Journal of System Simulation

Volume 35 | Issue 7 Article 8

8-25-2023

Detection of False Data Injection Attack in Smart Grid Based on Improved UKF

Lisheng Wei
Anhui Key Laboratory of Electric Drive and Control, Wuhu 241000, China; School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China, shwei_11@163.com

Qian Zhang
School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China

Detection of False Data Injection Attack in Smart Grid Based on Improved UKF

Abstract

Abstract: Due to the disruption and threat of false data injection attack (FDIA) on grid cyber-physical systems (GCPS), and to address the problem that false data is difficult to be detected, *a method for smart grid false data detection based on weighted least squares (WLS) and improved unscented Kalman filter (UKF) is proposed.* FDIA is modeled mathematically, and the residual analysis shows that the FDIA is difficult to be detected. In the case of the injection attack vector, the improved UKF is applied to state estimation. Meanwhile, the state estimation of the system is performed by the WLS, which is sensitive to the changes in the system. The results of the state estimation of the above two methods are used to execute a consistency test, and the situation of the FDIA is accurately determined based on the test results. Experimental analysis was conducted on the IEEE14 and IEEE57 systems and the detection rate was compared with the detection method of the support vector machine. The simulation results indicate that the FDIA can be detected accurately, thus the feasibility and effectiveness of the proposed method are demonstrated.

Keywords

smart grid, FDIA, improved UKF, state estimation, attack detection

Recommended Citation

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.

第 35 卷第 7 期 系统仿真学报© Vol. 35 No. 7
2023 年 7 月 Journal of System Simulation Jul. 2023

基于改进的UKF智能电网虚假数据攻击检测

魏利胜[1,2]，张倩[2]
(1. 安徽省电气传动与控制重点实验室，安徽 芜湖 241000；2. 安徽工程大学 电气工程学院，安徽 芜湖 241000)

摘要：由于虚假数据注入攻击(false data injection attack，FDIA)对电力信息物理系统(grid cyber-physical systems，GCPS)的破坏性较强，且威胁性较大，针对其难以被有效检测难题，*提出一种基于加权最小二乘法(weighted least squares，WLS)和改进的无迹卡尔曼(unscented Kalman filter，UKF)的电网虚假数据检测方法*。对FDIA进行了数学建模，并通过对残差进行分析以说明FDIA的难以检测性，在有攻击向量的情况下，将改进的UKF用于系统的状态估计，同时利用WLS对系统迅速响应的优势，也对系统进行状态估计，采用一致性检验对2种方法的估计结果进行检测，最终判断是否存在FDIA。在IEEE14节点和IEEE57节点上进行实验分析并与支持向量机的检测方法进行检测成功率的对比，仿真结果表明，FDIA可被准确检测，从而验证了本文方法的可行性及有效性。

关键词：智能电网；虚假数据注入攻击；改进的无迹卡尔曼；状态估计；攻击检测
中图分类号：TM73；TP391 文献标志码：A 文章编号：1004-731X(2023)07-1508-09
DOI: 10.16182/j.issn1004731x.joss.22-0292
引用格式: 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.
Reference format: 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.

Detection of False Data Injection Attack in Smart Grid Based on Improved UKF

Wei Lisheng[1,2], *Zhang Qian*[2]
(1. Anhui Key Laboratory of Electric Drive and Control, Wuhu 241000, China;
2. School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China)

Abstract: Due to the disruption and threat of false data injection attack (FDIA) on grid cyber-physical systems (GCPS), and to address the problem that false data is difficult to be detected, *a method for smart grid false data detection based on weighted least squares (WLS) and improved unscented Kalman filter (UKF) is proposed.* FDIA is modeled mathematically, and the residual analysis shows that the FDIA is difficult to be detected. In the case of the injection attack vector, the improved UKF is applied to state estimation. Meanwhile, the state estimation of the system is performed by the WLS, which is sensitive to the changes in the system. The results of the state estimation of the above two methods are used to execute a consistency test, and the situation of the FDIA is accurately determined based on the test results. Experimental analysis was conducted on the IEEE14 and IEEE57 systems and the detection rate was compared with the detection method of the support vector machine. The simulation results indicate that the FDIA can be detected accurately, thus the feasibility and effectiveness of the proposed method are demonstrated.

Keywords: smart grid; FDIA; improved UKF; state estimation; attack detection

收稿日期：2022-03-30 修回日期：2022-06-30
基金项目：安徽省教育厅重大项目(KJ2020ZD39)；安徽省检测技术与节能装置重点实验室开放基金(DTESD2020A02)
第一作者：魏利胜(1978-)，男，教授，博士，研究方向为图像识别与应用、嵌入式仪器仪表及系统。E-mail：lshwei_11@163.com

0 引言

在电力系统中，伴随着自动化、控制工程、计算机、通信等技术的不断发展，信息系统、物理系统两大系统联系愈加紧密，耦合形成了一种新的系统——电力信息物理系统，有助于电力系统的实时分析与科学决策[1]。但是，由于信息物理系统是复杂且多样的，与此同时由于通信环境的开放，通信网络或信息设备收到攻击的概率大幅增加，故而电力系统的可靠性也受到了威胁性[2]。虚假数据注入攻击(false data injection attacks，FDIA)会改变电网状态的估计值，使得数据的完整性遭受到一定程度的破坏，因此其属于需要防范的攻击，一旦发生FDIA，将造成控制中心作出错误决断，进而会引发威胁性很大的安全事故[3]。因此，对FDIA的检测问题十分重要。

FDIA是目前恶意攻击的典型代表，专家学者对其进行了深度研究并有了许多成果[4]。FDIA的问题，大致可以从建模、防御和检测三个角度划分。文献[5]提出一种攻击者在无法得知电网的全部拓扑信息及参数的情况下FDIA的建模，当前基于针对FDIA的检测是利用正常数据和虚假数据的特征来进行区分的。文献[6]提出一种基于卡尔曼滤波计算攻击前后残差序列巴氏距离的方法，该方法的不足之处在于FDIA的残差是保持不变的，因而巴氏距离无法判别。文献[7]使用$H\infty$范数来检测随机的攻击，但是该方法的检测准确率过于依赖于阈值的设置，效果较差。文献[8]利用卡尔曼滤波和目标函数进行检测，该方法不需要经过复杂的训练，就可以较快地检测出FDIA。文献[9]提出一种改进的卡尔曼滤波算法，准确地估计出了系统中的未知噪声，实验证明了该方法的适用性较强。文献[10]通过数据递归来进行FDIA的检测，该方法需要的计算配置较低，并能够较为有效地预测出攻击，但是扩展卡尔曼的雅可比矩阵求解并不容易。

在以上文献的基础上，状态估计的方法可以考虑运用到检测方向。在电力系统中，状态估计可以划分为静态和动态两种，其中静态方法已经较为成熟。然而由于没有考虑到系统的动态性，因此局限性较大[11]。而卡尔曼滤波器能够动态地进行状态估计和预报，且跟踪性较强，因此大量学者对其进行了研究[12-14]。本文在以上研究的基础上，针对卡尔曼在非线性系统中的估计不适应的问题，提出了一种基于最小二乘法(weight least squares, WLS)和改进的(unscented Kalman filter, UKF)的虚假数据注入攻击检测方法。首先，利用WLS和改进的UKF对电网的状态量进行估计，通过对估计结果进行判断从而检测是否有攻击的产生；其次，在MATPOWER的IEEE14节点与IEEE57节点进行验证，结果确认了该方法检测FDIA的可行性；最后与支持向量机的方法进行检测率的对比，验证了本文所提方法的有效性。

1 问题描述

1.1 FDIA

FDIA具有很强的威胁性，其模型在2009年被创建出来[15]。针对电网系统中的状态估计，一旦攻击者掌握了部分信息，此类攻击便具有将任意一个错误引入系统中特定状态变量的能力，再想对其进行准确检测具有一定的挑战性。

直流状态估计模型可表示为

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

式中：$\boldsymbol{z}$，$\boldsymbol{x}$及$\boldsymbol{e}$分别为量测量，状态量和误差；$\boldsymbol{H}$为雅克比矩阵。

在攻击前，量测量为$\boldsymbol{z}$，估计的状态向量表示为$\hat{\boldsymbol{x}}$。假设电网系统遭到了虚假数据的注入攻击，令正在被攻击的量测量为$\boldsymbol{z}_{\mathrm{f}}$，估计的状态向量表示为$\hat{\boldsymbol{x}}_{\mathrm{f}}$，在量测量中注入$m$维攻击向量$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]$，FDIA引起的误差向量表示为$\boldsymbol{c}=[c_1,c_2,\cdots,c_n]$。那么此时的量测量可以表示为$\boldsymbol{z}_{\mathrm{f}}=\boldsymbol{z}+\boldsymbol{a}$，而估计的状态向量表示为$\hat{\boldsymbol{x}}_{\mathrm{f}}=\hat{\boldsymbol{x}}+\boldsymbol{c}$。用最大标准化残差的方法来表示攻击前和攻击后的残差，

分别用r和r_{f}来表示：

攻击前：

$$r=\left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\right\| \tag{2}$$

攻击后：

$$r_{\mathrm{f}}=\left\|\boldsymbol{z}_{\mathrm{f}}-\boldsymbol{H}\hat{\boldsymbol{x}}_{\mathrm{f}}\right\|=\left\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\right\|=\left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\right\| \tag{3}$$

对比式(2)，(3)可得，当攻击向量$\boldsymbol{a}$满足$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$时，残差在遭受攻击前后没有变化，表明传统的残差检验很难在关键时刻被“委以重任”。$\boldsymbol{a}$为理想的攻击向量，达到了隐蔽型FDIA的效果。

1.2 状态方程的辨识

电力系统的状态方程为

$$x_{k+1}=f(x_k)+\boldsymbol{w}_k \tag{4}$$

式中：k为时刻；在k时刻的状态变量用$\boldsymbol{x}_k$表示，一般在电力系统中，状态变量包含电压幅值与相角，即$\boldsymbol{x}_k=[V_k,\theta_k]^{\mathrm{T}}$；$f(\cdot)$为非线性函数；$\boldsymbol{w}_k$为系统过程噪声，$\boldsymbol{w}_k\sim(0,Q_k)$，其中，$Q_k$为协方差。

为降低识别系统的状态方程时占用的内存，本文采用Holt两参数法来平滑指数，该方法对电网系统的短期负荷预测表现不俗，求解速度快为其优势[16]。假设系统在k时刻，$x_{k|k-1}$为状态的预测值，$\hat{x}_k$为系统估计值，对$k+1$时刻进行预测，则数值大小为

$$x_{k+1|k}=a_k+b_k \tag{5}$$

$$a_k=\alpha_{\mathrm{H}}x_k+(1-\alpha_{\mathrm{H}})x_{k|k-1} \tag{6}$$

$$b_k=\beta_{\mathrm{H}}(a_k-a_{k-1})+(1-\beta_{\mathrm{H}})b_{k-1} \tag{7}$$

式中：a_k为水平分量；b_k为倾斜分量；α_{H}和β_{H}为平滑参数，通常介于[0, 1]，在本文中，$\alpha_{\mathrm{H}}=0.85$，$\beta_{\mathrm{H}}=0.05$；

1.3 量测方程

电力系统的量测方程描述为

$$\boldsymbol{z}_k=h(\boldsymbol{x}_k)+\boldsymbol{v}_k \tag{8}$$

式中：$\boldsymbol{z}_k$为k时刻的量测量，$\boldsymbol{z}_k=[P_i,Q_i,P_{ij},Q_{ij}]^{\mathrm{T}}$，其中，$P_i$，$Q_i$，$P_{ij}$，$Q_{ij}$为节点$i$与支路$ij$的有功和无功功率；$h(\cdot)$为非线性函数；$v_k$为系统量测噪声，$v_k\sim(0,R_k)$。

具体的$h(\cdot)$可描述为

$$\begin{cases}P_i=\sum\limits_{j\in i}V_iV_j(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij})\\ Q_i=\sum\limits_{j\in i}V_iV_j(G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij})\\ P_{ij}=V_i^2g_{ij}-V_iV_jg_{ij}\cos\theta_{ij}-V_iV_jb_{ij}\sin\theta_{ij}\\ Q_{ij}=-V_i^2(b_{ij}+y_{\mathrm{c}})-V_iV_jg_{ij}\sin\theta_{ij}-V_iV_jb_{ij}\cos\theta_{ij}\end{cases} \tag{9}$$

式中：V_i，V_j为电压幅值；G_{ij}，B_{ij}分别为支路ij导纳元素中的实部与虚部；g_{ij}，b_{ij}分别为支路ij的电导与电纳；y_{c}是对地导纳。

1.4 改进的无迹卡尔曼滤波原理

电网系统经常表现出复杂的非线性问题，针对此，常见的改进滤波策略为扩展卡尔曼滤波(extended Kalman filter, EKF)方法，研究结果表明，结构简单为该算法的显著特点，与之相对，其缺点也相对明显，如计算量仍然较大，鲁棒性和估计精度都较低，且由于采用的是现行的函数，滤波器存在发散的可能。针对EKF算法所展现的不足，本文采用UKF方法，并利用文献[17]的方法对其进行改进。

(1) UT变换过程

对于非线性系统$\boldsymbol{y}=f(\boldsymbol{x})$，$\boldsymbol{x}$是状态向量，大小为$n$维，平均值为已知$\bar{\boldsymbol{x}}$，已知方差$\boldsymbol{P}$，使用UT变换构造出$2n+1$个Sigma点，并获取这些点相应的权值，即可能求出y的统计特性。

首先，对称采样求Sigma点集：

$$\boldsymbol{\chi}_i=\begin{cases}\bar{\boldsymbol{x}},\ i=0\\ \bar{\boldsymbol{x}}+[\sqrt{(n+\lambda)\boldsymbol{P}}]_i,\ i=1,2,\cdots,n\\ \bar{\boldsymbol{x}}-[\sqrt{(n+\lambda)\boldsymbol{P}}]_i,\ i=n+1,n+2,\cdots,2n\end{cases} \tag{10}$$

式中：$(\sqrt{\boldsymbol{P}})^{\mathrm{T}}(\sqrt{\boldsymbol{P}})=\boldsymbol{P}$，$(\sqrt{\boldsymbol{P}})_i$为矩阵方根的第$i$列。

然后，计算出采样点相对应的权值为

$$\begin{cases}\omega_0^m=\dfrac{\lambda}{n+\lambda}\\ \omega_0^c=\dfrac{\lambda}{n+\lambda}+(1-\alpha^2+\beta)\\ \omega_i^m=\omega_i^c=\dfrac{\lambda}{2(n+\lambda)},i=1,2,\cdots 2n\end{cases}\tag{11}$$

式中：m为均值；c为产生的协方差；i为第i个采样点；$\lambda=\alpha^2(n+\kappa)-n$是比例缩放系数。

通常情况下，α、β与κ分别取$\alpha=1$，$\beta=2$，$\kappa=0$，因此Sigma点的分布是固定的，但是Sigma点集选取得越合适，电力系统就能达到更加优良的估计效果，在此处考虑通过令α的值实时改变来调节Sigma点与均值的分布距离。具体步骤如下：

将$\lambda=\alpha^2(n+\kappa)-n$代入式(10)，则有：

$$\boldsymbol{\chi}_i=\begin{cases}\bar{x},\ i=0\\ \bar{x}+[\alpha\sqrt{(n+\kappa)\boldsymbol{P}}]_i,\ i=1,2,\cdots,n\\ \bar{x}-[\alpha\sqrt{(n+\kappa)\boldsymbol{P}}]_i,\ i=n+1,n+2,\cdots,2n\end{cases}\tag{12}$$

引入一个新概念，均值到Sigma点的距离：

$$d=\chi_i-\bar{x}\tag{13}$$

式(13)可以进一步改写，假设在$k-1$时刻，状态量和$\boldsymbol{P}_{k-1}$已知，则有

$$d_{k-1}=[\alpha_{k-1}\sqrt{(n+\kappa)\boldsymbol{P}_{k-1}}]\tag{14}$$

利用式(13)进行Sigma点采样操作，在k时刻进行状态估计，此时α_k的值可以表示为式(15)。再将α_k代入式(12)重采样获得一个新的Sigma点集，按照本节后续的步骤对$k+1$时刻进行估计。

$$\alpha_k=\frac{tr(\boldsymbol{P}_{k-1})}{d_{\max}^{k-1}}\tag{15}$$

式中：$d_{\max}^{k-1}=\{\max(d_{k-1}(i,i),\ i\in I\}$，用$I$表示Sigma点集。

(2) UKF滤波过程

在k时刻，$\boldsymbol{x}_k$为状态量，$\boldsymbol{P}_k$为协方差，Sigma点集用$\{\chi_{i,k}\}$表示，对应权值为ω_i^m，ω_i^c。

第一步：预测

一步预测Sigma点:

$$\boldsymbol{\chi}_{i,k+1|k}=f(\boldsymbol{\chi}_{i,k|k})+\boldsymbol{\omega}_k\tag{16}$$

一步预测状态值:

$$\boldsymbol{x}_{k+1|k}=\sum_{i=0}^{2n}\omega_i^m\boldsymbol{\chi}_{i,k+1|k}\tag{17}$$

一步预测误差协方差矩阵：

$$\boldsymbol{P}_{k+1|k}=\boldsymbol{Q}_k+\sum_{i=0}^{2n}\omega_i^c(\boldsymbol{x}_{k+1|k}-\boldsymbol{\chi}_{i,k+1|k})(\boldsymbol{x}_{k+1|k}-\boldsymbol{\chi}_{i,k+1|k})^{\mathrm{T}}\tag{18}$$

第二步：更新

用UT变换来获得一组新的Sigma点。将$\chi'_{i,k+1|k}$代入到量测方程中，即可以得出Sigma点集的预测值。而与其相对应的几个值为

$$\boldsymbol{z}_{i,k+1|k}=h(\boldsymbol{\chi}'_{i,k+1|k})+v_k\tag{19}$$

$$\bar{\boldsymbol{z}}_{k+1|k}=\sum_{i=0}^{2n}\omega_i^m\boldsymbol{z}_{i,k+1|k}\tag{20}$$

$$\boldsymbol{P}_{zk,zk}=\sum_{i=0}^{2n}\omega_i^c(\boldsymbol{z}_{i,k+1|k}-\bar{\boldsymbol{z}}_{k+1|k})(\boldsymbol{z}_{i,k+1|k}-\bar{\boldsymbol{z}}_{k+1|k})^{\mathrm{T}}\tag{21}$$

$$\boldsymbol{P}_{xk,zk}=\sum_{i=0}^{2n}\omega_i^c(\boldsymbol{\chi}_{i,k+1|k}-\boldsymbol{x}_{k+1|k})(\boldsymbol{z}_{i,k+1|k}-\bar{\boldsymbol{z}}_{k+1|k})^{\mathrm{T}}\tag{22}$$

式中：$\bar{\boldsymbol{z}}_{k+1|k}$，$\boldsymbol{z}_{i,k+1|k}$分别为加权量测和量测量预测值；$\boldsymbol{P}_{zk,zk}$，$\boldsymbol{P}_{xk,zk}$分别为预测误差与状态量预测值误差的协方差。通过$\boldsymbol{P}_{zk,zk}$和$\boldsymbol{P}_{xk,zk}$，可以得出UKF的增益矩阵：

$$\boldsymbol{K}_{k+1}=\boldsymbol{P}_{xk,zk}\boldsymbol{P}_{zk,zk}^{-1}\tag{23}$$

同时，对$\boldsymbol{x}_{k+1|k}$和$\boldsymbol{P}_{k+1|k}$进行更新，得到$\boldsymbol{x}_{k+1|k+1}$，$\boldsymbol{P}_{k+1|k+1}$：

$$\boldsymbol{x}_{k+1|k+1}=\boldsymbol{x}_{k+1|k}+\boldsymbol{K}_{k+1}(\boldsymbol{z}_{k+1|k}-\bar{\boldsymbol{z}}_{k+1|k})\tag{24}$$

$$\boldsymbol{P}_{k+1|k+1}=\boldsymbol{P}_{k+1|k}-\boldsymbol{K}_{k+1}\boldsymbol{P}_{zk,zk}\boldsymbol{K}_{k+1}^{\mathrm{T}}\tag{25}$$

2 FDIA检测方法

从本文第1节所提的攻击模型可知，当攻击$\boldsymbol{a}=\boldsymbol{Hc}$时，由于残差的值变化幅度在正常区间内，此时如果继续使用传统的方法来检测，将无法检测出残差。若采用UKF的电力系统状态估计，由于状态转移方程和过程噪声会对状态估计产生一

定的影响，因此UKF会出现一个收敛过渡的过程。而通过采用WLS的状态估计方式，状态值会加快收敛并且进行更新。为了验证本文采用的WLS和改进的UKF算法的效果，在此，提出了一种基于状态估计的FDIA检测方法。本文使用的FDIA检测算法流程如图1所示。

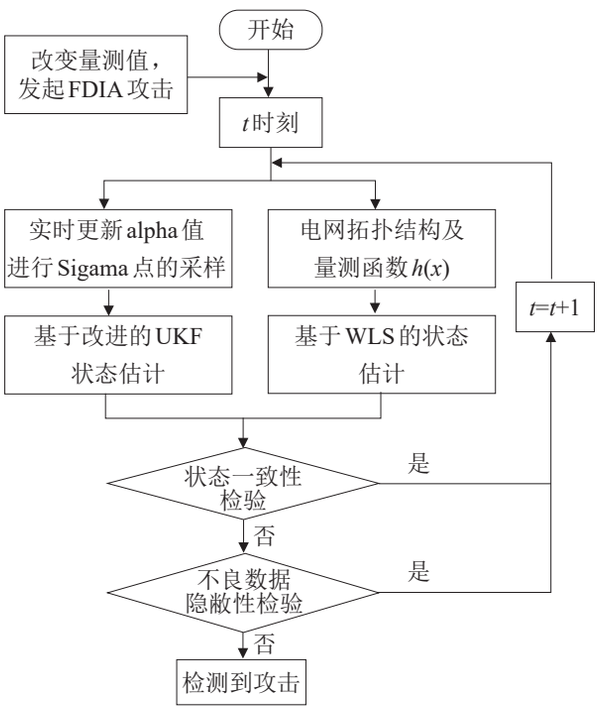

图1 虚假数据检测算法流程
Fig. 1 False data detection algorithm process

图1中，首先对t时刻的电力系统做潮流计算，并把t时刻得到的数据将作为状态量的真值，然后在此基础上添加符合高斯分布的扰动误差，将其作为系统当前的量测数据。然后，分别使用改进的UKF和WLS对系统进行状态估计。最后对两者状态估计的结果进行判断。

在进行判断的时候，首先需要对系统进行一致性检验，其公式为

$$\left\| \hat{\boldsymbol{x}}^{\mathrm{UKF}} - \hat{\boldsymbol{x}}^{\mathrm{WLS}} \right\|_2 \leqslant \tau \tag{26}$$

式中：τ为一致性检验阈值；$\hat{x}^{\mathrm{UKF}}$，$\hat{x}^{\mathrm{WLS}}$分别为经过改进的UKF预测和经过WLS预测的状态估计值。

由于在UKF过程中使用Holt两参数法进行辨识，因此，电网中会存在其他的干扰影响到FDIA。

$$\left\| z - h(\hat{\boldsymbol{x}}^{\mathrm{UKF}}) \right\|_2 \leqslant \tau\_\chi \tag{27}$$

式中：τ_χ为在检测时设置的阈值，本文采用的是卡方检测阈值；z为系统的量测量；$h(\hat{\boldsymbol{x}}^{\mathrm{UKF}})$为经过改进的UKF估计的系统量测量。

当确实有攻击产生时，在一致性检测环节中，两种状态估计的结果会远大于一致性检测的阈值，需要区分是由于突变干扰的影响还是此时确实有攻击发生，选择再利用对改进的UKF预测的量测值进行残差检验的方式来进行判断。只有当残差检验的结果也大于卡方阈值时，才可确切判断是有FDIA的发生。反之，残差检验的结果小于卡方阈值，则说明此时的一致性检验是受到了负荷突变等的干扰，应当输出结果无攻击发生。

3 仿真验证

本文采用Matlab2018b与MATPOWER7.1进行仿真实验。在IEEE14和IEEE57中，在潮流计算结果的基础上，对于电压幅值的量测误差是满足均值为0，$\Delta=0.005$的高斯分布，对于电压相角的量测误差是满足均值为0，$\Delta=0.002$，以潮流计算值为真值加上量测误差得到的就是量测值，其中Δ为标准差。

3.1 改进的UKF性能分析

UKF用于时序预测，其显著优势是简单快速。电网正常运行时会有波动，但是范围很小，利用历史数据可以对电网进行快速的在线预测。为了模拟正常的电网波动，在负荷中加入随机噪声，对IEEE14电网进行状态估计，选取节点3，一共有60个采样时刻。在无FDIA的电网正常运行状态下的改进的UKF和EKF分别对电压幅值的状态估计，分析在同等情况下两种估计器的预测性能。图2是节点3的电压真实值和两种算法的预测估计值。

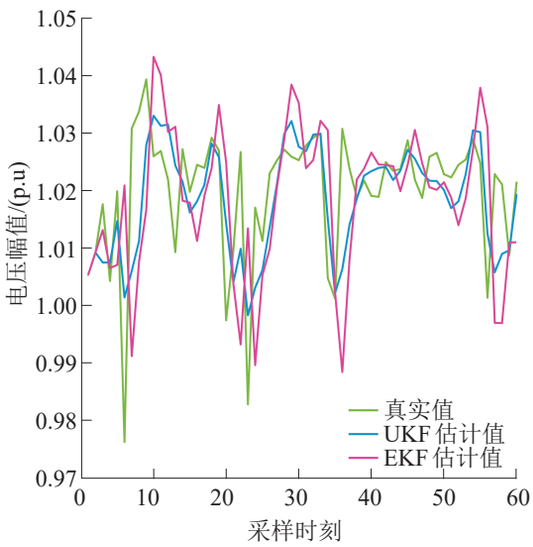

图2 无FDIA情况下的状态估计
Fig. 2 State estimation without FDIA

由图2可知，在同样的条件下，改进的UKF的状态估计效果更为精确，误差较小。为了更加直观的判断EKF与改进的UKF的估计效果，利用均方根误差(root mean square error，RMSE)指标来反映：

$$RMSE(k)=\sqrt{\frac{1}{N}\sum_{j=1}^{N}(\hat{\boldsymbol{x}}_{k,j}-\boldsymbol{x}_{k,j}^{t})^{2}} \tag{28}$$

式中：N为状态量维数；$\hat{\boldsymbol{x}}_{k,j}$为估计值的第$i$个分量；$\boldsymbol{x}_{k,j}^{t}$为真值的第$i$个分量，得到电压幅值的均方根误差如图3所示。

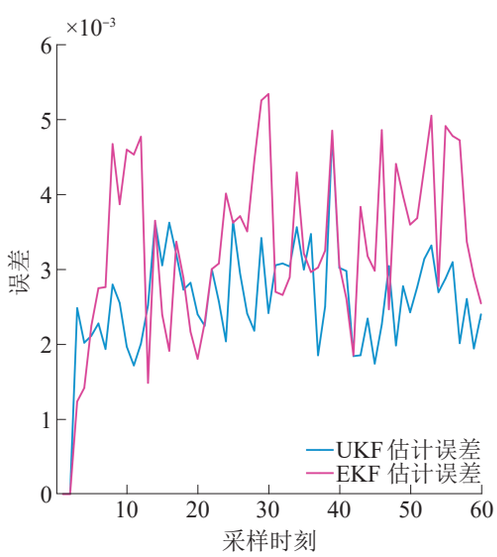

图3 两种算法的电压幅值均方根误差
Fig. 3 RMSE of voltage amplitude of two algorithms

RMSE反映的是真值与选用算法估计值的偏差，能够体现算法整体的估计效果的优劣情况，表1是选取60个时刻的2种算法的电压幅值与相角的RMSE对比。

表1 两种方法均方根误差对比
Table 1 Comparison of the results of two estimation methods

算法	平均电压误差	平均相角误差
EKF	0.003 7	0.007 5
改进的UKF	0.002 3	0.003 9

由图3与表1可知，改进的UKF整体的估计性能要优于EKF，尤其是在相角的估计方面。因此，在对FDIA的检测过程中，采用改进的UKF方法有利于提高检测精度。

3.2 FDIA检测实验与分析

本节将选取文献[18]的假数据攻击模型，利用所提算法对其进行仿真分析，通过得到的虚假数据能够符合残差检验的标准，以验证本文方法的合理性及有效性。由于UKF的状态方程辨识采用了Holt两参数法，当系统不满足一致性检验时，也需要考虑是否会是由负荷突变等干扰引起的误检情况。只有当不满足式(26)一致性检验的同时也不满足式(27)，才能判定为有FDIA的产生。否则，应当认定为是干扰引起的误检假阳性情况。通过仿真，可得到IEEE14节点系统遭到了攻击后电压幅值变化以及电压相角变化对比变化分别如图4，5所示。

由图4，5可以看出，在攻击发生之前后，虽然电压幅值与相角均已改变，然而分布情况仍近似与原有的状态变量保持一致，经过计算攻击前后状态估计的残差由1.873 4变为2.016 7，变化很小。首先利用式(26)进行一致性检验。在无假数据向量攻击时，一致性检验为1.051 4，而当假数据向量注入后，一致性检验为23.336 2，注入攻击后的数值约为注入攻击前的23倍，差异十分明显。此时的检验阈值取值为5.711 7，可以看出攻击后的二范数远大于在此量测精度下的检测阈值。进一步判断是否存在干扰导致的误检，利用式(27)进

DOI: 10.16182/j.issn1004731x.joss.22-0292

行残差检验。此时将显著性水平设置成0.05，在该系统中量测值$m=41$，状态变量$n=27$，冗余度$k=m-n$，则查阅卡方表可得阈值为23.68，攻击后的残差结果为30.515 6，大于卡方表阈值，说明不是因为受到干扰才判定攻击产生。因此，在这两个条件下，可以成功检测系统受到了FDIA。

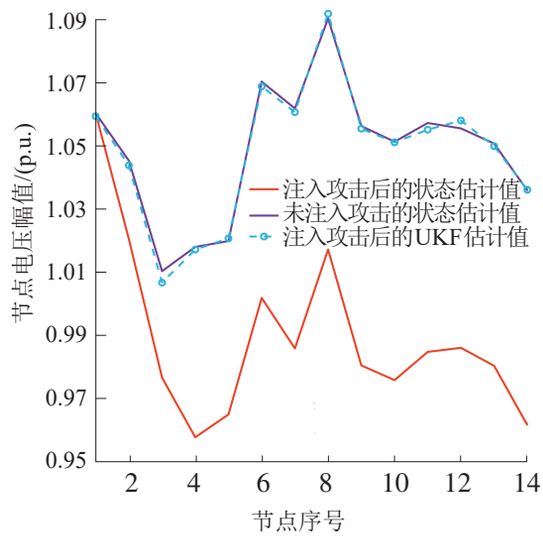

图4 IEEE14攻击前后电压幅值变化对比

Fig. 4 IEEE14 comparison of voltage amplitude changes before and after attack

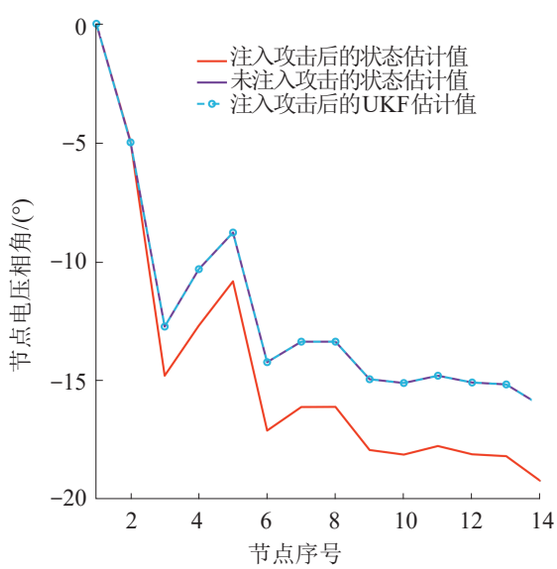

图5 IEEE14攻击前后电压相角变化对比

Fig. 5 IEEE14 comparison of voltage phase angle changes before and after attack

为了进一步验证本方法的合理性及适用性，进一步选取节点更多、拓扑结构更复杂的IEEE57节点系统进行检验，得到在正常情况下系统的状态估计量和下一时刻系统遭到攻击后的经改进的UKF的状态估计，经WLS的估计电压幅值与相角图分别如图6，7所示。

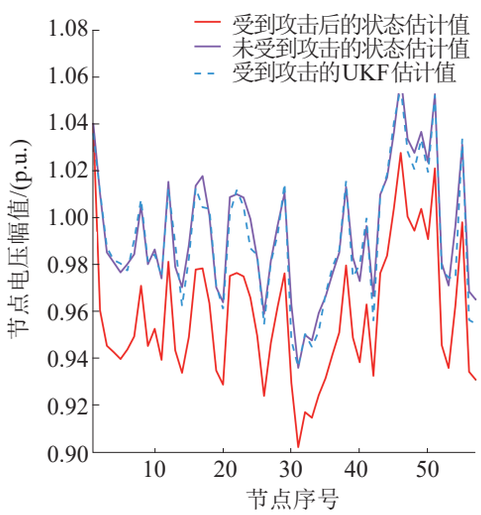

图6 IEEE57攻击前后电压幅值变化对比

Fig. 6 IEEE57 comparison of voltage amplitude changes before and after attack

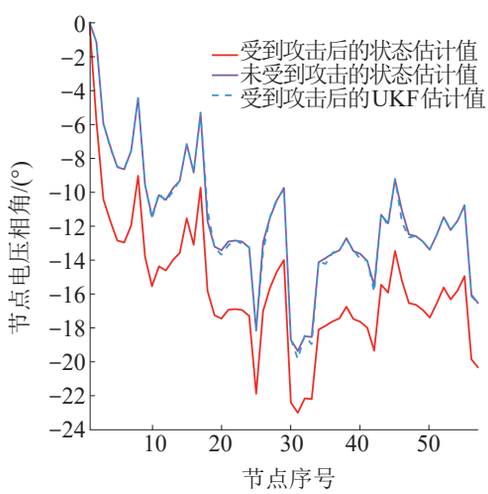

图7 IEEE57攻击前后电压相角变化对比

Fig. 7 IEEE57 comparison of voltage phase angle changes before and after attack

通过图6，7可知，攻击前后系统的残差仍然变化不大，在系统残差检测阈值范围内。首先利

用式(26)进行一致性检验。在无假数据向量攻击时，一致性检验为1.004 7，而当假数据向量注入后，一致性检验为30.045 6，注入攻击后的数值约为注入攻击前的30倍，差异十分明显，攻击后的二范数远大于在此量测精度下的检测阈值。进一步判断是否存在干扰导致的误检，利用式(27)进行残差检验。此时我们将显著性水平设置成0.05，在该系统中量测值 $m=161$，状态变量 $n=113$，冗余度 $k=m-n$，则查阅卡方表可得阈值为65.17，攻击后的残差结果为82.26，大于卡方表阈值，说明不是因为受到干扰才判定攻击产生。因此，在这两个条件下，可以成功检测系统受到了FDIA。

3.3 算法性能分析

为了验证本文提出的算法检测FDIA的性能，考虑与支持向量机(support vector machine, SVM)的FDIA检测方法[19]进行对比。将攻击强度定义为攻击量测注入增量与参考的攻击量测注入增量的比值。攻击强度由1.0逐渐递增到1.9，共十组攻击强度，每组包含100个攻击向量，分析两种方法在不同攻击强度下的检测成功率，得到不同攻击强度下的成功率对比如图8所示。

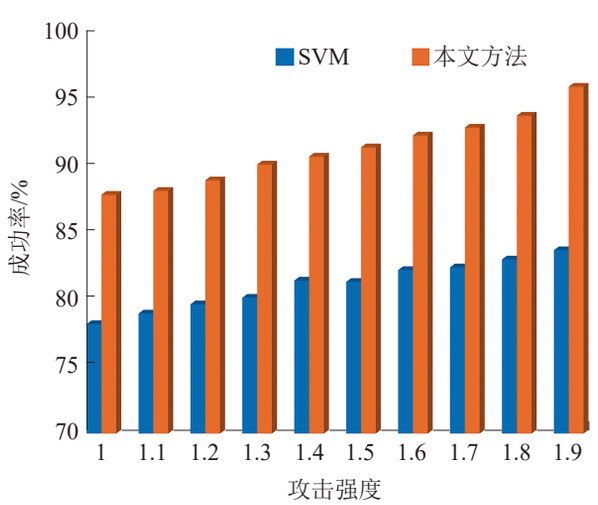

图8 不同攻击强度下的成功率对比

Fig. 8 Comparison of success rates under different attack intensities

由图8可知，攻击强度越大，本文采用的基于改进的UKF的检测方法效率越高，由88.1%到96.4%。而采用SVM的检测方法，效果一直较差。对于本文的检测方法，攻击强度逐渐递增，改进的UKF抑制FDIA的效果保持不变，而静态估计的方法反应更加明显，采用一致性检测手段的残差值就比阈值更大，检测率也就更高。

4 结论

本文提出了一种适用于FDIA的基于改进的UKF检测方法。首先在无FDIA的情况下，分别利用改进的UKF和EKF对电力系统进行状态估计，在电网正常波动情况下，改进的UKF能够起到比EKF更好的状态估计效果，更加有利于后续的FDIA的检测辨识，使得检测具有快速性、准确性和实时性的优点。又利用一致性检验与FDIA检验两个步骤，对改进的UKF估计值和WLS估计值进行判断，在IEEE14与IEEE57系统中进行实验，验证了本文检测方法的有效性。在不同的攻击强度下，与机器学习中常采用的SVM检测方法相比较，本文方法的检测成功率更高。接下来的工作可以考虑如何精确地定位到FDIA的具体位置并剔除假数据，需要进一步对其展开研究。

参考文献：

[1] 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.

[2] 蒋建波, 李鹏, 苗爱敏, 等. GCPS时滞稳定性分析的整体建模方法[J]. 系统仿真学报, 2018, 30(9): 3274-3282.
Jiang Jianbo, Li Peng, Miao Aimin, et al. Integrated Modeling for Time Delay Stability Analysis in GCPS[J]. Journal of System Simulation, 2018, 30(9): 3274-3282.

[3] 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

https://dc-china-simulation.researchcommons.org/journal/vol35/iss7/8
DOI: 10.16182/j.issn1004731x.joss.22-0292

(1): 196-205.

[4] 童晓阳, 王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化, 2016, 40(7): 144-148.
Tong Xiaoyang, Wang Xiaoru. Inference and Countermeasure Presuppostion of Network Attack in Incident on Ukrainian Power Grid[J]. Automation of Electric Power Systems, 2016, 40(7): 144-148.

[5] 王琦, 邰伟, 汤奕, 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.

[6] Liu Xuan, Li Zuyi. False Data Attacks Against AC State Estimation With Incomplete Network Information[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2239-2248.

[7] Mohammadi A, Plataniotis K N. Noncircular Attacks on Phasor Measurement Units for State Estimation in Smart Grid[J]. IEEE Journal of Selected Topics in Signal Processing, 2018, 12(4): 777-789.

[8] Gu Yun, Liu Ting, Wang Dai, et al. Bad Data Detection Method for Smart Grids Based on Distributed State Estimation[C]//2013 IEEE International Conference on Communications (ICC). Piscataway, NJ, USA: IEEE, 2013: 4483-4487.

[9] 王勇, 武津园, 陈雪鸿, 等. 基于卡尔曼滤波的电力虚假数据注入攻击检测方法[J]. 上海电力大学学报, 2021, 37(2): 205-210.
Wang Yong, Wu Jinyuan, Chen Xuehong, et al. Intrusion Detection Method of False Data Injection Attack in Power System Based on Kalman Filter[J]. Journal of Shanghai University of Electric Power, 2021, 37(2): 205-210.

[10] 罗小元, 朱鸣皋, 王新宇, 等. 基于自适应卡尔曼滤波器的智能电网隐蔽假数据攻击检测[J]. 信息与控制, 2018, 47(1): 16-21.
Luo Xiaoyuan, Zhu Minggao, Wang Xinyu, et al. Adaptive Kalman Filter-based Detection of Covert False Data Injection Attacks in Smart Grids[J]. Information and Control, 2018, 47(1): 16-21.

[11] 何耀, 周聪, 郑凌月, 等. 基于扩展卡尔曼滤波的虚假数据攻击检测方法[J]. 中国电力, 2017, 50(10): 35-40.
He Yao, Zhou Cong, Zheng Lingyue, et al. Detection Method Against False Data Injection Attack Based on Extended Kalman Filter[J]. Electric Power, 2017, 50(10): 35-40.

[12] 方航, 葛愿, 余诺, 等. 电力系统状态估计多算法融合[J]. 计算机工程与设计, 2015, 36(2): 502-506.
Fang Hang, Ge Yuan, Yu Nuo, et al. Fusion Algorithm for State Estimation in Power Systems[J]. Computer Engineering and Design, 2015, 36(2): 502-506.

[13] 李江, 王义伟, 魏超, 等. 卡尔曼滤波理论在电力系统中的应用综述[J]. 电力系统保护与控制, 2014, 42(6): 135-144.
Li Jiang, Wang Yiwei, Wei Chao, et al. A Survey on the Application of Kalman Filtering Method in Power System[J]. Power System Protection and Control, 2014, 42(6): 135-144.

[14] 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.

[15] 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.

[16] 贺觅知. 基于卡尔曼滤波的电力系统动态状态估计算法研究[D]. 成都: 西南交通大学, 2006.
He Mizhi. Power System Dynamic State Estimation Algorithm Based on Kalman Filter[D]. Chengdu: Southwest Jiaotong University, 2006.

[17] 曲正伟, 董一兵, 王云静, 等. 用于电力系统动态状态估计的改进鲁棒无迹卡尔曼滤波算法[J]. 电力系统自动化, 2018, 42(10): 87-92.
Qu Zhengwei, Dong Yibing, Wang Yunjing, et al. Improved Robust Unscented Kalman Filtering Algorithm for Dynamic State Estimation of Power Systems[J]. Automation of Electric Power Systems, 2018, 42(10): 87-92.

[18] 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.

[19] 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.