拒绝服务攻击下基于 UKF 的智能电网动态状态估计研究

李 雪 [1] 李雯婷 [1] 杜大军 [1] 孙 庆 [1] 费敏锐 [1]

摘 要 针对连续拒绝服务 (Denial of service, DoS) 攻击导致量测数据丢失使得动态状态估计失效、进而破坏智能电网安全经济运行问题, 本文提出了一种适用拒绝服务攻击的改进无迹卡尔曼滤波 (Unscented Kalman filter, UKF) 方法, 以进行智能电网动态状态估计. 首先, 分析拒绝服务攻击引起数据丢包特性并设计了数据补偿策略, 以重构电力系统动态模型; 然后, 结合 Holt′s 双参数指数平滑和无迹卡尔曼滤波方法, 构造了融合补偿信息的新状态估计方程, 并进一步基于估计误差协方差矩阵推导了状态增益更新方法, 从而得到了无迹卡尔曼滤波动态状态估计新方法. 最后, 针对 IEEE 30 和 118 节点系统进行仿真, 验证了所提方法的可行性和有效性.

关键词 智能电网, 动态状态估计, 拒绝服务攻击, 无迹卡尔曼滤波

引用格式 李雪, 李雯婷, 杜大军, 孙庆, 费敏锐. 拒绝服务攻击下基于 UKF 的智能电网动态状态估计研究. 自动化学报, 2019, **45**(1): 120−131

DOI 10.16383/j.aas.2018.c180431

Dynamic State Estimation of Smart Grid Based on UKF Under Denial of Service Attacks

LI Xue[1] LI Wen-Ting[1] DU Da-Jun[1] SUN Qing[1] FEI Min-Rui[1]

Abstract When continuous denial of service (DoS) attacks cause measurement data losses in smart grid, the traditional dynamic state estimation is useless, destroying the running safety of smart grid seriously. To solve the problem, an improved unscented Kalman filter (UKF) is proposed, which can estimate the dynamic state of smart grid under DoS attacks. Firstly, the characteristics of data packet losses resulting from DoS attacks are analyzed and data compensation strategy is designed to reconstruct the dynamic model of power system. Integrating Holt′s two-parameter exponential smoothing and unscented Kalman filter algorithms, a new state estimation equation including the compensation information is then constructed. Furthermore, a state gain updating method is derived from the estimated error covariance matrix, which produces a new enhanced UKF dynamic state estimation algorithm. Finally, simulations on IEEE 30-bus and 118-bus system confirm the feasibility and effectiveness of the proposed method.

Key words Smart grid, dynamic state estimation, denial of service (DoS) attacks, unscented Kalman filter (UKF)

Citation Li Xue, Li Wen-Ting, Du Da-Jun, Sun Qing, Fei Min-Rui. Dynamic state estimation of smart grid based on UKF under denial of service attacks. *Acta Automatica Sinica*, 2019, **45**(1): 120−131

近些年来, 信息通讯技术 (Information and communication technology, ICT) 应用不断推动着传统的电力系统向智能电网 (Smart grid, SG)[1−3] 快速发展. 智能电网是一种典型的物理信息融合系统 (Cyber physical system, CPS)[4−5], 它深度融合物理电网与信息网络, 有效实现信息流与能量流的双向流动, 通过信息化不断提高智能电网的自动化水平和运行效率.

在智能电网中, 量测数据通常存在着不完备、数据异常等问题, 必须进行状态估计 (State estimation, SE) 以准确和有效地监控传输线路负载或母线电压大小等状态信息, 从而为基于系统实时状态数据进行安全评估等提供支撑[6−9].

智能电网状态估计分为静态状态估计和动态状态估计. 静态状态估计算法目前较为成熟, 以最小二乘法等为主, 但其没有考虑系统的动态变化过程. 实际智能电网量测量与状态量实时变化, 动态状态估计比静态状态估计更符合电力系统的本质. 电力系统动态状态估计算法主要以扩展卡尔曼滤波 (Extend Kalman filter, EKF) 方法为主[10], 但

收稿日期 2018-07-17 录用日期 2018-09-27
Manuscript received July 17, 2018; accepted September 27, 2018
国家自然科学基金 (61773253, 61803252, 61633016, 61533010), 中国博士后科学基金 (2018M630425) 资助
Supported by National Natural Science Foundation of China (61773253, 61803252, 61633016, 61533010), and China Postdoctoral Science Foundation (2018M630425)
本文责任编委 吴立刚
Recommended by Associate Editor WU Li-Gang
1. 上海大学机电工程与自动化学院上海市电站自动化技术重点实验室 上海 200072
1. Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronics Engineering and Automation, Shanghai University, Shanghai 200072

EKF 算法在计算雅可比矩阵时存在线性化误差. 为解决该问题, Julier 等[11] 提出了无迹卡尔曼滤波 (Unscented Kalman filter, UKF) 方法, 通过无迹变换 (Unscented transform, UT) 近似地获取非线性变换后的统计特性, 与 EKF 算法相比, 无需求解雅可比矩阵, UKF 算法的精度与数值稳定性更好. 为此, 国内外学者已经开始研究基于 UKF 算法的电力系统状态估计. 文献 [12] 针对电力系统测量噪声统计特性未知的问题, 提出一种鲁棒广义极大似然的 UKF 算法进行状态估计. 文献 [13] 提出一种考虑测量相关性的 UKF 算法进行电力系统状态估计. 文献 [14] 提出了一种保证正定估计误差协方差的新 UKF 算法并用于状态估计. 以上研究工作主要集中在电力系统中如何提高 UKF 算法的估计精度和稳定性, 还未涉及网络安全引起的智能电网状态估计问题.

智能电网安全主要分为物理安全和网络安全两类. 物理安全指的是智能电网在严重干扰下仍能保持正常运行的能力, 而网络安全则是指支撑智能电网运行的通讯网络和计算机控制系统的安全[15−19]. 随着智能电网不断发展, 其网络安全问题不断暴露并且日益受到重视. 如 2015 年, 乌克兰电网遭受网络攻击造成大面积停电故障, 电网遭受包括拒绝服务 (Denial of service, DoS) 的多类型网络攻击[20]. 网络安全会严重影响通信性能, 进一步影响物理电网和通信网络深度融合的智能电网安全. 因此, 在智能电网状态估计中必须考虑网络攻击问题.

DoS 攻击是一种典型的网络攻击, 攻击者在通信网络信道上持续发送伪造数据包, 使得控制中心与远程终端的通信处于不可用状态, 信息无法正常地接收和送达[21], 这将导致数据包丢失 (即数据丢包), 从而影响智能电网状态估计性能. 无迹卡尔曼滤波动态状态估计利用过去的状态估计值及动态模型对当前时刻的状态量进行预测, 预测值通过网络参数和结线信息与系统量测值进行校正, 得到可靠性更高的当前时刻的状态量和辨识系统模型, 这是建立在数据有效的基础上. 然而, DoS 攻击引起量测量数据丢失, 无法进行正常的预测校正, 导致对智能电网的安全性和经济性进行错误的分析和判断, 从而威胁智能电网安全经济运行.

从以上分析可知, 现有基于 UKF 的智能电网动态状态估计主要集中在如何提高算法的估计精度和稳定性, 当发生 DoS 攻击导致量测量数据丢失时, 文献 [22] 采用伯努利分布描述其特性, 但对量测量丢失数据未补偿研究相关的 UKF 方法. 因此, 解决由于网络攻击导致的智能电网量测信息丢失问题面临新的困难和挑战: 1) DoS 攻击导致的数据连续丢包破坏了量测数据的完整性, 如何对丢失数据进行补偿并重构智能电网动态模型是一个挑战; 2) 传统基于完整性数据的 UKF 算法不能简单直接地应用于 DoS 攻击下的智能电网状态估计, 如何设计基于 UKF 的动态状态估计新方法是另一个挑战.

为了解决以上困难和挑战, 本文基于霍尔特指数平滑和无迹卡尔曼滤波技术, 提出了一种适用拒绝服务攻击的改进无迹卡尔曼滤波新方法, 主要贡献如下: 1) 从智能电网受到 DoS 攻击的角度研究 UKF 算法, 运用伯努利分布描述了 DoS 攻击的量测数据丢失特性并设计了数据补偿策略, 以重构智能电网动态模型; 2) 采用 Holt′s 双参数指数平滑方法刻画电力系统状态方程, 构造了融合补偿信息的新状态估计方程, 并进一步基于估计误差协方差矩阵推导了状态增益更新方法, 得到了无迹卡尔曼滤波动态状态估计新方法.

1　问题阐述

交流电力系统的动态空间模型由状态方程和量测方程表示:

$$\begin{aligned} x_{k+1} &= g\left(x_k\right) + w_k \\ z_k &= h\left(x_k\right) + v_k \end{aligned} \tag{1}$$

其中, $x_k \in \mathbf{R}^{n\times 1}$ 为 k 时刻系统状态向量, $z_k \in \mathbf{R}^{m\times 1}$ 为 k 时刻量测向量, $g(\cdot)$ 是一个 n 维的状态非线性函数向量, $h(\cdot)$ 是一个 m 维的量测非线性函数向量, $w_k \in \mathbf{R}^{n\times 1}$ 是均值为零、方差为 Q_k 的白噪声[23], $v_k \in \mathbf{R}^{m\times 1}$ 是均值为零、方差为 R_k 的测量噪声, 并且 w_k 和 v_k 不相关. 通常, 在给定电力网络结构和参数时, 状态量包括节点电压的幅值和相角, 量测向量包括节点电压、节点注入功率和支路潮流等.

传统电力系统长期运行在封闭的物理环境中, 在状态估计时不考虑通信网络安全带来的问题. 然而, 在智能电网中, 通信网络与传统电力网深度融合, 使得其从 “封闭” 走向 “开放” 极易导致恶意网络攻击, 其中 DoS 攻击是最典型的网络攻击之一. 当智能电网遭受 DoS 攻击, 一方面会导致传感器测量数据包丢失甚至有时连续丢失; 另一方面由于 DoS 能量有限会导致数据包丢失具有时变特性. 这将不可避免地影响状态估计结果, 进而危害系统安全运行. 因此, 为了降低数据包丢失影响, 首先需要分析数据丢包特性并设计有效的数据补偿策略.

针对数据包丢失, 首先可采用网络分析工具 (如无线网络 Airo Peek 和以太网 Ethereal 等) 捕获数据包, 然后根据数据包的类型标识、序号和时间戳等标记分析数据包是否正常或丢失, 再运用统计分析

方法建立系统模型. 目前针对数据包丢失的建模通常有两种, 第一种是采用伯努利分布来描述[24]; 第二种是采用马尔科夫链来描述[25]. 本文考虑 DoS 攻击导致的数据包连续丢失随机特性, 接下来采用第一种方法伯努利分布来进行刻画.

当攻击者发起最多 d 次连续 DoS 攻击时, 将会导致数据包连续丢失, 例如: 如果 $k-d$ 时刻的数据包成功传输, 攻击者从下一时刻开始发起攻击, 则连续攻击时间从 $k-d+1$ 时刻至 k 时刻, 在这段时间内最多有 d 个数据包丢失, 在本文中运用伯努利分布刻画拒绝服务攻击引起的数据丢包特性. 为了描述 $z_k, z_{k-1}, \cdots, z_{k-d+1}, z_{k-d}$ 传输情况, 首先定义行矩阵 $\lambda_k \in \mathbf{R}^{1\times(d+1)}$, 其元素均服从伯努利分布特性, 可表示如下:

$$\begin{aligned}&\Pr(\lambda_k(i)=0)=\rho\ ,\ \Pr(\lambda_k(i)=1)=1-\rho,\\&\mathrm{var}(\lambda_k(i))=\rho\,(1-\rho)\end{aligned}\tag{2}$$

其中, $\Pr(\cdot)$ 表示概率, $\mathrm{var}(\cdot)$ 表示方差, $\lambda_k(i)$ 表示矩阵 λ_k 中的第 i 个元素, $i\in[1,d+1]$, 它代表着 $k-i+1$ 时刻的量测量 z_{k-i+1} 的传输状态, 其值为 0 或 1; 如果 $\lambda_k(i)=0$, 则表明量测量 z_{k-i+1} 丢失, 而如果 $\lambda_k(i)=1$, 则表明量测量 z_{k-i+1} 成功传输; $\rho\in(0,1)$ 表示数据包丢失概率.

在分析 DoS 攻击导致的数据丢包特性后, 接下来对丢失数据进行补偿. 在 $z_{k-1}, \cdots, z_{k-d+1}, z_{k-d}$ 的传输状态由矩阵 λ_k 确定条件下, 首先设 k 时刻的连续丢包数 (即矩阵 λ_k 中从第一个元素开始的连续零元素数目) 为 ϕ_k, $\phi_k\in[0,d]$. 为补偿丢失的量测量, 定义新的行矩阵 $M_k\in\mathbf{R}^{1\times(d+1)}$ 来查找 k 时刻前最近一次接收到的数据包, 并利用该数据包对丢失数据进行补偿. 在矩阵 M_k 中, 有且仅有第 τ_k^{th} $(\tau_k=\phi_k+1)$ 个元素的值为 1, 其他元素的值均为 0, 因此, 当 k 时刻的量测量丢失时, 可以通过矩阵 M_k 进行补偿. 例如, 在量测量传输状态矩阵 $\lambda_k=[0\ 1\ 0\ 1]$ 情况下, 量测量 z_k、z_{k-2} 丢失, 而量测量 z_{k-1}、z_{k-3} 成功传输; 由于矩阵 λ_k 中第一个元素的值为 0, 第二个元素的值为 1, 有 $\phi_k=1$, $\tau_k=2$, 因此, 矩阵 $M_k=[0\ 1\ 0\ 0]$, 即量测量 z_k 由量测量 z_{k-1} 进行补偿. 在此注意: λ_k 可视作一个滑窗, 丢失的量测量 z_{k-2} 在 k 时刻之前已经被量测量 z_{k-3} 补偿了, 因而在 k 时刻只需要探讨量测量 z_k 的传输和补偿情况.

注 1. 当攻击者最多发起 d 次连续攻击时, 则连续数据包丢失的数目受到 d 的限制, 在 λ_k 中至少有一个 1, 并且在矩阵 M_k 中只有一个元素值等于 1, 即在状态估计过程中使用 $z_k, z_{k-1}, \cdots, z_{k-d+1}, z_{k-d}$ 中最近一次接收到的量测数据.

根据上述分析, 拒绝服务攻击后 k 时刻的状态估计器实际接受的量测量数据可表示为

$$\bar{z}_k=M_k\begin{bmatrix}z_k\\z_{k-1}\\\vdots\\z_{k-d}\end{bmatrix}=z_{k-\tau_k+1}\tag{3}$$

接下来, 举例对式 (3) 进行说明. 若攻击者最大连续攻击次数 $d=2$, 在 k 时刻, 量测量传输情况包含以下三种可能情形:

1) $\lambda_k(1)=1$, 即: $\phi_k=0, \tau_k=1$;

2) $\lambda_k(1)=0$, $\lambda_k(2)=1$, 即: $\phi_k=1, \tau_k=2$;

3) $\lambda_k(1)=0$, $\lambda_k(2)=0$, $\lambda_k(3)=1$, 即: $\phi_k=2, \tau_k=3$.

表 1 反映了以上三种情形下量测量传输情况, 其中每列元素分别表示对应时刻的量测量状态.

表 1 网络数据包传递表

Table 1 Data packet transmission in network

k	$\lambda_k(1)$	$\lambda_k(2)$	$\lambda_k(3)$	ϕ_k	τ_k	$k-\tau_k+1$	$\bar{z}_k$
1	1			0	1	1	z_1
2	1			0	1	2	z_2
3	0	1		1	2	2	z_2
4	0	0	1	2	3	2	z_2
5	1			0	1	5	z_5
6	0	1		1	2	5	z_5
7	1			0	1	7	z_7
8	0	1		1	2	7	z_7
9	1			0	1	9	z_9
10	1			0	1	10	z_{10}

从表 1 中可以看出, 量测量 z_1, z_2, z_5, z_7, z_9 和 z_{10} 成功传输, 而量测量 z_3, z_4, z_6 和 z_8 丢失, 其中, z_3 和 z_4 是连续丢包的. 丢失的量测数据在最后一行 $\bar{z}_k$ 中得到相应补偿. 根据式 (2) 的概率分布和式 (3) 采取补偿策略后的量测量描述, 可以构建新的量测方程:

$$\bar{z}_k=h\left(x_{k-\tau_k+1}\right)+v_{k-\tau_k+1}\tag{4}$$

在连续拒绝服务攻击下, 考虑数据补偿后的量测方程 (4), 重建新的交流电力系统动态模型如下:

$$\begin{aligned}x_{k+1}&=g\left(x_k\right)+w_k\\\bar{z}_k&=h\left(x_{k-\tau_k+1}\right)+v_{k-\tau_k+1}\end{aligned}\tag{5}$$

注 2. 根据式 (3), 新的量测量可由式 (4) 表示, 且由此重构的新交流电力系统动态模型如式 (5) 所示, 该模型考虑了电力网络遭受 DoS 网络攻击, 与传统动态电力系统模型相比更具实际意义. 针对

新模型式 (5), 为了得到智能电网的最优状态, 估计误差被定义为 $\hat{e}_{k|k}=x_k-\hat{x}_{k|k}$, 则估计误差协方差矩阵应该最小, 即

$$P_{k|k}=\mathrm{E}[\hat{e}_{k|k}\hat{e}_{k|k}^{\mathrm{T}}] \tag{6}$$

注 3. 根据 $e_{k|k}$ 的定义无法求解式 (6), 因为 $\hat{x}_{k|k}$ 还未知. 因此, 在智能电网遭受 DoS 攻击时, 根据非线性模型 (5) 和 (6), 结合能够针对非线性系统进行状态估计的传统无迹卡尔曼滤波算法, 提出了一种适用拒绝服务攻击的改进无迹卡尔曼滤波动态状态估计方法.

2 拒绝服务攻击下基于 UKF 的动态状态估计

UKF 以 UT 变换为基础[26], 摒弃了对非线性函数进行线性化的传统做法, 以非线性最优高斯滤波器为基本理论框架, 使用 UT 变换近似系统状态的后验均值以及后验协方差.

1) UT 采样

UT 变换是根据随机变量先验统计信息 (包括均值和方差), 基于采样策略[27] 设计一系列 Sigma 点; 对设定的 Sigma 点计算其经过非线性方程的结果 η_i; 然后基于 η_i 计算随机变量的后验统计信息. 本文的 UKF 采样策略选用比例对称采样, 初始状态条件为 n 维状态变量 x_0 和 $n\times n$ 维状态误差协方差矩阵 P_0, 首先得到 $2n+1$ 个 Sigma 点的位置和权值, 即

$$\begin{cases}\chi_{i,k-1|k-1}=\hat{x}_{k-1|k-1},\ i=0\\ \chi_{i,k-1|k-1}=\hat{x}_{k-1|k-1}+\left(\sqrt{(n+\lambda)P_{k-1}}\right)_i,\\ \qquad\qquad i=1,2,\cdots,n\\ \chi_{i,k-1|k-1}=\hat{x}_{k-1|k-1}-\left(\sqrt{(n+\lambda)P_{k-1}}\right)_i,\\ \qquad\qquad i=n+1,n+2,\cdots,2n\\ \omega_i^{(m)}=\frac{\lambda}{n+\lambda},\quad i=0\\ \omega_i^{(c)}=\frac{\lambda}{n+\lambda}+(1-\alpha^2+\beta),\quad i=0\\ \omega_i^{(m)}=\omega_i^{(c)}=\frac{1}{2(n+\lambda)},\quad i=1,2,\cdots,2n\end{cases} \tag{7}$$

其中, $\hat{x}_{k-1|k-1}=[\hat{x}^1_{k-1|k-1},\hat{x}^2_{k-1|k-1},\cdots,\hat{x}^n_{k-1|k-1}]^{\mathrm{T}}$; $\lambda=\alpha^2(n+\kappa)-n$, $\alpha\in[0.0001,1]$ 是比例因子, 改变 α 的数值来调节粒子的分布距离, 减小预测误差; κ 为冗余量, 一般在状态估计时设为 0; β 是与状态向量的先验分布相关的参数, 对高斯分布, $\beta=2$ 为最优[28]; $\left(\sqrt{(n+\lambda)P_{k-1}}\right)_i$ 是矩阵平方根的第 i 列; $\omega_i^{(m)}$ 是均值加权值; $\omega_i^{(c)}$ 是协方差加权值.

注 4. 采用 $2n+1$ 个 Sigma 点的比例对称采样策略可以解决随着维数增加非局部效应增强的问题, 而且兼顾了协方差的半正定性[29], 该采样策略同时以三阶泰勒精度逼近状态的后验均值和后验协方差.

注 5. 在 Sigma 点采样中, 计算量主要在平方根形式 $\sqrt{(n+\lambda)P_{k-1}}$, 一般通过 Cholesky 分解, 其计算复杂度为 $\mathrm{O}(n^2)$.

2) Holt′s 双参数指数平滑法

式 (5) 状态方程中的 $g(x_k)$ 可用 Holt′s 双参数指数平滑法近似替代:

$$\begin{cases}x_k=F_{k-1}x_{k-1}+u_{k-1}\\ a_{k-1}=\alpha x_{k-1|k-1}+(1-\alpha)x_{k-1|k-2}\\ b_{k-1}=\beta(a_{k-1}-a_{k-2})+(1-\beta)b_{k-2}\\ F_{k-1}=\alpha(1+\beta)I\\ u_{k-1}=(1+\beta)(1-\alpha)x_{k-1|k-2}-\\ \qquad\beta a_{k-2}+(1-\beta)b_{k-2}\end{cases} \tag{8}$$

其中, α、β 为 Holt′s 双参数指数平滑方法的平滑参数, 取值范围为 $[0,1]$.

3) 预测方程

首先, 定义预测估计误差 $\tilde{e}_{k|k-1}=x_k-\tilde{x}_{k|k-1}$, 则预测误差协方差矩阵[30] 为

$$\begin{aligned}P_{k|k-1}=&\mathrm{E}[\tilde{e}_{k|k-1}\tilde{e}_{k|k-1}^{\mathrm{T}}]=\\ &\mathrm{E}\{[(F_{k-1}x_{k-1}+u_{k-1})-\\ &(F_{k-1}\hat{x}_{k-1|k-1}+u_{k-1})]\times\\ &[(F_{k-1}x_{k-1}+u_{k-1})-(F_{k-1}\hat{x}_{k-1|k-1}+\\ &u_{k-1})]^{\mathrm{T}}\}+Q_{k-1}\end{aligned} \tag{9}$$

接下来, 预测 Sigma 采样点, 将其进行 Holt′s 双参数指数平滑变换, 参考式 (8), 可得到每个点的状态一步预测值, 即

$$\chi_{i,k|k-1}=F_{k-1}\chi_{i,k-1|k-1}+u_{k-1} \tag{10}$$

根据 k 时刻的 Sigma 点集得到状态向量的预测值和预测误差协方差矩阵

$$\tilde{x}_{k|k-1}=\sum_{i=0}^{2n}\omega_i^{(m)}\chi_{i,k|k-1} \tag{11}$$

$$\begin{aligned}P_{k|k-1}=&\sum_{i=0}^{2n}\omega_i^{(c)}[\chi_{i,k|k-1}-\tilde{x}_{k|k-1}]\times\\ &[\chi_{i,k|k-1}-\tilde{x}_{k|k-1}]^{\mathrm{T}}{}_k+Q_{k-1}\end{aligned} \tag{12}$$

其中, Q_{k-1} 为 $k-1$ 时刻状态噪声的方差.

进一步, 通过量测方程, 由 Sigma 点计算出量测向量的预测 Sigma 点集

$$\gamma_{i,k|k-1}=h\left(\chi_{i,k|k-1}\right) \tag{13}$$

则, 量测值 $z_{k|k-1}$ 的预测值为

$$\tilde{z}_{k|k-1}=\sum_{i=0}^{2n}\omega_i^{(m)}\gamma_{i,k|k-1} \tag{14}$$

注 6. 式 (5) 状态方程中的 $g(x_k)$ 可用 Holt′s 双参数指数平滑法近似替代, 该方法具有储存变量少、计算速度快的优点, 为此将其引入到 Sigma 点集计算中, 即式 (10). 其进一步经过加权处理就可得到状态向量的预测值和预测误差协方差矩阵如式 (11) 和式 (12) 所示. 式 (13) 表示对所有状态向量预测 Sigma 点进行非线性量测函数运算得到量测向量预测 Sigma 点, 经过加权处理即得到量测向量预测值, 即式 (14).

4) 更新方程

当遭受 DoS 攻击后, 需采用新的补偿后量测量 $\bar{z}_k$ 对预测的状态变量 $\tilde{x}_{k|k-1}$ 进行修正, 以得到新的状态估计量 $\hat{x}_{k|k}$, 以及相应的估计误差协方差矩阵 $P_{k|k}$. 最优状态估计量可由以下方程计算得到

$$\begin{aligned}\hat{x}_{k|k}&=\tilde{x}_{k|k-1}+K_k(\bar{z}_k-h(\tilde{x}_{k|k-1}))=\\&\quad\tilde{x}_{k|k-1}+K_k(\bar{z}_k-\tilde{z}_{k|k-1})\end{aligned} \tag{15}$$

根据式 (15), 可以推导出修正后的估计误差为

$$\begin{aligned}\hat{e}_{k|k}&=x_k-\hat{x}_{k|k}=\\&\quad x_k-(\tilde{x}_{k|k-1}+K_k(\bar{z}_k-\tilde{z}_{k|k-1}))=\\&\quad\tilde{e}_{k|k-1}-K_k(\bar{z}_k-\tilde{z}_{k|k-1})\end{aligned} \tag{16}$$

进一步, 估计误差协方差矩阵为

$$\begin{aligned}P_{k|k}&=\mathrm{E}[\hat{e}_{k|k}\hat{e}_{k|k}^{\mathrm{T}}]=\\&\quad P_{k|k-1}+\mathrm{E}[(K_kv_{k-\tau_k+1})(K_kv_{k-\tau_k+1})^{\mathrm{T}}]+\\&\quad\mathrm{E}\{[K_k(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})]\times\\&\quad[K_k(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})]^{\mathrm{T}}\}-\\&\quad\mathrm{E}\{(x_k-\tilde{x}_{k|k-1})[K_k(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})]^{\mathrm{T}}\}-\\&\quad\mathrm{E}\{[K_k(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})](x_k-\tilde{x}_{k|k-1})^{\mathrm{T}}\}\end{aligned} \tag{17}$$

为了获得最优的增益矩阵 K_k, 最小化估计误差协方差矩阵, 即 $P_{k|k}$ 对 K_k 的偏导数为 0, 即

$$\frac{\partial\mathrm{tr}(P_{k|k})}{\partial K_k}=0 \tag{18}$$

化简式 (18), 可得到最优增益矩阵为

$$\begin{aligned}K_k&=\mathrm{E}[(x_k-\tilde{x}_{k|k-1})(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]\times\\&\quad\{\mathrm{E}[(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})\times\\&\quad(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]+\\&\quad\mathrm{E}(v_{k-\tau_k+1}v_{k-\tau_k+1}^{\mathrm{T}})\}^{-1}=\\&\quad\mathrm{E}[(x_k-\tilde{x}_{k|k-1})(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]\times\\&\quad\{\mathrm{E}[(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})\times\\&\quad(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]+R_{k-\tau_k+1}\}^{-1}\end{aligned} \tag{19}$$

将式 (19) 代入式 (17), 可得

$$\begin{aligned}P_{k|k}&=P_{k|k-1}-K_kR_{k-\tau_k+1}K_k^{\mathrm{T}}-\\&\quad K_k\mathrm{E}[(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})\times\\&\quad(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]K_k^{\mathrm{T}}\end{aligned} \tag{20}$$

注 7. 根据最小均方误差估计准则, 通过极小化式 (17) 的估计误差协方差矩阵 $P_{k|k}$ 的迹求解 K_k, 并得到估计误差协方差矩阵的极小值. 式 (19) 和式 (20) 为考虑融合补偿信息的最优增益矩阵和估计误差协方差矩阵, 若直接求解关于 $h(x_{k-\tau_k+1})$ 的协方差矩阵及相关矩阵, 由于 $h(\cdot)$ 具有非线性, 状态后验信息不能通过非线性函数直接传递得到, 因此对 (19) 和 (20) 难以直接求解, 故接下来将对其进行 UT 变换近似求解.

为了进一步求解式 (19), 令:

$$\begin{aligned}C_k&=\mathrm{E}[(x_k-\tilde{x}_{k|k-1})(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})^{\mathrm{T}}]\\S_k&=\mathrm{E}[(h(x_{k-\tau_k+1})-\tilde{z}_{k|k-1})(h(x_{k-\tau_k+1})-\\&\quad\tilde{z}_{k|k-1})^{\mathrm{T}}]+R_{k-\tau_k+1}\end{aligned}$$

根据对称采样策略 Sigma 点, UT 变换系统状态后验协方差及互协方差计算方法[31], 式 (19) 中 C_k 和 S_k 采用对相应的 Sigma 点集进行加权处理近似得到

$$\begin{aligned}C_k&=\sum_{i=0}^{2n}\omega_i^{(c)}[\chi_{i,k|k-1}-\tilde{x}_{k|k-1}]\times\\&\quad[h(\chi_{i,k-\tau_k+1|k-\tau_k})-\tilde{z}_{k|k-1}]^{\mathrm{T}}=\\&\quad\sum_{i=0}^{2n}\omega_i^{(c)}[\chi_{i,k|k-1}-\tilde{x}_{k|k-1}]\times\\&\quad[\gamma_{i,k-\tau_k+1|k-\tau_k}-\tilde{z}_{k|k-1}]^{\mathrm{T}}\end{aligned} \tag{21}$$

$$\begin{aligned}S_k&=\sum_{i=0}^{2n}\omega_i^{(c)}[h(\chi_{i,k-\tau_k+1|k-\tau_k})-\tilde{z}_{k|k-1}]\times\\&\quad[h(\chi_{i,k-\tau_k+1|k-\tau_k})-\tilde{z}_{k|k-1}]^{\mathrm{T}}=\\&\quad\sum_{i=0}^{2n}\omega_i^{(c)}[\gamma_{i,k-\tau_k+1|k-\tau_k}-\tilde{z}_{k|k-1}]\times\\&\quad[\gamma_{i,k-\tau_k+1|k-\tau_k}-\tilde{z}_{k|k-1}]^{\mathrm{T}}+R_{k-\tau_k+1}\end{aligned} \tag{22}$$

根据式 (21) 和式 (22), 则无迹卡尔曼增益式 (19) 可改写为

$$K_k=\frac{C_k}{S_k} \tag{23}$$

将式 (23) 代入式 (15) 可计算得到 $\hat{x}_{k|k}$, 并且估

计误差协方差矩阵可改写为

$$P_{k|k} = P_{k|k-1} - K_k S_k K_k^{\mathrm{T}}. \tag{24}$$

注 8. 式 (21) 和式 (22) 表示采用 UT 变换近似求解量测量相关性矩阵及协方差矩阵, 式 (19) 的无迹卡尔曼增益即为两个方差矩阵比较值, 故而可化简如式 (23) 所示, 也可对估计误差协方差矩阵进一步化简如式 (24) 所示. 当智能电网受到拒绝服务攻击时, 改进无迹卡尔曼滤波算法对丢失的量测数据进行补偿, 先通过式 (7) 构造 Sigma 点集, 接着根据式 (8) 进行参数辨识, 再根据式 (10) ∼ (12) 进行状态预测, 最后根据式 (15)、(23)、(24) 进行状态更新, 可以有效地减少量测数据丢失对系统状态估计的影响.

拒绝服务攻击下基于 UKF 的智能电网动态状态估计算法步骤如下, 其中步骤 2) ∼ 5) 流程如图 1 所示:

1) 初始化. 设置初始系统状态量 x_0 和初始估计误差协方差矩阵 P_0;

2) UT 采样. 根据 $k-1$ 时刻的状态变量估计值 $\hat{x}_{k-1|k-1}$ 和估计误差的协方差矩阵 $P_{k-1|k-1}$, 如式 (7) 所示构造 Sigma 点集;

3) Holt′s 双参数指数平滑法. 式 (5) 状态方程中的 $g(x_k)$ 采用 Holt′s 双参数指数平滑方法近似替代;

4) 状态预测. 根据构造的 Sigma 点集, 并根据式 (10) ∼ (12) 得到 k 时刻的状态变量预测值 $\tilde{x}_{k|k-1}$ 和预测误差协方差矩阵 $P_{k|k-1}$;

5) 状态更新. 根据式 (4) 得到 k 时刻经过数据补偿的量测量 $\bar{z}_k$, 根据式 (23) 计算增益矩阵, 并根据式 (15)、(24) 计算 k 时刻的状态变量估计值 $\hat{x}_{k|k}$ 和估计误差协方差矩阵 $P_{k|k}$;

6) 判断迭代过程是否满足终止条件, 如果当前时刻超过估计总时长, 则动态状态估计流程结束, 否则, 重新回到第 2) 步, 开始下一时刻智能电网状态的估计.

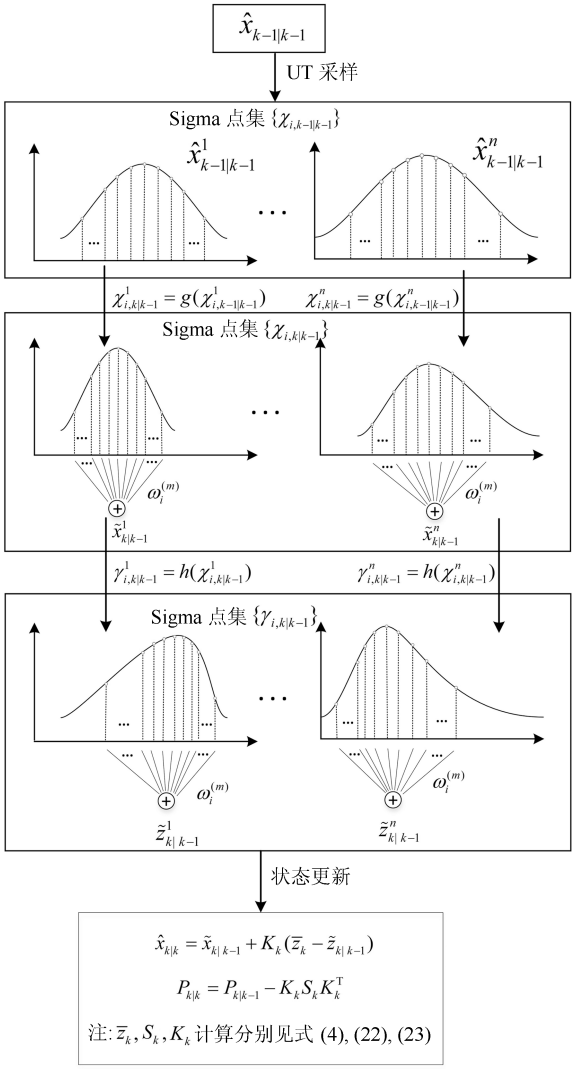


图 1　拒绝服务攻击下基于改进 UKF 动态状态估计流程图

Fig. 1　Flowchat of new-UKF dynamic state estimation algorithm under DoS attacks

3　算例仿真

针对 IEEE 30 和 118 标准节点系统, 在拒绝服务攻击下, 对本文所提出的改进无迹卡尔曼滤波动态状态估计算法进行仿真验证, 并采用如下指标对估计结果的误差进行评价:

1) 估计误差

$$\varepsilon_k = \frac{\sum\limits_{i=1}^{n} \left|\hat{x}_{k|k}(i) - x_k(i)\right|}{n} \times 100\,\% \tag{25}$$

2) 性能指标

$$J_k = \frac{\sum\limits_{i=1}^{m} \left|\hat{z}_{k|k}\,(i) - z_k\,(i)\,\right|}{\sum\limits_{i=1}^{m} \left|\bar{z}_k\,(i) - z_k\,(i)\,\right|} \tag{26}$$

其中, ε_k 表示 k 时刻的状态估计平均误差, n 表示状态向量的维度, $\hat{x}_{k|k}$ 表示 k 时刻的状态估计值, x_k 表示 k 时刻的状态真值; J_k 表示 k 时刻的状态估计性能指标, m 表示量测向量的维度, $\hat{z}_{k|k}$ 表示 k 时刻状态估计值对应的量测估计值, $\bar{z}_k$ 表示 k 时刻补偿后的量测值, z_k 表示 k 时刻的量测真值.

3.1　IEEE 30 算例

IEEE 30 节点系统如图 2 所示, 有 127 个量测量包括 1 个电压幅值、22 个节点有功注入功率、22

个节点无功注入功率、41 个支路两端的有功潮流和 41 个支路两端的无功潮流, 其中选择 1 号节点为平衡节点, 其电压相角设为零, 系统的状态真值和量测量真值由 100 次潮流计算得到, 而实际量测值通过在量测量真值的基础上添加高斯白噪声获得, 设定电压值为 0.1 % 的偏差, 功率为 2 % 的偏差, 且在分析的整个时间段内, 设量测误差协方差矩阵 R 为常数.

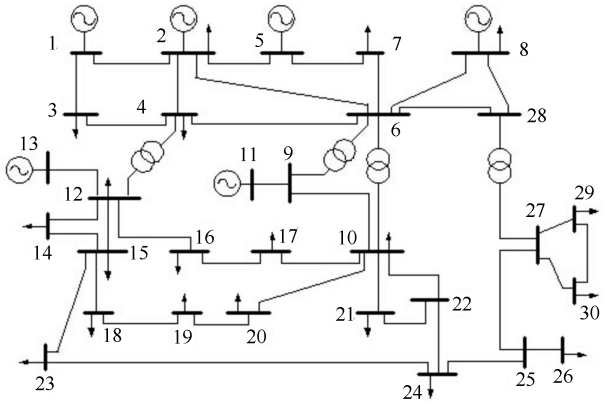


图 2 IEEE 30 节点系统结构图

Fig. 2 IEEE 30-bus system diagram

Holt′s 双参数指数平滑法从 $k = 0, 1$ 两个时刻后的系统状态开始, 参数 $\alpha = 0.8$, $\beta = 0.5$, 即估计算法从时刻 $k = 2$ 开始. F_0 和 P_0 的对角元素分别设为 1.0 和 10^{-6}, Q 的对角元素设为 10^{-6}.

下面从 4 个方面对 DoS 攻击下基于所提出的改进无迹卡尔曼滤波算法进行智能电网动态状态估计的有效性分析:

1) 智能电网遭受 DoS 攻击导致量测数据丢失对状态估计影响分析. 假设受到 DoS 攻击, 以量测数据丢失的概率 ρ 为 0.05 为例. 相应的数据包丢失序列如图 3 所示, 其中 “0” 表示数据包丢失, “1” 表示数据包传输正常.

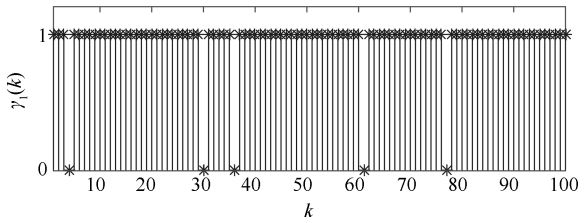


图 3 IEEE 30 节点系统丢包时序图 ($\rho = 0.05$)

Fig. 3 Data packet loss sequence of IEEE 30-bus system ($\rho = 0.05$)

当遭受 DoS 攻击导致数据包丢失概率 $\rho = 0.05$ 时, 针对 IEEE 30 节点系统, 采用改进无迹卡尔曼滤波算法进行动态状态估计结果见图 4 和表格 2. 由于节点较多, 在此仅以 2 号节点对应的电压相角和幅值为例进行分析, 图 4 实线表示采用本文提出的改进 UKF 算法计算出的状态估计值, 点划线表示系统状态真值, 从仿真结果可以发现电压相角和幅值的估计值在真值附近波动, 这表明所提算法能够有效进行系统的动态状态估计. 表 2 列举了 $k = 25, 50, 75, 100$ 时刻下系统的状态估计值 (由于状态量较多, 在此仅列出部分状态估计值), 其中 $x_2 \sim x_{30}$ 代表电压相角, $x_{32} \sim x_{58}$ 代表电压幅值, 可以发现随着迭代次数的增加, 动态状态估计结果非常接近真值, 这再次表明所提算法能够有效进行系统的动态状态估计. 图 5 进一步展示了状态估计结果的估计误差和估计性能指标, 可以看出估计误差低于 3×10^{-3}, 并且性能指标小于 1, 这验证了在 DoS 攻击下本文所提的改进无迹卡尔曼滤波算法能够有效实现智能电网动态状态估计.

表 2 IEEE 30 节点系统动态状态估计结果

Table 2 Dynamic state estimation results of IEEE 30-bus system

k	25	50	75	100	状态真值
x_2	−0.1314	−0.1322	−0.1312	−0.1312	−0.1311
x_4	−0.2497	−0.2495	−0.2493	−0.2505	−0.2481
x_6	−0.2259	−0.2261	−0.2256	−0.2252	−0.2249
x_8	−0.2450	−0.2456	−0.2456	−0.2463	−0.2460
x_{10}	−0.2443	−0.2462	−0.2443	−0.2473	−0.2460
x_{12}	−0.2636	−0.2627	−0.2625	−0.2655	−0.2656
x_{14}	−0.2800	−0.2816	−0.2807	−0.2791	−0.2809
x_{16}	−0.2776	−0.2792	−0.2783	−0.2807	−0.2780
x_{18}	−0.2935	−0.2941	−0.2923	−0.2937	−0.2940
x_{20}	−0.2822	−0.2859	−0.2842	−0.2841	−0.2842
x_{22}	−0.2826	−0.2863	−0.2847	−0.2837	−0.2844
x_{24}	−0.2838	−0.2788	−0.2842	−0.2824	−0.2815
x_{26}	−0.2739	−0.2715	−0.2746	−0.2708	−0.2741
x_{28}	−0.2929	−0.2898	−0.2966	−0.2923	−0.2963
x_{30}	1.0606	1.0603	1.0599	1.0595	1.0600
x_{32}	1.0127	1.0150	1.0119	1.0132	1.0135
x_{34}	0.9986	1.0012	1.0015	0.9973	1.0000
x_{36}	0.9906	0.9935	0.9925	0.9900	0.9924
x_{38}	1.0299	1.0327	1.0280	1.0309	1.0305
x_{40}	1.0711	1.0718	1.0690	1.0747	1.0720
x_{42}	1.0734	1.0743	1.0687	1.0718	1.0710
x_{44}	1.0202	1.0214	1.0184	1.0208	1.0194
x_{46}	1.0085	1.0140	1.0085	1.0136	1.0116
x_{48}	0.9994	1.0019	0.9952	1.0031	0.9996
x_{50}	1.0000	1.0020	0.9980	1.0005	1.0008
x_{52}	1.0005	1.0025	0.9985	1.0013	1.0012
x_{54}	0.9955	0.9961	0.9926	0.9919	0.9945
x_{56}	1.0058	1.0086	1.0052	1.0037	1.0053
x_{58}	0.9863	0.9889	0.9860	0.9845	0.9851

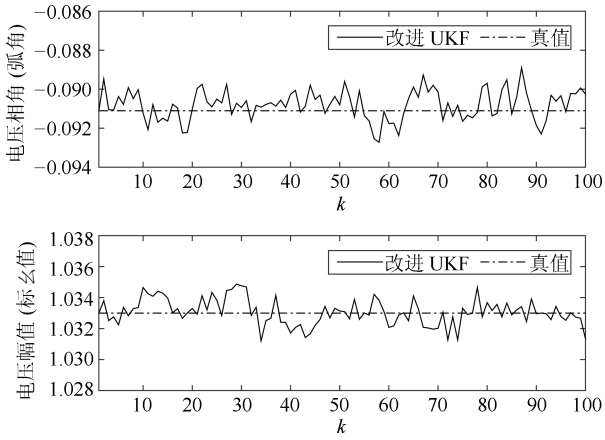


图 4　DoS 攻击下节点 2 的电压幅值和相角的估计值 ($\rho = 0.05$)

Fig. 4　Estimated voltage magnitude and phase angle at bus 2 under DoS attacks ($\rho = 0.05$)

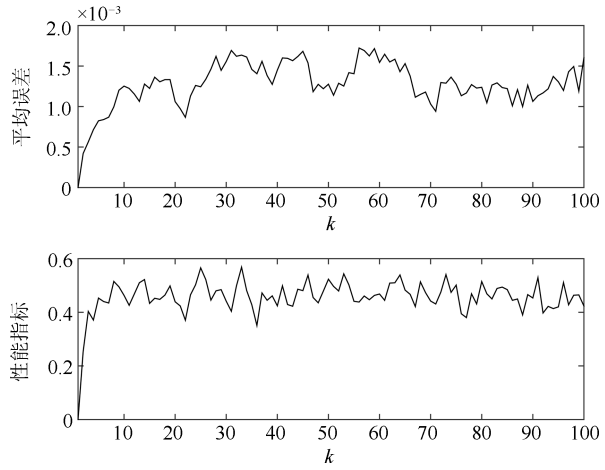


图 5　DoS 攻击下系统状态估计误差和性能指标 ($\rho = 0.05$)

Fig. 5　State estimation error and performance index of the system under DoS attacks ($\rho = 0.05$)

2) 不同程度拒绝服务攻击对动态状态估计影响分析. 图 6 和图 7 首先展示遭受 DoS 攻击导致数据包丢失概率 $\rho = 0.1$ 情况下, 本文提出的改进 UKF 算法的动态状态估计结果, 图 6 中实线表示采用本文提出的改进 UKF 算法计算出的状态估计值, 点划线表示系统状态真值, 从仿真结果可以发现虽然丢包率不同, 本文所提的改进 UKF 算法仍然能够有效实现智能电网动态状态估计. 图 8 进一步展示了在 4 种不同数据包丢失概率 ($\rho = 0.05, 0.1, 0.15, 0.2$) 下, IEEE 30 节点系统的状态估计结果, 所有估计误差低于 3×10^{-3} 并且性能指标小于 1, 这进一步表明本文所提改进 UKF 算法进行智能电网动态状态估计是可行且有效的.

3) 本文提出的改进 UKF 算法与传统 UKF 算法进行动态状态估计性能比较. 针对 IEEE 30 节点系统, 以量测数据遭受 DoS 攻击导致数据包丢失概率 $\rho = 0.05$ 情况下为例, 两种算法分别进行动态状态估计, 结果如图 9 所示. 从图 9 中可以明显地看到, 传统的 UKF 算法状态估计的平均误差和性能指标明显大于本文提出的改进 UKF 算法的结果, 从而表明传统的 UKF 算法的估计效果明显比本文提出的改进 UKF 算法性能差, 这是因为量测值丢失导致传统 UKF 算法无法进行正确的系统预测与校正, 进而导致状态估计性能变差.

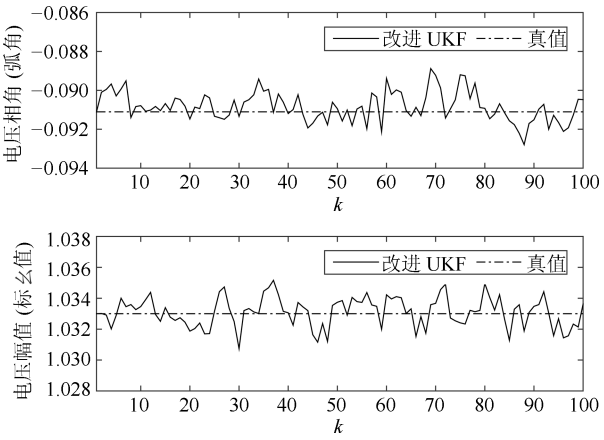


图 6　在 DoS 攻击下节点 2 的电压幅值和相角估计值 ($\rho = 0.1$)

Fig. 6　Estimated voltage magnitude and phase angle at bus 2 under DoS attacks ($\rho = 0.1$)

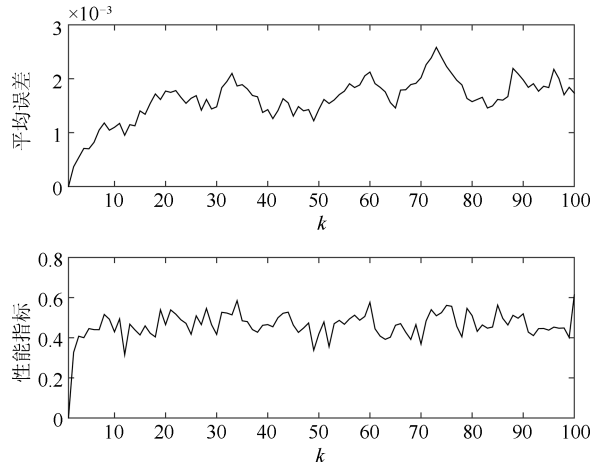


图 7　DoS 攻击下系统状态估计误差和性能指标 ($\rho = 0.1$)

Fig. 7　State estimation error and performance index of the system under DoS attacks ($\rho = 0.1$)

4) 本文提出的改进 UKF 算法与文献 [22] 算法进行动态状态估计性能比较. 针对 IEEE 30 节点系统, 在 4 种不同数据包丢失概率 ($\rho = 0.05, 0.1, 0.15, 0.2$) 下, 本文提出的改进 UKF 算法和文献 [22] 算法分别进行动态状态估计, 结果如图 10 所示. 从图 10 可以看到, 4 种不同数据包丢失概率下本文提出的改进 UKF 算法的平均误差和性能

指标均小于文献 [22] 所提算法, 从而进一步表明本文提出的改进 UKF 算法具有较好的状态估计性能.

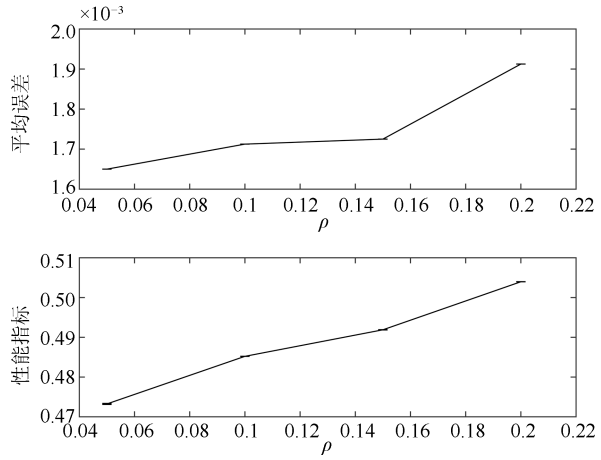


图 8 DoS 攻击导致 4 种不同数据丢包概率下 IEEE 30 节点系统的状态估计误差和性能指标

Fig. 8 State estimation error and performance index of IEEE 30-bus system with four different ρ values

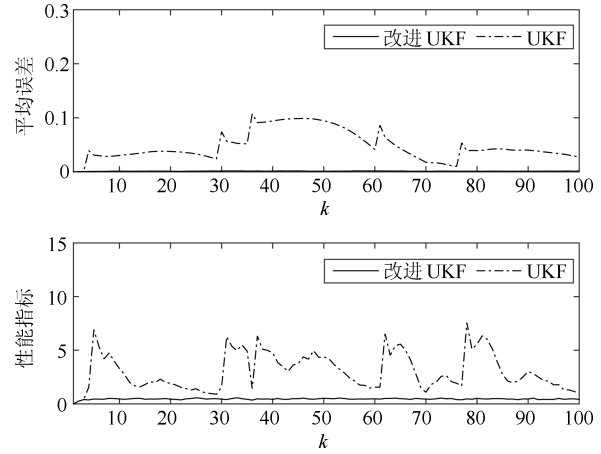


图 9 DoS 攻击下 IEEE 30 节点系统采用改进 UKF 算法和传统 UKF 算法状态估计误差和性能指标比较 ($\rho = 0.05$)

Fig. 9 Comparison of state estimation error and performance index of IEEE 30-bus system by using new-UKF and UKF methods under DoS attacks ($\rho = 0.05$)

3.2 IEEE 118 算例

为了进一步验证所提算法在大规模电力系统上的性能, 选取 IEEE 118 节点系统为研究对象, 该系统有 487 个量测量包括 1 个电压幅值、64 个节点有功注入功率、64 个节点无功注入功率、358 个支路两端的有功潮流和无功潮流, 其中选择 69 号节点为平衡节点, 其电压相角设为零, 系统的状态真值和量测量真值由 100 次潮流计算得到, 而实际量测值通过在量测量真值的基础上添加高斯白噪声获得, 设定电压值为 0.1 % 的偏差, 功率为 2 % 的偏差, 且在分析的整个时间段内, 设量测误差协方差矩阵 R 为常数. 具体从下面三种情况说明在 DoS 攻击下所提出的基于无迹卡尔曼滤波的智能电网状态估计算法的有效性.

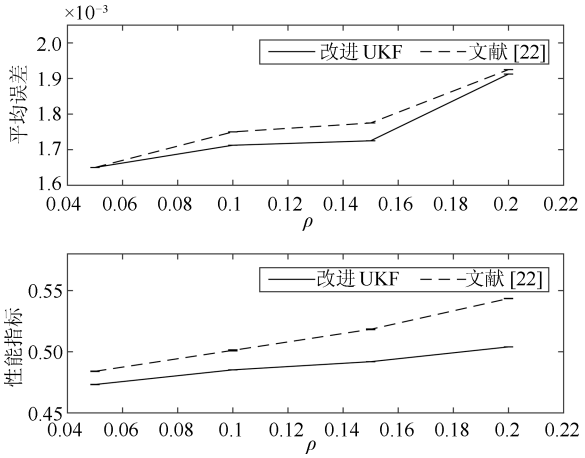


图 10 DoS 攻击导致 4 种不同数据丢包概率下 IEEE 30 节点系统采用改进 UKF 算法和文献 [22] UKF 算法状态估计误差和性能指标比较

Fig. 10 Comparison of state estimation error and performance index of IEEE 30-bus system with four different ρ values by using new-UKF and review [22]′s UKF methods under DoS attacks

1) 不同程度拒绝服务攻击对动态状态估计影响分析. 图 11 表示 4 种不同数据包丢失概率 ($\rho = 0.05, 0.1, 0.15, 0.2$) 情况下, 针对 IEEE 118 节点系统进行动态状态估计的估计误差和性能指标. 估计误差低于 1.2×10^{-3} 且性能指标小于 1, 从中可以看出, 本文所提的改进 UKF 算法的状态估计平均误差和估计性能指标在不同丢包率情况下均表现良好, 这表明所提出的改进 UKF 算法进行智能电网动态状态估计是可行且有效的.

2) 本文提出的改进 UKF 算法与传统 UKF 算法进行动态状态估计性能比较. 针对 IEEE 118 节点系统, 量测数据遭受 DoS 攻击导致数据包丢失概率 $\rho = 0.05$ 情况下, 两种算法分别进行动态状态估计, 结果如图 12 所示. 从图 12 中可以明显地看到, 传统的 UKF 算法状态估计的平均误差和性能指标明显大于本文提出的改进 UKF 算法的结果, 从而表明传统的 UKF 算法的估计效果明显比本文提出的改进 UKF 算法性能差, 这是因为量测值丢失导致传统 UKF 算法无法进行正确的系统预测与校正, 进而导致状态估计性能变差.

3) 本文提出的改进 UKF 算法与文献 [22] 算法进行动态状态估计性能比较. 针对 IEEE 118 节点系统, 在 4 种不同数据包丢失概率 ($\rho = 0.05, 0.1, 0.15, 0.2$) 下, 本文提出的改进 UKF 算法

和文献 [22] 算法分别进行动态状态估计, 结果如图 13 所示. 由图 13 可以看到, 4 种不同数据包丢失概率下本文提出的改进 UKF 算法的平均误差和性能指标均小于文献 [22] 所提算法, 从而进一步表明本文提出的改进 UKF 算法具有较好的状态估计性能.

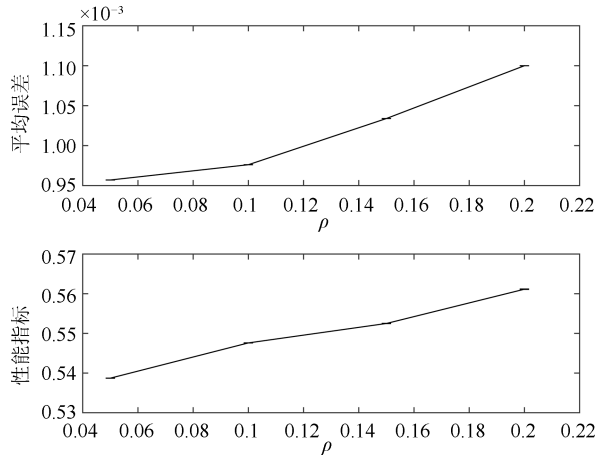


图 11　DoS 攻击导致 4 种不同数据丢包概率下 IEEE 118 节点系统的状态估计误差和性能指标

Fig. 11　State estimation error and performance index of IEEE 118-bus system with four different ρ values

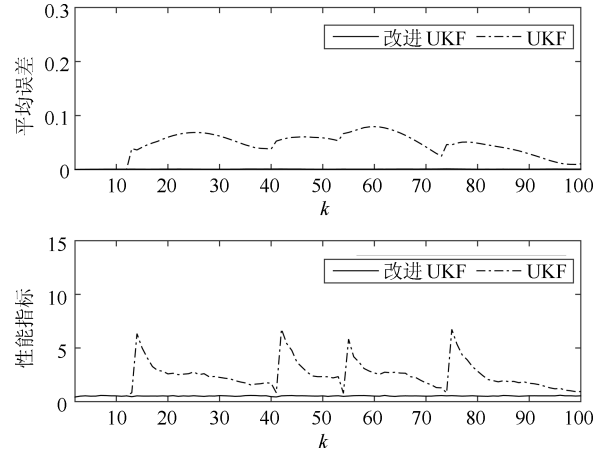


图 12　DoS 攻击下 IEEE 118 节点系统采用改进 UKF 算法和传统 UKF 算法状态估计误差和性能指标比较 ($\rho = 0.05$)

Fig. 12　Comparison of state estimation error and performance index of IEEE 118-bus system by using new-UKF and UKF methods under DoS attacks ($\rho = 0.05$)

4　结论

本文提出了一种适用拒绝服务攻击的改进无迹卡尔曼滤波方法以进行智能电网动态状态估计, 首先, 利用伯努利分布描述 DoS 攻击造成的数据丢包特征, 并设计了数据补偿策略以重构电力系统动态模型; 然后, 结合 Holt′s 双参数指数平滑和无迹卡尔曼滤波方法, 构造了融合补偿信息的新状态估计方程, 基于估计误差协方差矩阵推导了状态增益更新方法, 得到了无迹卡尔曼滤波动态估计新方法, 为 DoS 攻击下智能电网动态状态估计提供了一种有效途径. 仿真算例表明改进 UKF 算法在 DoS 攻击下进行智能电网动态状态估计是可行有效的, 且其状态估计性能明显优于传统 UKF 算法. 未来的工作可以进一步探讨如何改进无迹卡尔曼滤波算法, 以解决智能电网中同时存在多种类型网络攻击所面临的状态估计问题.

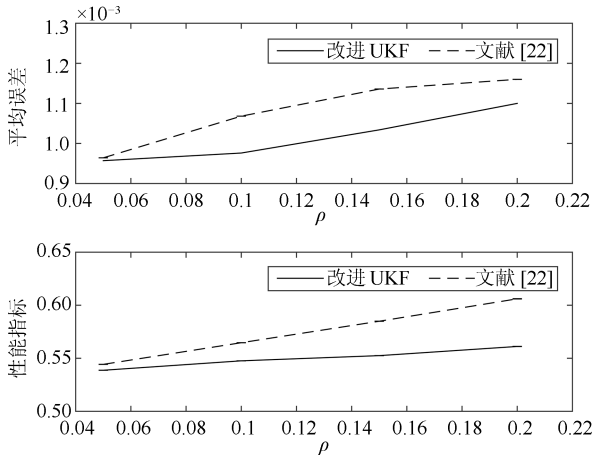


图 13　DoS 攻击导致 4 种不同数据丢包概率下 IEEE 118 节点系统采用改进 UKF 算法和文献 [22] UKF 算法状态估计误差和性能指标比较

Fig. 13　Comparison of state estimation error and performance index of IEEE 118-bus system with four different ρ values by using new-UKF and review [22]′s UKF methods under DoS attacks

References

1 Rehmani M H, Reisslein M, Rachedi A, Kantarci M E, Radenkovic M. Integrating renewable energy resources into the smart grid: recent developments in information and communication technologies. *IEEE Transactions on Industrial Informatics*, 2018, **14**(7): 2814−2825

2 Tuballa M L, Abundo M L. A review of the development of smart grid technologies. *Renewable & Sustainable Energy Reviews*, 2016, **59**: 710−725

3 Li X, Tian Y C, Ledwitch G, Mishra Y, Han X Q, Zhou C J. Constrained optimization of multicast routing for wide area control of smart grid. *IEEE Transactions on Smart Grid*, 2018, DOI: 10.1109/TSG.2018.2835487

4 Chakrabortty A, Bose A. Smart grid simulations and their supporting implementation methods. *Proceedings of the IEEE*, 2017, **105**(11): 2220−2243

5 Sun Qiu-Ye, Teng Fei, Zhang Hua-Guang. Energy internet and its key control issues. *Acta Automatica Sinica*, 2017, **43**(2): 176−194
(孙秋野, 滕菲, 张化光. 能源互联网及其关键控制问题. 自动化学报, 2017, **43**(2): 176−194)

6 Uzunoglu B, Ulker M A. Maximum likelihood ensemble filter state estimation for power systems. *IEEE Transactions on Instrumentation & Measurement*, 2018, **67**(9): 2097−2106

7 Ghosal M, Rao V. Fusion of multirate measurements for nonlinear dynamic state estimation of the power systems. *IEEE Transactions on Smart Grid*, 2019, **10**(1): 216−226

8 Hu L, Wang Z, Rahman I, Liu X. A constrained optimization approach to dynamic state estimation for power systems Including PMU and missing measurements. *IEEE Transactions on Control Systems Technology*, 2016, **24**(2): 703−710

9 Yan H, Zhou X, Zhang H, Yang F, Wu Z G. A novel sliding mode estimation for microgrid control with communication time delays. *IEEE Transactions on Smart Grid*, 2017, DOI: 10.1109/TSG.2017.2771493

10 Zhao J, Netto M, Mili L. A robust iterated extended Kalman filter for power system dynamic state estimation. *IEEE Transactions on Power Systems*, 2017, **32**(4): 3205−3216

11 Julier S J, Uhlmann J K, Durrant-Whyte H F. A new approach for filtering nonlinear systems. In: Proceedings of the American Control Conference. Seattle, WA, USA: IEEE, 1995. 1628−1632

12 Zhao J, Mili L. Robust unscented Kalman filter for power system dynamic state estimation with unknown noise statistics. *IEEE Transactions on Smart Grid*, 2017, DOI: 10.1109/TSG.2017.2761452

13 Zhao J. Power system dynamic state estimation considering measurement correlations. *IEEE Transactions on Energy Conversion*, 2017, **32**(4): 1630−1632

14 Qi J, Sun K, Wang J, 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

15 Liang G, Zhao J, Luo F, Weller S, Dong Z Y. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, 2016, **8**(4): 1630−1638

16 Liang Yao, Feng Dong-Qin, Xu Shan-Shan, Chen Si-Yuan, Gao Meng-Zhou. Feasibility analysis of encrypted transmission on security of industrial control systems. *Acta Automatica Sinica*, 2018, **44**(3): 434−442
(梁耀, 冯冬芹, 徐珊珊, 陈思媛, 高梦州. 加密传输在工控系统安全中的可行性研究. 自动化学报, 2018, **44**(3): 434−442)

17 Liang J, Sankar L, Kosut O. Vulnerability analysis and consequences of false data Injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 2016, **31**(5): 3864−3872

18 Li Z, Shahidehpour M, Aminifar F. Cybersecurity in distributed power systems. *Proceedings of the IEEE*, 2017, **105**(7): 1367−1388

19 Wolf M, Serpanos D. Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, 2018, **106**(1): 9−20

20 Zhang B, Li Q, Zhang Y, Chen X. The proactive defense of energy internet terminals edge-access using the network topology autoassociation. *IEEE Journal on Emerging & Selected Topics in Circuits & Systems*, 2017, **7**(3): 432−446

21 Zhang H, Qi Y, Wu J, Fu L, He L. DoS attack energy management against remote state estimation. *IEEE Transactions on Control of Network Systems*, 2018, **5**(1): 383−394

22 Li L, Xia Y. Stochastic stability of the unscented Kalman filter with intermittent observations. *Automatica*, 2012, **48**(5): 978−981

23 Zhao S, Ma Y, Huang B. Robust FIR state estimation of dynamic processes corrupted by outliers. *IEEE Transactions on Industrial Informatics*, 2019, **15**(1): 139−147

24 Zhang H, Cheng P, Shi L, Chen J. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 2016, **24**(3): 843−852

25 Befekadu G K, Gupta V, Antsaklis P J. Risk-Sensitive control under Markov modulated denial-of-service (DoS) attack strategies. *IEEE Transactions on Automatic Control*, 2015, **60**(12): 3299−3304

26 Li Yun, Sun Shu-Li, Hao Gang. Weighted measurement fusion unscented Kalman filter based on Gauss-Hermite approximation for nonlinear systems. *Acta Automatica Sinica*, 2018, DOI: 10.16383/j.aas.2018.c170534
(李云, 孙书利, 郝钢. 基于 Gauss-Hermite 逼近的非线性加权观测融合无迹 Kalman 滤波器. 自动化学报, 2018, DOI: 10.16383/j.aas.2018.c170534)

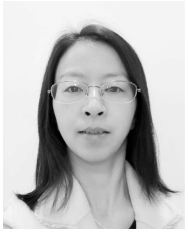
27 Havangi R. Robust SLAM: SLAM base on H_∞ square root unscented Kalman filter. *Nonlinear Dynamics*, 2016, **83**(1-2): 767−779

28 Yu S, Emami K, Fernando T, Iu H H C, Wong K P. State estimation of doubly fed induction generator wind turbine in complex power systems. *IEEE Transactions on Power Systems*, 2016, **31**(6): 4935−4944

29 Julier S J. The scaled unscented transformation. In: Proceedings of the American Control Conference. Anchorage, AK, USA: IEEE, 2002. 4555−4559

30 Sun Q, Lim C C, Shi P, Liu F. Design and stability of moving horizon estimator for Markov jump linear systems. *IEEE Transactions on Automatic Control*, 2018, DOI: 10.1109/TAC.2018.2816102

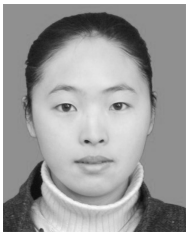
31 Guo L, Huang D G, Maximum likelihood principle based adaptive UKF algorithm. *International Journal of Signal Processing*, 2016, **9**(9): 167−175



李 雪 上海大学机电工程与自动化学院副教授. 主要研究方向为智能电网安全控制与性能评估.
E-mail: lixue@shu.edu.cn
(**LI Xue** Associate professor at the School of Mechatronics Engineering and Automation, Shanghai University. Her research interest covers security control and performance assessment of smart grid.)

李雯婷 上海大学机电工程与自动化学院硕士研究生. 主要研究方向为网络攻击下智能电网状态估计及性能分析.
E-mail: lwting@shu.edu.cn
(**LI Wen-Ting** Master student at the School of Mechatronics Engineering and Automation, Shanghai University. Her research interest covers state estimation and performance analysis of smart grid under cyber attacks.)

杜大军 上海大学机电工程与自动化学院教授. 主要研究方向为机器视觉和网络化系统安全控制. 本文通信作者.
E-mail: ddj@shu.edu.cn
(**DU Da-Jun** Professor at the School of Mechatronics Engineering and Automation, Shanghai University. His research interest covers machine vision and security control for networked control systems. Corresponding author of this paper.)



孙 庆 上海大学机电工程与自动化学院博士后. 主要研究方向为混杂系统的状态估计及其应用.
E-mail: qingsun@shu.edu.cn
(**SUN Qing** Postdoctor at the School of Mechatronics Engineering and Automation, Shanghai University. Her research interest covers state estimation for the hybrid dynamic systems and its application.)

费敏锐 上海大学机电工程与自动化学院教授. 主要研究方向为网络化控制系统及实现.
E-mail: mrfei@staff.shu.edu.cn
(**FEI Min-Rui** Professor at the School of Mechatronics Engineering and Automation, Shanghai University. His research interest covers networked control system and its implementation.)