文章编号：1000-3673（2025）03-1246-11　　中图分类号：TM 721　　文献标志码：A　　学科代码：470·40

基于自适应加权混合预测的电网虚假数据注入攻击检测

束洪春[1,2,3]，杨永银[2,3]，赵红芳[1,2]，许畅[2,3]，赵学专[2,3]

（1．昆明理工大学信息工程与自动化学院，云南省 昆明市 650500；
2．昆明理工大学(云南省绿色能源与数字电力量测及控保重点实验室)，云南省 昆明市 650500；
3．昆明理工大学电力工程学院，云南省 昆明市 650500）

Grid False Data Injection Attack Detection Based on Adaptive Weighted Hybrid Prediction

SHU Hongchun[1,2,3], YANG Yongyin[2,3], ZHAO Hongfang[1,2], XU Chang[2,3], ZHAO Xuezhuan[2,3]

(1. Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, Yunnan Province, China;
2. Yunnan Key Laboratory of Green Energy, Electric Power Measurement Digitalization, Control and Protection (Kunming University of Science and Technology), Kunming 650500, Yunnan Province, China;
3. Faculty of Electric Power Engineering, Kunming University of Science and Technology, Kunming 650500, Yunnan Province, China)

ABSTRACT: As a cyber-physical power system (CPPS) that integrates real-time information and energy, accurate identification of false data injection attacks (FDIAs) is essential to ensure the secure and stable operation of the CPPS. To achieve accurate and efficient day-ahead load forecasting, Kendall's tau-b coefficient is first used to quantify the values of data types, and weighted grey relational analysis is introduced to select similar days. Then, a day-ahead load forecasting model based on the least squares support vector machine (LSSVM) is established. The predicted load is mixed adaptively with the system's state variables obtained from power flow calculation and unscented Kalman filter (UKF) dynamic state estimation. Finally, an attack detection index (ADI) is proposed based on the deviation between the mixed prediction values and static estimation values. FDIAs are detected based on the distribution of ADI. If FDIAs are detected, the mixed prediction state variables are used to correct the measured values at that time. The effectiveness and feasibility of the proposed method are verified through simulations on the IEEE-14 and IEEE-39 node systems.

KEY WORDS: cyber-physical power system; weighted grey correlation analysis;untraced Kalman filter; least squares support vector machine; false data injection attacks;attack detection index

摘要：电力系统作为实时信息与能源高度融合的电力信息物理融合系统(cyber-physical power system，CPPS)，虚假数据注入攻击(false data injection attacks，FDIAs)的准确辨识将有效保证 CPPS 安全稳定运行。为准确、高效地完成日前负荷预测，首先使用肯德尔相关系数(Kendall's tau-b)量化日期类型的取值，引入加权灰色关联分析选取相似日，再建立基于最小二乘支持向量机(least squares support vector machine，LSSVM)的日前负荷预测模型。将预测负荷通过潮流计算求解的系统节点状态量与无迹卡尔曼滤波(unscented Kalman filter，UKF)动态状态估计得到的状态量进行自适应加权混合，最后基于混合预测值和静态估计值间的偏差变量提出了攻击检测指数(attack detection index，ADI)，根据 ADI 的分布检测 FDIAs。若检测到 FDIAs，使用混合预测状态量对该时刻的量测量进行修正。使用 IEEE-14 和 IEEE-39 节点系统进行仿真，结果验证了所提方法的有效性与可行性。

关键词：电力信息物理系统；加权灰色关联分析；无迹卡尔曼滤波；最小二乘支持向量机；虚假数据攻击；攻击检测指数

DOI：10.13335/j.1000-3673.pst.2023.0582

0　引言

随着信息技术的不断发展，电力系统逐渐发展成为电力信息物理融合系统(cyber-physical power system，CPPS)[1-3]，其不再具有传统电力系统封闭性的特点，极易遭受网络攻击。2011 年 2 月，伊朗不什尔核电站受到名为“震网”(Stuxne)的病毒攻击，剥夺了核电设备的控制权，通过恶意操作使得大量核电站离心机停用。2015 年 12 月，因恶意网络攻击导致乌克兰国家电网遭受重大损失[4]。现有

基金项目：国家自然科学基金重点项目(52037003)；云南省重大科技专项计划项目(202002AF080001)。

Project Supported by the National Natural Science Foundation of China (52037003) and Major Science and Technology Special Project of Yunnan Province, China (202002AF080001).

网络攻击策略从对电网结构影响可分为以破坏电力网络拓扑结构为目的的攻击[5-9]和不以破坏电力网络拓扑结构为目的的攻击，后者主要包括虚假数据注入攻击(false data injection attacks，FDIAs)[10-13]、负荷的重分配[14-15]，拒绝服务攻击[16]等。FDIAs 是 2009 年 Yao Liu 等人[10]提出的一种新型电力网络攻击，具有较强的隐蔽性，攻击者利用传统状态估计对不良数据检测的漏洞，能够成功地向 CPPS 注入 FDIAs，影响电力系统的状态估计[5,10,17]。因此，如何实现 FDIAs 的检测与辨识已成为保障 CPPS 安全运行的一个新挑战。

近年来，国内外针对 FDIAs 进行了大量研究，文献[18]提出了基于无迹卡尔曼滤波(unscented Kalman filter，UKF)和加权最小二乘相结合的状态估计算法来实时检测虚假数据攻击。文献[19]针对 FDIAs 将改进的噪声估计器与 UKF 动态估计相结合建立安全预测状态估计模型。文献[20]提出了一种伪量测模型与自适应无迹卡尔曼滤波(adaptive unscented Kalman filter，AUKF)相结合的状态估计方法，并基于估计值偏差进行虚假数据的辨识。上述检测方法均基于动态估计与静态估计值间的偏差量或者欧氏距离等指标来检测攻击，但当 UKF 更新过程中存在虚假数据时，FDIAs 检测误警率增大。文献[21]提出了一种基于历史数据库的短期状态预测检测方法。文献[22]利用可信的历史数据提出了基于马尔科夫链理论和欧氏距离相结合的攻击检测方法。文献[23]提出一种基于双向门控循环单元和自注意力的攻击检测方法。文献[24]提出了一种基于最大信息系数-双层置信极端梯度提升树的电网虚假数据注入攻击定位检测方法。文献[25]提出了基于长短时记忆网络和生成对抗网络的 VRB 储能系统虚假数据注入攻击检测方法。文献[26]提出一种低成本对抗性隐蔽虚假数据注入攻击方案及对应的检测方法。文献[27]提出了一种基于极端梯度提升结合无迹卡尔曼滤波的电网虚假数据注入攻击的检测方法。上述检测方法通过深入挖掘历史数据信息对状态量进行预测实现攻击检测，此类方法需要大量的历史数据，优点是不受量测量中虚假数据的影响。但随着新能源的大量接入使得电力系统波动性增加，使用历史数据进行预测的方法难以应对系统中的波动问题，预测状态量精确度降低，导致 FDIAs 检测率降低。

针对上述问题，本文针对 FDIAs 的检测进行研究，首先使用肯德尔相关系数对日期类型进行量化取值，再使用加权灰色关联分析进行相似日的选取，在此基础上建立基于最小二乘支持向量机的日前负荷预测模型。然后将预测负荷通过潮流计算求解的节点状态量与 UKF 动态状态估计得到的状态量进行加权混合预测。最后，求解出状态量混合预测值和静态估计值间的偏差变量，基于偏差变量提出攻击检测指数(attack detection index，ADI)，根据 ADI 的分布进行 FDIAs 检测。若检测到量测数据中存在 FDIAs，则用混合预测状态量对该时刻的量测状态量进行修正。

1　虚假数据注入攻击模型

将实际交流电网视为非线性状态估计系统，向电网中注入 FDIA，则攻击后的量测量为

$$z_i^{\text{bad}}=\begin{cases}z_i+a_i & ,i\in n\\ z_i & ,i\notin n\end{cases} \tag{1}$$

式中：z_i 为无攻击状态下第 i 个测量向量；z_i^{bad} 为第 i 个受攻击后的测量向量；i 为系统节点数；n 为受攻击的节点集；a_i 为攻击向量 a 的第 i 个攻击量；根据电力系统状态估计可知系统受到攻击前后的状态量分别为 $\hat{x}$、$\hat{x}^{\text{bad}}$，其攻击前后产生的偏差向量为 c，则受到攻击后状态量为 $\hat{x}^{\text{bad}}=\hat{x}+c$。由于系统不良检测机制是根据系统量测数据残差来确定检测阈值 $\dot{\tau}$，则攻击前后的量测残差分别为 δ_1 和 δ_2。

$$\begin{cases}\delta_1=\|z-h(\hat{x})\|_2\\ \delta_2=\|z+a-h(\hat{x}+c)\|_2\end{cases} \tag{2}$$

式中：z 为测量向量；$h(\cdot)$ 为系统的非线性量测函数。当攻击向量 a 满足 $a=h(\hat{x}+c)-h(\hat{x})$ 时，攻击前后的量测残差满足 $\delta_2\le\delta_1$，则注入的虚假数据可成功避开不良数据检测机制。

2　基于 UKF 的电力系统动态状态估计

电力系统动态估计的数学模型主要由动态方程和量测方程组成[28]，其表达式为

$$x_{k+1}=f(x_k)+q_k \tag{3}$$

$$z_{k+1}=h(x_{k+1})+r_{k+1} \tag{4}$$

式中：x_{k+1} 和 x_k 分别为 $k+1$ 和 k 时刻的状态量，包含电压幅值、电压相角；z_{k+1} 为 $k+1$ 时刻的量测量；q_k 为 k 时刻的系统噪声；r_{k+1} 为 $k+1$ 时刻的量测噪声；$f(\cdot)$ 为非线性的状态转移函数。

UKF 通过引入无迹变换对状态转移函数 $f(\cdot)$ 进行近似[28]，其基本原理是根据状态量均值点构造方差为状态量方差的 Sigma 点集，再对 Sigma 点集中的各个点进行非线性变换，通过加权求和获得非线性变换后的状态量和方差。在本文中使用 UKF

动态状态估计对电力系统所采集到的量测数据进行迭代计算，根据选取的状态转移函数以及系统状态量的变化趋势实现对系统中各个节点状态量的预测估计，得到系统下一时刻各节点的电压幅值和相角值。基于 UKF 的动态估计的主要步骤主要包括预测和更新两部分。

1）预测。

P_k 为 k 时刻状态量的协方差，根据所选取的采样策略构造 Sigma 点集 $\{\chi_{i,k}\}$，通过无迹变换得到状态量和方差的下一步预测值。

$$\chi_{i.k+1|k}=f(\chi_{i,k})+q_k \tag{5}$$

$$x_{k+1|k}=\sum_{i=1}^{L}w_i^m\chi_{i,k+1|k} \tag{6}$$

$$P_{k+1|k}=\sum_{i=1}^{L}w_i^c[(\chi_{i,k+1|k})-x_{k+1|k}][(\chi_{i,k+1|k})-x_{k+1|k}]^{\mathrm{T}}+Q_k \tag{7}$$

式中：$k+1|k$ 表示利用 k 时刻的量测量来预测 $k+1$ 时刻的状态量；Q_k 为 k 时刻的系统噪声协方差阵；L 为 Sigma 点集个数；w_i^c 和 w_i^m 分别为采样策略决定的均值和方差的权值。

2）更新。

根据状态预测中的 $x_{k+1|k}$，$P_{k+1|k}$ 构造 Sigma 点集 $\{\chi_{i,k}\}$，实现对量测值进行预测：

$$y_{i,k+1}=h(\xi_{i,k+1|k})+r_k \tag{8}$$

$$\bar{y}_{k+1}=\sum_{i=0}^{n+1}w_i^m y_{i,k+1} \tag{9}$$

$$S_{k+1}=\sum_{i=0}^{n+1}w_i^c(y_{i.k+1}-\bar{y}_{k+1})(y_{i.k+1}-\bar{y}_{k+1})^{\mathrm{T}}+R_{k+1} \tag{10}$$

$$C_{k+1}=\sum_{i=0}^{n+1}w_i^c(\chi_{i,k+1|k}-\bar{x}_{k+1|k})(y_{i,k+1}-\bar{y}_{k+1})^{\mathrm{T}} \tag{11}$$

$$K_{k+1}=S_{k+1}C_{k+1}^{-1} \tag{12}$$

$$\bar{x}_{k+1}=\bar{x}_{k+1|k}+K_{k+1}(z_{k+1}-\bar{y}_{k+1})= \tag{13}$$

$$P_{k+1}=P_{k+1|k}-K_{k+1}S_{k+1}K_{k+1}^{\mathrm{T}}= \tag{14}$$

式中：$y_{i,k+1}$ 为 $k+1$ 时刻第 i 个量测量的预测值；$\bar{y}_{k+1}$ 为 $k+1$ 时刻预测值的均值；S_{k+1} 为 $k+1$ 时刻预测值的协方差矩阵；r_k 为 k 时刻的量测噪声量；R_{k+1} 为 $k+1$ 时刻量测噪声量 r_{k+1} 的方差矩阵，在本文中，r_{k+1} 的均值为 0，标准差为 0.02[28]；C_{k+1} 为 $k+1$ 时刻状态量与量测量间的相关性协方差矩阵；K_{k+1} 为卡尔曼增益；$\bar{x}_{k+1}$ 为状态量的滤波值；P_{k+1} 为状态量的协方差矩阵。在本文中，UKF 状态估计使用的状态转移函数 $f(\cdot)$ 为两参数指数平滑法。

从式(13)中可知，在预测更新过程中，UKF 更新过程会受到量测数据 z_{k+1} 中的虚假数据影响，当 z_{k+1} 中存在虚假数据时，会导致状态量滤波值 $\bar{x}_{k+1}$ 精度降低，检测误报率增加。

3 基于相似日的最小二乘支持向量机日前负荷预测模型

在实际电力网络中，日负荷曲线会受多个因素影响，其中占主导的是气象因素[29-30]和日期类型[31]。因此，本文选取历史日负荷数据集时引入了影响该地区负荷变化的主要气象因素，包括平均温度、最高温度、最低温度、相对湿度、日期类型和日期距离因子[32-33]。通过对影响因子进行加权灰色关联分析，求出历史日与待预测日的相似度，选取相似度较大的历史日作为训练集。

在文献[29,32]中将日期类型划分为工作日、双休日，其由于忽略了日期类型间的时间过渡关系，使得日期类型的量化取值不够精确，无法真正反映日期类型与负荷间的关系。因此，本文首先将历史日负荷数据按日期类型分为 7 类，然后将各日期类型负荷数据均值作为 7 个典型的日期类型负荷数据，再通过计算典型日期类型负荷间的肯德尔相关系数(Kendall's tau-b)来量化日期类型的取值。

设 $S=\{(x_i,y_i)\}_{i=1}^{n}$ 为 n 对独立同分布的数据序列，n 为数据序列中数据的个数。当集合 S 中任两个元素 (x_i,y_i) 与 (x_j,y_j) 满足 $x_i>x_i$ 且 $y_i>y_j$ 或 $x_i<x_i$ 且 $y_i<y_j$，则两个元素为同序对；反之，为逆序对；当 $x_i=x_i$ 或 $y_i=y_j$ 时，则既不为同序也不为逆序。则肯德尔相关系数 τ 的计算公式为

$$\tau=\frac{c-d}{\sqrt{(T_0-T_1)(T_0-T_2)}} \tag{15}$$

$$T_0=\frac{1}{2}n(n-1) \tag{16}$$

$$T_1=\sum\frac{1}{2}a_i(a_i-1) \tag{17}$$

$$T_2=\sum\frac{1}{2}b_i(b_i-1) \tag{18}$$

式中：c 为 S 中的同序对元素对数；d 为 S 中的逆序对元素对数；a_i、b_i 分别为序列 x、y 中第 i 个相同元素组成的集合中所包含的元素个数。日期类型的量化取值结果如表 1 所示。

由表 1 可知，周一到周日的 7 种日类型与对应的日负荷曲线的关联特性存在较大差异，如周日的日负荷与周一至周六的日负荷相关性较弱，而周一至周六的日负荷彼此相关性较强。因此，通过对日期类型对应的日负荷进行相关性分析，得出日负荷与日期类型间的变化关联特性，实现对日期类型的量化取值，进一步在对负荷预测时准确的引入影响

表 1　日期类型的量化取值

Table 1　Quantization value of the date type

类型	周一	周二	周三	周四	周五	周六	周日
周一	1	0.953	0.957	0.947	0.919	0.936	0.767
周二	0.953	1	0.977	0.976	0.961	0.952	0.785
周三	0.957	0.977	1	0.983	0.961	0.966	0.789
周四	0.947	0.976	0.983	1	0.969	0.962	0.796
周五	0.919	0.961	0.961	0.969	1	0.955	0.809
周六	0.936	0.952	0.996	0.962	0.955	1	0.816
周日	0.767	0.785	0.789	0.796	0.809	0.816	1

负荷变化的日期影响因子，能够避免人为取值的主观性，使得日期类型特征取值更加具有科学性。

选取各影响因子构建历史日的特征向量序列：

$$\boldsymbol{X}=[\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n]^{\mathrm{T}} \tag{19}$$

$$\boldsymbol{X}_i=[x_{i1},x_{i2},\cdots,x_{im}] \tag{20}$$

$$\boldsymbol{X}_0=[x_{01},x_{02},\cdots,x_{0m}] \tag{21}$$

式中：$\boldsymbol{X}_i$ 为第 i 个历史日的主要影响因子序列；x_{im} 为第 i 个历史日的各类影响因子；$\boldsymbol{X}_0$ 为待预测日的主要影响因子序列；$i=1,2,\cdots,n$，n 为历史日天数；$k=1,2,\cdots,m$，m 为影响因子个数。对历史日数据序列进行均值化无量纲处理得：

$$x'_{ik}=\frac{x_{ik}}{x_{0k}} \tag{22}$$

待预测日特征向量与各个历史日特征向量中对应影响因子的差值为

$$\Delta x_{ik}=|x'_{0k}-x'_{ik}| \tag{23}$$

待预测日特征向量与各个历史日特征向量中对应影响因子的关联系数为

$$\omega_{\mathrm{ik}}=\frac{\min\limits_i\min\limits_k\Delta x_{ik}+\rho\max\limits_i\max\limits_k\Delta x_{ik}}{\Delta x_{ik}+\rho\max\limits_i\max\limits_k\Delta x_{ik}} \tag{24}$$

式中：$\min\limits_i\min\limits_k\Delta x_{ik}$ 为预测日与历史日对应的第 k 个影响因子的差值最小值；$\max\limits_i\max\limits_k\Delta x_{ik}$ 为对应的第 k 个影响因子的差值最大值；ρ 为分辨系数，$\rho\in(0,1)$，ρ 值越小，其分辨率越高。在本文中 ρ 取值为 0.5。从而得到灰色关联系数矩阵：

$$\boldsymbol{\omega}=\begin{bmatrix}\omega_{01} & \omega_{02} & \cdots & \omega_{0\mathrm{m}}\\ \omega_{11} & \omega_{12} & \cdots & \omega_{1m}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n1} & \omega_{n2} & \cdots & \omega_{nm}\end{bmatrix} \tag{25}$$

式中：ω_{nm} 为历史日 n 的第 m 个影响因子的关联系数。将式(25)系数矩阵中各行向量相加即可得到影响因子与负荷间的加权关联度：

$$\boldsymbol{\gamma}=[\gamma_1,\gamma_2,\cdots,\gamma_n]^{\mathrm{T}} \tag{26}$$

引入日期距离量化因子 a^t，采用文献[34]进行取值，$a=0.95$；T 为历史日与预测日相距的天数。则有：

$$\boldsymbol{\gamma}'=[a\gamma_1,a^2\gamma_2,\cdots,a^t\gamma_t]^{\mathrm{T}} \tag{27}$$

将所得的关联度进行排序，选取关联度大于 0.9 以上的 15 个历史日作为待预测日的相似日。

3.1　最小二乘支持向量机模型

LSSVM 是将支持向量机(support vector machines，SVM)中的二次规划问题转化为线性规划问题，使得计算的复杂性大幅度降低，求解速度得以增强。假设数据样本集表示为

$$Z=\{(x_i,y_i),x_i\in R^n,y_i\in R^n\} \tag{28}$$

式中：x_i 为第 i 个输入向量；y_i 为第 i 个输出向量；$i\in[1,N]$，N 为训练样本数；n 为输入样本维数。将样本集 Z 通过非线性映射 $\phi(x)$ 到高维特征空间，再进行线性回归，其回归函数表达式为

$$f=\omega\phi(x)+b \tag{29}$$

式中：ω 为权值向量；$\phi(x)$ 为核函数，表征低维空间到高维空间的映射关系；b 为偏置因子。

为使 LSSVM 结构风险最小化，其优化求解的目标函数与约束条件为

$$\begin{cases}\min J(\omega,b,e)=\dfrac{1}{2}\|\omega\|^2+\dfrac{1}{2}\eta\sum\limits_{i=1}^{n}e_i^2\\ \text{s.t.}\quad y_i=\omega^{\mathrm{T}}\varphi(x_i)+b+e_i\end{cases} \tag{30}$$

式中：η 为惩罚系数；e_i 为第 i 个松弛变量。利用拉格朗日乘子 λ_i 对式(30)进行求解，则：

$$L(\omega,b,e,\lambda)=J(\omega,b,e)-\sum_{i=1}^{N}\lambda_i[\omega^{\mathrm{T}}\phi(x_i)+b+e_i-y_i] \tag{31}$$

根据 KKT 条件，对其求解有：

$$\begin{cases}\dfrac{\partial J}{\partial\omega}=0\rightarrow\sum\limits_{i=1}^{i}\lambda_i\phi(x_i)\\ \dfrac{\partial J}{\partial\omega}=0\rightarrow\sum\limits_{i=1}^{i}\lambda_i=0\\ \dfrac{\partial J}{\partial\omega}=0\rightarrow\lambda_i=\gamma e_i\\ \dfrac{\partial J}{\partial\omega}=0\rightarrow\omega^{\mathrm{T}}\phi(x_i)+b+e_i-y_i=0\end{cases} \tag{32}$$

通过将式中的 ω、e 消除后获得预测函数为

$$y(x)=\sum_{i=1}^{N}\lambda_iK(x_i,x_j)+b \tag{33}$$

式中：$K(\cdot)$ 为径向基核函数，$K(x_i,x_j)=e^{\mu}$，$\mu=-\|x_i-x_j\|^2/2\sigma^2$；$\sigma$ 为核函数宽度，表征低维空间到高维空间的映射关系。

4　自适应加权混合预测

针对本文第 2 节中所提到的基于 UKF 状态估计进行虚假数据检测时存在的弊端，本文采用自适应加权混合预测方法，将 UKF 与第 3 节所建立的

基于 LSSVM 的日前负荷预测模型结合，以应对虚假数据对 UKF 的影响，将两种预测模型的预测结果进行加权求和，依据预测结果偏差对权值进行实时修正，具体方法为

假设 k 时刻，基于 UKF 动态估计得到 $k+1$ 时刻的状态量为 $\hat{x}_{k+1}^{U}$，基于 LSSVM 日前负荷预测得到的负荷结果经潮流计算得到的 $k+1$ 时刻的状态量为 $\hat{x}_{k+1}^{l}$，将两种模型预测得到的状态量进行自适应加权求和得到的混合预测状态量为

$$\hat{x}_{k+1}=w_{k+1}\hat{x}_{k+1}^{l}+(1-w_{k+1})\hat{x}_{k+1}^{U} \tag{34}$$

式中：w_{k+1} 为自适应混合权值，由于两种方法在不同时刻的状态量预测值的准确度不同，为使得混合后预测效果最佳，则需根据 k 时刻的预测偏差对 $k+1$ 时刻的 w_{k+1} 进行修正。当基于 UKF 预测精度更高时给予较高权重，否则给予后者较高权重，表达式如式(35)—(36)所示：

$$w_{k+1}=(1-c_{k+1})w_k+c_{k+1}\frac{|x_k-\hat{x}_k^{U}|}{|x_k-\hat{x}_k^{U}|+|x_k-\hat{x}_k^{l}|} \tag{35}$$

$$c_{k+1}=\begin{cases}0 & \|z_k-h(\hat{x}_k)\|_2\geq\dot{\tau}\\ \dfrac{\|z_k-h(\hat{x}_k)\|_2}{\dot{\tau}} & \|z_k-h(\hat{x}_k)\|_2<\dot{\tau}\end{cases} \tag{36}$$

式中：c_{k+1} 为 $k+1$ 时刻的遗忘因子，并且 $c_{k+1}\in[0,1]$，其取值越大表明对前一时刻的权重保留越小；当系统中 k 时刻量测量 z_k 满足 $\|z_k-h(\hat{x}_k)\|<\dot{\tau}$ 时，则 z_k 不存在虚假数据。利用式(37)计算 $k+1$ 时刻的遗忘因子，当 k 时刻状态量值预测误差越小，在 $k+1$ 时刻多保留 k 时刻的权重，即在 $k+1$ 时刻 c_{k+1} 取值越小；反之成立。当 k 时刻存在虚假数据并成功的被检测出时，表明当前时刻的混合预测精度较高，保留当前时刻的预测权重值，即在 $k+1$ 时刻 c_{k+1} 取值为 0。x_k 为剔除虚假数据后存入历史库的状态量；z_k 为 k 时刻系统的量测状态量；$\dot{\tau}$ 的取值根据 γ 分布表可知，在本文中，m 为量测值的个数，且 $m=41$；n 为状态量的个数，且 $n=27$；$m-n$ 为冗余度；当显著性水平为 0.95 时，$\dot{\tau}=23.685$，自适应加权混合预测流程如图 1 所示。

本文所提的日前负荷预测模型的精确度取决于历史相似日的选取以及 LSSVM 模型参数的选取。但由于系统状态多变，所提的 LSSVM 日前负荷预测模型的预测值与实际会存在一定的偏差，导致预测状态量存在偏差；UKF 状态估计的精度取决于状态转移函数的选取以及系统状态量的变化趋势。在本文中 LSSVM 日前负荷预测与 UKF 动态估计进行状态量预测时相互独立，保证了两者的预测精度互不影响，通过引入自适应权重值将两种预测值进行加权求和，使得混合预测值结合了 UKF 实时在线估计的优势和基于 LSSVM 的日前负荷预测模型可充分挖掘历史数据信息且不受虚假数据攻击影响的优势，通过预测偏差量进行权重值的实时修正，将各自模型的优劣进行互补，实现更高精度的状态值预测，进而更有效应对 FDIAs。

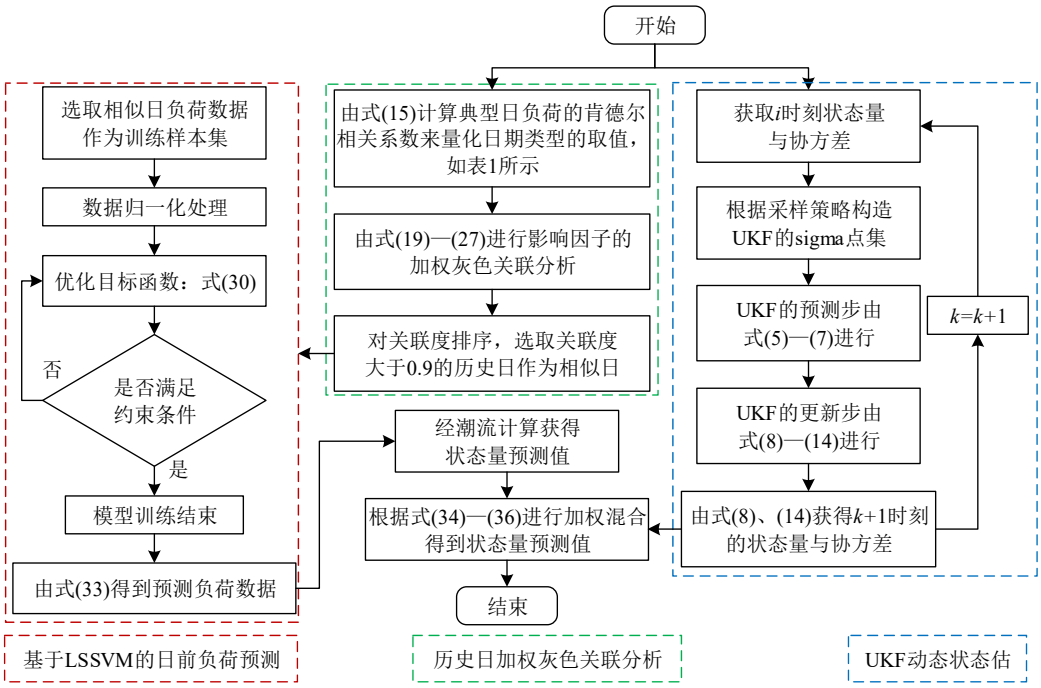

图 1　自适应混合预测流程

Fig. 1　Adaptive hybrid prediction process

5　FDIA 的攻击检测和修正

为了检测虚假数据攻击，本文根据混合预测值和静态估计值间的偏差向量提出了一种攻击检测指数(attack detection index，ADI)，其表达式如下：

$$x'_{i+1}=\hat{x}_{i+1}-\hat{x}_{i+1} \tag{37}$$

$$I_{i+1}^{\mathrm{ADI}}=\frac{|x'_{i+1}|}{\sqrt{\mathrm{cov}(x',\bar{x}')}} \tag{38}$$

$$\begin{cases} H_0: I_{i+1}^{\mathrm{ADI}}\le\tilde{\tau}, & \text{未受到攻击} \\ H_1: I_{i+1}^{\mathrm{ADI}}>\tilde{\tau}, & \text{受到攻击} \end{cases} \tag{39}$$

式中：$\hat{x}_{i+1}$ 为 $i+1$ 时刻的静态状态估计值；$\tilde{x}_{i+1}$ 为 $i+1$ 时刻的状态混合预测值；x'_{i+1} 为 $i+1$ 时刻预测值与静态估计值的偏差；x' 为 $i=1$ 到 $i+1$ 时刻的偏差向量；$\bar{x}'$ 为 x' 的平均值；cov(.) 为协方差函数；$\tilde{\tau}$ 为检测边界阈值。

根据无攻击情况下的状态预测与静态状态估计值间的偏差向量经式(38)计算出正常情况下的攻击检测指数序列 κ，再根据序列 κ 中各个变量的分布范围确定检测阈值 $\tilde{\tau}$，本文中，$\tilde{\tau}=\max(\kappa)$。假设前 i 时刻状态量不存在虚假数据攻击，然后加入 $i+1$ 时刻的预测值计算 $i+1$ 时刻状态量的攻击检测指数 I_{i+1}^{ADI}，将 I_{i+1}^{ADI} 与 $\tilde{\tau}$ 作比较；若 $I_{i+1}^{\mathrm{ADI}}\le\tilde{\tau}$，则 $i+1$ 时刻量测量不存在虚假数据攻击；否则 $i+1$ 时刻量测量存在虚假数据攻击，则将 $i+1$ 时刻预测值 $\tilde{x}_{i+1}$ 替换静态估计值 $\hat{x}_{i+1}$，然后继续下一时刻状态量的攻击检测，流程如图 2 所示。

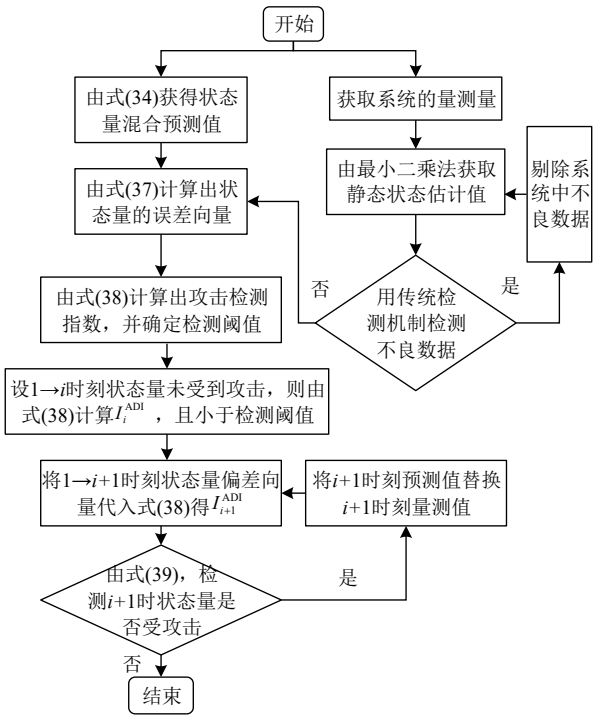

图 2　FDIAs 的检测与修正流程

Fig. 2　FDIAs detection and correction process

6　仿真分析

本文通过选用 IEEE-14 和 IEEE-39 节点测试系统进行仿真分析。加权灰色关联的相似日选取部分、最小二乘向量机预测、UKF 动态状态估计以及攻击检测部分使用 Matlab R2019a 实现，处理器为 Intel(R) Core(TM)i7-7700HQ CPU@2.80GHz，RAM8.0GB；仿真数据选用云南某地区 8 月 1 日至 9 月 27 日负荷，数据采集每 15min 一次，一天共 96 次负荷数据和 96 次气象数据。参照文献[35]将负荷数据分为 14、39 两个区域并分别接入到 IEEE-14、IEEE-39 节点系统中。

选取 9 月 27 日作为攻击检测日，首先通过加权灰色关联分析选取相似日，然后通过 LSSVM 对 9 月 27 日负荷进行预测，根据负荷预测求出状态量，将求出的状态量与 UKF 的估计值进行加权求和，再利用混合预测值与静态估计值间的偏差量求出攻击检测指数 ADI，并根据 ADI 的分布进行 FDIAs 的检测与辨识。

6.1　日前负荷预测仿真分析

以预测 9 月 27 日节点 9 的负荷为例，按照本文第 3 节的方法对日类型进行特征量化，对历史气象数据、日期距离以及预测日的气象数据进行数据预处理，构建影响日负荷曲线的影响因子母序列及子序列，再通过加权灰色关联分析法对影响因素进行关联相似度计算，选出相似度大于 0.9 的 15 个历

史日作为相似日，结果如表 2 所示。

表 2 关联分析选出的相似日

Table 2 Similar days selected by correlation analysis

日期	相似度	日期	相似度
8 月 2 日	0.907	9 月 18 日	0.901
8 月 15 日	0.902	9 月 20 日	0.902
8 月 23 日	0.903	9 月 21 日	0.911
8 月 28 日	0.901	9 月 22 日	0.902
8 月 30 日	0.902	9 月 24 日	0.901
9 月 1 日	0.907	9 月 25 日	0.931
9 月 13 日	0.901	9 月 26 日	0.942
9 月 17 日	0.910		

将相似日、非相似日与预测日的日负荷曲线进行对比，如图 3 所示。由图可知，使用加权灰色关联选取出的相似日与预测日的日负荷特性更为接近。因此将相似日作为预测日的训练集，能够大幅度降低数据内存、提高模型训练效率与预测精度。

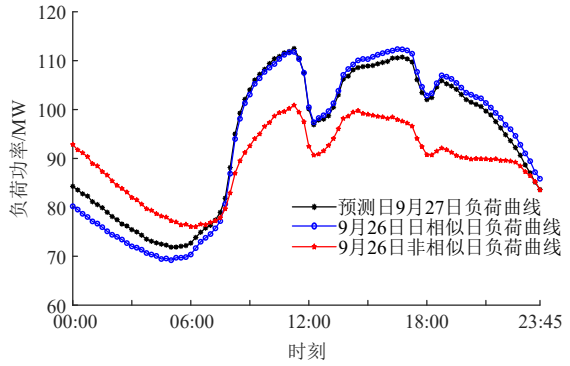

图 3 不同日负荷曲线对比

Fig. 3 Comparison of different daily load curves

将选取出的 15 组历史日负荷数据以及对应的气象数据和 9 月 27 日的气象预测数据作为 LSSVM 模型的输入量，对 9 月 27 日的负荷进行预测。此外，从 8 月 1 日到 9 月 26 日的历史负荷数据中随机选取 15 天数据导入 LSSVM 模型中作为预测对照实验。在本文中，LSSVM 模型的参数 gam 取值为 10，sig2 取值为 1000，训练集为 15。相似日样本数据与随机日样本数据经 LSSVM 预测模型得到的负荷预测结果如图 4 所示。

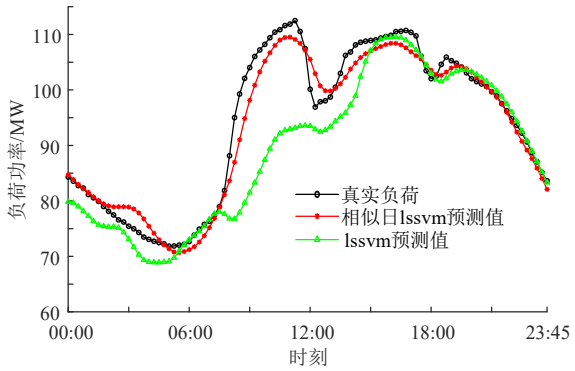

图 4 预测负荷曲线对比

Fig. 4 Comparison of predicted load curve

为验证本文方法与随机历史日下 LSSVM 模型的负荷预测准确率，使用平均绝对百分比误差(mean absolute percentage error，MAPE)作为量化指标，其计算公式为

$$y_{\mathrm{MAPE}}=\frac{1}{n}\sum_{i=1}^{n}\left|\frac{P_i'-\mathrm{P}_i}{\mathrm{P}_i}\right|\times 100\% \tag{40}$$

式中：n 为负荷的量测次数，$n=96$；P_i' 为预测负荷；P_i 为预测日的真实负荷。

各方法的 MAPE 计算结果如表 3 所示。

表 3 各类方法 MAPE 对比

Table 3 MAPE comparison of various methods

方法	MAPE/%
本文方法	2.06
随机日下的 LSSVM 方法	5.32

由表 3 可知，本文所提方法的 MAPE 值为 2.06%，相较于随机日下的 LSSVM 模型的 MAPE 值降低了 3.26%，本文所提出的方法能够有效提升负荷预测的精度。

6.2 自适应加权混合状态预测仿真分析

场景 1：首先将本文方法的预测负荷代入 IEEE-14 节点系统中求出节点 9 的状态量。设当前系统未受到 FDIA 的攻击，即攻击强度为零，将通过潮流计算出的状态量作为系统的真实状态量。为使得量测信息更加的接近实际情况，在真实状态量中加入均值为 0，方差为 1%的高斯白噪声作为系统的量测量。根据本文第 4 节的自适应加权混合预测方法求出状态量的预测值 $\hat{x}_{k+1}$，各方法下的状态量预测结果对比如图 5、图 6 所示。

由图 5 和图 6 可知，本文方法对状态量预测效果最好，通过相似日选取出的历史日与待预测日的负荷特征高度相似，降低了非相似日负荷对训练集数据的影响，提升了日前负荷预测模型的准确性，使得预测的状态量准确度更高；最后使用自适应加权将日前负荷预测模型所得状态值与 UHF 状态估计值进行加权求和，将两种预测模型的优缺点进行互补融合，进一步提高了状态预测的精度。

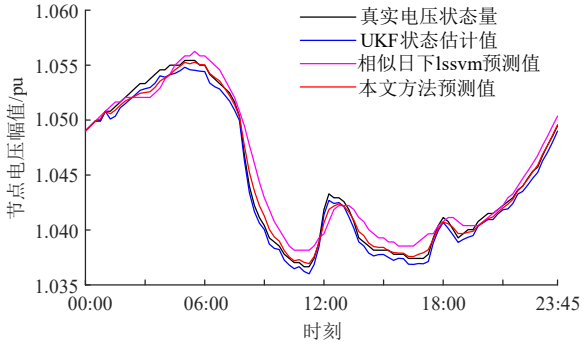

图 5 电压幅值状态预测对比

Fig. 5 Voltage amplitude state prediction comparison

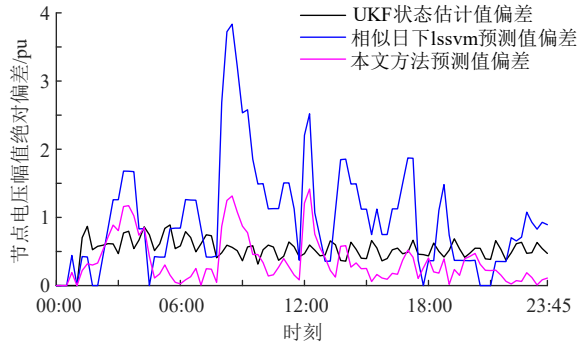

图 6　电压幅值绝对偏差对比

Fig. 6　Voltage amplitude absolute deviation comparison

场景 2：在场景 1 中的第 55~65 次量测数据中注入攻击强度为电压幅值量 3%的攻击量，其攻击量采用文献[10]的攻击模型进行构造。其各方法所得的状态量预测结果如图 7 所示。

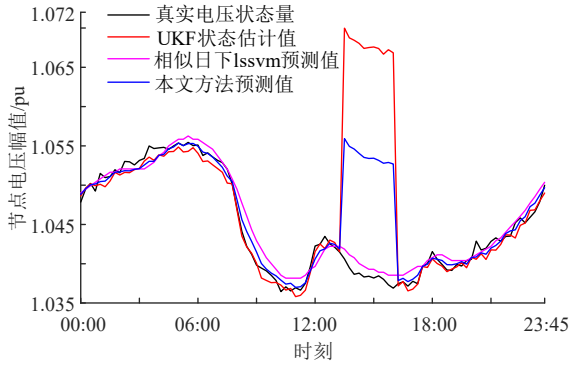

图 7　连续注入强度为 3%的攻击后预测值对比

Fig. 7　Comparison of predicted value after attack with continuous injection intensity of 3%

场景 3：在 9 月 27 日的 96 个量测数据中随机注入 5 个攻击强度为电压幅值量 3%的攻击量，随机注入攻击后的电压幅值预测值比较如图 8 所示。

由图 7 和图 8 可知，当节点 9 处的量测数据中发生虚假数据注入攻击时，相似日下 LSSVM 模型的状态预测效果最好，由于 UKF 动态估计容易受量测数据中虚假数据的影响，导致在状态预测时效果最差，本文方法的效果介于两者之间；由图 6 可知，在无虚假数据注入时，相似日下 LSSVM 模型的状态预测效果比 UKF 动态估计的效果差，使得相似日下 LSSVM 模型的状态预测值不易满足误报率的要求。因此本文方法将 UKF 动态估计与 LSSVM 日前负荷预测模型相结合，可在有虚假数据注入攻击的情况下相比单一方法提高了检测率，在不发生虚假数据注入攻击时降低检测的误报率。

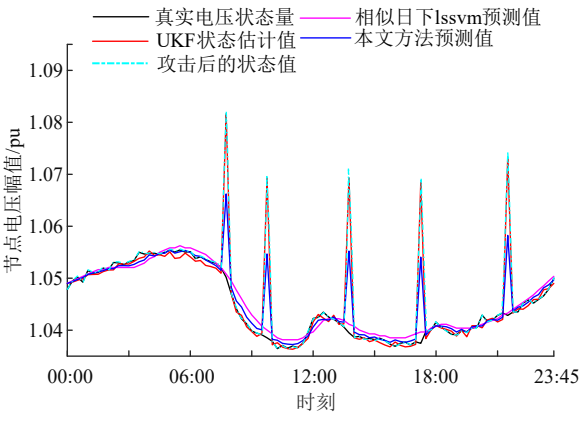

图 8　攻击强度为 3%的电压幅值预测比较

Fig. 8　Comparison of voltage amplitude prediction with attack strength of 3%

6.3　FDIA 的检测仿真效果对比分析

按照场景 3 的攻击方式，向节点 9 的 96 个量测量中随机注入 3 组攻击强度为电压幅值量 0%、3%和 5%的 5 个攻击向量，并对其进行残差检验，以验证所注入的攻击量能否躲避传统检测机制的检测，其在不同时刻受攻击后残差结果如表 4 所示。

表 4　不同攻击时刻的残差结果

Table 4　Residual results at different attack times

攻击时刻 k	32	40	56	70	87
3%攻击量	19.732	17.637	14.286	19.256	20.478
攻击时刻 k	22	36	53	61	81
5%攻击量	21.839	18.989	21.411	23.649	21.131

由表 4 可知，注入攻击强度为 3%和 5%的攻击量后，经残差计算在不同攻击时刻其残差结果均小于第 4 节中所求出的传统检测阈值 $\dot{\tau}=23.685$，说明本文所注入的攻击量能够躲避传统检测机制，具有隐蔽性。进一步，根据式(37)—(39)计算出各种攻击强度下的攻击检测指数 ADI。不同攻击强度下 ADI 分布如图 9 所示。

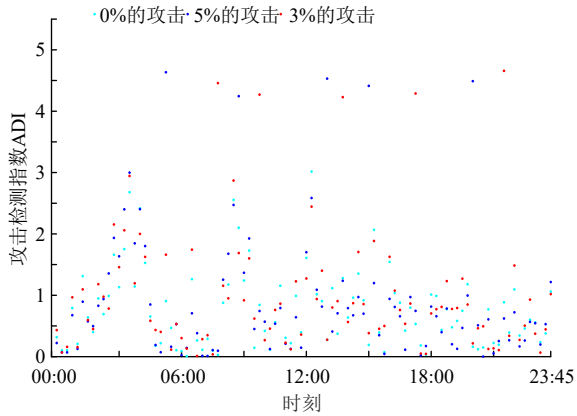

图 9　不同攻击强度下的 ADI 分布

Fig. 9　ADI distribution under different attack intensity

由图 9 可知，在发生攻击的情况下，由于攻击量注入，致使攻击检测指数远大于正常情况下的攻击检测指数。因此，本文根据攻击强度为 0%时的 ADI 分布确定攻击检测阈值为 3.14，不仅能够准确的识别出量测数据中是否存在虚假数据攻击，而且能够降低波动性的影响。但随着攻击强度的降低，所提出的攻击检测指数 ADI 与正常时的 ADI 会趋

于同一分布，导致依据正常状态下的 ADI 确定检测边界阈值会使得误报率增加，导致检测难度加大。

为了验证本文所提方法检测的性能，将本文所提方法与基于短期状态预测的 FDIAs 检测方法[11]、基于支持向量机(support vector machine，SVM)的 FDIA 检测方法[12]、基于 UKF 动态状态估计的 FDIA 检测方法[18]进行对比。分别向 IEEE-14 和 IEEE-39 节点系统中随机注入 20 次攻击强度为电压幅值量 3%~5%的攻击量，其攻击量采用文献[10]的攻击模型进行构造。检测效果采用检测率 P_{A0}、误报率 P_{A1} 两个指标进行量化，表达式为

$$\begin{cases} P_{A0}=\dfrac{C_{TP}+C_{TN}}{C_{TP}+C_{FP}+C_{TN}+C_{FN}} \\ P_{A1}=\dfrac{C_{FP}+C_{FN}}{C_{TP}+C_{FP}+C_{TN}+C_{FN}} \end{cases} \tag{41}$$

式中：C_{TP} 为成功检测出攻击的次数；C_{TN} 为成功检测出正常的次数；C_{FP} 为检测为异常的正常数据次数；C_{FN} 为检测为正常的异常数据次数；不同系统下的检测结果比较如表 5、6 所示。

表 5 IEEE-14 节点下系统检测结果比较
Table 5 Comparison of detection results in IEEE-14 bus system

方法	检测率/%	误报率/%
本文检测方法	95.83	4.17
基于 UKF 检测方法	89.58	10.42
基于 SVM 检测方法	87.50	12.50
本文 LSSVM 日前预测检测方法	92.71	7.29
基于短期状态预测检测方法	91.67	8.33

表 6 IEEE-39 节点系统下检测结果比较
Table 6 Comparison of detection results in IEEE-39 bus system

方法	检测率/%	误报率/%
本文检测方法	93.75	6.25
基于 UKF 检测方法	90.63	9.37
基于 SVM 检测方法	86.46	13.54
本文 LSSVM 日前预测检测方法	91.66	8.34
基于短期状态预测检测方法	90.63	9.37

由表 5、6 可知，本文检测方法在 IEEE-14、IEEE-39 节点系统中检测率分别达到 95.83%、93.75%，并且本文方法的检测率比其他基于单一方法的检测率均有不同程度的提高，说明本文所提方法能够有效应对 FDIAs。

7 结论

针对 CPPS 中存在的虚假数据注入攻击，本文在使用肯德尔相关系数对日期类型进行量化的基础上，引入加权灰色关联分析进行相似日的选取，建立基于 LSSVM 的日前负荷预测模型，通过潮流计算节点状态量；再利用 UKF 动态估计进行系统状态量预测，通过自适应加权混合将两种方法所得状态量进行求和，并根据混合预测值与静态估计值间的偏差向量提出了攻击检测指数 ADI。然后基于 ADI 的分布来检测 FDIAs。若系统遭受 FDIAs，则使用该时刻的混合预测状态量替换该时刻的量测状态量。最后在 IEEE-14 和 IEEE-39 节点系统中进行仿真，可得到如下结论：

通过使用肯德尔相关系数进行日期类型的量化特征值计算，避免了人为取值的主观性，引入加权灰色关联分析选取出与待预测日高度相似的历史日作为相似日，提高了负荷预测的精确性并降低数据迭代时间。

通过将 UKF 动态估计与基于 LSSVM 的日前预测模型进行自适应混合，能够有效克服 UKF 受虚假数据的影响以及 LSSVM 预测模型受系统负荷突变的影响，根据预测误差进行自适应权重的不断修正，提高了状态量预测精度。

根据预测值与静态估计值间偏差向量提出了一种攻击检测指数 ADI，并根据 ADI 的分布进行 FDIAs 的攻击检测，能够有效的应对 FDIAs。

参考文献

[1] 王琦，邰伟，汤弈，等．面向电力信息物理系统的虚假数据注入攻击研究综述[J]．自动化学报，2019，45(1)：72-83．
WANG Qi，TAI Wei，TANG Yi，et al．A review on false data injection attack toward cyber-physical power system[J]．Acta Automatica Sinica，2019，45(1)：72-83(in Chinese)．

[2] 郭庆来，辛蜀骏，孙宏斌，等．电力系统信息物理融合建模与综合安全评估：驱动力与研究构想[J]．中国电机工程学报，2016，36(6)：1481-1489，1761．
GUO Qinglai，XIN Shujun，SUN Hongbin，et al．Power system cyber-physical modelling and security assessment：motivation and ideas[J]．Proceedings of the CSEE，2016，36(6)：1481-1489，1761(in Chinese)．

[3] 赵俊华，文福拴，薛禹胜，等．电力 CPS 的架构及其实现技术与挑战[J]．电力系统自动化，2010，34(16)：1-7．
ZHAO Junhua，WEN Fushuan，XUE Yusheng，et al．Cyber physical power systems：architecture，implementation techniques and challenges[J]．Automation of Electric Power Systems，2010，34(16)：1-7(in Chinese)．

[4] 赵俊华，梁高琪，文福拴，等．乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J]．电力系统自动化，2016，40(7)：149-151．
ZHAO Junhua，LIANG Gaoqi，WEN Fushuan，et al．Lessons learnt from Ukrainian blackout：protecting power grids against false data injection attacks[J]．Automation of Electric Power Systems，2016，40(7)：149-151(in Chinese)．

[5] 阳育德，蓝水岚，覃智君，等．电力信息物理融合系统的网络-物理协同攻击[J]．电力自动化设备，2020，40(2)：97-102．
YANG Yude，LAN Shuilan，QIN Zhijun，et al．Coordinated cyber-physical attacks of cyber-physical power system[J]．Electric Power Automation Equipment，2020，40(2)：97-102(in Chinese)．

[6] 田继伟，王布宏，李夏．智能电网状态维持拓扑攻击及其对经济

运行的影响[J]. 电力系统保护与控制，2018，46(1)：50-56.
TIAN Jiwei，WANG Buhong，LI Xia. State-preserving topology attacks and its impact on economic operation of smart grid[J]. Power System Protection and Control，2018，46(1)：50-56(in Chinese).

[7] 张殷，肖先勇，李长松. 基于攻击者视角的电力信息物理融合系统脆弱性分析[J]. 电力自动化设备，2018，38(10)：81-88.
ZHANG Yin，XIAO Xianyong，LI Changsong. Vulnerability analysis of cyber physical power system from attacker's perspective[J]. Electric Power Automation Equipment，2018，38(10)：81-88(in Chinese).

[8] LIANG Gaoqi，WELLER S R，ZHAO Junhua，et al. A framework for cyber-topology attacks：line-switching and new attack scenarios[J]. IEEE Transactions on Smart Grid，2019，10(2)：1704-1712.

[9] ZHANG Jiazi，SANKAR L. Physical system consequences of unobservable state-and-topology cyber-physical attacks[J]. IEEE Transactions on Smart Grid，2016，7(4)：2016-2025.

[10] LIU Yao， NING Peng，REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security，2011，14(1)：13.

[11] 刘鑫蕊，吴泽群. 面向智能电网的空间隐蔽型恶性数据注入攻击在线防御研究[J]. 中国电机工程学报，2020，40(8)：2546-2558.
LIU Xinrui，WU Zequn. Online defense research of spatial-hidden malicious data injection attacks in smart grid[J]. Proceedings of the CSEE，2020，40(8)：2546-2558(in Chinese).

[12] 杨杉，谭博，郭静波. 基于双马尔科夫链的新型能源互联网虚假数据注入攻击检测[J]. 电力自动化设备，2021，41(2)：131-137.
YANG Shan，TAN Bo，GUO Jingbo. Detection of false data injection attack for new-type energy internet based on double Markov chains[J]. Electric Power Automation Equipment，2021，41(2)：131-137(in Chinese).

[13] 李青芯，孙宏斌，盛同天，等. 变电站状态估计中互感器虚假数据注入攻击分析[J]. 电力系统自动化，2016，40(17)：79-86.
LI Qingxin，SUN Hongbin，SHENG Tongtian，et al. Injection attack analysis of transformer false data in substation state estimation[J]. Automation of Electric Power Systems，2016，40(17)：79-86(in Chinese).

[14] 陈凡，史杰，刘海涛，等. 考虑负荷重分配攻击和脆弱线路防御的发输电系统可靠性评估[J]. 电力系统自动化，2022，46(2)：65-72.
CHEN Fan，SHI Jie，LIU Haitao，et al. Reliability evaluation of power generation and transmission system considering load redistribution attack and defense of vulnerable line[J]. Automation of Electric Power Systems，2022，46(2)：65-72(in Chinese).

[15] YUAN Yanling，LI Zuyi，REN Kui. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid，2011，2(2)：382-390.

[16] ZHANG Bo，LI Qianmu，ZHANG Yiying，et al. The proactive defense of energy internet terminals edge-access using the network topology autoassociation[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems，2017，7(3)：432-446.

[17] DENG Ruilong，XIAO Gaoxi，LU Rongxing. Defending against false data injection attacks on power system state estimation[J]. IEEE Transactions on Industrial Informatics，2017，13(1)：198-207.

[18] ŽIVKOVIĆ N，SARIĆ A T. Detection of false data injection attacks using unscented Kalman filter[J]. Journal of Modern Power Systems and Clean Energy，2018，6(5)：847-859.

[19] XU Junjun，WU Zaijun，ZHANG Tengfei，et al. A secure forecasting-aided state estimation framework for power distribution systems against false data injection attacks[J]. Applied Energy，2022，328：120107.

[20] 陈碧云，李弘斌，李滨. 伪量测建模与 AUKF 在配电网虚假数据注入攻击辨识中的应用[J]. 电网技术，2019，43(9)：3226-3234.
CHEN Biyun，LI Hongbin，LI Bin. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network[J]. Power System Technology，2019，43(9)：3226-3234(in Chinese).

[21] 朱杰，张葛祥. 基于历史数据库的电力系统状态估计欺诈性数据防御[J]. 电网技术，2016，40(6)：1772-1777.
ZHU Jie，ZHANG Gexiang. Defense against false data in power system state estimation based on historical database[J]. Power System Technology，2016，40(6)：1772-1777(in Chinese).

[22] KARIMIPOUR H，DINAVAHI V. Robust massively parallel dynamic state estimation of power systems against cyber-attack[J]. IEEE Access，2018，6：2984-2995.

[23] 陈冰，唐永旺. 基于 Bi-GRU 和自注意力的智能电网虚假数据注入攻击检测[J]. 计算机应用与软件，2021，38(7)：339-344，349.
CHEN Bing，TANG Yongwang. False data injection attacks detection in smart grid based on BI-GRU and self-attention[J]. Computer Applications and Software，2021，38(7)：339-344，349(in Chinese).

[24] 席磊，王文卓，白芳岩，等. .基于最大信息系数-双层置信极端梯度提升树的电网虚假数据注入攻击定位检测[J/OL]. 电网技术. https://doi.org/10.13335/j.1000-3673.pst.2024.0298
XI Lei，WANG Wenzhuo，BAI Fangyan，et al. Grid False Data Injection Attack Localization Detection based on MIC-Double-deck Confidence XGBoost Tree[J/OL]. Power System Technology. https://doi.org/10.13335/j.1000-3673.pst.2024.0298

[25] 陆鹏，付华，卢万杰. 基于长短时记忆网络和生成对抗网络的 VRB 储能系统虚假数据注入攻击检测[J]. 电网技术，2024，48(1)：383-393.
LU Peng，FU Hua，LU Wanjie. Detection of False Data Injection Attacks for VRB Energy Storage Systems Based on Long-Short-term Memory and Generative Adversarial Networks[J]. Power System Technology，2024，48(1)：383-393.

[26] 黄冬梅，丁仲辉，胡安铎，等. 低成本对抗性隐蔽虚假数据注入攻击及其检测方法[J]. 电网技术，2023，47(4)：1531-1540.
HUANG Dongmei，DING Zhonghui，HU Anduo，et al. Low-cost Adversarial Stealthy False Data Injection Attack and Detection Method[J]. Power System Technology，2023，47(4)：1531-1540.

[27] 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)：5462-5475.
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)：5462-5475(in Chinese).

[28] 赵洪山，田甜. 基于自适应无迹卡尔曼滤波的电力系统动态状态估计[J]. 电网技术，2014，38(1)：3790-3794.
ZHAO Hongshan，TIAN Tian. Dynamic state estimation for power system based on an adaptive unscented Kalman filter[J]. Power System Technology，2014，38(1)：3790-3794(in Chinese).

[29] 金义雄，段建民，徐进，等. 考虑气象因素的相似聚类短期负荷组合预测方法[J]. 电网技术，2007，31(19)：60-64，82.
JIN Yixiong，DUAN Jianmin，XU Jin，et al. A combinational short-term load forecasting method by use of similarity clustering and considering weather factors[J]. Power System Technology，2007，31(19)：60-64，82(in Chinese).

[30] 张凯，姚建刚，李伟，等. 基于功率谱分解和实时气象因素的短期负荷预测[J]. 电网技术，2007，31(23)：47-51.

ZHANG Kai，YAO Jiangang，LI Wei，et al. Short-term load forecasting based on power spectrum decomposition and hourly weather factors[J]. Power System Technology，2007，31(23)：47-51(in Chinese).

[31] 高亚静，孙永健，杨文海，等．基于新型人体舒适度的气象敏感负荷短期预测研究[J]．中国电机工程学报，2017，37(7)：1946-1954.
GAO Yajing，SUN Yongjian，YANG Wenhai，et al. Weather-sensitive load’s short-term forecasting research based on new human body amenity indicator[J]. Proceedings of the CSEE，2017，37(7)：1946-1954(in Chinese).

[32] 周宇．计及气象因素影响的短期电力负荷预测方法[J]．自动化技术与应用，2020，39(6)：107-113.
ZHOU Yu. A short-term load forecasting method considering the influence of meteorological factors[J]. Techniques of Automation and Applications，2020，39(6)：107-113(in Chinese).

[33] 康重庆，周安石，王鹏，等．短期负荷预测中实时气象因素的影响分析及其处理策略[J]．电网技术，2006，30(7)：5-10.
KANG Chongqing，ZHOU Anshi，WANG Peng，et al. Impact analysis of hourly weather factors in short-term load forecasting and its processing strategy[J]. Power System Technology，2006，30(7)：5-10(in Chinese).

[34] 陈弘川，蔡旭，孙国歧，等．基于智能优化方法的相似日短期负荷预测[J]．电力系统保护与控制，2021，49(13)：121-127.
CHEN Hongchuan，CAI Xu，SUN Guoqi，et al. Similar day short-term load forecasting based on intelligent optimization method[J]. Power System Protection and Control，2021，49(13)：121-127(in Chinese).

[35] GU Chaojun，JIRUTITIJAROEN P，MOTANI M. Detecting false data injection attacks in AC state estimation[J]. IEEE Transactions on Smart Grid，2015，6(5)：2476-2483.

束洪春

在线出版日期：2024-01-29。
收稿日期：2023-04-13。

作者简介：

束洪春(1961)，男，博士，教授，博士生导师，研究方向为电力系统新型继电保护与故障测距、故障录波、数字信号处理及 DSP 应用，E-mail：kmshc@sina.com；

杨永银(1998)，男，硕士研究生，研究方向为电力系统新型继电保护，E-mail：2640403546@qq.com；

赵红芳(1993)，女，通信作者，博士研究生，研究方向为电力系统韧性评估与供电恢复策略、可靠性分析，E-mail：angel199381@126.com。

（责任编辑　赵梓含）