引用格式:陈将宏,饶佳黎,李伟亮,等.基于向量自回归模型的电网虚假数据注入攻击检测[J].电力科学与技术学报,2024,39(3):1-9.
Citation:CHEN Jianghong,RAO Jiali,LI Weiliang,et al.Grid false data injection attack detection based on vector auto-regressive model[J].Journal of Electric Power Science and Technology,2024,39(3):1-9.

基于向量自回归模型的电网虚假数据注入攻击检测

陈将宏[1,2],饶佳黎[1,2],李伟亮[1,2],胡 炀[1,2]
(1.三峡大学电气与新能源学院,湖北 宜昌 443002;2.湖北省输电线路工程技术研究中心,湖北 宜昌 443002)

摘 要:虚假数据注入攻击(false data injection attack,FDIA)是威胁电网运行安全的主要因素之一,其主要通过攻击电网中的一些通信环节,误导电力系统的状态估计结果,给电网安全运行带来巨大威胁。针对FDIA难以有效检测及电力系统状态估计中过程噪声与量测噪声两者协方差矩阵非正定问题,将向量自回归(vector auto regression,VAR)模型引入电力系统状态估计,提出一种基于VAR和加权最小二乘法(weighted least squares,WLS)的FDIA检测方法。首先,建立VAR状态估计模型,将量测噪声视为稳定量,只对过程噪声进行估计,解决两者协方差矩阵的非正定问题;其次,分别采用VAR与WLS对电力系统进行状态估计,采用一致性检验与量测量残差检验对2种方法的结果进行检测,以判定是否存在FDIA;最后,IEEE 14节点和IEEE 30节点仿真结果表明,本文所提检测方法能够成功检测到FDIA,且检测成功率较高,从而验证了该方法的可行性及有效性。

关 键 词:虚假数据注入攻击;向量自回归;加权最小二乘法;状态估计;攻击检测
DOI:10.19781/j.issn.1673-9140.2024.03.001 **中图分类号**:TM734 **文章编号**:1673-9140(2024)03-0001-09

Detection method of false data injection attacks on power grids based on vector auto-regression model

CHEN Jianghong[1,2],RAO Jiali[1,2],LI Weiliang[1,2],HU Yang[1,2]
(1.College of Electrical Engineering and New Energy, China Three Gorges University, Yichang 443002, China;2.Hubei Provincial Engineering Technology Research Center for Power Transmission Line, Yichang 443002, China)

Abstract: False data injection attack (FDIA) is one of the major factors threatening the operational security of power grids. It primarily targets communication links within power grids, misleading the state estimation results of the power system and posing significant risks to grid security. Addressing the challenges of effectively detecting FDIA and the non-positive definite covariance matrix of process noise and measurement noise in power system state estimation, this paper introduces the vector auto-regression (VAR) model into power system state estimation and proposes an FDIA detection method based on VAR and weighted least squares (WLS). Firstly, a VAR state estimation model is established, treating measurement noise as a stable quantity and estimating only process noise, thereby resolving the non-positive definite issue of the covariance matrix. Secondly, both VAR and WLS are used for power system state estimation, and the results of the two methods are detected using consistency checks and measurement residual tests to determine the presence of FDIA. Finally, simulation results from IEEE 14-bus and IEEE 30-bus systems demonstrate that the proposed detection method can successfully detect FDIA with a high success rate, verifying the feasibility and effectiveness of the method.

Key words: false data injection attack;vector auto-regression;weighted least squares;state estimation;attack detection

收稿日期:2022-11-14;**修回日期**:2023-10-10
基金项目:国家自然科学基金(52107108)
通信作者:陈将宏(1979—),男,博士,讲师,主要从事电力系统可靠度分析研究;E-mail:chenjh97@126.com

随着电力系统中信息技术应用的普遍化，电网逐渐融合了信息和物理两大系统，耦合形成了一种电网信息物理系统(grid cyber-physical systems，GCPS)。GCPS的形成，使电力系统的实时分析与决策变得更加便捷、高效[1-4]。但是，由于GCPS的复杂性，且伴随着通信环境的开放，其受到外界攻击的概率也大幅增加，其中最突出的问题就是虚假数据注入攻击(false data injection attack，FDIA)[5]。FDIA会改变电网的状态估计值，致使电网量测数据异常，一旦发生FDIA，将造成控制中心作出错误决策，进而引发安全事故[6-7]。因此，如何准确地对FDIA进行检测是保障GCPS安全可靠运行的关键。

现有能量管理系统中的不良数据检测机制虽然已经具备抵御一些隐蔽性不强的攻击的能力，但当虚假数据具有较强隐蔽性时，以状态预测的残差为指标的传统检测方法往往难以有效检测[8]。

目前，针对FDIA常用的检测方法主要为时间序列类型，其检测流程一般分为两步：一是系统的状态估计[9]，二是攻击的检测[10]。对此，许多专家学者进行了深度研究，并取得了成果[11-19]。文献[11]充分利用历史数据库中可用有效信息，提出了一种基于历史数据的短期状态预测方法，能够有效避免欺诈性数据对状态预测结果的影响，但短期状态预测要求电力系统相邻时刻状态量之间存在关联，因此具有一定的局限性。文献[12]基于优化聚类算法对电网脆弱节点进行分类，再结合自回归模型的状态预测结果进行虚假数据检测，该方法在保持较高的检测率下误检率更小。文献[13]基于改进无迹卡尔曼滤波(untraced kalman filtering，UKF)算法与加权最小二乘法(weighted least squares，WLS)算法之间的状态估计偏差来检测FDIA，该方法虽然对状态值的估计较准确，但是其假设电网过程噪声与量测噪声均服从正态分布，而实际电网中的噪声都是未知的，导致检测效果受影响较大。文献[14]针对自适应卡尔曼滤波状态估计时量测噪声和过程噪声的协方差矩阵非正定问题，提出一种非负定自适应卡尔曼滤波算法，算法中认为量测噪声稳定，只对过程噪声协方差进行估计。文献[15]结合短期预测与动态预测特点，提出一种基于极端梯度提升与无迹卡尔曼滤波的混合预测方法，实验证明其有效提升了状态预测的精度，但是其需要大量的历史数据对系统的日前负荷进行预测，且静态状态估计采用WLS方法获得，无法排除系统干扰可能造成的不良数据误检测。文献[16]提出基于向量自回归模型的电压相角状态估计模型，并在FDIA检测中采用了∞－范数的残差检验指标，但是单一的残差检验仍然无法排除系统突变干扰引起的状态估计偏差。

针对上述问题，本文将VAR模型应用于电力系统状态估计，并提出一种基于VAR与WLS相结合的双重FDIA检测方法。首先，针对电力系统状态估计时量测噪声和过程噪声的协方差矩阵非正定问题，引入向量自回归(vector auto regression，VAR)模型对电力系统进行状态估计，将量测噪声视为稳定量，仅考虑过程噪声的分布特性，构建出基于VAR的状态估计模型，解决2个噪声协方差矩阵非正定问题；其次，针对系统突变干扰造成的误检测以及单一残差检测率低问题，提出一种基于VAR和WLS相结合的FDIA检测方法，利用VAR模型不受参数估计量的一致性约束的特点，避免系统突变干扰造成的误检测，采用状态一致性检验与量测量残差检验的双重检验方式，克服单一残差检测率低的问题。最后，通过IEEE 14节点和IEEE 30节点系统验证，该方法能够有效检测出FDIA。

1 FDIA模型与电力系统状态估计

1.1 FDIA模型

FDIA模型最早由Liu团队于2009年提出[20]。FDIA主要针对电网系统的状态估计过程，通过对电网中信息通信发起攻击，使得系统状态量估计值发生改变。状态估计模型主要分为直流状态估计模型和交流状态估计模型2类。其中直流状态估计模型为

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{\varepsilon} \tag{1}$$

式中，$\boldsymbol{z}$、$\boldsymbol{x}$分别为量测量、状态量；$\boldsymbol{\varepsilon}$为误差；$\boldsymbol{H}$为雅克比矩阵。

若无FDIA时的量测量为$\boldsymbol{z}$，状态量估计值为$\hat{\boldsymbol{x}}$。当系统遭受FDIA后的量测量为$\boldsymbol{z}_{\mathrm{b}}$，状态量估计值为$\hat{\boldsymbol{x}}_{\mathrm{b}}$，攻击向量为$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$，引起的系统误差向量为$\boldsymbol{c}=[c_1,c_2,\cdots,c_n]^{\mathrm{T}}$。此时系统量测量与状态量估计值可表示为

$$\boldsymbol{z}_{\mathrm{b}}=\boldsymbol{z}+\boldsymbol{a} \tag{2}$$

$$\hat{\boldsymbol{x}}_{\mathrm{b}}=\hat{\boldsymbol{x}}+\boldsymbol{c} \tag{3}$$

系统遭受攻击前后的残差为

$$r=\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\|_2 \tag{4}$$

$$r_{\mathrm{b}}=\|\boldsymbol{z}_{\mathrm{b}}-\boldsymbol{H}\hat{\boldsymbol{x}}_{\mathrm{b}}\|_2=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2=\|(\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}})+(\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c})\|_2 \tag{5}$$

式中，r为攻击前的残差；r_b为遭受攻击后的残差；$\|\cdot\|_2$为取2-范数。当攻击向量$\boldsymbol{a}$满足$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$时，根据残差检测FDIA是无效的，此时的攻击向量具有隐蔽性，为理想攻击向量。

1.2　电力系统状态估计

电力系统状态估计主要根据状态方程以及量测方程进行[21]，其中状态方程可表示为

$$\boldsymbol{x}_{k+1}=f(\boldsymbol{x}_k)+\boldsymbol{w}_k \tag{6}$$

式中，$\boldsymbol{x}_k$为k时刻状态量真实值，主要包含系统节点电压幅值与相角；$f(\cdot)$为非线性函数；$\boldsymbol{w}_k$为过程噪声，$\boldsymbol{w}_k\sim N(0,\boldsymbol{Q}_k)$。

量测方程可表示为

$$\boldsymbol{z}_k=h(\boldsymbol{x}_k)+\boldsymbol{v}_k \tag{7}$$

式中，$\boldsymbol{z}_k$为系统量测量实际值，一般有$\boldsymbol{z}_k=[P_i,Q_i,P_{ij},Q_{ij}]^{\mathrm{T}}$，包含系统节点与支路的有功和无功功率；$\boldsymbol{v}_k$为量测噪声，$\boldsymbol{v}_k\sim N(0,\boldsymbol{R}_k)$，本文中电压幅值$R_k=0.005$、电压相角$R_k=0.002$；$h(\cdot)$为非线性函数，具体可表示为

$$\begin{cases}P_i=\sum\limits_{j\in i}V_iV_j(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij})\\ Q_i=\sum\limits_{j\in i}V_iV_j(G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij})\\ P_{ij}=V_i^2g_{ij}-V_iV_j(g_{ij}\cos\theta_{ij}+b_{ij}\sin\theta_{ij})\\ Q_{ij}=-V_i^2(b_{ij}+y_c)-V_iV_j(g_{ij}\sin\theta_{ij}-b_{ij}\cos\theta_{ij})\end{cases} \tag{8}$$

式中，V为节点电压幅值；G_{ij}、B_{ij}为节点导纳矩阵第ij个元素的实部与虚部；g_{ij}、b_{ij}为与节点i连接的并联支路的电导、电纳；y_c为对地导纳。

2　基于VAR的状态估计模型

2.1　VAR模型

VAR模型是一种统计模型，用于解释多个随时间变化的变量之间的关系以及分析随机扰动对变量系统的动态影响，是自回归(auto regressive，AR)模型的扩展。AR模型主要应用于单个变量的问题中，而电力系统状态估计为多变量问题，VAR模型可以将多个变量以向量的形式表示，克服了AR模型的局限性。因此，VAR模型适用于电力系统状态估计问题。

2.1.1　模型表达式

在VAR模型中的每一个变量都有一个与时间相关的方程，具体表示为

$$\boldsymbol{x}_k=\boldsymbol{T}_{k-1}\boldsymbol{x}_{k-1}+\cdots+\boldsymbol{T}_{k-p}\boldsymbol{x}_{k-p}+\boldsymbol{\varepsilon}_k \tag{9}$$

式中，$\boldsymbol{x}$为变量构成的向量，主要包含系统节点电压与幅值等；k表示时间；p为常数；$\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_{k-p}$为滞后向量$\boldsymbol{x}_k$不同时间的量；$\boldsymbol{T}$为时不变参数矩阵，主要包含系统支路阻抗矩阵等；$\boldsymbol{\varepsilon}_k$为$k$时刻的干扰误差项。

2.1.2　滞后期确定

一般的VAR模型主要根据赤池信息量准则(Akaike information criterion，AIC)和贝叶斯信息准则(Bayesian information criterion，BIC)准则来确定其滞后阶数。

$$A_{\mathrm{IC}}=2k-2\ln(L) \tag{10}$$

$$B_{\mathrm{IC}}=k\ln(n)-2\ln(L) \tag{11}$$

式(10)、(11)中，k为模型参数个数；L为似然函数；n为样本数量。由于电力系统状态估计一般采用前一时刻的潮流计算结果对下一时刻进行预测，所以其滞后阶数为$p=1$。

2.2　VAR状态估计模型

电力系统FDIA检测关键在于对系统状态量的估计，根据状态方程与量测方程可知，预测$k+1$时刻的状态量估计值需要已知k时刻状态量，因此状态估计为典型的时间序列预测问题。当VAR模型的滞后期$p=1$，采用线性状态估计时，状态方程如下：

$$\hat{\boldsymbol{x}}_{k+1}=\boldsymbol{T}_k\hat{\boldsymbol{x}}_k+\boldsymbol{w}_{k+1} \tag{12}$$

式中，$\hat{\boldsymbol{x}}_{k+1}$为状态量预测值；$\boldsymbol{T}_k$为参数矩阵；$\hat{\boldsymbol{x}}_k$为$k$时刻的状态量估计值，其维数为$n\times 1$；$\boldsymbol{w}_{k+1}$为系统误差，等效为均值为0的高斯白噪声。

根据式(12)，同时求其等式两边数学期望，得到状态量预测值$\hat{\boldsymbol{x}}_{k+1}$的协方差矩阵$\boldsymbol{R}_{\hat{x}_{k+1}}$如下：

$$\boldsymbol{R}_{\hat{x}_{k+1}}=\boldsymbol{T}_k\boldsymbol{R}_{\hat{x}_k}\boldsymbol{T}_k^{\mathrm{T}}+\boldsymbol{R}_{\hat{\boldsymbol{w}}_{k+1}} \tag{13}$$

$$\boldsymbol{R}_{\hat{x}_k}=E[(\boldsymbol{x}_k-\hat{\boldsymbol{x}}_k)\cdot(\boldsymbol{x}_k-\hat{\boldsymbol{x}}_k)^{\mathrm{T}}] \tag{14}$$

$$\boldsymbol{R}_{\boldsymbol{w}_{k+1}}=E(\boldsymbol{w}_k\boldsymbol{w}_{k+1}) \tag{15}$$

式(13)～(15)中，$\boldsymbol{R}_{\hat{x}_k}$为$k$时刻系统的状态量预测误差矩阵，服从正态分布；$E(\cdot)$为期望算子；根据$\boldsymbol{R}_{\hat{x}_k}$与$\boldsymbol{w}_k$均服从正态分布，故$\boldsymbol{R}_{\hat{x}_{k+1}}$也服从正态分布，由此，$k+1$时刻的系统量测量的预测值可根据$k+1$时刻的系统状态量预测值求得。

考虑量测噪声与过程噪声两者协方差矩阵之间的非正定问题，本文将量测噪声视为稳定量，状态估计过程只对过程噪声进行估计，则状态估计的量测方程变为如下：

$$\hat{\boldsymbol{z}}_{k+1}=\boldsymbol{H}\hat{\boldsymbol{x}}_{k+1} \tag{16}$$

根据式(16)可求量测量的预测误差协方差矩阵：

$$\mathrm{Cov}(\hat{\boldsymbol{z}}_{k+1})=\boldsymbol{H}\mathrm{Cov}(\hat{\boldsymbol{x}}_{k+1})\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{H}\boldsymbol{R}_{\hat{\boldsymbol{x}}_{k+1}}\boldsymbol{H}^{\mathrm{T}} \quad (17)$$

式中，Cov(•)为求协方差矩阵算子。

量测量估计值与实际值之间的残差为

$$r=\|\boldsymbol{z}_k-\hat{\boldsymbol{z}}_k\|_2 \quad (18)$$

3 FDIA检测方法

根据虚假数据攻击模型可知，当攻击向量为理想攻击向量时，传统方法基于2－范数的残差检验将无法检测出残差。而采用加权最小二乘法的状态估计方法，对虚假数据具有较强的“敏感性”，注入一个强度较低的攻击向量，基于加权最小二乘法检测出的残差值都将很大[22]。

在文献[13]中，采用UKF等与WLS相结合的FDIA检测方法，验证了一致性检验与残差检验的双重检测方法的有效性。但是在状态量突变时UKF检测方法预测效果较差，需用量测量进行修正，此时若量测量存在虚假数据，FDIA检测的误检率将大幅上升。而VAR模型由于其解释变量中不包含当期变量，不用考虑参数估计量的一致性问题，故不受状态量突变影响，误检率更低。同时，基于UKF的检测方法假设电网过程噪声与量测噪声均服从正态分布，导致状态估计存在较大不确定性，而VAR模型中将量测噪声视为稳定量，仅对过程噪声进行估计，与UKF方法相比，其状态估计更精准。鉴于此，本文提出并采用基于VAR和WLS的状态一致检验与量测量残差检验相结合的双重FDIA检测方法。FDIA检测流程如图1所示。

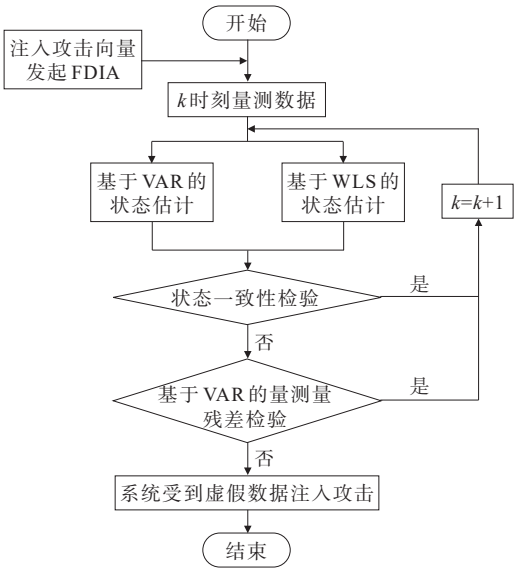


图1 FDIA检测流程

Figure 1 Detection process of FDIA

图1中的状态一致性检验按照如下：

$$\|\hat{\boldsymbol{x}}^{\mathrm{VAR}}-\hat{\boldsymbol{x}}^{\mathrm{WLS}}\|_2\leqslant\tau \quad (19)$$

式中，$\hat{\boldsymbol{x}}^{\mathrm{VAR}}$与$\hat{\boldsymbol{x}}^{\mathrm{WLS}}$分别为2种方法的状态量估计值；$\tau$为状态一致性检验阈值。考虑电网的其他因素干扰造成误检测，取VAR预测的量测值进行残差检验，其残差计算按式(18)进行，残差检验满足：

$$r\leqslant\tau_{k,a^2} \quad (20)$$

式中，τ_{k,a^2}为卡方检测阈值。

当系统遭受不良数据注入攻击时，2种方法得到的状态估计值相差较大，在状态一致性检验中会远大于其检验阈值。此时为了排除电网突变干扰的影响，需要对VAR预测的量测值进行残差检验，当残差检验也大于其卡方检测阈值时，则认定系统遭受虚假数据注入攻击。否则认为是系统突变干扰，系统没有遭受虚假数据注入攻击。其具体检测步骤如下：

1）在k时刻，对电力系统进行潮流计算，取计算结果作为初始状态量真值；

2）对初始状态量真值添加高斯分布扰动误差，得到量测值真值；

3）采用WLS方法和VAR方法对系统进行状态估计，得出2种方法下的状态量估计值与量测量预测值；

4）采用状态一致性检验与量测量残差检验的双重检验方式对状态估计结果进行诊断。

4 算例分析

本文采用MATLAB 2020a平台，结合MATPOWER 7.1电力系统仿真数据包进行算例分析。由于发起FDIA需要对电力系统相应的量测量进行攻击，往往系统越复杂，发起攻击越困难，因此选取IEEE 14和IEEE 30节点进行仿真实验。首先对2个系统进行潮流计算，得到状态量真值，再在其基础上加上量测误差得到系统量测量真值。

4.1 VAR状态估计性能分析

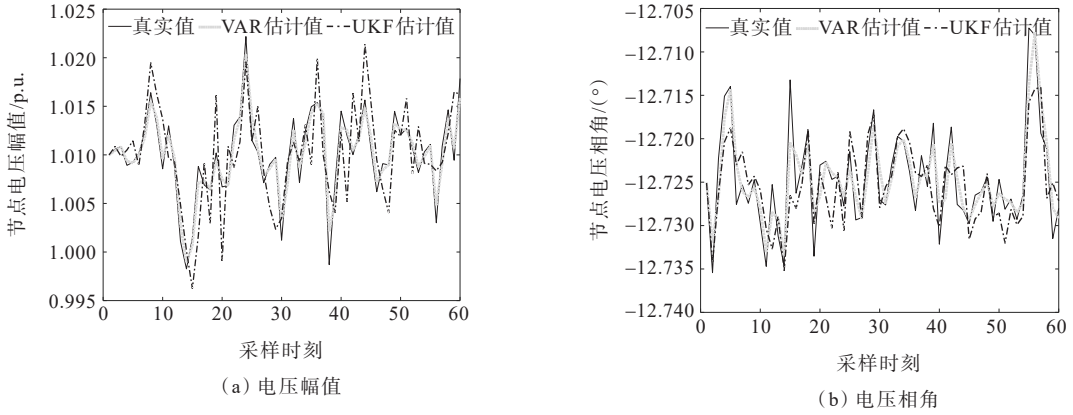
电网运行时的负荷存在一定的波动，为模拟真实情况，对其加入随机噪声。选取IEEE 14节点系统的3号节点作为研究对象。采样时刻设置为60个点。在无FDIA时，分别采用本文VAR方法与UKF方法对3号节点电压幅值和相角进行状态估计，对比分析2种估计方法的性能。60个采样时刻的3号节点电压幅值与相角估计值如图2所示。

可以看出，与UKF方法相比，VAR方法的状态估计值更加精确，更接近真实值。为更加直观地展示VAR状态估计与UKF方法的优劣，采用均方根误差作为其评价指标，其计算公式为

$$e_{\mathrm{MSE}}(k)=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(\hat{\boldsymbol{x}}_{k,i}-\boldsymbol{x}_{k,i})^2} \tag{21}$$

式中，N为维数；$\hat{\boldsymbol{x}}_{k,i}$为估计值的第$k$个采样时刻第$i$个分量值；$\boldsymbol{x}_{k,i}$为真实值的第$k$个采样时刻第$i$个分量值。

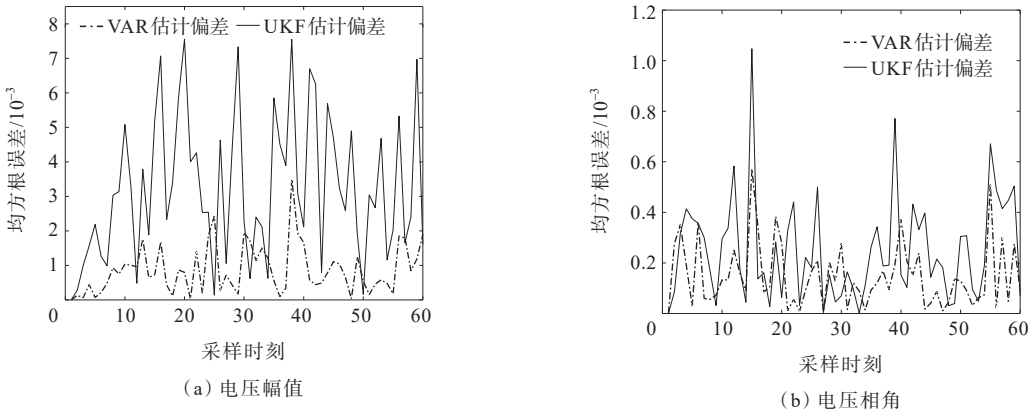
节点3电压幅值与相角均方根误差如图3所示，可以看出在60个采样时刻下，本文所提VAR估计方法下的估计偏差水平明显低于UKF方法估计结果。



(a) 电压幅值　　(b) 电压相角

图2　无FDIA时电压幅值与相角状态估计

Figure 2　Estimation of voltage amplitude and phase angle state without FDIA



(a) 电压幅值　　(b) 电压相角

图3　电压幅值与相角均方根误差

Figure 3　RMS error of voltage amplitude and phase angle

为了定量比较2种方法的估计效果，统计60个采样时刻下的估计值平均偏差如表1所示。

表1　2种算法平均偏差对比

Table 1　Comparison of average deviation between two algorithms

算法	平均电压偏差	平均相角偏差
UKF	0.003 9	0.004 1
VAR	0.001 1	0.002 5

根据表1可知，通过VAR算法得到的状态估计值，其均方根误差小于UKF，尤其是电压幅值估计。说明VAR算法状态估计的精度更高，因此，其更加适用于FDIA检测过程中。

4.2　FDIA检测与分析

以文献[22]中的虚假数据攻击向量为基础，利用所提算法分别对2个系统进行仿真分析，通过状态估计得到的状态量估计值与量测量预测值分别能够符合状态一致性检验与量测量残差检验标准，以验证本文所提检测模型的可行性及有效性。当状态估计结果同时不满足状态一致性检验与量测量残差检验时，才判定系统遭受FDIA。当仅不满足状态一致性检验时，认为其是系统波动干扰引起的误差，系统没有遭受FDIA。

4.2.1　IEEE 14节点系统仿真分析

IEEE 14节点系统含有14个节点、20条支路、

状态量包含电压幅值与相角各14个、量测量41个，在无FDIA时，系统电压幅值与电压相角如图4、5所示。

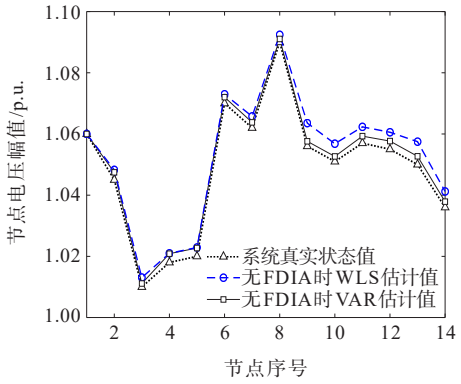


图4 无FDIA时电压幅值估计对比

Figure 4 Comparison of voltage amplitude estimation without FDIA

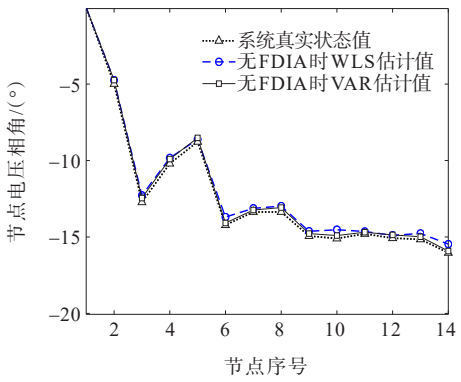


图5 无FDIA时电压相角估计对比

Figure 5 Comparison of voltage phase angle estimation without FDIA

由图4、5可以看出，在攻击发生之前，2种方法均能够较好地对系统状态进行估计，各状态量估计值与系统真实值趋势变化保持一致。此时的系统状态量估计值残差为0.101 6。进行状态一致性检验，其值为0.275 8，此时的检验阈值取1.905 9，满足状态一致性检验要求，故判定无FDIA。

为模拟系统遭受FDIA的情况，选取文献[16]中IEEE 14节点系统攻击向量对系统发起攻击。电网在遭受FDIA后的电压幅值与相角估计值分别如图6、7所示。

由图6、7可知，攻击发生后，WLS状态估计值虽然变化较大，但其分布情况仍然与系统初始状态值分布情况基本保持一致，攻击后的状态估计的残差由攻击前的0.101 6变为0.133 9，变化非常小。

在状态一致性检验中，检验值由攻击前的0.278 5变为7.668 7，变化非常明显，大于阈值1.905 9。根据式(20)对预测的量测量进行残差检验，以判断系统状态量变化是否由系统波动干扰造成。当显著性水平为0.5时，IEEE 14节点量测量残差检测阈值为13.339，而攻击后的量测量残差为14.156 3，大于此时的检测阈值，说明系统所受影响不是由系统波动干扰造成的，判定系统遭受FDIA。综上，在状态一致性检验与量测量残差检验共同检验下，可以对FDIA进行有效检测。攻击前后的状态一致性检验值与量测量残差检验值如表2所示。

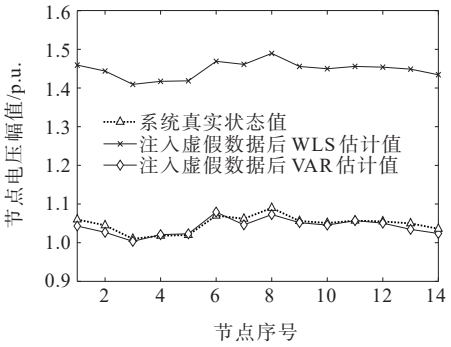


图6 有FDIA时电压幅值估计对比

Figure 6 Comparison of voltage amplitude estimation with FDIA

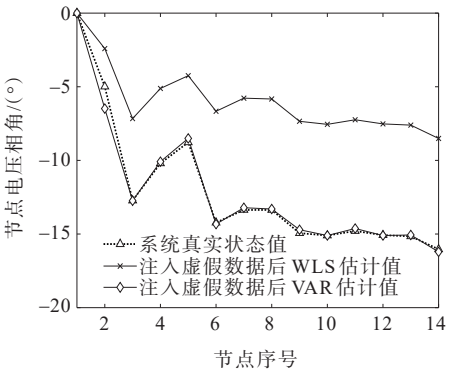


图7 有FDIA时电压相角估计对比

Figure 7 Comparison of voltage phase angle estimation with FDIA

表2 IEEE 14节点检测结果统计

Table 2 Detection results for IEEE 14-node

检测项目	检测阈值	攻击前	攻击后
状态量残差		0.101 6	0.133 9
状态一致性检验	1.905 9	0.275 8	7.668 7
量测量残差检验	13.339 0		14.156 3
检测结果		无FDIA	有FDIA

4.2.2　IEEE 30节点系统仿真分析

为了进一步验证所提方法的适用性，选取IEEE 30节点系统进行检验，系统含有30个节点、41条支路，状态量包含电压幅值与相角各30个、量测量93个，系统无FDIA情况下WLS状态估计和VAR的状态估计结果如图8、9所示。

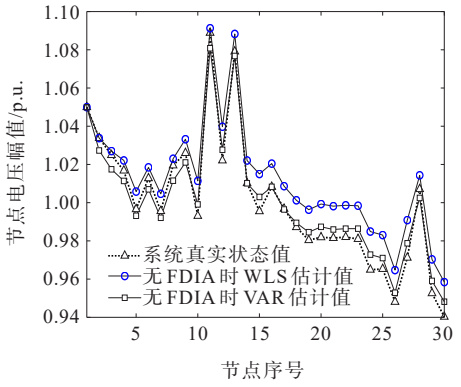


图8　无FDIA时电压幅值估计对比

Figure 8　Comparison of voltage amplitude estimation without FDIA

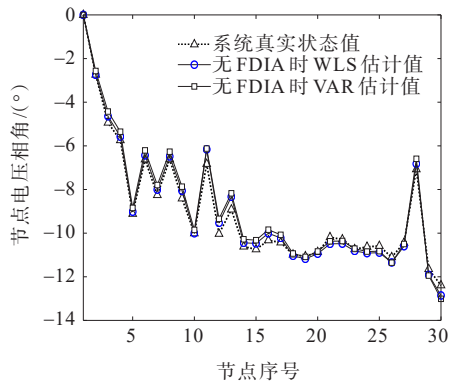


图9　无FDIA时电压相角估计对比

Figure 9　Comparison of voltage phase angle estimation without FDIA

由图8、9可以看出，在攻击发生之前的系统状态量估计值残差为0.615 2。进行状态一致性检验，其值为0.152 0，此时的检验阈值取2.697 3，满足状态一致性检验要求，故判定无FDIA。

为了模仿系统遭受FDIA，选取文献[22]中IEEE 30节点系统模拟攻击向量对系统发起攻击。电网在遭受FDIA后的电压幅值估计值如图10所示，电压相角估计值如图11所示。

由图10、11可以看出，攻击后的状态估计的残差由攻击前的0.615 2变为1.333 5，变化仍然不大，处于阈值范围之内，而系统的电压幅值与相角均已发生变化，说明攻击向量对系统成功进行攻击。

进行状态一致性检验，状态一致性检验值由攻击发生前的0.152 0变为5.087 8，差异非常明显，且大于此时的状态一致性检测阈值2.697 3。根据式(20)对预测的量测量进行残差检验，以判断系统状态量变化是否由系统波动干扰造成。当显著性水平为0.5时，IEEE 30节点量测量残差检测阈值为29.34，而攻击后的量测量残差为33.803 0，大于此时的检测阈值，说明系统所受影响不是由系统波动干扰造成的，判定系统遭受FDIA。综上，在状态一致性检验与量测量残差检验共同检验下，可以对FDIA进行有效的检测。攻击前后的状态一致性检验值与量测量残差检验值如表3所示。

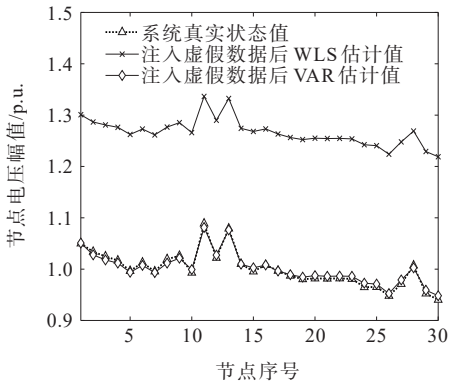


图10　有FDIA时电压幅值估计对比

Figure 10　Comparison of voltage amplitude estimation with FDIA

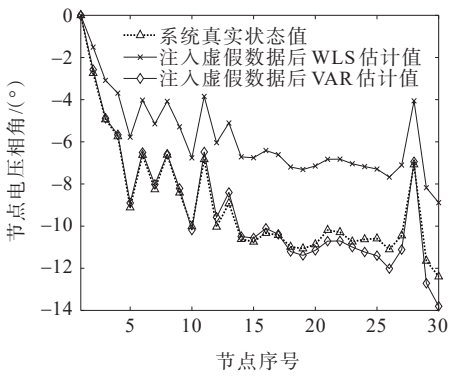


图11　有FDIA时电压相角估计对比

Figure 11　Comparison of voltage phase angle estimation with FDIA

表3　IEEE 30节点检测结果统计

Table 3　Detection results for IEEE 30-node

检测项目	检测阈值	攻击前	攻击后
状态量残差		0.615 2	1.333 5
状态一致性检验	2.697 3	0.152 0	5.087 8
量测量残差检验	29.340 0		33.803 0
检测结果		无FDIA	有FDIA

4.3 检测效果分析

为探究本文检测方法的有效性，以文献[13]随机虚假数据注入攻击模型为基础，在IEEE 30节点系统中进行仿真，随机虚假数据注入攻击可以对任意状态量进行攻击。分别在不同的误检率下对比不同检测方法的效果，包含基于UKF的检测方法，基于短期状态预测的检测方法和本文检测方法。3种检测方法下接收者操作特征（receiver operating characteristic，ROC）曲线如图12所示。

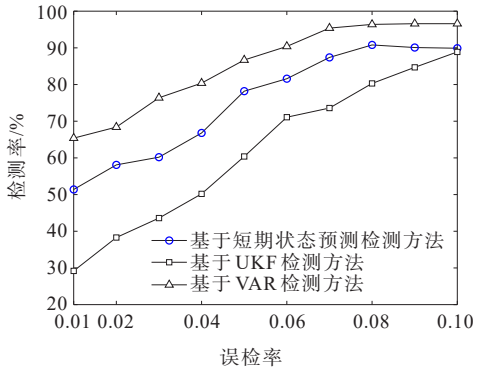


图12 3种检测方法ROC曲线对比

Figure 12 Comparison of ROC curves among three detection methods

根据图12可知，本文所提基于VAR的检测方法相比于基于短期状态预测和基于UKF的检测方法在误检率相同时具有更高的检测率，进一步说明本文所提检测方法具有一定的优越性，能够有效检测到FDIA，且检测率较高。

5 结语

针对GCPS面临的FDIA，本文基于VAR模型提出了一种FDIA检测方法，并利用IEEE 14和IEEE 30节点系统进行仿真分析，得出以下结论：

1）在无FDIA情况下，采用基于VAR模型的状态估计方法对电力系统进行状态估计较UKF方法估计效果更好，精度更高；

2）采用基于VAR与WLS的状态一致性检验方法和基于VAR量测量预测值的残差检验方法的双步检验，解决了单一残差检验的高误检率问题，能够有效检测到系统是否受到FDIA，说明了所提检测方法的有效性；

3）在相同的误检率下，本文方法的检测成功率高于现有基于UKF的检测方法和基于短期状态预测的方法。

参考文献：

[1] 周孝信,鲁宗相,刘应梅,等.中国未来电网的发展模式和关键技术[J].中国电机工程学报,2014,34(29):4999-5008.
ZHOU Xiaoxin, LU Zongxiang, LIU Yingmei, et al. Development models and key technologies of future grid in China[J].Proceedings of the CSEE,2014,34(29):4999-5008.

[2] 张晶,陈垚,孙俊,等.基于协同执行器的GCPS自适应调度模型[J].系统仿真学报,2019,31(10):2112-2121.
ZHANG Jing,CHEN Yao,SUN Jun,et al.GCPS adaptive scheduling model based on cooperative executor[J]. Journal of System Simulation,2019,31(10):2112-2121.

[3] 蔡文亮,赵正晖,汪洋,等.面向新型能源结构的系统调频技术回顾与展望[J].电测与仪表,2023,60(10):1-9.
CAI Wenliang, ZHAO Zhenghui, WANG Yang, et al. Review and prospect of frequency modulation technology for new energy structure[J]. Electrical Measurement & Instrumentation,2023,60(10):1-9.

[4] 李晓,许剑冰,李满礼,等.考虑信息失效影响的配电网信息物理系统安全性评估方法[J].中国电力,2022,55(2):73-81.
LI Xiao, XU Jianbing, LI Manli, et al. A security evaluation method for cyber physical distribution system considering influence of information failure[J]. Electric Power,2022,55(2):73-81.

[5] 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.

[6] 彭大天,董建敏,蔡忠闽,等.假数据注入攻击下信息物理融合系统的稳定性研究[J].自动化学报,2019,45(1):196-205.
PENG Datian, DONG Jianmin, CAI Zhongmin, et al. On the stability of cyber-physical systems under false data injection attacks[J]. Acta Automatica Sinica, 2019, 45(1): 196-205.

[7] 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.

[8] 武津园,王勇,刘丽丽,等.电力假数据注入攻击的残差检测方法效率分析[J].上海电力大学学报,2020,36(6):591-597.
WU Jinyuan, WANG Yong, LIU Lili, et al. Efficiency

analysis of residual detection method for power false data injection attack[J]. Journal of Shanghai University of Electric Power,2020,36(6):591-597.

[9] 李振华,陶渊,赵爽,等.智能配电网状态估计方法研究现状分析[J].电力科学与技术学报,2019,34(1):115-122.
LI Zhenhua, TAO Yuan, ZHAO Shuang, et al. Research situation analysis of state estimation in smart distribution networks[J]. Journal of Electric Power Science and Technology,2019,34(1):115-122.

[10] 罗小元,潘雪扬,王新宇,等.基于自适应Kalman滤波的智能电网假数据注入攻击检测[J].自动化学报,2022,48(12):2960-2971.
LUO Xiaoyuan, PAN Xueyang, WANG Xinyu, et al. Detection of false data injection attack in smart grid via adaptive Kalman filtering[J]. Acta Automatica Sinica, 2022,48(12):2960-2971.

[11] 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.

[12] XU R Z,WANG R,GUAN Z T,et al.Achieving efficient detection against false data injection attacks in smart grid [J].IEEE Access,2017,5:13787-13798.

[13] 魏利胜,张倩.基于改进的UKF智能电网虚假数据攻击检测[J].系统仿真学报,2023,35(7):1508-1516.
WEI Lisheng, ZHANG Qian. Detection of false data injection attack in smart grid based on improved UKF[J]. Journal of System Simulation,2023,35(7):1508-1516.

[14] 许浩文,郭观凯,余玲玲,等.基于非负定自适应卡尔曼滤波的电力系统虚假数据攻击检测[J].科学技术与工程,2020,20(9):3611-3616.
XU Haowen, GUO Guankai, YU Lingling, et al. Nonnegative-definite adaptive Kalman filter-based detection of false data attack in power system[J].Science Technology and Engineering,2020,20(9):3611-3616.

[15] 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.

[16] CHEN Y, HAYAWI K, ZHAO Q, et al. Vector auto-regression-based false data injection attack detection method in edge computing environment[J].Sensors,2022, 22(18):6789.

[17] 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.

[18] 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.

[19] 方陈,姚维强,魏新迟,等.考虑节点时空相关性的有限配电网PMU装置优化部署[J].电网与清洁能源,2023,39(8):105-115.
FANG Chen, YAO Weiqiang, WEI Xinchi, et al.Optimal placement of limited distribution PMU considering spatiotemporal correlation of nodes[J]. Power System and Clean Energy, 2023, 39(8): 105-115.

[20] LIU Y,NING P,REITER M K.False data injection attacks against state estimation in electric power grids[C]// Proceedings of the 16th ACM conference on Computer and Communications Security. Chicago Illinois USA. ACM,2009:21-32.

[21] 潘浩,卫志农,黄蔓云,等.基于时域模型的电–气综合能源系统分布式鲁棒状态估计[J].电力系统自动化,2023,47(17):89-98.
PAN Hao, WEI Zhinong, HUANG Manyun, et al. Distributed robust state estimation of integrated electricity-gas system based on time-domain model[J]. Automation of Electric Power Systems,2023,47(17):89-98.

[22] 常盛.考虑虚假数据攻击的电力信息物理系统检测方法研究[D].秦皇岛:燕山大学,2020.
CHANG Sheng.Research on detection method of power cyber-physical system considering false data attacks[D]. Qinhuangdao:Yanshan University,2020.