文章编号：2095-2163(2023)06-0168-06 中图分类号：TM932 文献标志码：A

基于自适应 UKF 算法的虚假数据注入攻击检测研究

伍 虹[1]，杨 超[1]，鲁 杰[2]，徐立立[1]
（1 贵州大学 电气工程学院，贵阳 550025；2 中国电建贵阳勘测设计研究院，贵阳 550081）

摘 要：虚假数据注入攻击利用电力系统不良数据辨识机制的漏洞，通过攻击量测值进而影响系统状态估计值，成为影响电力系统安全和稳定运行的严重隐患。针对不良数据检测机制漏洞，本文提出一种基于自适应无迹卡尔曼滤波的虚假数据检测方法，在获得静态状态估计加权最小二乘法和自适应无迹卡尔曼滤波二者状态估计结果的基础上，采用欧几里得距离公式计算二者状态估计偏差值，并根据全局节点欧氏距离设定检测阈值，判断当前时刻是否受到虚假数据注入攻击。以 IEEE-14 标准节点系统进行仿真分析，仿真结果表明自适应无迹卡尔曼滤波能够弥补不良数据检测机制的缺陷，并成功检测出虚假数据的注入。

关键词：虚假数据注入攻击；自适应无迹卡尔曼滤波；状态估计；欧几里得距离

Research on false data injection attack detection based on adaptive unscented Kalman filter algorithm

WU Hong[1], YANG Chao[1], LU Jie[2], XU Lili[1]
(1 College of Electrical Engineering, Guizhou University, Guiyang 550025, China;
2 Power China Guiyang Engineering Corporation Limited, Guiyang, 550081, China)

【Abstract】 False data injection attack utilizes the vulnerability of the bad data detection mechanism of power system to affect the result of state estimation by tampering the state estimation, which poses a serious threat to the security and stable operation of power system. Aiming at the vulnerability of bad data detection mechanism, this paper proposes a false data detection method based on adaptive unscented Kalman filter. Based on the results of static state estimation weighted least square method and adaptive unscented Kalman filter, the Euclidean distance is accustomed to calculate the deviation of the two estimates, and the detection threshold is set according to the Euclidean distance of global node to judge whether the system is attacked by false data injection in real-time. The IEEE-14 standard node system is used for simulation analysis. The simulation results show that the adaptive unscented Kalman filter can make up for the defects of the bad data detection mechanism and successfully detect the injection of false data.

【Key words】 false data injection attack; adaptive unscented Kalman filter; state estimation; Euclidean distance

0 引 言

近年来，随着通信技术以及自动化技术的迅速发展，传统工业设备需面向信息化、网络化发展，与人们日常生活息息相关的电力系统正逐渐发展成一个典型的信息物理系统（Cyber-Physical System, CPS）[1]。但是由于基础通信网络和信息化设备自身的缺陷以及弊端，电力 CPS 在加速构建的同时，电力系统的安全稳定运行也面临新的挑战[2]。

数据采集和监视控制系统（Supervisory Control And Data Acquisition, SCADA）作为电力系统控制中心取得基础量测数据和指令传输控制的关键环节，已成为电力 CPS 网络攻击的重要目标，例如：2016 年乌克兰国家电网因遭到黑客发起的电力网络攻击而发生区域大面积停电，造成乌克兰西部停电超 3 小时，波及数以百万计人口的正常生活[3]。2009 年 Liu Yao[4] 等首次提出虚假数据注入攻击（False Data Injection Attack, FDIA）定义，指出了静态状态估计中存在的不良数据检测（Bad Data Detection, BDD）

基金项目：贵州省科学技术基金（黔科合基础-ZK[2021]一般 277）。

作者简介：伍 虹（1998-），男，硕士研究生，主要研究方向：智能电网信息安全；杨 超（1971-），女，学士，副教授，主要研究方向：配电网规划及电能质量管理；鲁 杰（1997-），男，硕士研究生，主要研究方向：智能电网虚假数据注入攻击检测；徐立立（1996-），男，硕士研究生，主要研究方向：配电网故障诊断。

通讯作者：杨 超 Email：785622539@qq.com

收稿日期：2022-07-12

原理性漏洞，黑客能在掌握一定电力系统拓扑信息的情况下，通过构造虚假数据攻击向量并注入关键量测装置，以达到既躲过不良数据检测又篡改系统状态估计数值的目的。作为能量管理系统（Energy Management System，EMS）中的重要组成部分，精准的状态估计对电力 CPS 安全控制和经济调度起到关键性作用。FDIA 作为一种针对电力系统量测数据完整性的新型攻击，由于其强大的破坏性和特殊的隐蔽性，成为近年来电力 CPS 中最具威胁性的攻击方式之一[5]。从攻击者的角度出发，国内外已有大量关于 FDIA 模型研究，针对虚假数据注入攻击的检测研究具有实际意义。如：文献[6]提出一种在未获得完整电网拓扑结构信息情况下，利用状态估计过程进行隐蔽注入攻击的方法；文献[7]认为可以在不需要电网任何拓扑结构和线路信息，黑客攻击者仍然能够发动一种广义上的 FDIA；文献[8]提出一种具有多项式的时间复杂度的注入攻击算法，最大程度平衡攻击向量引起的攻击影响和被检验到的概率；文献[9]研究考虑对多个系统状态变量进行注入攻击时，如何最小化攻击向量建模的问题。

本文以静态状态估计—加权最小二乘法（Weighted Least Square，WLS）和自适应无迹卡尔曼滤波（Adaptive Unscented Kalman Filter，AUKF）之间的估计值为基础，以欧几里得距离作为检测指标并设定检测阈值，通过实时比较二者偏差值来判定系统是否遭到虚假数据注入攻击。以 IEEE-14 标准节点系统为例进行仿真，仿真结果表明此方法能够有效检测出虚假数据注入攻击。

1　虚假数据注入攻击

1.1　不良数据检测

在电力系统潮流计算中，量测方程表示为式（1）：

$$z = h(x) + e \tag{1}$$

其中，z 表示基于 SCADA 系统采集得到的量测值（m 维列向量）；x 表示待估计的状态变量集合（n 维列向量，包含节点电压的幅值和相角）；e 为量测误差；$h(\cdot)$ 表示量测量和状态变量之间的非线性关系。

由于电力系统的高度非线性，直接对于式（1）应用加权最小二乘法求解状态变量存在计算量大，易发散等问题，因此在实际应用中，往往将其简化为直流模型进行计算，即式（1）简化为式（2）：

$$z = \boldsymbol{H}x + e \tag{2}$$

其中，$\boldsymbol{H}$ 为 $m \times n$ 维雅可比矩阵。

当量测值中存在不良数据，则可以通过最大标准化残差（Largest Normalized Residual，LNR）方法进行不良数据检测，残差 r 定义为式（3）：

$$r = z - \boldsymbol{H}x \tag{3}$$

在系统正常运行下，由量测噪声引起的残差 r 服从自由度为 $k = m - n$（其中 m 为量测装置数，n 为状态变量），显著性水平为 α 的 $\chi^2_{k,a}$ 分布。由检测机制可知，当 $\| r \|_2 > \tau$ 时，即系统量测数据中存在不良数据；若 $\| r \|_2 < \tau$，则认为没有不良数据，其中 τ 为检测阈值。

1.2　虚假数据注入攻击

虚假数据注入攻击是利用不良数据检测缺陷。假设 $a = [a_1, a_2, a_3, \cdots, a_m]^{\mathrm{T}}$ 表示为攻击发起者在量测数据中注入的一组攻击向量，则实际量测数据为 $z_a = z + a$；从而状态变量变化为 $x_a = x + \boldsymbol{c}$，其中 $\boldsymbol{c}$ 为受攻击后偏差向量，$\boldsymbol{c} = [c_1, c_2, c_3, \cdots, a_n]^{\mathrm{T}}$。此时残差表达式经式（4）和式（5）的推导后，可表示为式（6）：

$$\| r_a \|_2 = \| z_a - \boldsymbol{H}x_a \|_2 \tag{4}$$

$$\| r_a \|_2 = \| z_a - \boldsymbol{H}x_a \|_2 = \| z + a - \boldsymbol{H}(x_a + \boldsymbol{c}) \|_2 \tag{5}$$

$$\| r_a \|_2 = \| z - \boldsymbol{H}x + a - H\boldsymbol{c} \|_2 \tag{6}$$

当攻击向量满足 $a = \boldsymbol{Hc}$ 时，则式（7）成立：

$$\| r_a \|_2 = \| z - \boldsymbol{H}x \|_2 < \tau \tag{7}$$

至此，在不良数据检测机制下，该组攻击向量成功绕过最大标准化残差检验，完成虚假数据注入攻击，成为危害电力系统稳定运行的隐患。

2　UKF 基本原理

无迹卡尔曼滤波（Unscented Kalman Filter，UKF）以卡尔曼滤波为基础，通过引入无迹变换（Unscented Transform，UT）来获取近似非线性变换后的特性。在动态状态估计中，状态方程和量测方程如式（8）和式（9）：

$$x_{k+1} = f(x_k) + q_k \tag{8}$$

$$z_{k+1} = h(x_{k+1}) + r_{k+1} \tag{9}$$

其中，$f(x_k)$ 为状态转移函数；$h(x_{k+1})$ 为状态变量和量测值的非线性关系；q_k 为系统误差；r_{k+1} 为服从均值为 0 的加性高斯白噪声的量测误差。

2.1　UT 变换

通过 UT 变换获得 Sigma 点集，同时为避免采样时的非局部效应和高阶项误差，本文采取对称比例

修正法的采样策略。对于一个 n 维系统,Sigma 采样策略和均值、方差的权值计算分别如式(10)和式(11)所示:

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

$$\begin{cases} W_i^m = \dfrac{\lambda}{(n+\lambda)}, & i = 0 \\ W_i^c = \dfrac{\lambda}{(n+\lambda)} + 1(1-\alpha^2+\beta), & i = 0 \\ W_i^m = W_i^c = \dfrac{\lambda}{2(n+\lambda)}, & i = 1,\cdots,2n \end{cases} \tag{11}$$

一共取 $2n+1$ 个 Sigma 点,式(10)中的 $\lambda = a^2(n+\kappa) - n$ 为尺度因子,用于控制预测误差;a 为比例修正因子,κ 为自由参数,通常取 0;β 为高阶矩阵信息的权系数,通常取 2。

经对称比例修正法采样得到的 Sigma 点集 $\{\chi_i\}$ 满足式(12)和式(13):

$$\bar{x} = \sum_{i=1}^{L} W_i^m \chi_i \tag{12}$$

$$P_x = \sum_{i=1}^{L} W_i^c (\chi_i - \bar{x})(\chi_i - \bar{x})^{\mathrm{T}} \tag{13}$$

其中,$\bar{x}$ 为均值;P_x 为协方差;L 为 Sigma 采样点数目;W^m 为均值权值;W^c 为协方差均值。

再一次对 Sigma 点集 $\{\chi_i\}$ 进行非线性变换,得到 $\{Y_i\}$,Sigma 点集 $\{Y_i\}$ 满足式(14)和式(15):

$$\bar{y} = \sum_{i=1}^{L} W_i^m Y_i \tag{14}$$

$$P_y = \sum_{i=1}^{L} W_i^c (Y_i - \bar{y})(Y_i - \bar{y})^{\mathrm{T}} \tag{15}$$

无迹卡尔曼滤波通过引入上述 UT 变换对 Sigma 点进行非线性变换,使得状态变量和协方差能够达到至少二阶以上的精度[10]。

2.2 UKF 预测和更新

2.2.1 状态预测

根据所选采样策略得到的 Sigma 点集,进行状态变量 $\bar{x}$ 和协方差阵 P_x 的一步预测,式(16)~式(18):

$$\chi_{i,k|k+1} = f(\chi_{i,k}) + q_k \tag{16}$$

$$\bar{x}_{k|k+1} = \sum_{i=1}^{L} W_i^m \cdot \chi_{i,k|k+1} \tag{17}$$

$$P_{k|k+1} = \sum_{i=1}^{L} W_i^c (\chi_{i,k|k+1} - \bar{x}_{k|k+1})(\chi_{i,k|k+1} - \bar{x}_{k|k+1})^{\mathrm{T}} + Q_k \tag{18}$$

2.2.2 量测预测

根据状态预测步得到的状态变量和协方差阵构造新的 Sigma 点集,并进行下一步预测,式(19)和式(20):

$$z_{k|k+1} = h(\zeta_k) + r_k \tag{19}$$

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

2.2.3 滤波更新

根据前两步预测结果计算卡尔曼增益,并对状态变量以及协方差阵进行更新,式(21)~式(25):

$$S_{k+1} = \sum_{i=0}^{2n} W_i^c (z_{k|k+1} - \bar{z}_{k|k+1})(z_{k|k+1} - \bar{z}_{k|k+1})^{\mathrm{T}} + R_{k+1} \tag{21}$$

$$C_{k+1} = \sum_{i=0}^{2n} W_i^m (\chi_{k|k+1} - \bar{x}_{k|k+1})(z_{k|k+1} - \bar{z}_{k|k+1})^{\mathrm{T}} \tag{22}$$

$$K_{k+1} = C_{k+1} \cdot S_{k+1}^{-1} \tag{23}$$

$$x_{k+1} = \bar{x}_{k|k+1} + K_{k+1}(z_{k+1} - \bar{z}_{k+1}) \tag{24}$$

$$P_{k+1} = P_{k|k+1} - K_{k+1} S_{k+1} K_{k+1}^{\mathrm{T}} \tag{25}$$

至此完成 UKF 的滤波过程。

3 AUKF 动态状态估计

3.1 Holt's 指数平滑法

由于电力系统的多维非线性,卡尔曼滤波一步预测值中的状态转移方程 $f(x_k)$ 较难确定。Holt's 两参数指数平滑法通过过去几个时刻的历史数据进行预测,可以近似得到状态转移函数 f_{Holt},具有计算速度快、不占用系统资源等优势[11]。其表达式为式(26)~式(28):

$$x_{k|k+1} = S_k + \boldsymbol{b}_k \tag{26}$$

$$S_k = \alpha x_{k|k} + (1-\alpha) x_{k|k-1} \tag{27}$$

$$\boldsymbol{b}_k = \beta(S_k - S_{k-1}) + (1-\beta)\boldsymbol{b}_{k-1} \tag{28}$$

其中,S_k 为水平分量;$\boldsymbol{b}_k$ 为倾斜向量;α 和 β 为平滑系数;取值为 $[0,1]$。

Holt's 两参数平滑法中的 α 和 β 选取通过 R 语言结合历史数据得到,当 α 取 0.957,β 取 0.145 时最为合适。

3.2 改进的 Sage-Husa 噪声估值器

使用两参数指数平滑法预测的系统噪声未知,有可能随时间发生变换,因此不能简单假设 Q_k 为常数阵。针对噪声时变问题,本文将基于渐消记忆指数加权法的 Sage-Husa 噪声估值器应用于无迹卡尔

曼滤波方法中，以此减小未知噪声对模型精度的影响。改进的 Sage－Husa 噪声估值器表达式为式(29)～式(31)：

$$l_{k-1} = (1 - e)/(1 - e^{k}) \tag{29}$$

$$q_k = (1 - l_{k-1})\, q_{k-1} + l_{k-1}\left(x_{k|k} - \sum_{i=1}^{L} W_i^m f(\chi_{i,k})\right) \tag{30}$$

$$Q_k = (1 - l_{k-1})\, Q_{k-1} + l_{k-1}\{K_k V_k V_k^{\mathrm{T}} K_k^{\mathrm{T}} + P_k - \sum_{i=1}^{L} W_i^c (\chi_{i,k|k+1} - x_{k|k+1})(\chi_{i,k|k+1} - x_{k|k+1})^{\mathrm{T}}\} \tag{31}$$

其中，$V_k = z_k - \bar{y}_k$ 为新息修正方差阵，通过实验验证 V_k 相比残差修正能取得更好估计效果，e 为遗忘因子并且 $0 < e < 1$，K_k 为卡尔曼增益。

将 Sage－Husa 噪声估值器引入无迹卡尔曼滤波中，实现自适应无迹卡尔曼滤波。

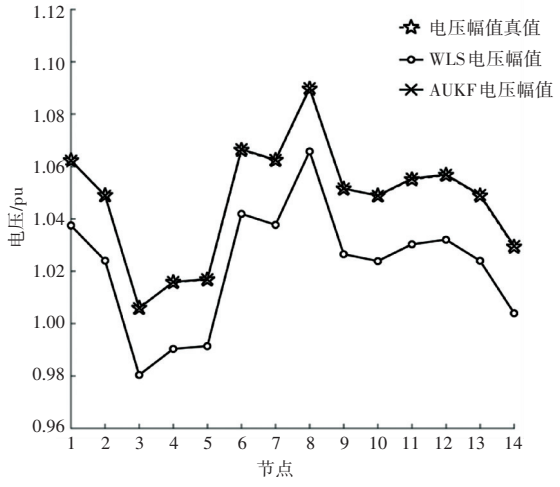
4　FDIAs 检测

传统电力系统在正常运行时，通常使用加权最小二乘法，根据某个时间断面采集得到的量测值来进行静态状态估计，以得到某时刻的状态结果。而在电力系统遭遇虚假数据注入攻击时，由于 WLS 等估计方法的静态特性，被恶意篡改的量测值会使得相应时刻的 WLS－SE 远离真实值。而 AUKF 由于 Holt′s 指数平滑法近似得到的转移函数，其状态估计过程具有一定的迟滞性，同时其估计值由预测值和量测值共同决定，由虚假数据注入引起的状态偏移量很小。因此，可以通过二者状态估计值之间的偏差来检测 FDIAs。本文采用欧几里得距离，即 n 维空间中两点的真实距离作为检测指标，式(32)：

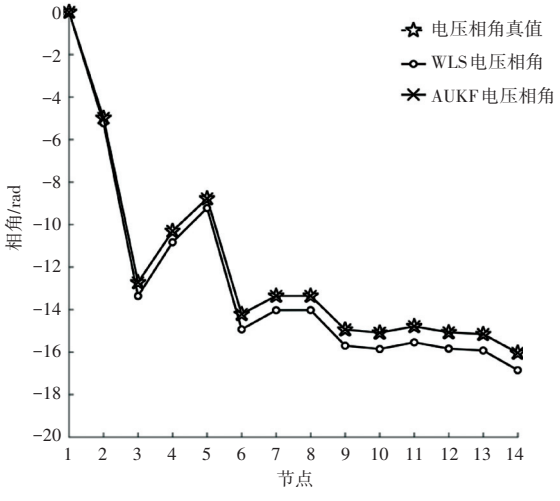
$$d_k = \left[\sum_{i=1}^{n} (x_{i,k}^{\mathrm{WLS}} - x_{i,k}^{\mathrm{AUKF}})^2\right]^{1/2} \tag{32}$$

为验证所提检测方法，本文采用 IEEE14 节点标准系统，用 MATLAB 软件及 MATPOWER 仿真包获取量测数据，并对系统每五分钟进行一次数据采样，一天二十四小时共计 288 次。基于 AUKF 检测虚假数据攻击的仿真结果如下：

(1)系统正常运行时，取某一时间断面 $T = 30$ 时刻，正常运行时 IEEE－14 节点电压幅值与相角如图 1 所示。通过仿真计算得到系统正常运行时残差 $\| r \|_2$ 为0.055 8。根据统计学理论，系统冗余度 $k = m - n = 14$，选择显著性水平为 0.05，由卡方分布表得到不良数据检测阈值 $\tau = \chi^2_{14,0.05} = 23.685$，此时由量测噪声引起的残差 $\| r \|_2$ 远小于不良数据检测阈值。同时，由欧式检测指标计算得该时刻电压幅值欧氏距离 d_u 为0.093 7，电压相角欧氏距离 d_θ 为2.429 8。



(a) 节点电压相角



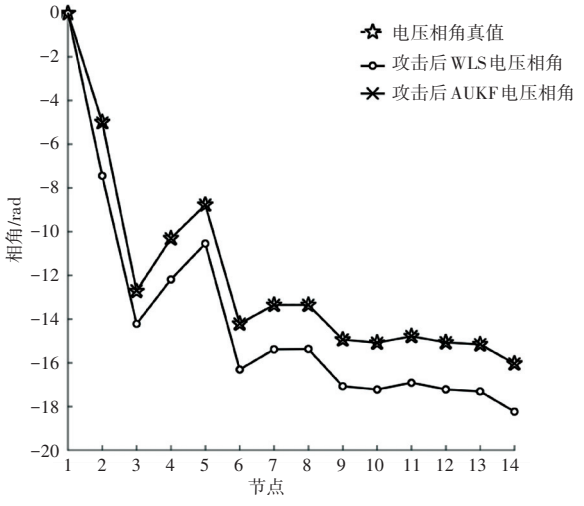
(b) 节点电压幅值

图 1　正常运行时 IEEE－14 节点电压幅值与相角

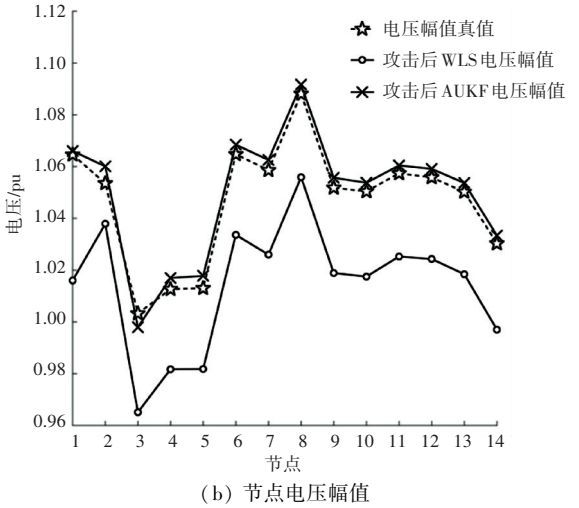
Fig. 1　Voltage amplitude and phase angle of IEEE－14 node during normal operation

(2)注入 2 攻击时，取 $T = 50$ 时刻，模拟对量测系统注入虚假数据攻击向量[12]。注入攻击时 IEEE－14 节点电压幅值与相角如图 2 所示，此时系统运行时残差 $\| r \|_2$ 为0.203 2，注入攻击后的残差远小于不良数据检测阈值 $\tau = \chi^2_{14,0.05} = 23.685$，无法触发不良数据检测机制。注入攻击前后线路功率对比如图 3 所示，此次虚假数据注入攻击造成线路 1－2(即 1 号量测装置)有功功率和无功功率阻塞，其中有功功率增涨至系统正常运行时的 131%，无功功率增涨至系统正常运行时的 364%，已成功发起一次虚假数据注入攻击。由此看见，虚假数据注入攻击在绕过传统不良数据检测的情况下，对电力系统的正常稳定运行已造成严重隐患。根据欧氏距离检测指

标,注入虚假数据攻击向量后,电压幅值欧氏距离 d_u 为 0.134 6,电压相角欧氏距离 d_θ 为 7.249 6。



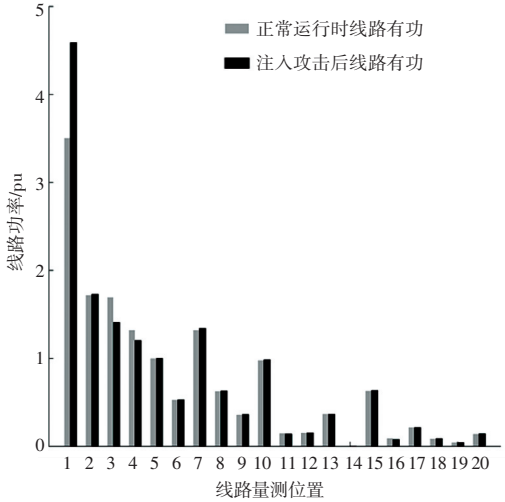
(a) 节点电压相角



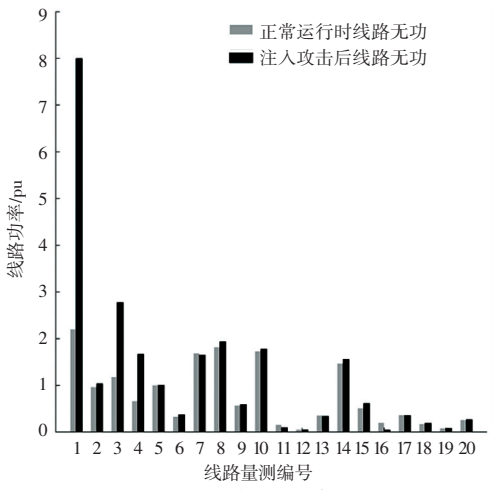
(b) 节点电压幅值

图 2 注入攻击时 IEEE-14 节点电压幅值与相角

Fig. 2 Voltage amplitude and phase angle of IEEE-14 node during injection attack



(a) 线路有功功率

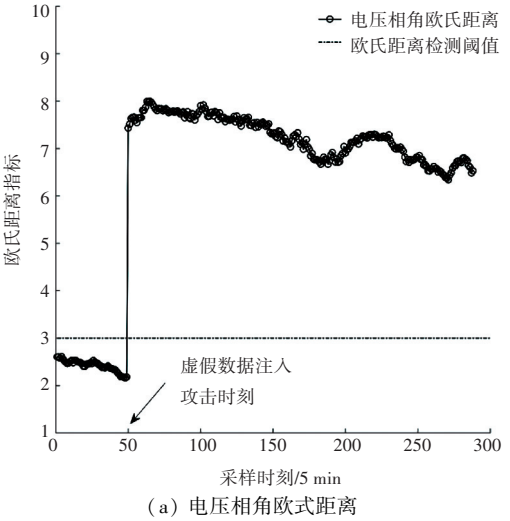


(b) 线路无功功率

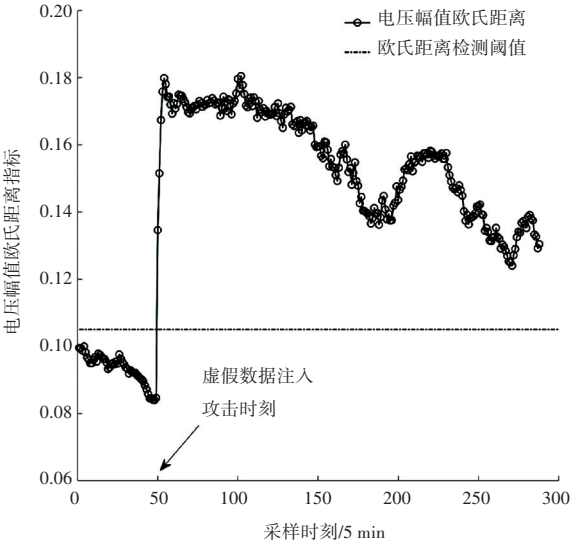
图 3 注入攻击前后线路功率对比

Fig. 3 Comparison of line power before and after injection attack

(3)对全局节点状态变量进行分析,全局节点欧氏距离 d_u 与 d_θ 的变化如图 4 所示。采样时刻



(a) 电压相角欧式距离



(b) 电压幅值欧式距离

图 4 全局节点欧式距离变化

Fig. 4 Euclidean distance change of global nodes

$T < 50$时，系统正常运行，全局 d_u 和 d_θ 保持一个较低水平；当采样时刻 $T = 50$，向系统注入虚假数据攻击向量，在遭遇到 FDIA 之后，电压幅值和电压相角欧式距离陡然增涨。全局残差变化如图 5 所示，可以看到在 $T = 50$ 时刻前后，全局残差均小于不良数据检测阈值。在此期间，根据全局节点欧氏距离变化趋势，分别设置电压幅值欧氏距离检测阈值 $\tau_U = 0.105$和电压相角欧氏距离检测阈值 $\tau_\theta = 3$，当 d_u 和 d_θ 二者指标超过攻击检测阈值 τ_U 和 τ_θ 时，即可立即检测出电力系统遭受虚假数据注入攻击；使用均方根误差（Root-Mean Square-Error，RMSE）指标对攻击前后电压幅值和电压相角的精度进行评价。攻击前后 AUKF 性能见表 1，在遭受虚假数据注入攻击后，AUKF 仍然能得到较好估计效果。

表 1　攻击前后 AUKF 性能

Tab. 1　AUKF performance before and after attack

指标	项目	攻击前 AUKF	攻击后 AUKF
RMSE - U/ %	平均值	0.000 19	0.009 61
	最大值	0.000 41	0.012 42
RMSE - θ/ %	平均值	0.001 3	0.079 4
	最大值	0.001 9	0.006 2

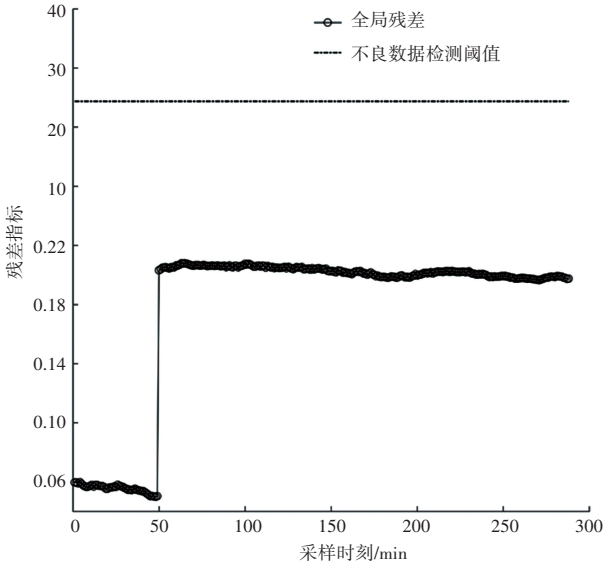


图 5　全局残差变化

Fig. 5　The global residual

5　结束语

本文提出了一种基于自适应无迹卡尔曼滤波的虚假数据注入攻击检测方法，对电力系统内部进行状态估计，同时利用静态状态估计的实时性和自适应无迹卡尔曼滤波的迟滞性，引入欧几里得距离作为检测系统是否注入虚假数据的指标，并通过设置合理阈值，在 IEEE-14 标准节点系统上进行仿真试验。试验表明：

（1）自适应无迹卡尔曼滤波相比传统静态状态估计具有估计精度高、抗干扰能力强等优点，即使受到虚假数据注入攻击，状态变量变化仍然很小；

（2）自适应无迹卡尔曼滤波能够同时评估当前系统运行状态并预测下一时刻系统的状态；

（3）本文所提方法能够有效、快速地检测出虚假数据的注入，避免电力系统因虚假数据注入攻击做出错误动作。

参考文献

[1] RAJKUMAR R, LEE I, SHA L, et al. Cyber-physical systems: the next computing revolution[C]//Proceedings of the 47th design automation conference. 2010: 731-736.

[2] WANG Xianpei, TIAN Meng, DONG Zhengcheng, et al. Survey of false data injection attacks in power transmission systems[J]. Power System Technology, 2016, 40(11): 3406-3414.

[3] LIANG Gaoqi, WELLER R S, ZHAO Junhua, et al. The 2015 ukraine blackout: implications for false data injection attacks[J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317-3318.

[4] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids [J]. Acm Transactions on Information & System Security, 2009, 14(1): 21-32.

[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)：74-85.

[6] LIU X, LI Z. Optimal protection strategy against false data injection attacks in power systems[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1802-1810.

[7] CHIN W L, LEE C H, JIANG T. Blind false data attacks against ac state estimation based on geometric approach in smart grid communications[J]. IEEE Transactions on Smart Grid, 2017, 9(6): 6298-6306.

[8] XUE Yusheng, LI Manli, LUO Jianbo, et al. Coupling modeling method of power grid information physical system based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11-19.

[9] DEKA D, BALDICK R, VISHWANATH S. Data attack on strategic buses in the power grid: design and protection[C]//PES General Meeting Conference & Exposition. Washington DC: PES General Meeting Conference & Exposition, 2014: 1-5.

[10] JULIER S J, UHLMANN J K, DURRANT-WHYTE H F. A new approach for filtering nonlinear systems[C]//Proceedings of the American Control Conference. Seattle, Washington: IEEE, 1995: 1628-1632.

[11] 卫志农，孙国强，庞博. 无迹卡尔曼滤波及其平方根形式在电力系统动态状态估计中的应用[J]. 中国电机工程学报，2011，31(16)：74-80.

[12] 阮嘉祺，彭建春，王怀智，等. 电力系统最小虚假数据攻击向量的建模与分析[J]. 智能电网，2017，7(3)：153-160.