基于自适应 Kalman 滤波的智能电网假数据注入攻击检测

罗小元 [1] 潘雪扬 [1] 王新宇 [1, 2] 关新平 [3]

摘 要 研究了一种针对智能电网中假数据注入攻击的有效检测方法. 假数据注入攻击可以保持攻击前后残差基本不变, 绕过传统的不良数据检测技术. 首先基于电网模型, 分析了假数据注入攻击的攻击特性, 针对噪声统计特性未知且无迹 Kalman 滤波 (Unscented Kalman filter, UKF) 不稳定的现象, 提出了自适应平方根无迹 Kalman 滤波改进算法. 基于状态估计值, 结合中心极限定理提出检测算法, 并与欧几里得检测方法、巴氏系数检测方法进行比较. 最后, 仿真表明本文所提检测算法的优越性.

关键词 智能电网, 虚假数据注入攻击, 攻击检测, 自适应平方根无迹卡尔曼滤波

引用格式 罗小元, 潘雪扬, 王新宇, 关新平. 基于自适应 Kalman 滤波的智能电网假数据注入攻击检测. 自动化学报, 2022, **48**(12): 2960−2971

DOI 10.16383/j.aas.c190636

Detection of False Data Injection Attack in Smart Grid via Adaptive Kalman Filtering

LUO Xiao-Yuan[1] PAN Xue-Yang[1] WANG Xin-Yu[1, 2] GUAN Xin-Ping[3]

Abstract In this paper, an effective detection method for false data injection attack in smart grid is studied. False data injection attack can keep the residual unchanged before and after the attack and bypass the traditional bad data detection technology. Firstly, based on the grid model, the attack characteristics of false data injection attack are analyzed. Aiming at the phenomenon that the noise statistical characteristics are unknown and the unscented Kalman filter (UKF) is unstable, an effective detection method for false data injection attack is proposed. An improved algorithm of adaptive square root unscented Kalman filter is proposed. Based on the state estimation and the central limit theorem, the algorithm is compared with Euclidean method and bayonet coefficient method. Finally, the simulation shows the superiority of the algorithm.

Key words Smart grid, false data injection, attack detection, adaptive square-root unscented Kalman filter

Citation Luo Xiao-Yuan, Pan Xue-Yang, Wang Xin-Yu, Guan Xin-Ping. Detection of false data injection attack in smart grid via adaptive Kalman filtering. *Acta Automatica Sinica*, 2022, **48**(12): 2960−2971

智能电网是一种新型的电网, 它采用先进的通信网络技术和控制技术来支持更高效的能源安全传输和分配. 然而, 由于智能电网系统的复杂性和开放性, 智能电网中进行数据交换的信息网络成为易受到恶意攻击的对象[1−2]. 例如, 2016 年, 黑客攻击乌克兰国家电力部门致使国内发生了一次大规模的停电事件[3], 造成严重经济损失. 因此, 智能电网的攻击检测研究具有重要意义.

隐蔽假数据攻击是目前恶意攻击的典型代表, 攻击者对传感器节点注入精心设计的错误数据, 接收错误数据的控制中心, 继而做出错误决策破坏系统的稳定性[4]. 在文献 [5] 中, 拒绝服务攻击旨在中断电力网络通信信道的可用性. 文献 [6] 构建了一种对智能电网中以完整性和可用性为目标的攻击分类方法. 文献 [7] 解决了在电力网络中攻击检测和拓扑隔离的问题. 文献 [8] 提出了一种算法来识别要操作的智能电表的最优数目, 从而找到最优攻击策略, 其目的是干扰电网系统的状态估计, 影响其稳定性. 文献 [9] 设计了具有隐蔽特性的虚假数据攻击, 它可以使攻击前后残差基本不变, 因此, 基于卡方检测器的检测技术是无效的. 近年来, 隐蔽性攻击检测成为了研究热点之一.

针对智能电网遭受虚假数据注入攻击的检测问

收稿日期 2019-09-06 录用日期 2020-02-23
Manuscript received September 6, 2019; accepted February 23, 2020
国家自然科学基金 (61873228, 62103357), 河北省教育厅青年基金 (QN2021139), 河北省自然基金 (F2021203043), 汽车测控与安全四川省重点实验室开放基金 (QCCK2022-006) 资助
Supported by National Natural Science Foundation of China (61873228, 62103357), Science and Technology Youth Foundation of Hebei Education Department (QN2021139), Natural Science Foundation of Hebei Province (F2021203043), and Open Research Fund of Vehicle Measurement, Control and Safety Key Laboratory of Sichuan Province (QCCK2022-006)
本文责任编委 孙健
Recommended by Associate Editor SUN Jian
1. 燕山大学电气工程学院 秦皇岛 066004 2. 西华大学汽车测控与安全四川省重点实验室 成都 610039 3. 上海交通大学电信学院 上海 200240
1. School of Electrical Engineering, Yanshan University, Qinhuangdao 066004 2. Vehicle Measurement, Control and Safety Key Laboratory of Sichuan Province, Xihua University, Chengdu 610039 3. School of of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240

题, 近年来有了很多成果. 文献 [10] 中, 以电机的电压模型为研究对象, 使用卡尔曼滤波 (Kalman filter, KF) 技术得到该系统的残差序列, 通过计算攻击前后残差序列之间的 Bhattacharyya 距离来判断系统中是否存在攻击. 该文献的不足之处有两点: 1) Bhattacharyya 距离无法辨别虚假数据注入攻击前后两个残差序列的相似性, 因为虚假数据注入攻击前后残差保持不变; 2) 该电压模型是线性的, 对于实际中存在的大多数的非线性系统, 该检测算法是失效的. 文献 [11]使用卡尔曼滤波技术得到系统的状态, 从系统状态角度考虑设计检测算法, 提出欧几里德检测方法, 该方法可以检测隐蔽假数据注入攻击. 该文献的不足之处是, 系统方程对于噪声是线性的, 即该噪声是加性噪声, 当系统方程对于噪声是非线性的时候, 噪声经过非线性变换, 不再服从高斯分布, 也就无法设计阈值, 无法检测攻击. 文献 [12] 中, 攻击者可能会缓慢改变多个传感器的测量值, 因此上述统计异常检测不会检测到个别受损的测量值, 所以提出检测思想, 这些测量值组合起来会导致状态变量远离其真值, 然而, 文中作出假设, 控制中心收集到的测量值都是服从高斯分布的, 并基于此性质设计了双边假设检验检测攻击. 该文献的不足之处是, 电网系统中的参数仅会在特定情况下服从高斯分布, 而这种情况并不常见, 且建模时没有考虑噪声, 所以该文中的检测算法局限性较大.

因此, 根据虚假数据注入攻击的特性, 考虑系统非线性和噪声统计特性未知情况, 本文提出一种基于自适应平方根无迹卡尔曼滤波器 (Unscented Kalman filter, UKF) 的智能电网隐蔽假数据攻击检测方法. 该算法可以有效地、稳定地应用于非线性系统中对系统状态作出估计, 依据系统状态设计检测算法检测攻击, 并从检测指标的角度与现有算法进行对比. 最后进行仿真实验, 实验结果证明, 所提出的基于该算法的攻击检测方法可以准确地给出状态估计值, 从而检测出隐蔽攻击.

1　电网模型、攻击特性及问题描述

1.1　电网模型

考虑一个由 3 条互连总线组成的电力网络, 与之对应的拓扑图 $G(V, \varepsilon)$, 如图 1 所示. $V = \{i\}_1^N$ 表示节点集, $i \in V$ 与总线 i 相对应, $\varepsilon \subseteq V \times V$ 是图 G 的边集. 对于总线 $i \in V$ 的相角, 建立一个连续时间二阶微分动力学方程, 称为摆动方程[7]

$$m_i\ddot{\delta}_i(t) + d_i\dot{\delta}_i(t) = u_i(t) + \eta_i(t) - \sum_{j\in N_i} P_{ij}(t) \quad (1)$$

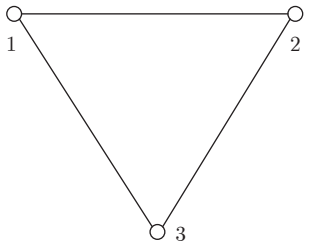

图 1　3 总线电网模型

Fig. 1　3-bus grid model

式中, δ_i 表示总线的相角, m_i 为转动惯量, d_i 为阻尼系数, u_i 为控制输入信号, η_i 是过程噪声, P_{ij} 是从总线 i 到 j 的有功功率流

$$P_{ij}(t) = V_iV_jb_{ij}\sin(\delta_i(t) - \delta_j(t))$$

式中, V 表示总线电压, b_{ij} 表示总线 i, j 之间的电纳.

引入角速度 ω, 将上式改写为一阶微分方程组的形式, 即

$$\begin{aligned}&\dot{\delta}_i(t) = \omega_i(t)\\ &\dot{\omega}_i(t) = -\frac{1}{m_i}(d_i\omega_i(t) + u_i + \varpi_i(t) - \sum_{j\in N_i} P_{ij}(t))\end{aligned} \quad (2)$$

每一条总线都安装有传感器, 将总线的数据传输回控制中心, 系统输出方程为

$$\boldsymbol{y}_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\boldsymbol{x}_i + \boldsymbol{\rho}(t) \quad (3)$$

式中, $\boldsymbol{y}_i$ 表示总线 i 的输出向量, $\boldsymbol{\rho}$ 是测量噪声.

针对上述系统, 本文采用欧拉离散化方法[13], 即对于一个非线性系统

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + B\tau + \varpi$$

离散化后的形式为

$$\boldsymbol{x}_k = \boldsymbol{x}_{k-1} + \tau f(\boldsymbol{x}_{k-1}) + \tau B\boldsymbol{u} + \tau\varpi + \mathrm{O}(\tau^2)$$

其中

$$\mathrm{O}(\tau^2) = \frac{\tau^2}{2}\dot{f}(\boldsymbol{x}) + \frac{\tau^3}{3}f^{(2)}(\boldsymbol{x}) + \cdots + \frac{\tau^k}{k!}f^{(k-1)}(\boldsymbol{x})$$

采样间隔值 τ 取值充分小以保证高阶项 $\mathrm{O}(\tau^2)$ 忽略不计, 本文中 $\tau = 0.1$ s.

对式 (2) 使用上述欧拉离散化算法对该系统离散化, 得到

$$\begin{cases}\boldsymbol{x}_k = f_o(\boldsymbol{x}_{k-1}) + B_o\boldsymbol{u} + \boldsymbol{\eta}_{k-1}\\ \boldsymbol{y}_k = H\boldsymbol{x}_k + \boldsymbol{\rho}_k\end{cases} \quad (4)$$

其中, $f_o(\cdot)$ 表示关于 x 的非线性函数, 将 $\boldsymbol{x}_{k-1} + \tau f(\boldsymbol{x}_{k-1})$ 合并在一起, $B_o = \tau B$, $\eta = \tau\varpi$.

假设 η 和 ρ 是互不相关的非零均值高斯白噪声, 统计特性为

$$\begin{cases} E(\boldsymbol{\eta}_k)=\boldsymbol{q}, & \mathrm{cov}(\boldsymbol{\eta}_k\boldsymbol{\eta}_j^{\mathrm{T}})=Q_k\delta_{kj} \\ E(\boldsymbol{\rho}_k)=\boldsymbol{r}, & \mathrm{cov}(\boldsymbol{\rho}_k\boldsymbol{\rho}_j^{\mathrm{T}})=R_k\delta_{kj} \\ E(\eta_k\rho_j^{\mathrm{T}})=0 \end{cases} \tag{5}$$

式中, Q 是非负定矩阵, R 是正定矩阵, δ_{kj} 是 $Krone\ cher$-δ 函数, 即

$$\delta_{kj}=\begin{cases}0, & k\neq j\\ 1, & k=j\end{cases}$$

将 η 和 ρ 改写为 $\eta_k=\boldsymbol{q}+\mu_k$, $\rho_k=\boldsymbol{r}+\boldsymbol{v}_k$, 有

$$\begin{cases} \boldsymbol{x}_k=f_o(\boldsymbol{x}_{k-1})+B_o\boldsymbol{u}+\boldsymbol{q}+\boldsymbol{\rho}_{k-1} \\ \boldsymbol{y}_k=H\boldsymbol{x}_k+\boldsymbol{r}+\boldsymbol{v}_{k-1} \end{cases} \tag{6}$$

式中, μ_k 和 $\boldsymbol{v}_k$是互不相关的零均值高斯白噪声. $\boldsymbol{x}_k=[\delta_1\quad\delta_2\quad\delta_3\quad\omega_1\quad\omega_2\quad\omega_3]^{\mathrm{T}}$, $\boldsymbol{y}_k\in\mathbf{R}^6$.

1.2 攻击描述和问题提出

假设一个恶意的第三方想要破坏第 1.1 节中描述的系统的完整性. 本文主要考虑虚假数据注入攻击.

假设攻击者具有系统知识, 知道系统矩阵, 控制矩阵, 测量矩阵, 可以控制一系列系统中的传感器数据.

考虑假数据注入攻击模型描述为

$$\boldsymbol{z}_a(k)=\begin{cases}H\boldsymbol{x}_k+\xi(k), & k\not\subset T\\ H\boldsymbol{x}_{a,\,k}+\xi(k)+\boldsymbol{y}_a(k), & k\subset T\end{cases} \tag{7}$$

式中, $\Gamma=\mathrm{diag}\{\gamma_1,\cdots,\gamma_n\}$ 代表传感器选择矩阵, T 是攻击的时间范围, 当 $\gamma_i=1$ 时, 代表第 i 个传感器遭受攻击, 否则 $\gamma_i=0$. 且 $\boldsymbol{y}_a(k)$ 是攻击者精心构建的攻击向量序列, 攻击框图如图 2 所示.

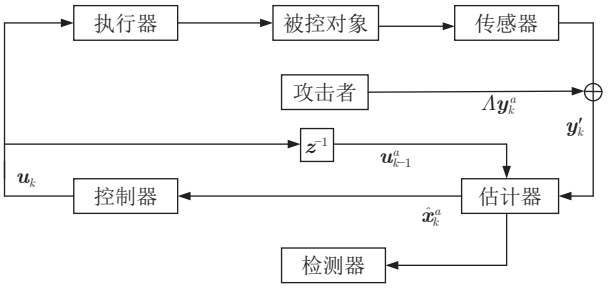

图 2 系统遭受攻击框图

Fig. 2 block diagram of system under attack

在隐蔽假数据注入攻击情况下, 在所考虑的攻击模型中, 攻击者构造攻击序列注入传感器, 在该序列下, 状态差值最终将发散到 ∞, 而不会触发卡方检测器. 该攻击序列满足以下性质[9]:

$$\begin{aligned} &\lim_{k\to T}\|\boldsymbol{x}_a(k)-\boldsymbol{x}(k)\|>\alpha,\ \alpha>0\\ &\lim_{k\to T}\|\boldsymbol{r}_a(k)\|\leq\varepsilon, \qquad 0<\varepsilon<1 \end{aligned} \tag{8}$$

其中, $\boldsymbol{x}_a(k)$ 和 $\boldsymbol{r}_a(k)$ 是遭受攻击时系统的状态变量和残差. 对攻击者克服检测机制的隐蔽性进行分析[4]. 由输出方程可得

$$\begin{aligned} \boldsymbol{r}_a=&\|(\boldsymbol{y}+\boldsymbol{a})-H(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\\ &\|(\boldsymbol{y}-H\hat{\boldsymbol{x}})+(\boldsymbol{a}-H\boldsymbol{c})\|\leq\\ &\|\boldsymbol{y}-H\hat{\boldsymbol{x}}\|+\|\boldsymbol{a}-H\boldsymbol{c}\|=\boldsymbol{r}+\tau_a \end{aligned} \tag{9}$$

式中, $\boldsymbol{a}$ 表示攻击信号, $\hat{\boldsymbol{x}}$ 表示状态估计值, $\boldsymbol{c}$ 表示状态变化量. 由式 (9) 知, 当 $\boldsymbol{a}=H\boldsymbol{c}$ 时, $\boldsymbol{r}_a=\boldsymbol{r}$, 从输出残差角度考虑, 实现了隐蔽性.

由上述分析可知, 从输出残差角度无法实现攻击检测. 所以, 需要借助滤波器从系统状态入手, 利用状态差值检测攻击信号. 本文考虑通过基于自适应平方根无迹卡尔曼滤波器的方法, 从系统状态入手来检测此种攻击.

2 自适应平方根无迹卡尔曼滤波

本文提出将噪声估计环节[14] 加入到无迹卡尔曼滤波算法中, 实现对于噪声统计特性的在线估计, 同时改变标准 UKF 中状态误差协方差矩阵的迭代方式来保证滤波器的稳定性.

2.1 平方根无迹变换

本小节给出平方根无迹变换的实现方式.

步骤 1. 利用 $k-1$ 时刻的估计状态及状态误差协方差矩阵来计算 sigma 采样点 ξ_i, 并给出其权值 $W_{m,\,i}$ 和 $W_{c,\,i}$.

$$\begin{cases} \xi_{\boldsymbol{i},\,k-1}=\hat{\boldsymbol{x}}_{k-1}, & i=1\\ \xi_{\boldsymbol{i},\,k-1}=\hat{\boldsymbol{x}}_{k-1}+\gamma(S_{k-1})_i, & i=2,\cdots,n+1\\ \xi_{\boldsymbol{i},\,k-1}=\hat{\boldsymbol{x}}_{k-1}-\gamma(S_{k-1})_i, & i=n+2,\cdots,2n+1 \end{cases}$$

式中, n 代表状态的维数, $\gamma=\sqrt{n+\lambda}$. 这里不再借助 $\hat{P}_{k-1}$ 构造采样点, 而用 S_{k-1}. S_{k-1} 是对状态误差协方差矩阵 P 进行 QR 分解得到的 P 的平方根, QR 分解返回的是 P 的 Cholesky 分解的平方根的转置, 即 $(\sqrt{(n+\lambda)P})^{\mathrm{T}}$, 故 $(\boldsymbol{S}_{k-1})_i$ 等于 $(\sqrt{(n+\lambda)P})_i^{\mathrm{T}}$, 这两种 sigma 点的选取方法在数学上是等价的.

$$W_{i,\,m}=\begin{cases}\frac{\lambda}{n+\lambda}, & i=1\\ \frac{1}{2(n+\lambda)}, & i=2,\cdots,2n+1\end{cases}$$

$$W_{i,\,c}=\begin{cases}\frac{\lambda}{n+\lambda}+(1+\beta-\alpha^2), & i=1\\ \frac{1}{2(n+\lambda)}, & i=2,\cdots,2n+1\end{cases}$$

式中, $\lambda=\alpha^2(n+\kappa)-n$ 用来控制采样点之间的距离, 一般 $10^{-4}\leq\alpha\leq1$, $\beta=2$, $n+\kappa=3$ [8].

步骤 2. 计算 sigma 点通过非线性函数的传播结果

$$\begin{aligned}&\tau_i = f(\xi_i),\quad i = 1, \cdots, 2n+1\\ &\boldsymbol{z} = \sum_{i=1}^{2n+1} W_{m,\,i}\boldsymbol{\tau}_i\\ &P_x = \sum_{i=1}^{2n+1} W_{c,\,i}(\boldsymbol{\tau}_i - \boldsymbol{z})(\boldsymbol{\tau}_i - \boldsymbol{z})^{\mathrm{T}}\end{aligned} \tag{10}$$

式 (10) 是无迹变换中的计算误差协方差矩阵的公式, 平方根无迹变换将式 (10) 换为

$$\begin{aligned}S_z = \boldsymbol{qr}(&\sqrt{\boldsymbol{W}_{c,\,1}}(\tau_1 - \boldsymbol{z}) \times \cdots \times\\ &\sqrt{\boldsymbol{W}_{c,\,2n+1}}(\tau_{2n+1} - \boldsymbol{z}))\end{aligned} \tag{11}$$

2.2　噪声估计方法

假设噪声是非零均值的高斯噪声, 本文使用的是 Sage-Husa 噪声估计器, 通过极大后验估计原理, 获得次优噪声估计值, 噪声估计部分可参考文献 [14].

对于系统 (6), 系统方程是非线性的, 输出方程是线性的, 所以噪声估计器为

$$\hat{\boldsymbol{q}}_{k+1} = \frac{1}{k}\left[(k-1)\hat{\boldsymbol{q}}_k + \hat{\boldsymbol{x}}_{k+1} - \sum_{i=1}^{2n+1} W_i^m f_o(\xi_{i,\,k})\right]$$

$$\begin{aligned}\hat{Q}_{k+1} = &\frac{1}{k}\big[(k-1)\hat{Q}_k + K_{k+1}\boldsymbol{\varepsilon}_{k+1}\boldsymbol{\varepsilon}_{k+1}K_{k+1}^{\mathrm{T}} + P_{k+1} -\\ &\sum_{i=1}^{2n+1} W_i^c(\boldsymbol{\tau}_{i,\,k+1|k} - \hat{\boldsymbol{x}}_{k+1|k})\times\\ &(\boldsymbol{\tau}_{i,\,k+1|k} - \hat{\boldsymbol{x}}_{k+1|k})^{\mathrm{T}}\big]\end{aligned}$$

$$\hat{\boldsymbol{r}}_{k+1} = \frac{1}{k}\left[(k-1)\hat{\boldsymbol{r}}_k + \boldsymbol{y}_{k+1} - H\hat{\boldsymbol{x}}_{k+1|k}\right]$$

$$\hat{\boldsymbol{R}}_{k+1} = \frac{1}{k}\left[(k-1)\hat{\boldsymbol{R}}_k + \boldsymbol{\varepsilon}_{k+1}\boldsymbol{\varepsilon}_{k+1}^{\mathrm{T}} - HP_{k+1|k}H_k^{\mathrm{T}}\right]$$

式中, $\boldsymbol{\varepsilon}_k = \boldsymbol{y}_k - \hat{\boldsymbol{y}}_{k|k-1}$ 代表残差, K 代表滤波器增益矩阵.

2.3　自适应平方根无迹卡尔曼滤波设计

本节用到了 MATLAB 中的 3 个函数, 分别为: qr 函数, cholupdate 函数, diag 函数.

1) $qr\,(\cdot)$ 表示 QR 分解, $A \in \mathbf{R}^{m\times l}$, $[Q,\,R] = qr(A)$, 该函数生成 $m \times l$ 上三角形矩阵 R 和 $m \times m$ 酉矩阵 Q, 从而, $A = Q \times R$.

2) $R1 = cholupdate(R,\,x)$, 返回 $A + xx'$ 的上三角 Cholesky 因子, x 是具有合适长度的一个列向量, 其中, $R = chol(A)$ 是 A 的原始 Cholesky 分解因子.

3) diag$\{\cdot\}$ 函数, $D = \mathrm{diag}\{v\}$, 返回以向量 $\boldsymbol{v}$ 的元素为主对角线的对角矩阵. $x = \mathrm{diag}\{A\}$, 返回 A 的主对角线元素的列向量. 对于式 (22) 中最外侧的 diag$\{\cdot\}$, 返回一个对角矩阵, 主对角线元素是每一次迭代得到的噪声矩阵主对角线元素的平方根的实时估计值.

自适应平方根无迹卡尔曼滤波 (Adaptive square-root UKF, ASRUKF) 算法的具体步骤如下.

步骤 1. 初始化 $(k = 1)$:

$$\begin{cases}\hat{\boldsymbol{x}}_1 = \mathrm{E}(\boldsymbol{x}_1)\\ S_1 = chol\left\{\mathrm{E}\left((\boldsymbol{x}_1 - \hat{\boldsymbol{x}}_1)(\boldsymbol{x}_1 - \hat{\boldsymbol{x}}_1)^{\mathrm{T}}\right)\right\}\\ \sqrt{\hat{Q}_1} = S_1\\ \hat{\boldsymbol{q}}_1 = 0\end{cases} \tag{12}$$

步骤 2. 对于 $k = 2, 3, \cdots,$ 进行迭代

a) 时间更新

计算 sigma 点, 构造矩阵

$$\boldsymbol{\xi}_{k-1} = [\hat{\boldsymbol{x}}_{k-1}\hat{\boldsymbol{x}}_{k-1} + \gamma(S_{k-1})_i\hat{\boldsymbol{x}}_{k-1} - \gamma(S_{k-1})_i] \tag{13}$$

$$\begin{cases}\tau_{i,\,k|k-1} = f(\boldsymbol{\xi}_{i,\,k-1}) + \boldsymbol{q}\\ \boldsymbol{x} = \sum\limits_{i=1}^{2n+1} W_{m,\,i}\tau_{i,\,k|k-1} + \hat{\boldsymbol{q}}\\ S_{k|k-1} = qr\left\{\left[\sqrt{W_{c,\,i}}(\tau_{2:2n+1} - \hat{\boldsymbol{x}}_{k|k-1})\sqrt{\hat{Q}_{k-1}}\right]\right\}\\ S = cholupdate\left\{\left[S_{k|k-1},\right.\right.\\ \qquad \left.\left.\sqrt{W_{c,\,i}}(\tau_{2:2n+1} - \hat{\boldsymbol{x}}_{k|k-1}),\,\pm\right]\right\}\end{cases} \tag{14}$$

b) 测量更新

$$\tilde{\boldsymbol{y}}_k = \boldsymbol{y}_k - H\hat{\boldsymbol{x}}_{k|k-1} \tag{15}$$

计算混合误差协方差矩阵平方根

$$P_{xy} = S_{k|k-1}^{\mathrm{T}}S_{k|k-1}H_k \tag{16}$$

计算新息协方差矩阵

$$S_{y,\,k} = qr\left\{\left[HS_{k|k-1})\sqrt{R}\right]^{\mathrm{T}}\right\} \tag{17}$$

计算滤波增益

$$K_k = \frac{\frac{P_{xy,\,k}}{S_{y,\,k}^{\mathrm{T}}}}{S_{y,\,k}} \tag{18}$$

更新状态值

$$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_{k|k-1} + K_k\tilde{\boldsymbol{y}}_k \tag{19}$$

更新状态误差协方差矩阵平方根

$$\begin{cases}U = K_kS_{y,\,k}^{\mathrm{T}}\\ S_k = cholupdate\left\{S_{k|k-1}U - 1\right\}\end{cases} \tag{20}$$

估计过程噪声均值

$$\hat{\boldsymbol{q}}_{k+1} = \frac{1}{k}\left[(k-1)\hat{\boldsymbol{q}}_k + \hat{\boldsymbol{x}}_{k+1} - \sum_{i=1}^{2n+1} W_i^m f_o(\boldsymbol{\xi}_{i,\,k})\right] \tag{21}$$

估计过程噪声协方差矩阵平方根

$$\begin{cases}\sqrt{Q1}=cholupdate\left\{\sqrt{\hat{Q}_{k-1}},\left|\hat{\boldsymbol{x}}_k-\hat{\boldsymbol{x}}_{k|k-1}\right|,\dfrac{1}{k}\right\}\\ \sqrt{Q2}=cholupdate\left\{\sqrt{Q1},U,-\dfrac{1}{k}\right\}\\ \sqrt{\hat{Q}_k}=\mathrm{diag}\left\{\sqrt{\mathrm{diag}\left\{\sqrt{Q2}\sqrt{Q2}^{\mathrm{T}}\right\}}\right\}\end{cases}\tag{22}$$

注 1. Sage-Husa 噪声估计器不能同时处理过程噪声和测量噪声都未知的情况, 否则会造成滤波发散, 故上述算法假设测量噪声的均值和方差均是已知的[15].

注 2. 式 (14) 的最后一个子式中, ± 表示当 $W_{c,1}>0$ 时, 取正; 反之, 取负, 以保证根号下不出现负数[16].

2.4 自适应平方根无迹卡尔曼滤波稳定性

本小节给出自适应平方根无迹卡尔曼滤波算法的估计误差保持随机有界性的充分条件, 并给出证明.

对于非线性电网系统 (6)

$$\begin{aligned}\boldsymbol{x}_k&=f_o(\boldsymbol{x}_{k-1})+B_o\boldsymbol{u}+\boldsymbol{q}+\boldsymbol{\mu}_{k-1}\\ \boldsymbol{y}_k&=H\boldsymbol{x}_{k-1}+\boldsymbol{r}+\boldsymbol{v}_k\end{aligned}\tag{23}$$

定义

$$\tilde{\boldsymbol{x}}_k=\boldsymbol{x}_k-\hat{\boldsymbol{x}}_k\tag{24}$$

$$\tilde{\boldsymbol{x}}_{k|k-1}=\boldsymbol{x}_k-\hat{\boldsymbol{x}}_{k|k-1}\tag{25}$$

在 $\hat{\boldsymbol{x}}_{k-1}$ 处对 $\boldsymbol{x}_k$ 泰勒级数展开

$$\begin{aligned}\boldsymbol{x}_k=&f_o(\hat{\boldsymbol{x}}_{k-1})+B_o\boldsymbol{u}+\boldsymbol{q}+\nabla f_o(\hat{\boldsymbol{x}}_{k-1})\tilde{\boldsymbol{x}}_{k-1}+\\ &\frac{1}{2}\nabla^2 f_o(\hat{\boldsymbol{x}}_{k-1})\tilde{\boldsymbol{x}}_{k-1}^2+\cdots+\omega\end{aligned}\tag{26}$$

其中

$$\nabla^i f_o(\hat{\boldsymbol{x}})\tilde{\boldsymbol{x}}^i=\left(\sum_{j=1}^{n}\tilde{\boldsymbol{x}}_j\frac{\partial}{\partial\boldsymbol{x}_j}\right)^i f_o(\boldsymbol{x})|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_{k-1}}$$

在 $\hat{x}_{k-1}$ 处对 $\hat{x}_{k|k-1}$ 泰勒级数展开

$$\begin{aligned}\hat{\boldsymbol{x}}_{k|k-1}=&\left(1-\frac{n}{n+\lambda}\right)\times(f(\hat{\boldsymbol{x}}_{k-1})+B\boldsymbol{u})+\boldsymbol{q}+\\ &\frac{1}{2(n+\lambda)}\times\sum_{i=2}^{n+1}\left(f\left[(\hat{\boldsymbol{x}}_{k-1})+\gamma(S_{k-1})_i\right]+\right.\\ &\left.B\boldsymbol{u}+\boldsymbol{q}\right)+\frac{1}{2(n+\lambda)}\times\sum_{i=2}^{n+1}\left(f\left[(\hat{\boldsymbol{x}}_{k-1})-\right.\right.\\ &\left.\left.\gamma(S_{k-1})_i\right]+B\boldsymbol{u}+\boldsymbol{q}\right)=\\ &f(\hat{\boldsymbol{x}}_{k-1})+B\boldsymbol{u}+\boldsymbol{q}+\nabla^2 f(\hat{\boldsymbol{x}}_{k-1})P_{k-1}\end{aligned}\tag{27}$$

将式 (26) 和式 (27) 代入式 (25), 得

$$\tilde{\boldsymbol{x}}_{k|k-1}=\beta_k F_k\tilde{\boldsymbol{x}}_{k-1}+\boldsymbol{\mu}_k\tag{28}$$

式中

$$F_k=\left.\frac{\partial f_o(\boldsymbol{x}_{k-1})}{\partial\boldsymbol{x}_{k-1}}\right|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_{k-1}}\tag{29}$$

其中, $\beta_k=\mathrm{diag}\{\beta_{1k},\cdots,\beta_{nk}\}$ 为未知的矩阵, 其作用是弥补建模一阶线性化引起的模型误差.

对于式 (24) 中的输出方程, 定义

$$\tilde{\boldsymbol{y}}_{k|k-1}=\boldsymbol{y}_k-\hat{\boldsymbol{y}}_{k|k-1}\tag{30}$$

式 (30) 可写成

$$\begin{aligned}\tilde{\boldsymbol{y}}_{k|k-1}=&H\boldsymbol{x}_k+\boldsymbol{r}+\boldsymbol{v}_k-(H\hat{\boldsymbol{x}}_{k|k-1}+\boldsymbol{r})=\\ &H\tilde{\boldsymbol{x}}_{k|k-1}+\boldsymbol{r}+\boldsymbol{v}_k\end{aligned}\tag{31}$$

由式 (14) 可知, $S_{k|k-1}$ 是 $\hat{P}_{k|k-1}$ 的平方根, 根据 $qr(\cdot)$ 函数的模式 $[Q,R]=qr(A)$, 此时

$$A=\left[\sqrt{W_{c,i}}\left(\boldsymbol{\tau}_{2:2n+1,k|k-1}-\hat{\boldsymbol{x}}_{k|k-1}\right)\sqrt{\hat{Q}_{k-1}}\right]^{\mathrm{T}}$$

使用 $qr(\cdot)$ 函数有 $A=Q\times R$, 那么

$$\begin{aligned}R^{\mathrm{T}}R=&RQ^{\mathrm{T}}QR=A^{\mathrm{T}}A=\\ &\sum_{i=2}^{2n+1}\omega_i\left(\boldsymbol{\tau}_{i,k|k-1}-\hat{\boldsymbol{x}}_{k|k-1}\right)^{\mathrm{T}}\times\\ &\left(\boldsymbol{\tau}_{i,k|k-1}-\hat{\boldsymbol{x}}_{k|k-1}\right)+\hat{Q}_k\end{aligned}$$

再根据 *cholupdate* 函数的模式, 此时

$$\begin{aligned}S_{k|k-1}^{\mathrm{T}}S_{k|k-1}=&R^{\mathrm{T}}R+\sqrt{W_{c,1}}\left(\boldsymbol{\tau}_{1,k|k-1}-\hat{\boldsymbol{x}}_{k|k-1}\right)\times\\ &\sqrt{W_{c,1}}\left(\boldsymbol{\tau}_{1,k|k-1}-\hat{\boldsymbol{x}}_{k|k-1}\right)^{\mathrm{T}}=\\ &P_{k|k-1}\end{aligned}\tag{32}$$

与之对比, 先验状态误差协方差矩阵的实际值为

$$\begin{aligned}P_{k|k-1}=&\mathrm{E}\left(\tilde{\boldsymbol{x}}_{k|k-1}\tilde{\boldsymbol{x}}_{k|k-1}^{\mathrm{T}}\right)=\\ &\mathrm{E}\left((\beta_k F_k\hat{\boldsymbol{x}}_{k-1}+\boldsymbol{\mu}_k)(\beta_k F_k\hat{\boldsymbol{x}}_{k-1}+\boldsymbol{\mu}_k)^{\mathrm{T}}\right)=\\ &\beta_k F_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\Delta P_{k|k-1}+Q_{k-1}\end{aligned}\tag{33}$$

式中, $\Delta P_{k|k-1}$ 是 $\mathrm{E}\left((\beta_k F_k\tilde{\boldsymbol{x}}_{k-1})(\beta_k F_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}\right)$ 与 $\beta_k\times F_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k$ 的差值. 引入 $\delta P_{k|k-1}$ 来表示误差协方差矩阵的真实值 $P_{k|k-1}$ 与 $\hat{P}_{k|k-1}$ 的差异, 式 (32) 可写为

$$\begin{aligned}\hat{P}_{k|k-1}=&P_{k|k-1}+\delta P_{k|k-1}=\\ &\beta_k F_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\Delta P_{k|k-1}+\\ &Q_k+\delta P_{k|k-1}=\\ &\beta_k F_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\Xi_{k-1}\end{aligned}\tag{34}$$

此时, $\delta P_{k|k-1}$ 中包含了 Q_k 与 $\hat{Q}_k$ 的差值, 因为在 ASRUKF 算法中噪声信息是未知的. 其中, $\Xi_k=$

$\Delta P_{k|k-1}+Q_k+\delta P_{k|k-1}$.

预测测量协方差矩阵 $\hat{P}_{yy}$、互协方差矩阵 $\hat{P}_{xy}$ 以及后验状态误差协方差矩阵 $\hat{P}_k$ 可以写成

$$\hat{P}_{yy}=H\hat{P}_{k|k-1}H^{\mathrm{T}}+R_k \tag{35}$$

$$\hat{P}_{xy}=\hat{P}_{k|k-1}H^{\mathrm{T}} \tag{36}$$

$$\hat{P}_k=\hat{P}_{k|k-1}-\hat{P}_{xy}\hat{P}_{yy}^{-1}\hat{P}_{xy}^{\mathrm{T}} \tag{37}$$

引理 1[17]**.** 对于一个随机变量 ξ_k 及其函数 $V(\xi_k)$, 实数 $\upsilon_{\min}$, $\upsilon_{\max}$, $\mu>0$, $0<\lambda\leq 1$ 对于任意的 k, 若满足以下两个不等式性质:

$$\begin{aligned}&\upsilon_{\min}\|\boldsymbol{\xi}_k\|^2\leq V(\xi_k)\leq\upsilon_{\max}\|\boldsymbol{\xi}_k\|^2\\&\mathrm{E}(V(\boldsymbol{\xi}_k)\,|\boldsymbol{\xi}_{k-1})-V(\boldsymbol{\xi}_{k-1})\leq\mu-\lambda V(\boldsymbol{\xi}_{k-1})\end{aligned} \tag{38}$$

则该随机变量均方有界, 即

$$\begin{aligned}\mathrm{E}\left(\|\xi_k\|^2\right)\leq&\frac{\upsilon_{\max}}{\upsilon_{\min}}\mathrm{E}\left(\|\xi_0\|^2\right)(1-\lambda)^k+\\&\frac{\mu}{\upsilon_{\min}}\sum_{i=1}^{k-1}(1-\lambda)^i\end{aligned} \tag{39}$$

引理 2[17]**.** 假设矩阵 $A\in\mathbf{R}^{n\times m}$, $B\in\mathbf{R}^{m\times n}$, $C\in\mathbf{R}^{n\times n}$, 如果 $A>0$, $C>0$, 则有

$$A^{-1}>B(B^{\mathrm{T}}AB+C)^{-1}B^{\mathrm{T}} \tag{40}$$

引理 3[17]**.** 假设矩阵 $A\in\mathbf{R}^{n\times n}$, $C\in\mathbf{R}^{n\times n}$, 如果 $A>0$, $C>0$, 则有

$$A^{-1}>(A+C)^{-1} \tag{41}$$

定理 1. 对于非线性系统 (23), 如果有如下假设条件成立

1) 对于任意的 k, 存在实数 $f_{\min}$, $h_{\min}$, $\beta_{\min}$, $f_{\max}$, $h_{\max}$, $\beta_{\max}\neq 0$, 使得下式成立:

$$\begin{aligned}&f_{\min}^2I\leq F_kF_k^{\mathrm{T}}\leq f_{\max}^2I\\&h_{\min}^2I\leq H_kH_k^{\mathrm{T}}\leq h_{\max}^2I\\&\beta_{\min}^2I\leq\beta_k\beta_k^{\mathrm{T}}\leq\beta_{\max}^2I\end{aligned} \tag{42}$$

2) 存在实数 $\Xi_{\max}$, $\Xi_{\min}$, $r_{\min}$, $p_{\max}$, $p_{\min}$, 使得下式成立:

$$\begin{aligned}&p_{\min}I\leq P_k\leq p_{\max}I\\&\Xi_{\min}I<\Xi_k\leq\Xi_{\max}I\\&r_{\min}I\leq R_k\end{aligned} \tag{43}$$

那么自适应平方根无迹卡尔曼滤波算法的状态估计误差将是均方有界的, 即自适应平方根无迹卡尔曼滤波器稳定.

证明. 选择函数

$$V_k(\tilde{x}_k)=\tilde{x}_k^{\mathrm{T}}\hat{P}_k^{-1}\tilde{x}_k \tag{44}$$

由式 (43) 可知

$$\frac{1}{p_{\max}}\|\tilde{x}_k\|^2\leq V(\tilde{x}_k)\leq\frac{1}{p_{\min}}\|\tilde{x}_k\|^2$$

满足了引理 1 中第 1 个性质, 为满足引理 1, 还需要得到式 (38) 中第 2 个性质 $\mathrm{E}[V_k(x_k)]-V_{k-1}(\tilde{x}_{k-1})$ 的上界.

后验状态误差协方差矩阵 $\hat{P}_k$ 的另一种表达式为

$$\hat{P}_k=\hat{P}_{k|k-1}-\hat{P}_{xy}\hat{P}_{yy}^{-1}\hat{P}_{xy}^{\mathrm{T}}=(I-K_kH_k)\hat{P}_{k|k-1} \tag{45}$$

其中

$$K_k=\hat{P}_{k|k-1}H_k^{\mathrm{T}}(H_k\hat{P}_{k|k-1}H_k^{\mathrm{T}}+R_k)^{-1} \tag{46}$$

$$\tilde{x}_k=x_k-(\hat{x}_{k|k-1}+\hat{P}_{xy}\hat{P}_{yy}^{-1}\tilde{y}_k)=\tilde{x}_{k|k-1}-K_k\tilde{y}_k \tag{47}$$

将式 (47) 代入式 (44), 得

$$\begin{aligned}V_k(\tilde{\boldsymbol{x}}_k)=&\left(\tilde{\boldsymbol{x}}_{k|k-1}-K_k\tilde{\boldsymbol{y}}_k\right)^{\mathrm{T}}\hat{P}_k^{-1}\left(\tilde{\boldsymbol{x}}_{k|k-1}-K_k\tilde{\boldsymbol{y}}_k\right)=\\&\tilde{\boldsymbol{x}}_{k|k-1}\hat{P}_k^{-1}\tilde{\boldsymbol{x}}_{k|k-1}-\left[H_k\tilde{\boldsymbol{x}}_{k|k-1}+v_k\right]^{\mathrm{T}}\times\\&K_k^{\mathrm{T}}\hat{P}_k^{-1}\tilde{\boldsymbol{x}}_{k|k-1}-\tilde{x}_{k|k-1}^{\mathrm{T}}\hat{P}_k^{-1}K_k\left[H_k\tilde{x}_{k|k-1}+\right.\\&\left.v_k\right]+\left[H_k\tilde{\boldsymbol{x}}_{k|k-1}+v_k\right]^{\mathrm{T}}K_k^{\mathrm{T}}\times\\&\hat{P}_k^{-1}K_k\left[H_k\tilde{\boldsymbol{x}}_{k|k-1}+v_k\right]\end{aligned} \tag{48}$$

式 (46) 的另一种等价形式为

$$K_k=(I-K_kH_k)\hat{P}_{k|k-1}H_k^{\mathrm{T}}R_k^{-1}=\hat{P}_kH_k^{\mathrm{T}}R_k^{-1} \tag{49}$$

式 (45) 用矩阵求逆公式得

$$\hat{P}_k^{-1}=\hat{P}_{k|k-1}^{-1}+H_k^{\mathrm{T}}R_k^{-1}H_k \tag{50}$$

将式 (49), 式 (50) 和式 (28) 代入式 (48) 中, 式 (48)的条件期望为

$$\begin{aligned}\mathrm{E}(V_k(\tilde{x}_k)\,|\tilde{x}_{k-1})=\mathrm{E}\Big(&(A_{k-1}\tilde{x}_{k-1}+\mu_k)^{\mathrm{T}}\times\\&\hat{P}_{k|k-1}^{-1}(A_{k-1}\tilde{x}_{k-1}+\mu_k)-\\&\left[B_k\left(A_{k-1}\tilde{x}_{k-1}+\mu_k\right)\right]^{\mathrm{T}}\\&\left(\Sigma_k^{-1}-\Sigma_k^{-1}B_k\hat{P}_kB_k^{\mathrm{T}}\Sigma_k^{-1}\right)\times\\&\left[B_k(A_{k-1}\tilde{x}_{k-1}+\mu_k)\right]+\\&v_k^{\mathrm{T}}\Sigma_k^{-1}B_k\hat{P}_kB_k^{\mathrm{T}}\Sigma_k^{-1}v_k\,|\tilde{x}_{k-1}\Big)\end{aligned} \tag{51}$$

将式 (34) 代入式 (51) 中, 并由引理 3 得

$$\begin{aligned}&\mathrm{E}\Big(V_k(\tilde{\boldsymbol{x}}_k)\,|\tilde{\boldsymbol{x}}_{k-1}\Big)\le\\&\mathrm{E}\Big((\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}\Big(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k\Big)^{-1}\times\\&(\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})+\omega_k^{\mathrm{T}}(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}\times\\&\omega_k-(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}\times[H_k\,(\beta_k\,F_k\hat{P}_{k-1}F_k^{\mathrm{T}}\times\\&\beta_k+\hat{Q}_k\Big)H_k^{\mathrm{T}}+R_k]^{-1}(H_k\beta_kF_k\times\tilde{\boldsymbol{x}}_{k-1})-\\&(H_k\omega_k)^{\mathrm{T}}[H_k\,\Big(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k\Big)\times H_k^{\mathrm{T}}+\\&R_k]^{-1}(H_k\omega_k)+v_k^{\mathrm{T}}R_k^{-1}H_k\hat{P}_kH_k^{\mathrm{T}}R_k^{-1}v_k|\tilde{\boldsymbol{x}}_{k-1}\Big)\end{aligned}\tag{52}$$

观察式 (52) 的第 1 项

$$\begin{aligned}&\mathrm{E}\Big((\beta_kF_k\tilde{x}_{k-1})^{\mathrm{T}}\Big(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k\Big)^{-1}\times\\&(\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\,|\tilde{\boldsymbol{x}}_{k-1}\Big)=\\&\tilde{\boldsymbol{x}}_{k-1}^{\mathrm{T}}\hat{P}_{k-1}\tilde{\boldsymbol{x}}_{k-1}=V_{k-1}(\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{53}$$

两边同时减去式 (53), 得

$$\begin{aligned}&\mathrm{E}\Big(V_k(\tilde{\boldsymbol{x}}_k)\,|\tilde{\boldsymbol{x}}_{k-1}\Big)-V_{k-1}(\tilde{\boldsymbol{x}}_{k-1})\le\\&\mathrm{E}\Big(\omega_k^{\mathrm{T}}(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}-\\&(H_k\omega_k)^{\mathrm{T}}\times[H_k\,(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\\&\hat{Q}_k)H_k^{\mathrm{T}}+R_k]^{-1}(H_k\omega_k)+v_k^{\mathrm{T}}R_k^{-1}H_k\times\\&\hat{P}_kH_k^{\mathrm{T}}R_k^{-1}v_k|\tilde{\boldsymbol{x}}_{k-1}\Big)-(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}\times\\&[H_k\,(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)H_k^{\mathrm{T}}+\\&R_k]^{-1}\times(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{54}$$

观察式 (54) 的最后 1 项, 根据引理 3, 得

$$\begin{aligned}&\hat{P}_{k-1}^{-1}>(H_k\beta_kF_k)^{\mathrm{T}}\Big[(H_k\beta_kF_k)\hat{P}_{k-1}(H_k\beta_kF_k)^{\mathrm{T}}+\\&H_k\hat{Q}_kH_k^{\mathrm{T}}+R_k\Big]^{-1}(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{55}$$

式 (55) 分别左右乘 $\tilde{\boldsymbol{x}}_{k-1}$, 有

$$\begin{aligned}&\tilde{\boldsymbol{x}}_{k-1}^{\mathrm{T}}\hat{P}_{k-1}^{-1}\tilde{\boldsymbol{x}}_{k-1}>(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}[(H_k\beta_kF_k)\hat{P}_{k-1}\times\\&(H_k\beta_kF_k)^{\mathrm{T}}+H_k\Xi_kH_k^{\mathrm{T}}+R_k]^{-1}(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{56}$$

选择

$$\begin{aligned}\lambda_k=&\Big\{(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})^{\mathrm{T}}\Big[(H_k\beta_kF_k)\hat{P}_{k-1}\times\\&(H_k\beta_kF_k)^{\mathrm{T}}+H_kQ_kH_k^{\mathrm{T}}+R_k\Big]^{-1}\times\\&(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\Big\}/(\tilde{\boldsymbol{x}}_{k-1}^{\mathrm{T}}\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{57}$$

由式 (56) 和式 (57) 可知, $\lambda_k<1$, 得

$$\begin{aligned}\lambda_k\ge&\,p_{\min}(h_{\min}\beta_{\min}f_{\min})^2\times\\&\big[p_{\max}(h_{\max}\beta_{\max}f_{\max})^2+\\&\hat{q}_{\max}h_{\max}^2+r_{\max}\big]^{-1}=\lambda_{\min}>0\end{aligned}\tag{58}$$

由式 (57), 得

$$\begin{aligned}&-(H_k\beta_kF_k)^{\mathrm{T}}[(H_k\beta_kF_k)\hat{P}_{k-1}(H_k\beta_kF_k)^{\mathrm{T}}+\\&H_k\hat{Q}_kH_k^{\mathrm{T}}+R_k]^{-1}(H_k\beta_kF_k\tilde{\boldsymbol{x}}_{k-1})\le\\&-\lambda_{\min}V_{k-1}(\tilde{\boldsymbol{x}}_{k-1})\end{aligned}\tag{59}$$

考虑式 (54) 中的其他项, 得

$$\begin{aligned}\mu_k=\mathrm{E}\Big(&\omega_k^{\mathrm{T}}\Big[(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}-\\&H_k{}^{\mathrm{T}}(H_k\,(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)H_k^{\mathrm{T}}+\\&R_k)^{-1}\times H_k\Big]\omega_k+\\&v_k^{\mathrm{T}}R_k^{-1}H_k\hat{P}_kH_k^{\mathrm{T}}R_k^{-1}v_k|\tilde{x}_{k-1}\Big)\end{aligned}\tag{60}$$

考虑式 (60) 两边都是标量, 取迹不会改变等式, 所以根据

$$\mathrm{tr}(AB)=\mathrm{tr}(BA)\tag{61}$$

得到

$$\begin{aligned}\mu_k=\mathrm{tr}\Big\{&\Big[(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}-H_k^{\mathrm{T}}\times\\&(H_k\,(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)H_k^{\mathrm{T}}+\\&R_k)^{-1}H_k\Big]Q_k\Big\}+\mathrm{tr}\{[R_k^{-1}H_k\hat{P}_kH_k^{\mathrm{T}}]\,|\tilde{\boldsymbol{x}}_{k-1}\}\end{aligned}\tag{62}$$

根据引理 2, 得

$$\begin{aligned}&(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}-\\&H_k^{\mathrm{T}}[H_k(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\\&\hat{Q}_k)H_k^{\mathrm{T}}+R_k)^{-1}H_k]>0\end{aligned}\tag{63}$$

由式 (63) 可知 $\mu_k>0$, 由式 (42) 和式 (43), 得

$$\begin{aligned}\mu_k\le&\,\mathrm{tr}[(\beta_kF_k\hat{P}_{k-1}F_k^{\mathrm{T}}\beta_k+\hat{Q}_k)^{-1}\hat{Q}_k]+\\&\mathrm{tr}(R_k^{-1}H_k\hat{P}_kH_k^{\mathrm{T}})\le\\&\frac{q_{\max}}{\hat{q}_{\min}}\times L+\frac{h_{\max^2}p_{\max}}{r_{\min}}\times M=\mu_{\max}\end{aligned}\tag{64}$$

因此根据引理 1, 得

$$\mathrm{E}(V_k(x_k)) - V_{k-1}(\tilde{x}_{k-1}) \le \mu_{\max} - \lambda_{\min} V_{k-1}(\tilde{x}_{k-1}) \tag{65}$$

保证是 $\tilde{x}_k$ 有界的, 即

$$\mathrm{E}(\|\tilde{\boldsymbol{x}}_k\|^2) \le \frac{p_{\max}}{p_{\min}}\mathrm{E}(\|\tilde{\boldsymbol{x}}_0\|^2)(1-\lambda_{\min})^k + \frac{\mu_{\max}}{p_{\min}}\sum_{i=1}^{k-1}(1-\lambda_{\min})^i \tag{66}$$

因此, 自适应平方根无迹卡尔曼滤波算法状态估计误差将是均方有界的, 即自适应平方根无迹卡尔曼滤波器是稳定的. □

注 3. 因为误差序列 $\{\hat{\boldsymbol{x}}_k, k \ge 1\}$ 是随机过程, $\mathrm{E}(\|\tilde{\boldsymbol{x}}_k\|^2)$ 是该随机过程的均值函数, 随机有界指该随机过程有界. 即对于任意时刻 k, 对于服从高斯分布的噪声 ω, 定理 1 确保了误差 $\tilde{\boldsymbol{x}}_k$ 的 2 范数平方的期望值是有界的, 即 $\mathrm{E}(\|\tilde{\boldsymbol{x}}_k\|^2) \le \alpha$ 上限 α 的值由定理 1 确定.

3　检测方法

本节分析了文献 [6], [10−11] 中所使用的检测方法的不足之处. 提出一种新的检测方法, 利用中心极限定理设计新的检测算法, 依据随机变量的统计特性提出双边假设检验法检测攻击, 从误检率方面对本文算法给出分析, 并与巴氏系数检测算法[10]、欧几里德检测算法[11] 进行对比与分析.

文献 [6] 针对虚假数据注入攻击, 构造了 CUSUM 算法来检测攻击. 该算法步骤如下:

$$\chi_t = (y_t - H_k\hat{x}_{t|t-1})\Sigma_t^{-1}(y_t - H_k\hat{x}_{t|t-1})$$

$$p_t = 1 - F(\chi_t)$$

$$s_t = \log\left(\frac{\alpha}{p_t}\right)$$

$$\Gamma = \inf\{t : g_t \ge h\}$$

$$g_t = \max\{0,\, g_{t-1} + s_t\}$$

文献 [6] 中假设噪声服从高斯分布, 可知 χ_t 服从 χ^2 分布. $F(\cdot)$ 表示 χ^2 分布的概率分布函数, p_t 表示 χ^2 分布的上 (右) 尾概率, α 表示系统给定的上 (右) 尾概率用于检验 y_t 是否是异常值. 根据 χ^2 分布的上 α 分位点性质, 当 y_t 是异常值时, $s_t > 0$; 当 y_t 是正常值时, $s_t \le 0$. 当 y_t 是异常值时, g_t 的值会随时间累积直到超过检测阈值 h (h 的确定参考文献 [6]), 此时发出警报. 该算法通过引入 h, 避免了欧氏检测算法那种仅考虑误检率的阈值设计方法, 在误检率和误检周期之间做到了平衡, 既降低了噪声的影响, 又可以尽快检测出攻击.

但是, 该算法实质上是依赖与噪声的高斯分布特性, 即, 实质上还是 χ^2 检测, 所以在遇到本文所研究的攻击时, 攻击前后的残差基本保持不变, 因此该算法是不可用的.

文献 [10] 中针对具有隐蔽性的复数域攻击, 提出一种检测思想, 滤波器在不受攻击下工作和滤波器在错误数据注入攻击下工作会产生两个服从高斯分布的残差序列, 通过计算上述两个服从高斯分布的残差序列的巴氏相似性系数 DB 来判断攻击是否发生.

当物理系统的基本动力学用线性系统和高斯统计特性的噪声进行建模时, 在正常操作期间, 残差序列 v^o 遵循零均值高斯分布 $v^o = \mathrm{N}(r^o, S^o)$, 攻击发生后残差序列 $v_k^a = \mathrm{N}(r_k^a, S_k^a)$.

$$DB(v^o, v_k^a) = \frac{1}{4}[R\{(r^o, r_k^a)^H \Lambda_k (r^o, r_k^a)\} + R\{(r^o, r_k^a)^H \tilde{\Lambda}_k (r^o, r_k^a)\}] + \frac{1}{2}\ln\frac{|\Gamma_k|}{\sqrt{|S^o|\,|S_k^a|}}$$

$$\Gamma_k = \frac{1}{2}(S^o + S_k^a) = \begin{bmatrix} \Gamma_k & \tilde{\Gamma}_k \\ \tilde{\Gamma}_k^* & \Gamma_k^* \end{bmatrix}$$

该检测方法的优点同时也是缺点, 即巴氏相似性系数 DB 能检测复数域攻击, 但也仅能检测复数域攻击. 因为系统中有无复数域攻击, 差异主要体现在 $DB(v^o, v_k^a)$ 的后两项上. 而本文的虚假数据注入攻击属于实数域范畴, 在正常操作期间, 残差序列 v^o 遵循零均值高斯分布 $v^o = \mathrm{N}(m_1, P_1)$, 攻击发生后残差序列 $v_k^a = \mathrm{N}(m_2, P_2)$, 实数域的巴氏距离计算式为

$$DB(v_k^o, v_k^a) = \frac{1}{8}[(m_1 - m_2)^{\mathrm{T}} P^{-1}(m_1 - m_2)] + \frac{1}{2}\ln\frac{\det P}{\sqrt{\det P_1 \times \det P_2}}$$

$$P = \frac{P_1 + P_1}{2}$$

Bhattacharyya 距离无法辨别虚假数据注入攻击前后两个残差序列的相似性, 因为虚假数据注入攻击前后残差保持不变. 除此之外, 该检测法的前提是线性系统, 因为线性运算虽然会改变系统中随机变量的均值和方差但并不会改变随机变量服从高斯分布的特性, 对于本文所研究的非线性系统, 这种方法是不可用的.

目前存在的检测方法大多是在加性噪声的基础上提出的, 在文献 [11] 中, 假设过程方程和量测方程相对于噪声是线性的, 即

$$\boldsymbol{x}_{k+1} = f(\boldsymbol{x}_k, u_k, t_k) + \omega_k$$

$$\boldsymbol{y}_{k+1} = h(\boldsymbol{x}_k,\, t_k) + v_k$$

文献 [11] 中, 欧氏检测法的阈值和误检率正是基于噪声项的附加性得到的, 因为噪声并不参与到非线性变换中, 所以噪声的特性就是假设的正态分布的特性, 使用正态分布的 3σ 原则设计阈值. 只有在这种前提下, 欧氏距离检测算法才是正确的. 实际上, 过程和量测方程相对于噪声也可能是非线性的, 即

$$\boldsymbol{x}_k = f(\boldsymbol{x}_k,\, u_k,\, t_k,\, \omega_k)$$

$$y_k = h(x_k,\, t_k,\, v_k)$$

在这种情况下, 欧氏距离检测法的阈值设计思想是行不通的, 因为噪声不再作为附加项, 而是直接参与到非线性变换中. 此时, 噪声不再服从正态分布, 统计特性未知, 因此阈值无法设计.

综上, 本文提出一种检测思想: 在攻击未发生时, 利用本文提出的非线性滤波方法, 根据总线 i 上传感器在时间范围 $[t_0,\, t_k]$ 收集到的测量数据获得系统状态估计值, 进而获得后验状态误差值 $\tilde{\boldsymbol{x}}_k$, 此时并不知道状态误差 $\tilde{\boldsymbol{x}}_k$ 这个随机变量服从什么分布, 而且也不用对该随机变量的统计特性作出假设. 本文将时间区间 $[t_0,\, t_k]$ 分成 l 个小区间, 对每一个小区间包含的 $\tilde{x}_k$ 使用中心极限定理[18] 构造随机变量 $\boldsymbol{S}_i\tilde{x} = \frac{1}{T}\sum_{k=1}^{T}\tilde{\boldsymbol{x}}_k$, 得到 l 个 $\boldsymbol{S}_i\tilde{x},\ i \in l$, 这 l 个随机变量是服从标准正态分布的, 当攻击发生时, $S_i\tilde{x}$ 会偏离标准整体分布, 从而达到检测攻击的目的.

本文所提出的检测方法从系统内部状态误差入手, 不受限于传感器参数的概率分布未知所带来的影响, 不受限于加性噪声和非加性噪声的情况, 可以成功地完成攻击检测, 并从数学角度给出了误检率与阈值之间的关系.

3.1 攻击检测

式 (24) 定义了随机变量 $\tilde{\boldsymbol{x}}_k$, 本节定义当系统未遭受攻击时, 变量为 $\tilde{\boldsymbol{x}}_k$; 当系统遭受攻击时, 变量为 $\tilde{\boldsymbol{x}}_k^a$. 下面分别计算这两个随机变量的两个统计特性, 均值和方差.

1) 当系统正常运行时

$$\begin{aligned}\mathrm{E}(\tilde{\boldsymbol{x}}_k) &= \mathrm{E}(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1} - K_k(\boldsymbol{y}_k - H_k\hat{\boldsymbol{x}}_{k|k-1})) = \\ &\quad \mathrm{E}(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1} - K_k(H_k\hat{\boldsymbol{x}}_k + v_k - H_k\hat{\boldsymbol{x}}_{k|k-1})) = \\ &\quad \mathrm{E}((I_k - K_kH_k)(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1}) - K_k\mathrm{E}(v_k)) = \\ &\quad (I_k - K_kH_k)\mathrm{E}(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1}) - K_k\mathrm{E}(v_k)\end{aligned} \tag{67}$$

当初值设置为 $\hat{\boldsymbol{x}}_0 = \mathrm{E}(\boldsymbol{x}_0)$ 时, 式 (67) 变为

$$\mathrm{E}(\tilde{\boldsymbol{x}}_k) = 0 \tag{68}$$

方差为

$$\begin{aligned}\hat{P}_k|k &= \mathrm{E}\left(\tilde{\boldsymbol{x}}_k\tilde{\boldsymbol{x}}_k^{\mathrm{T}}\right) = \\ &\quad \mathrm{E}\left[(I_k - K_kH_k)(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1}) - K_k\mathrm{E}(v_k\right] \times \\ &\quad [(I_k - K_kH_k)(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1}) - K_k\mathrm{E}(v_k)]^{\mathrm{T}} = \\ &\quad (I_k - K_kH_k)\hat{P}_{k|k-1}(I_k - K_kH_k)^{\mathrm{T}} + K_kR_kK_k^{\mathrm{T}}\end{aligned} \tag{69}$$

2) 当系统遭受攻击时

$$\begin{aligned}\mathrm{E}(\tilde{\boldsymbol{x}}_k^a) &= \mathrm{E}(\boldsymbol{x}_k^a - \hat{\boldsymbol{x}}_{k|k-1}^a - K_k(\boldsymbol{y}_k^a + a_k - H_k\hat{\boldsymbol{x}}_{k|k-1}^a)) = \\ &\quad \mathrm{E}(\boldsymbol{x}_k^a - \hat{\boldsymbol{x}}_{k|k-1}^a - \\ &\quad K_k(H_k\boldsymbol{x}_k^a + v_k + a_k - H_k\hat{\boldsymbol{x}}_{k|k-1}^a)) = \\ &\quad \mathrm{E}((I_k - K_kH_k)(\boldsymbol{x}_k^a - \hat{\boldsymbol{x}}_{k|k-1}^a) - K_k\mathrm{E}(v_k))\end{aligned} \tag{70}$$

方差为

$$\begin{aligned}\hat{P}_{k|k}^a &= \mathrm{E}[(\tilde{\boldsymbol{x}}_k^a)(\tilde{\boldsymbol{x}}_k^a)^{\mathrm{T}}] = \\ &\quad \mathrm{E}\{[(I_k - K_kH_k)(\boldsymbol{x}_k^a - \hat{\boldsymbol{x}}_{k|k-1}^a) - K_k\mathrm{E}(v_k + a_k)] \times \\ &\quad [(I_k - K_kH_k)(\boldsymbol{x}_k^a - \hat{\boldsymbol{x}}_{k|k-1}^a) - K_k\mathrm{E}(v_k + a_k)]^{\mathrm{T}} = \\ &\quad (I_k - K_kH_k)\hat{P}_{k|k-1}^a(I_k - K_kH_k)^{\mathrm{T}} + K_kR_kK_k^{\mathrm{T}}\end{aligned} \tag{71}$$

根据第 3.1 节的描述, 虽然得到了 $\tilde{x}_k$ 和 $\tilde{x}_k^a$ 的均值和方差, 但是无法确定随机变量 $\tilde{x}_k$ 和 $\tilde{x}_k^a$ 服从何种分布. 此时, 对于利用 $\tilde{x}_k$ 应用中心极限定理的性质, n 个独立随机变量之和的分布函数趋于正态分布函数.

现构造随机变量 $S\tilde{x} = \frac{1}{T}\sum_{k=1}^{T}\tilde{\boldsymbol{x}}_k$, 根据中心极限定理, 可知

$$S\tilde{x} \sim \mathrm{N}\left(\frac{1}{T}\sum_{k=1}^{T}\mathrm{E}(\tilde{\boldsymbol{x}}),\, \frac{1}{T}\sum_{k=1}^{T}\hat{P}_{k|k}\right)$$

同时按照上述形式构造 $S\tilde{x}^a = \frac{1}{T}\sum_{k=1}^{T}\tilde{\boldsymbol{x}}_k^a$, 注意此时 $S\tilde{x}^a$ 并不服从正态分布, 构造 $S\tilde{x}^a$ 是为了保持变量形式上的一致, 记 $S\tilde{x}^a$ 服从的分布为 A, 得

$$S\tilde{x}^a \sim A\left(\frac{1}{T}\sum_{k=1}^{T}\mathrm{E}(\tilde{\boldsymbol{x}}_k^a),\, \frac{1}{T}\sum_{k=1}^{T}\hat{P}_{k|k}^a\right)$$

为书写简便, 将 $S\tilde{x}$ 和 $S\tilde{x}^a$ 分别记为

$$S\tilde{x} \sim \mathrm{N}(m,\, \upsilon),\quad S\tilde{x}^a \sim A(m + r\upsilon,\, q\upsilon)$$

其中, q 和 r 分别表示系统遭受攻击后均值和方差的变化. 本文使用 m 和 υ 作为系统正常行为的度量. 接下来, 建立了一对阈值 T_l 和 T_h, 用于检测系统是否遭受攻击, $T_l = m - k\upsilon$, $T_h = m + k\upsilon$, 表示允许偏离原数据的最大范围. 当随机变量 $S \notin [T_l,\, T_h]$ 时, 则确定系统遭受攻击[19]. 基于此, 提出一个双边假设检验

$$\begin{cases} H_0,\ S \in [T_l,\ T_h] \\ H_1,\ S \notin [T_l,\ T_h] \end{cases} \tag{72}$$

式中, H_0 代表系统没有遭受攻击, H_1 代表系统遭受攻击.

误检率 P_F 的定义是攻击没有发生却宣布攻击发生的概率, 即 $S\tilde{x} \sim \mathrm{N}(m,\ v)$, 同时, $|S\tilde{x} - m| > kv$.

$$P_F(k) = 1 - \int_{m-kv}^{m+kv} \frac{\exp(\frac{-(u-m)^2}{(2v^2)})}{v\sqrt{2\pi}}\mathrm{d}u = 1 - \Phi(k) + \Phi(-k)$$

4　仿真

本节验证本文设计的自适应平方根无迹卡尔曼滤波算法估计状态及所提出检测算法检测攻击有效性, 并与欧几里得检测方法进行对比. 仿真参数和初始值为 $m = [8.9,\ 8.8,\ 8.5]$, $d = [3.1,\ 3.4,\ 3.7]$, $u = [6.3,\ 1.6,\ 8.5]^{\mathrm{T}}$, $B = [0_{3\times 3};\mathrm{diag}\{1/m\}]$.

为了最小化由噪声引起的误报率, 欧几里得检测法的阈值设计采用 3σ 准则 (σ 是噪声信号的标准差), 那么得到先验阈值 $f = 3\sigma = 0.3$.

4.1　ASRUKF 滤波算法的有效性

对于模型 (6), 未遭受攻击时的状态估计, 从图 3 可以看出, ASRUKF 滤波器的滤波性能很好, 滤波精度很高.

4.2　虚假数据注入攻击下的三种检测方法

1) 欧几里得检测法[11]. 由图 4可知, 在迭代步数 $k = 30$ 时刻对系统注入攻击, 在 $k = 80$ 时刻成功检测到攻击, 欧几里得检测法可以成功检测出虚假数据注入攻击.

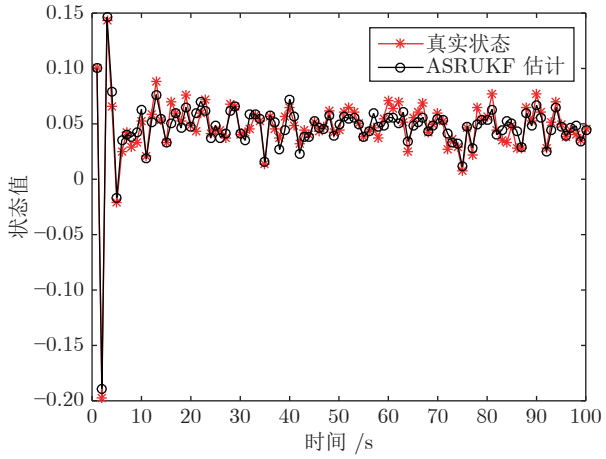

图 3　ASRUKF 下的状态估计

Fig. 3　State estimation in ASRUKF

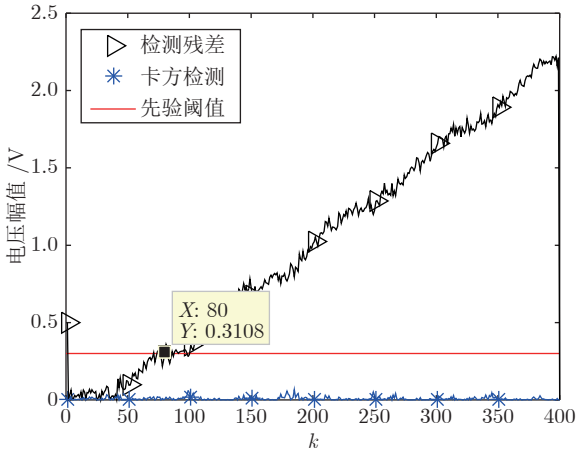

图 4　两种检测方法针对隐蔽假数据攻击

Fig. 4　Two detection methods for covert false data attack

2) 巴氏相似性系数检测法[10]. 巴氏系数范围为 0 到 1 之间. 越接近 0, 证明两序列越相似. 由图 5 可知, 巴氏相似性系数无法辨别虚假数据注入攻击前后两个残差序列的相似性, 不可以检测出虚假数据注入攻击.

3) 本文所提的检测方法. 首先, 使用分位数–分位数 (Quantile-quantile, Q-Q) 图来确定前面根据中心极限定理构造的 $S\tilde{x}$ 分布可以近似为高斯分布. 因为根据中心极限定理, 随机变量的数量越多, 它们的和也越近似服从高斯分布. 然而, 考虑实际情况, 取无限多的独立随机变量是不符合实际的, 所以在近似高斯分布的同时, 要尽量选取较少的独立随机变量. 要利用 Q-Q 图鉴别样本数据是否近似于高斯分布, 只需观察 Q-Q 图上的点是否近似地在一条直线附近.

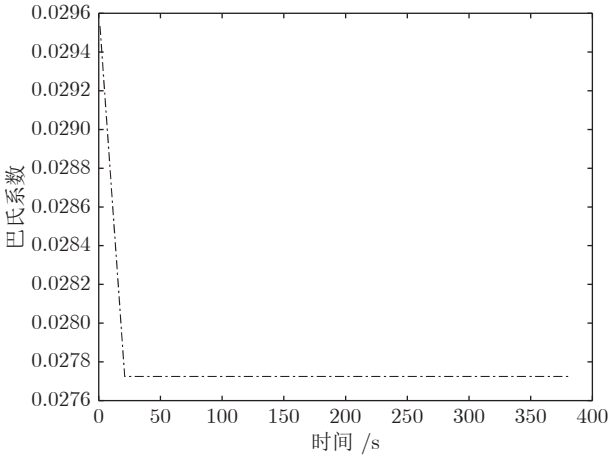

图 5　巴氏相似性系数

Fig. 5　Bhattacharyya coefficient

本文的检测算法选取了 $T = 30$ 个独立随机变量参与运算, 由图 6 可知, 数据的分布非常接近直线, 这证明 $S\tilde{x}$ 的分布可以视为高斯分布.

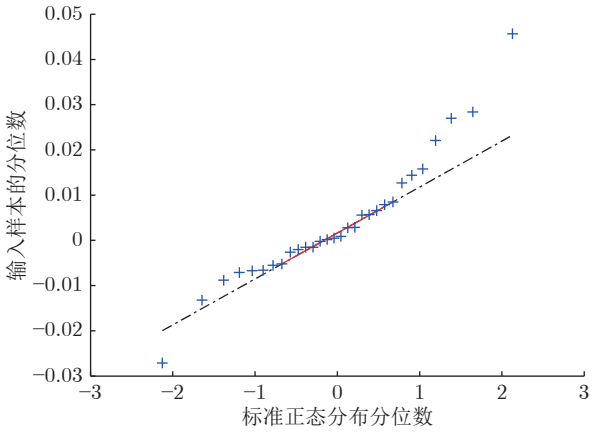

图 6 $S\tilde{x}$ 的 Q-Q 图

Fig. 6 Quantile-quantile plot of $S\tilde{x}$

由图 7 可以看出, 本文的检测算法对于隐蔽假数据攻击的有效性, 在迭代步数 $k = 30$ 处注入攻击, 选取 30 个迭代步骤下的随机变量构造出 $S\tilde{x}$, 所以在 $k = 60$ 处超过了阈值, 实现了攻击检测.

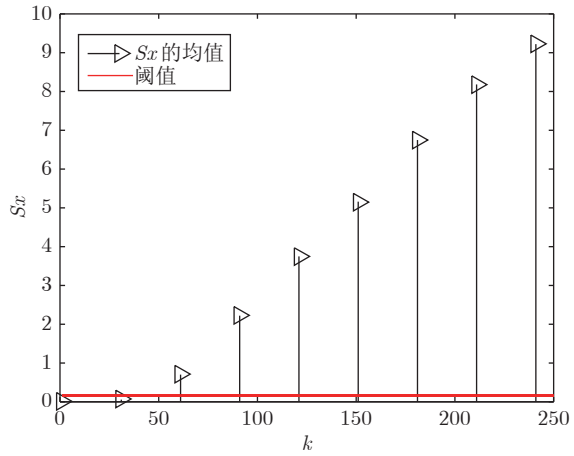

图 7 本文提出的攻击检测方法

Fig. 7 Attack detection proposed in this paper

图 8 给出了误检率随 k 变化的曲线.从图 8 可知, 一个算法的误检率过高, 是因为阈值设置得太低, 导致攻击之外的因素也会使得被检测的量超过阈值. 随着 k 值增大, 阈值变高, 误检率自然随之下降.

在图 8 中, 当 $k = 3$ 时, 误检率 $P_F = 0.0027$, 除此之外, 由图 4 可知, 欧氏检测法检测到攻击所用时间是 $\Delta k = 50$; 由图 8 可知, 检测到攻击所用时间是 $\Delta k = 30$, 检测用时更短.

综上, 对比三种检测方法可知, 本文提出的检测方法可以成功检测攻击不受限于传感器参数统计特性未知所带来的影响, 不受限于加性噪声和非加性噪声的情况, 对于实际系统的适用性更强.

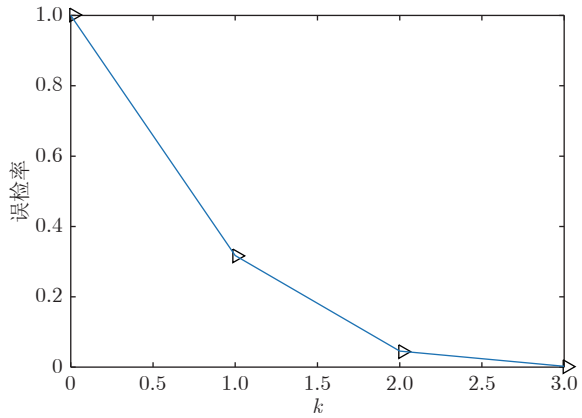

图 8 误检率 P_F

Fig. 8 False alarm rate P_F

5 结束语

本文研究了智能电网系统中虚假数据注入攻击的检测问题. 针对非线性系统, 噪声统计特性未知的情况, 本文使用自适应平方根无迹卡尔曼滤波算法对系统内部状态和噪声作出估计. 针对传感器参数统计特性未知和非加性噪声的情况, 利用中心极限定理构造出符合正态分布的随机变量, 基于该随机变量提出了一种攻击检测方法, 并从评价指标的角度对算法进行分析, 该算法对于实际系统的适用性更强.

References

1 Peng Da-Tian, Dong Jian-Min, Cai Zhong-Min, Zhang Chang-Qing, Peng Qin-Ke. On the stability of cyber-physical systems under false data injection attacks. *Acta Automatica Sinica*, 2019, **45**(1): 196−205
(彭大天, 董建敏, 蔡忠闽, 张长青, 彭勤科. 假数据注入攻击下信息物理融合系统的稳定性研究. 自动化学报, 2019, **45**(1): 196−205)

2 Wang Qi, Tai Wei, Tang Yi, Ni Ming. A review on false data injection attack toward cyber-physical power system. *Acta Automatica Sinica*, 2019, **45**(1): 72−83
(王琦, 邰伟, 汤奕, 倪明. 面向电力信息物理系统的虚假数据注入攻击研究综述. 自动化学报, 2019, **45**(1): 72−83)

3 Tong Xiao-Yang, Wang Xiao-Ru. Inferrence and countermeasure presuppostion of network attack in incdient on Ukrainian power grid. *Automation of Electric Power Systems*, 2016, **40**(7): 144−148
(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. 电力系统自动化, 2016, **40**(7): 144−148)

4 Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 2011, **14**(1): 1−34

5 Yang C, Yang W, Shi H. DoS attack in centralised sensor network against state estimation. *IET Control Theory and Applications*, 2018, **12**(9): 1244−1253

6 Kurt M N, Yılmaz Y, Wang X D. Secure distributed dynamic state estimation in wide-area smart grids. *IEEE Transactions on Information Forensics and Security*, 2020, **15**: 800−815

7 Weimer J, Kar S, Johansson K H. Distributed detection and isolation of topology attacks in power networks. In: Proceedings of the 1st ACM International Conference on High Confidence Networked Systems, Beijing, China. 2012. 65−71

8 Qi J J, Sun K, Wang J H, Liu H. Dynamic state estimation for multi-machine power system by unscented Kalman filter with enhanced numerical stability. *IEEE Transactions on Smart Grid*, 2018, **9**(2): 1184−1196

9 Mo Y L, Garone E, Casavola A, Sinopoli B. False data injection attacks against state estimation in wireless sensor networks. In: Proceedings of the 49th IEEE Conference on Decision and Control, Atlanta, USA: IEEE, 2010. 5967−5972

10 Mohammadi A, Plataniotis K N. Noncircular. Attacks on phasor measurement units for state estimation in smart grid. *IEEE Journal of Selected Topics in Signal Processing*, 2018, **12**(4): 777−789

11 Manandhar K, Cao X J, Hu F. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Transactions on Control of Network Systems*, 2014, **1**(4): 370−379

12 Yang Q Y, Yang J, Yu W, An D, Zhang N, Zhao W. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Transactions on Parallel and Distributed Systems*, 2014, **25**(3): 717−729

13 Liang Tian-Tian, Wang Mao. Robust algorithm for a class of sampled-data descriptor systems with missing measurements. *Journal of Chinese Inertial Technology*, 2018, **26**(2): 81−86
(梁天添, 王茂. 一类广义连续–离散系统量测丢失情况下鲁棒滤波算法. 中国惯性技术学报, 2018, **26**(2): 81−86)

14 Zhao Lin, Wang Xiao-Xu, Sun Ming, Ding Ji-Cheng, Yan Chao. Adaptive UKF filtering algorithm based on maximum a posterior estimation and exponential weighting. *Acta Automatica Sinica*, 2010, **36**(7): 1008−1019
(赵琳, 王小旭, 孙明, 丁继成, 闫超. 基于极大后验估计和指数加权的自适应UKF滤波算法. 自动化学报, 2010, **36**(7): 1008−1019)

15 Shi Yong, Han Chong-Zhao. Adaptive UKF method with applications to target tracking. *Acta Automatica Sinica*, 2011, **37**(6): 755−759
(石勇, 韩崇昭. 自适应UKF算法在目标跟踪中的应用. 自动化学报, 2011, **37**(6): 755−759)

16 Van der Merwe R, Wan E A. The square-root unscented Kalman filter for state and parameter estimation. In: Proceedings of the 2001 International Conference on Acoustics, Speech, and Signal Processing. New York, USA: IEEE, 2001. 3461−3464

17 Xiong K, Zhang H Y, Chan C W. Performance evaluation of UKF-based nonlinear filtering. *Automatica*, 2006, **42**(2): 261−270

18 Yu W, Griffith D, Ge L Q, Bhattarai S, Golmie N. An integrated detection system against false data injection attacks in the smart grid. *Security and Communication Networks*, 2015, **8**(2): 91−109

19 Hu J, Wang Z D, Gao H J. Recursive filtering with random parameter matrices, multiple fading measurements and correlated noises. *Automatica*, 2013, **49**(11): 3440−3448

罗小元 燕山大学自动化系教授. 2005 年获得燕山大学控制科学与工程学科博士学位. 主要研究方向为网络控制系统, CPS 网络攻击检测.
E-mail: xyluo@ysu.edu.cn
(**LUO Xiao-Yuan** Professor at the School of Electrical Engineering, Yanshan University. He received his Ph.D. degree in control science and engineering from Yanshan University in 2005. His research interest covers detection of cyber attack of CPS and networked control systems.)

潘雪扬 燕山大学控制科学与工程专业硕士研究生. 主要研究方向为卡尔曼滤波和智能电网攻击检测.
E-mail: onty123@126.com
(**PAN Xue-Yang** Master student in the Department of Control Science and Engineering, Yanshan University. His research interest covers Kalman filter and smart grid attack detection.)

王新宇 燕山大学电气工程系讲师. 2020 年获得燕山大学控制科学与工程学科博士学位. 主要研究方向为智能电网攻击检测与防御. 本文通信作者. E-mail: wangxinyuphd@163.com
(**WANG Xin-Yu** Lecturer in the Department of Electrical Engineering, Yanshan University. He received his Ph.D. degree in control science and engineering from Yanshan University in 2020. His research interest covers attack detection and defense in smart grid. Corresponding author of this paper.)

关新平 上海交通大学电子信息与电气工程学院教授. 1999 年获得哈尔滨工业大学控制科学与工程学科博士学位.主要研究方向为无线网络系统, CPS 网络攻击检测.
E-mail: xpguan@sjtu.edu.cn
(**GUAN Xin-Ping** Professor at the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. He received his Ph.D. degree in control science and engineering from Harbin Institute of Technology in 1999. His research interest covers wireless networked systems and detection of cyber attack in CPS.)