol{x}_{k|k-1}\tag{29}$$

然后，通过量测方程对容积点进行变换，得到量测预报值的容积点$\boldsymbol{z}_{k|k-1}^i$：

$$\boldsymbol{z}_{k|k-1}^i=\boldsymbol{C}_k\boldsymbol{x}_{k|k-1}^i+\boldsymbol{v}_k+\boldsymbol{s}_k\tag{30}$$

最后，加权得到量测预报值$\boldsymbol{z}_{k|k-1}$：

$$\boldsymbol{z}_{k|k-1}=\frac{1}{2n}\sum_{i=1}^{2n}\boldsymbol{z}_{k|k-1}^{i} \tag{31}$$

量测值预测值误差协方差阵 $\boldsymbol{P}_{k|k-1}^{zz}$ 为

$$\boldsymbol{P}_{k|k-1}^{zz}=\frac{1}{2n}\sum_{i=1}^{2n}(\boldsymbol{z}_{k|k-1}^{i}-\boldsymbol{z}_{k|k-1})(\boldsymbol{z}_{k|k-1}^{i}-\boldsymbol{z}_{k|k-1})^{\mathrm{T}}+\boldsymbol{R} \tag{32}$$

式中，$\boldsymbol{R}$ 为量测误差协方差阵。

互协方差矩阵 $\boldsymbol{P}_{k|k-1}^{xz}$ 为

$$\boldsymbol{P}_{k|k-1}^{xz}=\frac{1}{2n}\sum_{i=1}^{2n}(\boldsymbol{x}_{k|k-1}^{i}-\boldsymbol{x}_{k|k-1})(\boldsymbol{z}_{k|k-1}^{i}-\boldsymbol{z}_{k|k-1})^{\mathrm{T}} \tag{33}$$

由式(28)、(29)得到卡尔曼滤波增益 K_k 为

$$K_k=\boldsymbol{P}_{k|k-1}^{xz}{\boldsymbol{P}_{k|k-1}^{zz}}^{-1} \tag{34}$$

结合实际值 $\boldsymbol{z}_k$ 和预测值 $\boldsymbol{z}_{k|k-1}$，对状态预测值进行后验校正，得到当前状态估计值 $\tilde{\boldsymbol{x}}_k$ 为

$$\tilde{\boldsymbol{x}}_k=\boldsymbol{x}_{k|k-1}+K_k(\boldsymbol{z}_k-\boldsymbol{z}_{k|k-1}) \tag{35}$$

因此协方差矩阵更新为

$$\boldsymbol{P}_k=\boldsymbol{P}_{k|k-1}-K_k\boldsymbol{P}_{k|k-1}^{zz}K_k^{\mathrm{T}} \tag{36}$$

更新后的协方差矩阵和状态估计值将用于下一步的状态估计。FDIA 下基于 ICKF 的电力系统状态估计的算法流程如图 4 所示。

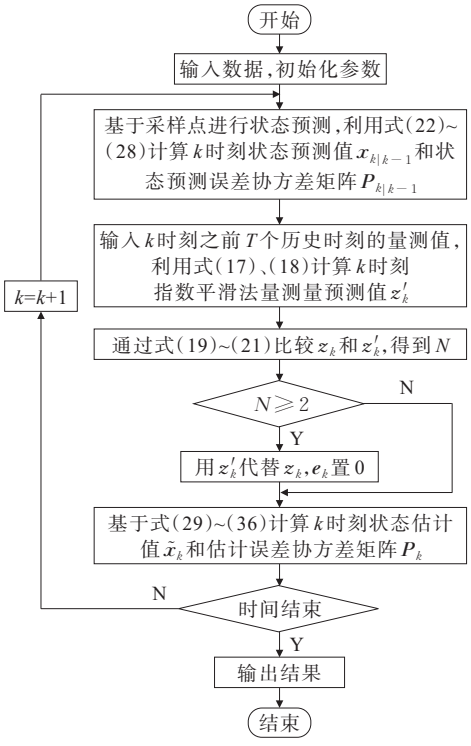


图 4　基于 ICKF 状态估计流程

Figure 4　Flow chart of state estimation based on ICKF

4　仿真结果及分析

以 FDIA 下的五机电力系统为例进行仿真验证，验证所提 ICKF 方法的有效性。

4.1　参数设置

CKF 过程噪声协方差满足高斯分布，设为 $10^{-7}I$，测量噪声协方差也满足高斯分布，每台发电机 3 个量测量对应的测量噪声协方差分别设为 $10^{-6}I$、$2\times10^{-6}I$、$3\times10^{-6}I$，电力系统的发电机参数如表 1 所示，电力系统的传输线路参数如表 2 所示。

表 1　发电机参数

Table 1　Parameters of generator

发电机序号	D_i	H_i	X'_{di}	X_{di}	T'_{doi}
1	3.14	4.60	0.033 9	0.102 6	5.67
2	3.77	4.75	0.033 9	0.102 6	5.67
3	3.45	4.53	0.339 0	1.026 0	5.67
4	4.08	4.04	0.033 9	0.102 6	5.67
5	3.50	5.00	0.339 0	1.026 0	5.67

发电机序号	b_{0i}	b_{1i}	c_{0i}	c_{1i}	V	θ
1	656	1 232	3.23	32.3	1.050	0
2	656	1 232	3.23	32.3	1.030	0.105 1
3	656	1 232	3.23	32.3	1.025	0.094 3
4	656	1 232	3.23	32.3	1.030	0.036 1
5	656	1 232	3.23	32.3	1.025	0.090 7

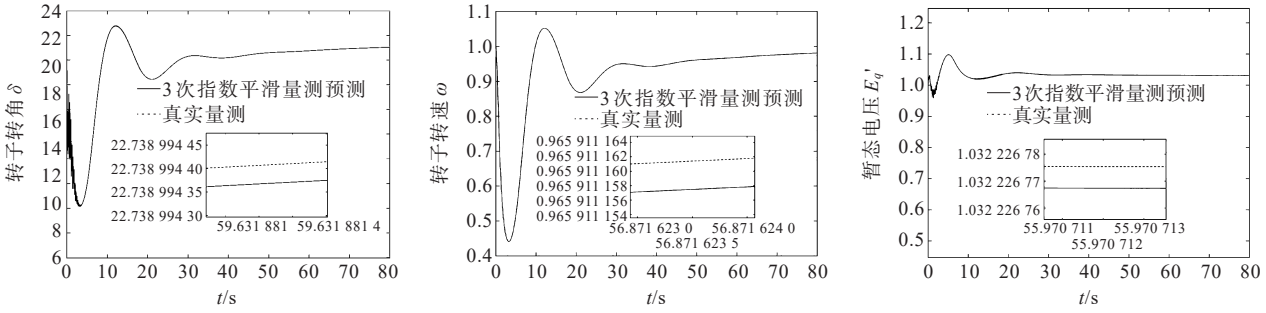
表 2　传输线路参数

Table 2　Parameters of transmission line

i	j	R_{ij}	X_{ij}	B_{ij}
1	7	0.004 35	0.010 67	0.015 36
2	6	0.002 13	0.004 68	0.004 04
3	6	0.020 04	0.062 44	0.064 08
4	8	0.005 24	0.011 84	0.017 56
5	6	0.007 11	0.023 31	0.027 32
6	7	0.040 32	0.1278 5	0.158 58
7	8	0.017 24	0.041 53	0.060 14

4.2　验证 3 次指数平滑法预测可行性

为了验证 3 次指数平滑法预测值可以代替攻击下的量测值进行状态估计，即验证 3 次指数平滑法预测发电机量测量的准确性，将量测量真实值与 3 次指数平滑预测值进行对比。系统的仿真结果如图 5 所示。由图 5 可以看出，发电机 1 量测真实值与指数平滑预测值之间的误差很小，经放大后才可以看出其细微的差别。验证了 3 次指数平滑法预测量测值的准确性，故可以采用 3 次指数平滑法检测是否存在不良数据并进行数据更新。



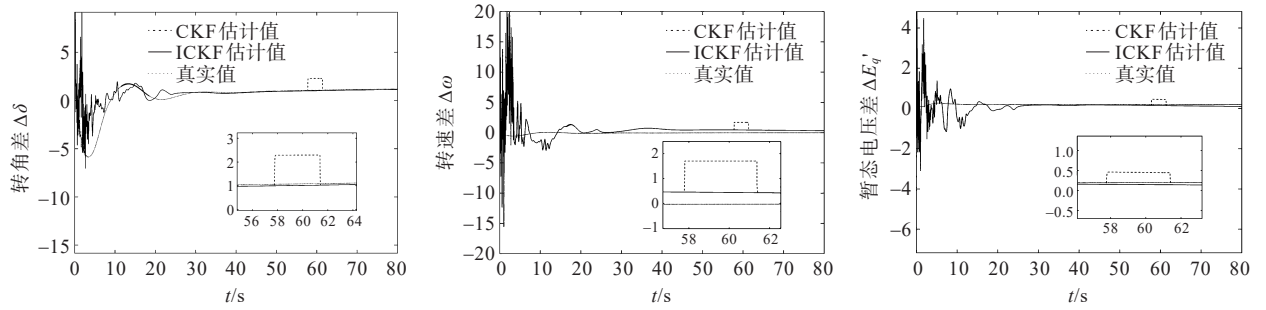
(a)发电机1的转角 (b)发电机1的转速 (c)发电机1的暂态电压

图5 对比发电机1的量测真实值与指数平滑预测值

Figure 5 Compare the true value of generator 1 with the predicted value

4.3 对比ICKF与CKF

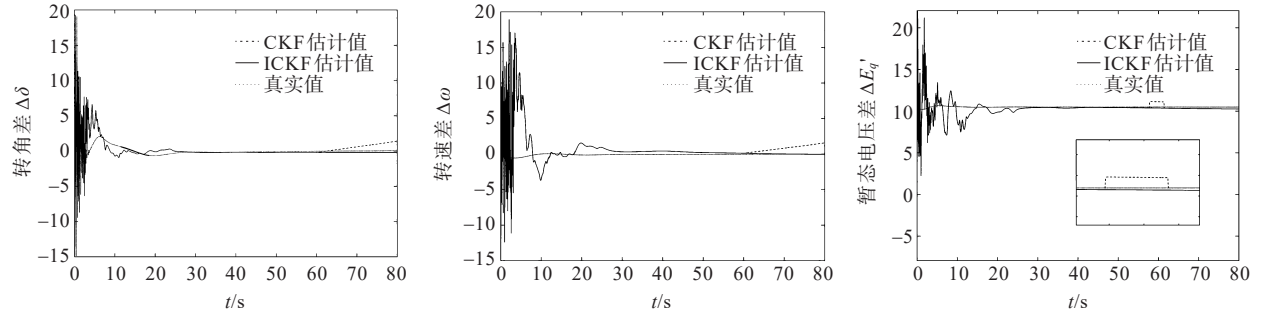
当发电机量测量受到FDIA时,采用传统的CKF和ICKF对系统进行状态估计,系统仿真结果如图6~8所示。



(a)发电机2的转角差 (b)发电机2的转速差 (c)发电机2的暂态电压差

图6 脉冲攻击下发电机2的状态量真实值与估计值

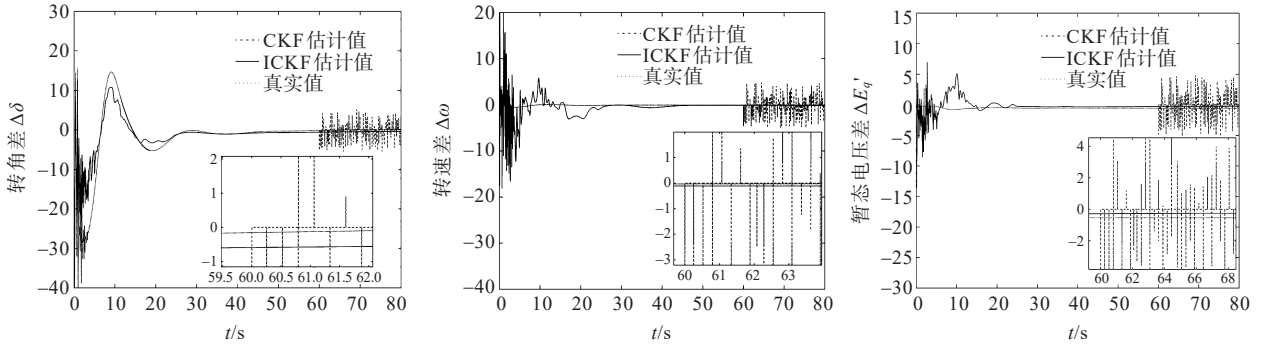
Figure 6 The true value and the estimated value of the state quantity of the pulse attack delivered generator 2



(a)发电机3的转角差 (b)发电机3的转速差 (c)发电机3的暂态电压差

图7 斜坡攻击下发电机3的状态量真实值与估计值

Figure 7 The true value and the estimated value of the state quantity of the ramp attack delivered generator 3



(a)发电机5的转角差 (b)发电机5的转速差 (c)发电机5的暂态电压差

图8 FDIA下发电机5的状态量真实值与估计值

Figure 8 The true value and the estimated value of the state quantity of the FDIA delivered generators 5

由图 6 可以看出，在 58 s 向发电机 2 注入式（14）的脉冲攻击后，传统的 CKF 无法抵御脉冲攻击的影响，系统的估计值与真实值产生较大偏差。而本文提出的 ICKF 的估计值与真实值接近，在抵御脉冲攻击的同时，对系统的状态进行准确地估计。

在 60 s 时向发电机 3 注入式（15）的斜坡攻击，由图 7 可以看出，传统的 CKF 的估计结果无法抵御斜坡攻击的影响，甚至会导致估计结果发散，而本文提出的 ICKF 估计值与真实值接近，验证了本文提出的 ICKF 可以抵御斜坡攻击。

在 60 s 向发电机 5 注入式（16）的随机攻击，由图 8 可知，未加入 FDIA 时，CKF 和 ICKF 均可实现状态估计，20 s 后预测值与真实值接近，但发生随机攻击后，CKF 预测值与真实值产生偏差，而 ICKF 在发生随机攻击后仍可以准确预测状态变量，验证了本文所设计方法的有效性。

5　结语

本文研究了 FDIA 下 CPPS 的状态估计。在检测 FDIA 的基础上，还考虑了 FDIA 下不良数据的恢复。首先提出了基于指数平滑法的量测量不良数据检测方法，用指数平滑法预测量测值，并更新 FDIA 下的不良数据，然后结合指数平滑法与 CKF 方法，提出一种 ICKF 方法，该方法克服了传统 CKF 无法检测与防御虚假数据注入攻击的缺陷，增强了电力系统抵御网络攻击的能力。未来可以进一步探讨如何改进已提出的 ICKF 法，以解决智能电网中同时存在多种类型网络攻击所面临的状态估计问题。

参考文献：

[1] 吴海涛，代尚林，乔中伟，等．基于 RBF-SVM 智能配变终端的网络安全态势评估[J]．电力科学与技术学报，2021，36(5)：35-40.
WU Haitao, DAI Shanglin, QIAO Zhongwei, et al. Research on network security situation awareness of intelligent distribution transformer terminal unit based on RBF-SVM[J]. Journal of Electric Power Science and Technology,2021,36(5):35-40.

[2] 赵化时，李胜，林子杰，等．电力系统低模型耦合智能状态估计[J]．电力科学与技术学报，2022，37(2)：116-128.
ZHAO Huashi, LI Sheng, LIN Zijie, et al. Smart power system state estimation with low model coupling[J]. Journal of Electric Power Science and Technology,2022, 37(2):116-128.

[3] 郭方洪，易新伟，徐博文，等．基于深度信念网络和迁移学习的隐匿 FDI 攻击入侵检测[J]．控制与决策，2022，37(4)：913-921.
GUO Fanghong, YI Xinwei, XU Bowen, et al. Stealthy FDI attack detection based on deep belief network and transfer learning[J]. Control and Decision, 2022, 37(4): 913-921.

[4] 王竞才，李琰，徐天奇．基于扩展卡尔曼滤波的智能电网虚假数据检测[J]．智慧电力，2022，50(3)：50-56.
WANG Jingcai, LI Yan, XU Tianqi. Detection of false data in smart grid based on extended Kalman filter[J]. Smart Power,2022,50(3):50-56.

[5] RANA M M, BO R, ABDELHADI A. Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach[J]. IEEE Systems Journal,2021,15 (2):1970-1978.

[6] YAN J J, YANG G H, WANG Y. Dynamic reduced-order observer-based detection of false data injection attacks with application to smart grid systems[J]. IEEE Transactions on Industrial Informatics,2022,18(10):6712-6722.

[7] 夏云舒，王勇，周林，等．基于改进生成对抗网络的虚假数据注入攻击检测方法[J]．电力建设，2022，43(3)：58-65.
XIA Yunshu, WANG Yong, ZHOU Lin, et al. False data injection attack detection method based on improved generative adversarial network[J]. Electric Power Construction,2022,43(3):58-65.

[8] ZHAO J B, ZHANG G X, LA SCALA M, et al. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks[J]. IEEE Transactions on Smart Grid,2017,8(4):1580-1590.

[9] 刘鑫蕊，常鹏，孙秋野．基于 XGBoost 和无迹卡尔曼滤波自适应混合预测的电网虚假数据注入攻击检测[J]．中国电机工程学报，2021，41(16)：5462-5476.
LIU Xinrui, CHANG Peng, SUN Qiuye. Grid false data injection attacks detection based on XGBoost and unscented Kalman filter adaptive hybrid prediction[J]. Proceedings of the CSEE,2021,41(16):5462-5476.

[10] ZHANG Y, WANG J H, CHEN B. Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach[J]. IEEE Transactions on Smart Grid, 2021,12(1):623-634.

[11] 李元诚，曾婧．基于改进卷积神经网络的电网假数据注入攻击检测方法[J]．电力系统自动化，2019，43(20)：97-104.
LI Yuancheng, ZENG Jing. Detection method of false data injection attack on power grid based on improved convolutional neural network[J]. Automation of Electric Power Systems,2019,43(20):97-104.

[12] 朱杰，张葛祥，王涛，等．电力系统状态估计欺诈性数据攻击及防御综述[J]．电网技术，2016，40(8)：2406-2415.
ZHU Jie, ZHANG Gexiang, WANG Tao, et al. Overview

of fraudulent data attack on power system state estimation and defense mechanism[J]. Power System Technology,2016,40(8):2406-2415.

[13] 杨奕贤,郭力,王洪达,等.基于数据驱动的直流微电网虚假数据注入攻击快速防御策略[J].电力自动化设备,2021,41(5):145-151.
YANG Yixian, GUO Li, WANG Hongda, et al. Fast defense strategy of false data injection attack in DC microgrid based on data-driven[J]. Electric Power Automation Equipment,2021,41(5):145-151.

[14] 郑瑶,张颉,姚文轩,等.基于空间特征的电网同步量测虚假数据注入攻击检测[J].电力系统自动化,2023,47(10):128-134.
ZHENG Yao, ZHANG Jie, YAO Wenxuan, et al. Spatial feature based detection of false data injection attack on synchronous grid measurements[J]. Automation of Electric Power Systems,2023,47(10):128-134.

[15] 李欣,易柳含,刘晨凯,等.基于数据驱动的电力系统虚假数据注入攻击检测[J].智慧电力,2023,51(2):30-37.
LI Xin,YI Liuhan,LIU Chenkai,et al.False data injection attacks detection in power system based on data-driven algorithm[J].Smart Power,2023,51(2):30-37.

[16] WANG X.Power systems dynamic state estimation with the two-step fault tolerant extended Kalman filtering[J]. IEEE Access,2021,9:137211-137223.

[17] 李扬,李京,陈亮,等.复杂噪声条件下基于抗差容积卡尔曼滤波的发电机动态状态估计[J].电工技术学报,2019,34(17):3651-3660.
LI Yang, LI Jing, CHEN Liang, et al. Dynamic state estimation of synchronous machines based on robust cubature Kalman filter under complex measurement noise conditions[J]. Transactions of China Electrotechnical Society,2019,34(17):3651-3660.

[18] 孙怡,何光宇,翟少鹏.基于无迹卡尔曼滤波的电力系统抗差动态估计[J].电测与仪表,2020,57(4):1-6.
SUN Yi,HE Guangyu,ZHAI Shaopeng.Robust dynamic estimation for power system based on unscented Kalman filter[J].Electrical Measurement & Instrumentation,2020,57(4):1-6.

[19] 尚彦赟,宋红为,杨照光,等.基于二阶RC模型的锂电池充放电特性分析[J].高压电器,2023,59(7):87-94.
SHANG Yanyun,SONG Hongwei,YANG Zhaoguang,et al. Charge and discharge characteristics analysis of lithium battery based on second-order RC model[J].High Voltage Apparatus,2023,59(7):87-94.

[20] 李伟康,马刚,高丛,等.基于改进UKF的电—气耦合系统状态估计[J].电网与清洁能源,2023,39(9):1-8,18.
LI Weikang, MA Gang, GAO Cong, et al. The state estimation of the electric-gas coupling system based on improved UKF[J].Power System and Clean Energy,2023,39(9):1-8,18.

[21] 黄蔓云,王天昊,卫志农,等.基于长短期记忆网络的UKF动态谐波状态估计[J].电力系统保护与控制,2022,50(11):1-11.
HUANG Manyun, WANG Tianhao, WEI Zhinong, et al. Dynamic harmonic state estimation of an unscented Kalman filter based on long short-term memory neural networks[J].Power System Protection and Control,2022,50(11):1-11.

[22] 朱茂林,刘灏,毕天姝.考虑风电场量测相关性的双馈风力发电机鲁棒动态状态估计[J].电工技术学报,2023,38(3):726-740.
ZHU Maolin,LIU Hao,BI Tianshu.Robust dynamic state estimation of doubly-fed induction generator considering measurement correlation in wind farms[J]. Transactions of China Electrotechnical Society,2023,38(3):726-740.

[23] RANA M M, LI L, SU S W, et al. Modelling the interconnected synchronous generators and its state estimations[J].IEEE Access,2018,6:36198-36207.

[24] LIU J Q,GUSRIALDI A,HIRCHE S,et al.Joint controller-communication topology design for distributed wide-area damping control of power systems[J].IFAC Proceedings Volumes,2011,44(1):519-525.

[25] 刘豹,唐万生.现代控制理论[M].北京:机械工业出版社,2006.
LIU Bao, TANG Wansheng. Modern control theory[M]. Beijing:China Machine Press,2006.

[26] 王国权,王森,刘华勇,等.基于自适应的动态三次指数平滑法的风电场风速预测[J].电力系统保护与控制,2014,42(15):117-122.
WANG Guoquan, WANG Sen, LIU Huayong, et al. Self-adaptive and dynamic cubic ES method for wind speed forecasting[J]. Power System Protection and Control,2014,42(15):117-122.

[27] 张叶贵,刘敏.基于容积卡尔曼滤波的配电网状态估计[J].电力科学与工程,2019,35(11):26-30.
ZHANG Yegui,LIU Min.State estimation of distribution network based on CKF[J]. Electric Power Science and Engineering,2019,35(11):26-30.