文章编号：2095-2163(2021)11-0162-03 中图分类号：TM73 文献标志码：A

基于容积卡尔曼滤波的虚假数据注入攻击检测研究

鲁 杰[1]，杨 超[1]，杜刃刃[2]，陈 飞[1]，陈名扬[1]
（1 贵州大学 电气工程学院，贵阳 550025；2 贵州电网有限责任公司 贵安供电局，贵州 贵安 550025）

摘 要：虚假数据注入攻击给电力系统的安全稳定运行带来严重威胁，研究其检测方法具有十分重大的意义。本文基于容积卡尔曼滤波提出了一种虚假数据注入攻击的检测方法，该方法首先利用容积卡尔曼滤波算法对系统进行状态估计；其次，将状态估计结果与加权最小二乘法的估计结果进行状态一致性检验；最后，以 IEEE-14 节点系统为试验对象，进行算例分析。结果表明，本文的方法能够有效地检测出注入到系统中的虚假数据。

关键词：电力系统；虚假数据注入攻击；容积卡尔曼滤波；状态一致性检验

False data injection attack detection based on volumetric kalman filter

LU Jie[1], YANG Chao[1], DU Renren[2], CHEN Fei[1], CHEN Mingyang[1]
(1 School of Electrical Engineering, Guizhou University, Guiyang 550025, China;
2 Guian Power Supply Bureau of Guizhou Power Grid Co., Ltd., Gui'an, Guizhou 550025, China)

【Abstract】 False data injection attack poses a serious threat to the safe and stable operation of power system. It is of great significance to study its detection methods. This paper proposes a detection method of false data injection attack based on volumetric Kalman filter. Firstly, the volumetric Kalman filter algorithm is used to estimate the state of the system, and then the consistency between the state estimation results and the estimation results of weighted least squares method is tested. Finally, the IEEE-14 bus system is taken as the test object for example analysis. The results show that the method in this paper can effectively detect the false data injected into the system.

【Key words】 power system; false data injection attack; volume kalman filter; state consistency inspection

0 引 言

近年来，随着信息化程度不断增高，网络攻击对电网的威胁越来越大。2015 年 12 月，由于网络攻击，乌克兰国家电网遭受重大损失，引起众多国家高度关注[1]。虚假数据注入攻击（False Data Injection Attack，FDIA）是网络攻击的形式之一，由 LIU 等人在 2009 年首次提出[2]。此种攻击由于是人为精心策划，可以避开状态估计中的坏数据检测模块，隐蔽性强，给电网的安全稳定运行造成威胁，因此研究 FDIA 的检测方法具有重要意义。

对于 FDIA 的检测法，Bobba 等提出确保战略选择所需要的基本测量的安全和独立验证战略性选择的状态变量的异常两种方法[3]；在此基础上，Gu Y 等通过分析量测残差中包含的局部异常，从而有效地检测出随机攻击，此方法的不足之处在于对隐蔽性的 FDIA 无法进行检测，而且阈值对检测的精度影响较大[4]；朱杰等基于历史数据库进行短期状态预测，基于状态预测结果，通过状态一致性检验和数据隐蔽性检验进行攻击检测[5]；Manandhar 等将欧几里德原理与卡尔曼滤波结合进行虚假数据检测[6]；Xu 等通过对节点进行分类，得出各节点不同的脆弱性等级类别，由此优先针对脆弱性高的节点进行检测[7]；Kwon 等提出状态可达集进行检测，该方法运用到卡尔曼滤波器，但是忽略了实际噪声变化的影响[8]；夏小虎等所提检测方法中，为提高状态估计精度，状态估计的算法运用交互多模型卡尔曼滤波，但是仍然忽略了噪声变化的影响[9]。

本文提出的检测方法是利用容积卡尔曼滤波（CKF）算法在攻击前后对系统进行状态估计，将此估计值与传统加权最小二乘法（WLS）所得估计值进行状态一致性检验，以此判定系统有无异常情况，为下一步决策提供依据。为验证本文所提方法的有效性，以 IEEE-14 节点系统为对象进行算例分析，

基金项目：贵州省科学技术基金（黔科合基础[2019]1100）。

作者简介：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研究；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；杜刃刃（1992-），男，硕士，副值调度监控员，主要研究方向：负荷识别；陈 飞（1995-），男，硕士研究生，主要研究方向：非侵入式负荷监测；陈名扬（1995），男，硕士研究生，主要研究方向：新能源消纳、需求响应。

收稿日期：2021-08-05

结果表明本文所提方法能够有效检测出恶意注入到系统中的虚假数据，避免对系统造成危害。

1　容积卡尔曼滤波

容积卡尔曼滤波是目前最接近贝叶斯滤波的一种非线性滤波算法，在电力系统动态状态估计问题中可以应用容积卡尔曼滤波。电力系统的准稳态模型可表示为式(1)和式(2)：

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

$$z_{k+1} = h(x_{k+1}) + r_{k+1} \tag{2}$$

式中：$f(x_k)$ 表示状态量 x_k 在相邻时刻的转移关系；$h(x_k)$ 表示状态量 x_k 与量测量 z_k 之间的关系；q_k 是方差阵为 Q_k 的系统误差；r_{k+1} 是方差阵为 R_{k+1} 的量测误差。

对式(1)、(2)所表示的电力系统，结合容积卡尔曼滤波进行动态状态估计的方法如下：

(1)初始化：需要初始化的量有 $\hat{x}_k$、P_k、Q、R；

(2)计算容积点：针对 P_k 进行 Cholesky 运算，式(3)：

$$S_k = chol(P_k) \tag{3}$$

容积点集，式(4)：

$$\xi = \sqrt{n}\,[I, -I] \tag{4}$$

式中：I 为 n 阶单位阵，n 为状态变量个数。

容积点计算，式(5)和式(6)：

$$x_k^i = S_k\xi_i + \hat{x}_k, \quad i = 1,2,\cdots,2n \tag{5}$$

$$x_{k+1|k}^i = f(x_k^i, u_k) \tag{6}$$

(3)预测状态量及误差协方差，式(7)和式(8)：

$$\hat{x}_{k+1|k} = \omega\sum_{i=1}^{2n} x_{k+1|k}^i \tag{7}$$

$$P_{k+1|k} = \omega\sum_{i=1}^{2n} x_{k+1|k}^i (x_{k+1|k}^i)^{\mathrm{T}} - \hat{x}_{k+1|k}(\hat{x}_{k+1|k})^{\mathrm{T}} + Q \tag{8}$$

(4)针对 $P_{k+1|k}$ 进行 Cholesky 运算，并计算容积点，式(9)~式(11)：

$$S_{k+1|k} = chol(P_{k+1|k}) \tag{9}$$

$$X_{k+1|k}^i = S_{k+1|k}\xi_i + \hat{x}_{k+1|k} \tag{10}$$

$$y_{k+1}^i = g(X_{k+1|k}^i, u_{k+1}) \tag{11}$$

(5)预测量测值，式(12)：

$$\hat{y}_{k+1|k} = \omega\sum_{i=1}^{2n} y_{k+1}^i \tag{12}$$

(6)测量误差协方差及互协方差，式(13)和式(14)：

$$P_{k+1}^y = \omega\sum_{i=1}^{2n} y_{k+1}^i (y_{k+1}^i)^{\mathrm{T}} - \hat{y}_{k+1}(\hat{y}_{k+1})^{\mathrm{T}} + R \tag{13}$$

$$P_{k+1}^{xy} = \omega\sum_{i=1}^{2n} X_{k+1|k}^i (y_{k+1|k}^i)^{\mathrm{T}} - \hat{x}_{k+1|k}(\hat{y}_{k+1})^{\mathrm{T}} \tag{14}$$

(7)卡尔曼增益 K，式(15)：

$$K_{k+1} = P_{k+1}^{xy}(P_{k+1}^y)^{-1} \tag{15}$$

(8)更新状态量及误差协方差，式(16)和式(17)：

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(y_{k+1} - \hat{y}_{k+1}) \tag{16}$$

$$P_{k+1} = P_{k+1|k} - K_{k+1}P_{k+1}^y K_{k+1}^{\mathrm{T}} \tag{17}$$

通过以上步骤，即可运用容积卡尔曼滤波对电力系统进行状态估计。

2　虚假数据注入攻击检测

为简便计，选用电力系统直流状态估计模型来阐述虚假数据注入攻击检测的基本原理。

直流状态估计模型可表示为式(18)：

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{18}$$

式中：$\boldsymbol{x}$ 为 n 维状态向量；$\boldsymbol{z}$ 为 m 维量测向量；$\boldsymbol{e}$ 为 m 维量测误差向量；$\boldsymbol{H}$ 为 $m \times n$ 维雅克比矩阵。

在无攻击时，系统残差为式(19)：

$$r = \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\|_2 < \tau \tag{19}$$

式中：τ 为检测阈值。

在有攻击时，假定与量测 $\boldsymbol{z}$ 同维数的攻击向量为 $\boldsymbol{a} = [a_1, a_2, \cdots, a_m]^{\mathrm{T}}$，攻击发生后，量测变为 $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$；若 $\boldsymbol{c} = [c_1, c_2, \cdots, c_n]^{\mathrm{T}}$ 为由攻击引起的状态变量误差向量，则状态估计向量为 $\hat{\boldsymbol{x}}_a = \hat{\boldsymbol{x}} + \boldsymbol{c}$。系统检测残差公式(20)如下：

$$\boldsymbol{r}_a = \|\boldsymbol{z}_a - \boldsymbol{H}\hat{\boldsymbol{x}}_a\|_2 = \|(\boldsymbol{z} + \boldsymbol{a}) - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c})\|_2 = \|(\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}) + (\boldsymbol{a} - \boldsymbol{H}\boldsymbol{c})\|_2 \tag{20}$$

由式(20)可知，当 $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ 时，有式(21)：

$$\boldsymbol{r}_a = \|\boldsymbol{z}_a - \boldsymbol{H}\hat{\boldsymbol{x}}_a\|_2 = \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\|_2 = r \tag{21}$$

由此可见，系统在受到恶意攻击之后仍能躲避不良数据检测模块，对系统造成威胁。

本文运用容积卡尔曼滤波进行状态估计，对式(1)中的 $f(x_k)$ 使用的是 Holt´s 两参数法来预测下一时刻状态值，结合状态估计结果进行虚假数据检测，检测公式(22)如下：

$$\|\tilde{\boldsymbol{x}} - \hat{\boldsymbol{x}}\|_2 \leqslant \tau_1 \tag{22}$$

式中：$\tilde{\boldsymbol{x}}$ 为 CKF 估计的状态值；$\hat{\boldsymbol{x}}$ 为 WLS 估计的状态值；τ_1 为一致性检测阈值。

通过式(22)对状态估计的结果进行一致性检验，若检验通过，则认为系统正常，反之则认为系统可能存在 FDIA。因为使用 *Holt´s* 两参数法进行一步预测，所以在发电机或负荷突变的情况下，也可能不能通过式(22)的状态一致性检验，因此式(22)在系统正常时也存在不成立的情况，这时需要进一步

进行残差验证,残差验证的公式(23)如下:

$$\| z - h(\tilde{x}) \|_2 \leqslant \tau_a \qquad (23)$$

式中:z 为量测数据;$h(\tilde{x})$ 为容积卡尔曼滤波估计的预测量测量;τ_a 为攻击检测阈值,其值查卡方分布表可得。

由上可知,当式(22)、式(23)都不成立时,可认为系统中被恶意注入了虚假数据。

3 算例分析

本文选取 IEEE-14 节点系统进行算例分析,虚假数据注入攻击模型采用最小虚假数据攻击向量的建模方法。

这里状态变量选取的是节点电压幅值及相角,共 27 个状态变量(除去参考节点的电压相角);取 41 个量测量,以常规潮流计算结果作为量测数据。由此可得冗余度 $k = 41-27=14$,这里显著性水平取 0.05,通过查卡方分布表得攻击检测阈值为 23.685。

虚假数据攻击前后利用容积卡尔曼滤波对系统进行状态估计后的电压幅值及相角变化示意图如图 1 和图 2 所示。

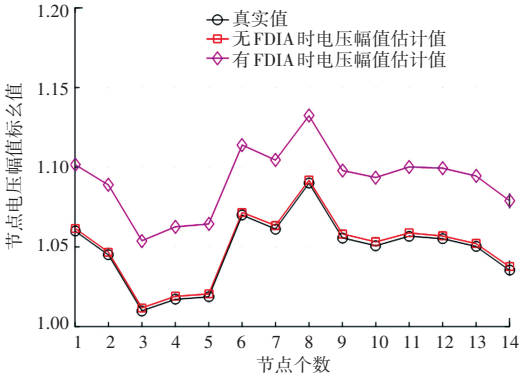

图 1 攻击前后电压幅值估计结果

Fig. 1 Voltage amplitude estimation results before and after attack

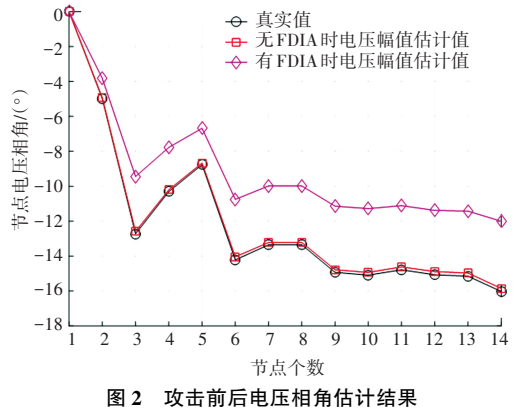

图 2 攻击前后电压相角估计结果

Fig. 2 Estimation results of voltage phase angle before and after attack

通过仿真计算,在虚假数据攻击前系统残差为 0.405 1,在虚假数据攻击后系统残差为 0.521 4。由此可见,虚假数据在攻击前和攻击后系统残差的变化并不明显,注入虚假数据后仍然可以躲避不良数据检测模块。

下一步进行一致性检验,虚假数据攻击前 $\| \tilde{x} - \hat{x} \|_2 = 0.472\ 8$,虚假数据攻击后 $\| \tilde{x} - \hat{x} \|_2 = 53.664\ 3$,该值远大于一致性检验阈值,则式(22)不成立。再计算式(23)得 $\| z - h(\tilde{x}) \|_2 = 36.285\ 4$,大于攻击检测阈值23.685,由此可知式(23)也不成立,从而检测异常,表明有虚假数据攻击系统。

4 结束语

为了检测系统中的虚假数据,本文采用了基于容积卡尔曼滤波的方法。在无攻击发生时,利用容积卡尔曼滤波进行状态估计的结果与真实值相差无几,偏差较小;但在系统中注入虚假数据后,再进行状态估计的结果明显偏离真实值,在此基础上,利用状态一致性检验进行检测,有效地检测到恶意注入到系统中的虚假数据。

参考文献

[1] 赵俊华, 梁高琪, 文福拴, 等. 乌克兰事件的启示:防范针对电网的虚假数据注入攻击[J]. 电力系统自动化, 2016, 40(7): 149 - 151.

[2] 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.

[3] BOBBA R B, ROGERS K M, WANG Q, et al. Detecting false data injection attacks on DC State estimation [C] //Preprints of the First Workshop on Secure Control Systems. Stockholm, Sweden: CPSWEEK, 2010: 1-9.

[4] GU Y, LIU T, WANG D, et al. Bad data detection method for smart grids based on distributed state estimation [C] //2013 IEEE International Conference on Communications. Piscataway, NJ, USA: IEEE, 2013: 4483-4487.

[5] 朱杰, 张葛祥. 基于历史数据库的电力系统状态估计欺诈性数据防御[J]. 电网技术,2016, 40(6): 1772-1777.

[6] MANANDHAR K, CAO X, HU F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter [J]. IEEE Transactions on Control of Network Systems, 2014, 1(4): 370-379.

[7] XU Ruzhi, WANG Rui, GUAN Zhitao, et al. Achieving efficient detection against false data injection attacks in smart grid [J]. IEEE Access, 2017: 13787-13798.

[8] KWON C, HWANG I. Reachability analysis for safety assurance of cyber - physical systems againstcyber - attacks [J]. IEEE Transactions on Automatic Control, 2017, 63(7): 2272-2279.

[9] 夏小虎, 刘明. 基于交互式多模型卡尔曼滤波的电池荷电状态估计[J]. 信息与控制, 2017, 46(5) : 519-524.