信息与控制　2019 年　第 48 卷　第 5 期：522 ~ 527

DOI：10.13976/j.cnki.xk.2019.9156　　文章编号：1002 - 0411(2019) - 05 - 0522 - 06

微电网在虚假数据注入攻击下的增量检测机制

彭华晔，彭　晨，孙洪涛，杨明锦

上海大学机电工程与自动化学院，上海　200444

基金项目：国家自然科学基金资助项目(61833011，61673255)；“111”引智基地(D18003)；上海市优秀学术带头人项目(18XD1401600)；上海市科委重点项目(10JC1405000)

通信作者：彭晨，c.peng@shu.edu.cn　收稿/录用/修回：2019 - 04 - 02/2019 - 07 - 22/2019 - 08 - 15

摘要

针对微电网环境下虚假数据注入攻击的状态估计问题，提出了一种基于分析状态测量值增量的攻击检测机制. 在假设系统稳态的情况下，对系统测量值的增量，进行关于χ^2的假设检验，能够有效检测出精心设计的攻击. 对本文提出的方法在 Matlab 中进行仿真，实验结果表明在特定的系统情况下，对于非恒定的攻击，该方法能提高检测出攻击的成功率.

关键词

微电网

虚假数据注入攻击

攻击检测

增量检测

中图法分类号：TP273.+2

文献标识码：A

Incremental Detection Mechanism of a Microgrid under False Data Injection Attacks

PENG Huaye, PENG Chen, SUN Hongtao, YANG Mingjin

School of Mechanical Engineering and Automation, Shanghai University, Shanghai 200444, *China*

Abstract

In this study, we propose an attack detection mechanism based on the incremental analysis of state measurements to solve the problem of state estimation of the false data injection attacks in microgrid environments. By assuming the steady state of the system, the increment of the measured value of the system can be detected by χ^2 hypothesis testing, which can effectively detect well-designed attacks. We simulated the proposed method in Matlab. The experimental results denote that the proposed method can improve the detection accuracy of unsteady attacks under specific system conditions.

Keywords

micro-grid;

false data injection attack;

attack detection;

incremental detection

0　引言

微电网(MG)是一种有别于主干电网的新型供电系统，通常一个微电网包含分布式负载、低压分布式电源和储能设备，其中分布式电源包括微型引擎、风力引擎、光能发电机，储能设备包括风轮发电存储系统(FESS)和电池储能系统(BESS)[1]. 其相比于主干电网，微电网能够更经济地应用于农村及偏远地区，而这些地区若采用主干网输电的话，则经济代价很大[2].

由于微电网的分布化，其控制通过网络来实现，具有典型的信息与物理装置目标结合的特征，是一个信息—物理系统. 对于一个电力系统，决策控制依据的是测量系统，主要通过测量电网主干和支路的有功和无功功率，然而用来评估电网运行的重要变量却是不可直接测量的(如电压、相位等)，因此需要通过状态估计器来估计这些状态变量. 同时网络具有易攻击性的特点，因此对微电网的攻击必须作为微电网应用所必须考虑的问题. 对于一般的网络攻击，可以使用残差检测法检测攻击的产生. 然而，对于虚假数据注入攻击，只要知道受攻击系统的配置信息，就能精心组织一种攻击，使得一般的残差检测无法发现[3]. 这样产生的后果也是严重的，如 2015 年发生的乌克兰大停电[4]. 近年来的研究表明，对虚假数据注入攻击，对策主要有两种[5]：基于防护的策略和基于检测的策略. 基于防护的策略主要是确定重要的节点使之不被攻击，如连续的监视，与互联网隔离开等[6]. 基于检测的策略主要是发现受到攻击的测量节点，并且使用正确的数据替换它[7]. 对于攻击的检测，文[8]通过残差的分布期望等信息来判断是否产生了攻击，但是这需要一段时间的数据才能提供判断. 文[9]研究的是对于已知系统状态方程的情况的状态估计，仍采用残差检测. 而文[10]基于测量

矩阵低秩的特性，化成稀疏最优问题，文[11]通过相互之间的信息熵来刻画受攻击与否，文[12]通过机器学习的方法进行错误数据检测，这些方法都是没有采用残差检测.

在系统波动不大的情况下，若攻击只是发生在测量端，即输出端，则如何区分攻击和噪声扰动，是一个棘手的问题. 为此，希望找到一种新的残差检测机制，使得在精心设计的攻击下依然能够发现攻击. 本文针对注入于测量端的虚假数据注入攻击，使得测量值的增量在状态波动不大的情况下仍然满足正态分布的特性；对增量进行χ^2检测，从而区分出是攻击还是噪声，以此来判断是否发生攻击；然后，采用攻击前的准确的测量值代替被攻击测量值进行控制.

1　问题描述

在通常的微电网中，第 i 条总线上的有功功率 P_i 和无功功率 Q_i 为[5]

$$P_i = V_i \sum_{j\in\Omega_i} V_j(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{1}$$

$$Q_i = V_i \sum_{j\in\Omega_i} V_j(G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \tag{2}$$

从第 i 条总线到第 j 条总线的有功功率 P_{ij} 和无功功率 Q_{ij} 为

$$P_{ij} = V_i^2(g_{si}+g_{ij}) - V_iV_j(g_{ij}\cos\theta_{ij} + b_{ij}\sin\theta_{ij}) \tag{3}$$

$$Q_{ij} = -V_i^2(b_{si}+b_{ij}) - V_iV_j(g_{ij}\sin\theta_{ij} - b_{ij}\cos\theta_{ij}) \tag{4}$$

其中，V_i 为 i 总线上的电压，θ_i 为 i 总线中的相角，$\theta_{ij}=\theta_i-\theta_j$，$G_{ij}+jB_{ij}$为 i 总线和 j 总线之间的线路阻抗，$g_{si}+jb_{si}$为分路支路中 i 总线的阻抗，Ω_i 为与 i 总线相连的总线集合.

由上述电网的电力潮流计算公式，可以得到电力系统测量系统数学模型[13]：

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{5}$$

其中，$\boldsymbol{z}=(z_1,\cdots,z_m)^{\mathrm{T}}$ 表示测量向量；$\boldsymbol{x}\in\mathrm{R}^{2n-1}$表示所要估计的状态变量，$n$ 为系统总线的数量，$\boldsymbol{x}=(\boldsymbol{\theta}^{\mathrm{T}},\boldsymbol{V}^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{V}=(V_1,\cdots,V_n)^{\mathrm{T}}$ 表示总线的电压值向量，$\boldsymbol{\theta}=(\theta_2,\cdots,\theta_n)^{\mathrm{T}}$ 表示每条总线相对于第 1 条总线的相位差值向量；$\boldsymbol{e}=(e_1,\cdots,e_m)^{\mathrm{T}}$ 表示量测误差，$\boldsymbol{e}\sim N(0,\boldsymbol{R})$是一个零均值的高斯变量，其协方差矩阵 $\boldsymbol{R}=\mathrm{diag}(\sigma_1^2,\cdots,\sigma_m^2)$，$\boldsymbol{h}(\boldsymbol{x})$是一个非线性向量函数.

定义残差向量 $\boldsymbol{r}(\boldsymbol{x})=\boldsymbol{z}-\boldsymbol{h}(\boldsymbol{x})$，则最小加权平方法的问题为[14]

$$\min_{\boldsymbol{x}\in\mathrm{R}^{2n-1}} J(\boldsymbol{x}) = \frac{1}{2}\boldsymbol{r}^{\mathrm{T}}(\boldsymbol{x})\boldsymbol{W}^{-1}\boldsymbol{r}(\boldsymbol{x}) \tag{6}$$

其中，$\boldsymbol{W}=\mathrm{diag}(w_1^2,\cdots,w_m^2)$.

对于离散系统，利用最小加权平方法可以得到对状态变量的估计[15]：

$$\hat{\boldsymbol{x}}(k+1) = \hat{\boldsymbol{x}}(k) + (\boldsymbol{H}^{\mathrm{T}}(k)\boldsymbol{W}^{-1}\boldsymbol{H}(k))^{-1}\boldsymbol{H}^{\mathrm{T}}(k)\boldsymbol{W}^{-1}\boldsymbol{r}(k) \tag{7}$$

其中，$\hat{\boldsymbol{x}}(k)$是 k 时刻的估计值，$\boldsymbol{H}(k)$是测量矩阵 $\boldsymbol{h}(k)$在 k 时刻关于 $\hat{\boldsymbol{x}}$ 的 Jacobi 矩阵，残差 $\boldsymbol{r}(k)=\boldsymbol{z}-\boldsymbol{h}(\hat{\boldsymbol{x}}(k))$.

令 $\boldsymbol{Q}=(\boldsymbol{H}^{\mathrm{T}}(k)\boldsymbol{W}^{-1}\boldsymbol{H}(k))^{-1}\boldsymbol{H}^{\mathrm{T}}(k)\boldsymbol{W}^{-1}$，从而有：

$$\hat{\boldsymbol{x}}(k+1) = \hat{\boldsymbol{x}}(k) + \boldsymbol{Q}\boldsymbol{r}(k) \tag{8}$$

Liu 等在文[3]中给出了直流线性系统的虚假数据注入攻击，将其扩展至交流非线性系统中，有：

$$\boldsymbol{r}_a(k) = \boldsymbol{z}_a(k) - \boldsymbol{h}(\hat{\boldsymbol{x}}_a) = \boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}}_a) \tag{9}$$

其中，$\boldsymbol{r}_a(k)$是受攻击后的残差；$\boldsymbol{a}$ 是注入的攻击数据，由于攻击注入的是测量端，所以并没有攻击状态量，因此攻击只影响状态估计；$\hat{\boldsymbol{x}}_a=\hat{\boldsymbol{x}}+\boldsymbol{c}$ 是受攻击后对状态的估计量. 对 $\boldsymbol{h}(\hat{\boldsymbol{x}}_a)$进行泰勒展开，略去高阶项，有：

$$\boldsymbol{h}(\hat{\boldsymbol{x}}_a) = \boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c}) \approx \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{H}(k)\boldsymbol{c} \tag{10}$$

则，若有：

$$\boldsymbol{a} = \boldsymbol{H}(k)\boldsymbol{c} \tag{11}$$

可得

$$\begin{aligned}\boldsymbol{r}_a(k) &= \boldsymbol{r}(k) - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{a} - \boldsymbol{H}(k)\boldsymbol{c}\\ &= \boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\\ &= \boldsymbol{r}(k)\end{aligned} \tag{12}$$

从而攻击后残差不变，因此传统的残差检测器不能发现有攻击产生. 为此采用测量值增量来进行卡方检测，在系统波动不大的情况下，将能够发现测量系统受到的攻击.

2　攻击检测机制

由于虚假数据注入攻击的隐蔽性使得其无法用一般的方法检测出来，因此有必要设计一个新的检测思路. 由于对于电网进入稳态环境后，状态值的波动有明确的限制指标，比如 GB/T15945《电能质量电力系统频率允许偏差》标准中规定："我国电网频率正常为 50 Hz，对电网容量在 300 万千瓦及以上者，偏差不超过 ±0.2 Hz；对电网容量在 300 万千瓦以下者，偏差不超过 ±0.5 Hz".

假设系统已经进入了稳态环境，从而波动几乎为零. 在此假设成立的情况下，考虑只对输出端也即测量端进行虚假数据注入攻击，攻击者目的是让控制系统接收到错误的测量数据，从而进行错误的控制，破坏系统的稳态.

在这种情况下，由于假设系统进入稳态，所以注意到状态在不受干扰的情况下波动几乎为零，测量值只受测量噪声的影响进行波动. 而干扰噪声 $\boldsymbol{e}\sim N(0,\boldsymbol{R})$是一个零均值的高斯变量，其协方差矩阵 $\boldsymbol{R}=\mathrm{diag}(\sigma_1^2,\cdots,\sigma_m^2)$，记 $\boldsymbol{x}(k)$为 $\boldsymbol{x}_k$，那么有：

$$\boldsymbol{z}(k) = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{e}_k \tag{13}$$

$$\boldsymbol{z}(k-1) = \boldsymbol{h}(\boldsymbol{x}_{k-1}) + \boldsymbol{e}_{k-1} \tag{14}$$

噪声 $\boldsymbol{e}_k\sim N(0,\boldsymbol{R}_k)$，$\boldsymbol{e}_{k-1}\sim N(0,\boldsymbol{R}_{k-1})$且相互独立，则有：

$$\boldsymbol{e}_k - \boldsymbol{e}_{k-1} \sim N(0,\boldsymbol{R}_k+\boldsymbol{R}_{k-1}) \tag{15}$$

即，稳态时测量值的增量满足：

$$\boldsymbol{z}(k) - \boldsymbol{z}(k-1) \sim N(0,\boldsymbol{R}_k+\boldsymbol{R}_{k-1}) \tag{16}$$

明显地，测量值的增量服从一个已知的分布，从而对于任何在统计上不服从该分布的数据，可以被当成攻击检测出来. 于是，可以定义新的增量χ^2 检测器：

$$\boldsymbol{d}(k) = \boldsymbol{z}(k) - \boldsymbol{z}(k-1) \tag{17}$$

其中，

$$\boldsymbol{d}(k) = (d_1(k),\cdots,d_m(k))^{\mathrm{T}} \tag{18}$$

本文假定攻击不是一直不变的. 这个假定很容易满足，因为攻击也受到能量等限制，从而增量也并不为零.

在测量值受攻击的情况下，有：

$$\boldsymbol{z}_a(k)=\boldsymbol{z}(k)+\boldsymbol{a}(k) \tag{19}$$

$$\boldsymbol{z}_a(k-1)=\boldsymbol{z}(k-1)+\boldsymbol{a}(k-1) \tag{20}$$

其中，$\boldsymbol{a}(k)\neq\boldsymbol{a}(k-1)$，所以攻击发生后的增量与攻击发生前的分布不同，也即：

$$\begin{aligned}\boldsymbol{d}_a(k)&=\boldsymbol{z}_a(k)-\boldsymbol{z}_a(k-1)\\&=\boldsymbol{d}(k)+\boldsymbol{a}(k)-\boldsymbol{a}(k-1)\\&\neq\boldsymbol{d}(k)\end{aligned} \tag{21}$$

假设对于增量的实际测量值为

$$\bar{\boldsymbol{d}}(k)=\begin{cases}\boldsymbol{d}(k), & \text{系统未受攻击}\\ \boldsymbol{d}_a(k), & \text{系统受到攻击}\end{cases} \tag{22}$$

可以对 $\bar{\boldsymbol{d}}(k)$ 进行基于已知分布的假设检验，对于第 i 个分量 $\bar{d}_i(k)$，选定一个显著性水平 α，对应第 i 个分量的置信区间为 $[\tau_i,\ +\infty)$. 一旦有 $\bar{d}_i(k)>\tau_i$，就认为系统受到攻击（$\bar{d}_i(k)>\tau_i$ 不满足随机干扰的分布，因此就认为引起的因素不是干扰而是攻击）.

定义攻击发生标志 φ_k：

$$\varphi_k=\begin{cases}0, & \forall\ \|\bar{d}_i(k)\|^2\leqslant\tau_i\\ 1, & \exists\ \|\bar{d}_i(k)\|^2>\tau_i\end{cases} \tag{23}$$

其中，τ_i 是一个预先设定好的阈值，$\|\cdot\|$ 表示欧几里得范数. 测量值的变化大于 τ_i 表示受到了攻击，通过对随机扰动的分布情况结合显著性水平的选取，从而确定 τ_i，而一旦数据的变化大于 τ_i，则受到了攻击. $\varphi_0=\varphi_1=0$，这里 $\varphi_k=1$ 表示受攻击，数据无效；反之，表示有效.

对于 τ_i，由于不同的测量分量服从不同参数的正态分布，所以进行假设检验的阈值也是不同的.

假设噪声干扰都是服从标准正态分布，所以测量值增量的内积服从自由度为 2 的 χ^2 分布. 对 χ^2 分布查表可知，显著性水平为 0.05 时的置信区间为 $[5.99,\ +\infty)$，所以可得 τ_i 为 5.99.

进行假设检验，检验假设 H_0 和备择假设 H_1：

$$H_0:\varphi_k=0$$

$$H_1:\varphi_k=1$$

在检验假设 H_0 成立的情况下，$\|\bar{d}_i(k)\|$ 落在置信区间外时的概率小于显著性水平 $\alpha=0.05$，则一旦落在置信区间外，就有足够的理由拒绝原假设，承认备择假设 H_1，从而判断系统受到攻击.

系统攻击检测的流程图如图 1 所示，其中 $\boldsymbol{z}'(k)$ 代表经过检测机制处理的测量值：

$$\boldsymbol{z}'(k)=\begin{cases}\boldsymbol{z}'(k-1), & \varphi_k=1\\ \boldsymbol{z}(k), & \varphi_k=0\end{cases} \tag{24}$$

即，在这种情况下，可以根据攻击发生标志来判断攻击发生与否，若攻击发生，则不将此时的测量值传递给控制器. 经过增量检测的状态估计器为

$$\tilde{\boldsymbol{x}}(k)=(1-\varphi_k)\boldsymbol{Q}\boldsymbol{z}'(k)+\varphi_k\tilde{\boldsymbol{x}}(k-1) \tag{25}$$

式中对于受攻击的测量值不予采用.

可以用上述算法得到的真实状态量来进行状态反馈控制. 而对于受攻击的数据直接采取舍弃的方法，相当于网络控制中的丢包问题. 丢包控制已有大量的文献予以解决[16-20].

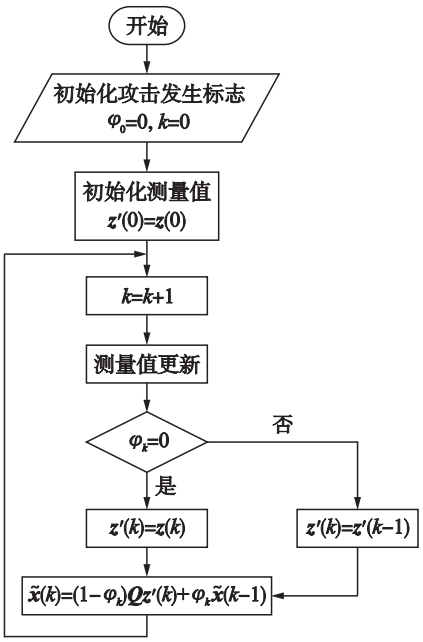

图 1 检测算法流程图

Fig.1 Flow chart of detection algorithm

3 实验结果

利用 Matlab 进行仿真实验，假定系统在不受干扰影响时状态量不变，而虚假数据注入只是攻击测量系统，并不会直接影响系统，系统状态只受到随机干扰的影响，所以只有在测量端需要进行攻击检测.

为此进行仿真实验，假定系统是二维的，测量系统[21]为 $\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}$，加权矩阵为单位矩阵. 其中，

$$\boldsymbol{H}=\begin{pmatrix}1 & 0\\ 0 & 1\\ -1 & -1\end{pmatrix}$$

虚假数据注入攻击条件的攻击向量需要满足条件(11). 求解式(11)，可以得到两个通解：

$$\boldsymbol{a}_1=\begin{pmatrix}0\\ -0.707\ 1\\ -0.707\ 1\end{pmatrix},\quad \boldsymbol{a}_2=\begin{pmatrix}0.816\ 5\\ -0.408\ 2\\ -0.4082\end{pmatrix}$$

对于不同时刻取通解的不同线性组合作为攻击向量 $\boldsymbol{a}$，结果如图 2 所示. 图 2 中的横坐标表示时间，纵坐标表示注入虚假的数据幅值，如电网中可以是电压电流或有功功率等. 不同颜色代表向量的不同分量.

由于系统状态波动不大，所以系统测量值保持不变，假定原系统测量值恒定为

$$\boldsymbol{z}_0=(1,\ 1,\ 1)^{\mathrm{T}}$$

加入随机干扰，随机干扰信号是均值为 0，方差为 1，长度为 100 的高斯变量.

取误差的协方差阵为 $\boldsymbol{e}\sim N(0,\ \boldsymbol{I})$，则有：

$$\boldsymbol{e}_k-\boldsymbol{e}_{k-1}\sim N(0,\ 2\times\boldsymbol{I})$$

对于传统的卡方检测，以每一个分量进行独立的卡方检测. 对于仿真实例，采用本文所提出的增量检测. 因为

假定 3 个分量的误差的都是方差为 1 的正态分布，所以对每个分量采用的置信区间是一致的.

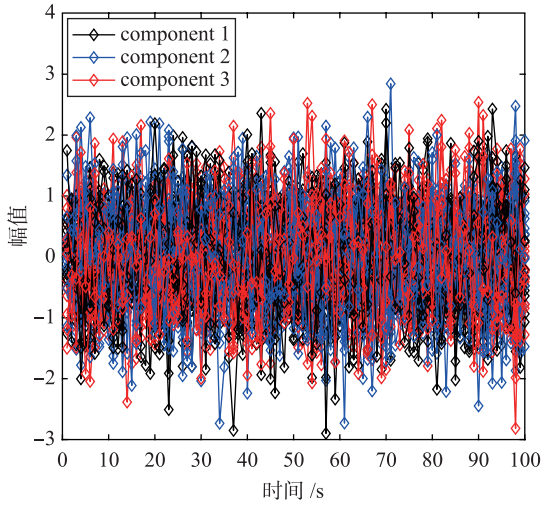

图 2　对测量端加入的虚假数据注入攻击

Fig.2　False data injection attack on measuring end

测量值的误差即是测量噪声，属于随机干扰，如图 3 所示，可以发现未受攻击时测量数据也波动剧烈.

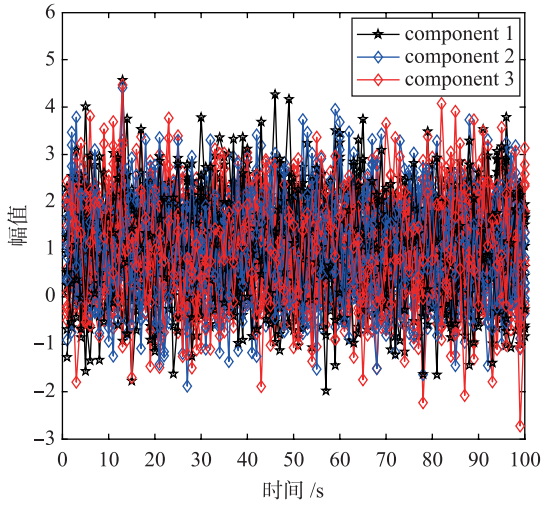

图 3　未受攻击的测量值（含噪声）

Fig.3　Unattacked measurements（including noise）

然后，进行测量值增量的检测. 因为正常未受攻击时刻测量值的增量满足 2 自由度的 χ^2 分布，所以进行 χ^2 检验.

受到攻击之后的测量值如图 4 所示. 图 5 是增量随时间变化的情形.

得到增量变化的数据后，利用 2 自由度的 χ^2 分布得到显著性水平是 0.05 时的假设检验 p 值 $\tau_i = 5.99\,(i = 1, 2, 3)$. 进行假设检验，凡是分量的增量大于 5.99 的情况，则认为该测量值受到攻击，基于该假设检验判断正确的概率有 95%.

攻击标志为 1 表示检测到攻击. 从图 6 可以看出，对于精心设计的虚假数据注入攻击，通用的残差检测几乎无法发现，从而验证了虚假数据注入攻击的隐蔽性. 而使用

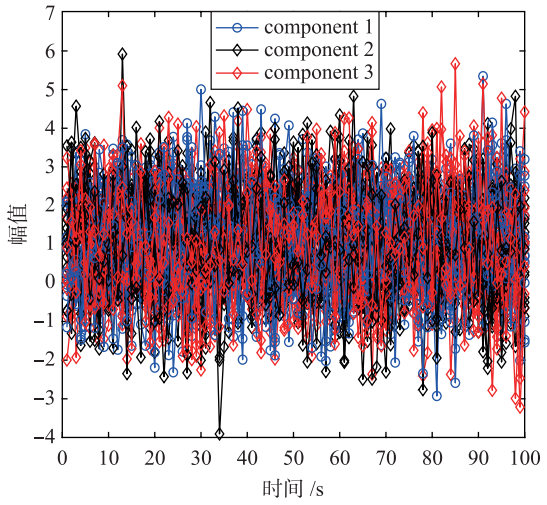

图 4　受到虚假数据注入攻击的测量值

Fig.4　Measurements attacked by false data injection

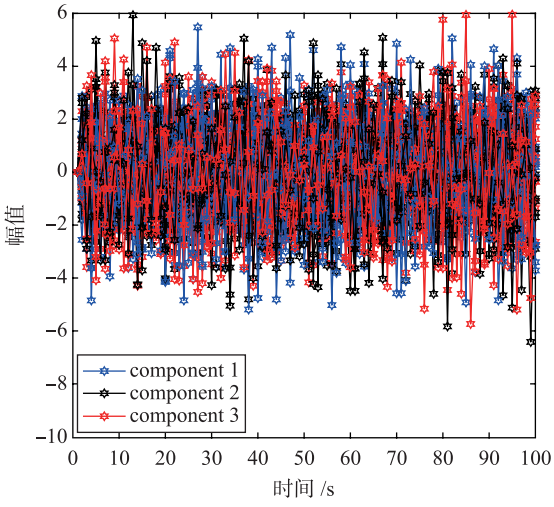

图 5　测量值的增量随时间变化图

Fig.5　Increment of measurements versus time

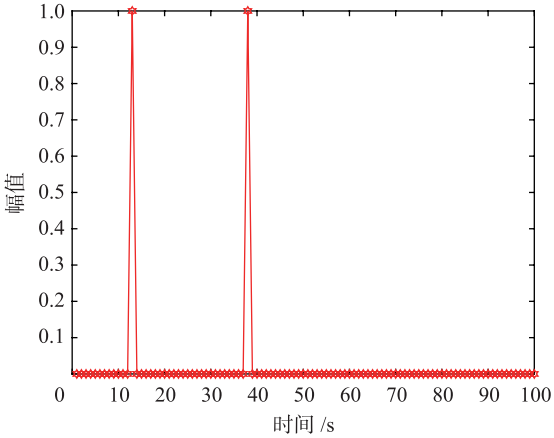

图 6　残差检测结果

Fig.6　Residual test results

本文提出的增量检测能检测出攻击的概率大为提高，如图7所示. 虽然无法完全检测出，但是检测成功的概率大大提高. 共检测出了45个攻击，多次实验检测率都在40%以上. 实验结果证明了本文提出方法的有效性. 未检出的攻击可以认为是随机干扰.

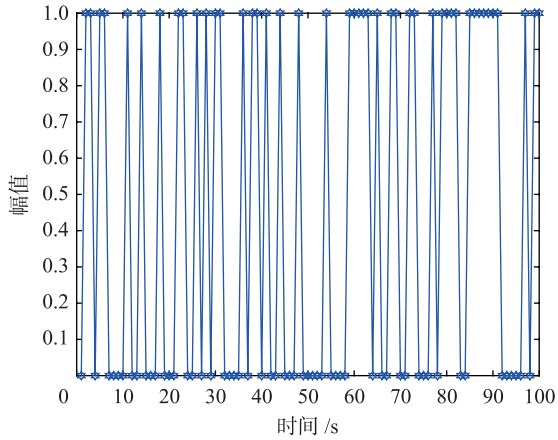

图7 增量检测结果

Fig.7 Incremental test results

4 结论

本文从微电网的电力潮流测量出发，研究了测量值受到攻击时的检测问题，提出了利用测量值增量的χ^2检验的方法检测是否发生攻击. 攻击被检测之后，由测量值去估计状态量，则应使用之前时刻的测量值. 增量检测的限制在于信号变化不能过小，否则将引起取伪错误，所以如何提高检测成功率将是一件有意义的事. 而对于如何与控制结合起来从而在波动的暂态环境也能成功检测，将是未来要研究的工作.

参考文献

[1] Khooban M H, Niknam T, Blaabjerg F, et al. A robust adaptive load frequency control for micro-grids[J]. ISA transactions, 2016, 65: 220 – 229.

[2] Bevrani H, Feizi M R, Ataee S. Robust frequency control in an islanded microgrid: H_∞ and μ-synthesis approaches[J]. IEEE Transactions on Smart Grid, 2016, 7(2): 706 – 717.

[3] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[C]//16th ACM Conference on Computer and Communications Security. New York, NJ, USA: ACM, 2009: 1 – 33.

[4] Liang G Q, Weller S R, Zhao J H, et al. The 2015 Ukraine blackout: Implications for false data injection attacks[J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317 – 3318.

[5] Gu C J, Panida J, Mehul M. Detecting false data injection attacks in AC state estimation[J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2476 – 2483.

[6] Bobba R B, Rogers K M, Wang Q Y, et al. Detecting false data injection attacks on DC state estimation[C]//First Workshop on Secure Control Systems CPS WeeK. 2010.

[7] Yang Q Y, Yang J, Yu W, et al. On false data-injection attacks against power system state estimation: Modeling and countermeasures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(3): 717 – 729.

[8] Huang Y, Tang J, Cheng Y, et al. Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis [J]. IEEE Systems Journal, 2016, 10(2): 532 – 543.

[9] Hu L, Wang Z D, Han Q L, et al. State estimation under false data injection attacks: Security analysis and system protection[J]. Automatica, 2018, 87: 176 – 183.

[10] Liu L, Esmalifalak M, Ding Q, et al. Detecting false data injection attacks on power grid by sparse optimization[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 612 – 621.

[11] Singh S K, Khanna K, Bose R, et al. Joint-transformation-based detection of false data injection attacks in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(1): 89 – 97.

[12] Esmalifalak M, Liu L, Nguyen N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2017, 11(3): 1644 – 1652.

[13] Hug G, Giampapa J A. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks[J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1362 – 1370.

[14] Liang G, Zhao J, Luo F, et al. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1630 – 1638.

[15] Teixeira A, Amin S, Sandberg H, et al. Cyber-security analysis of state estimators in electric power systems[C]//49th IEEE Conference on Decision and Control. Piscateway, NJ, USA: IEEE, 2010: 5991 – 5998.

[16] 朱其新，胡寿松，侯霞. 长时滞网络控制系统的随机稳定性研究[J]. 东南大学学报(自然科学版)，2003，33(3)：368 – 371.
Zhu Q X, Hu S S, Hou X. Stochastic stability of networked control systems with long time delays[J]. Journal of Southeast University (Natural Science Edition), 2003, 33(3): 368 – 371.

[17] 彭晨，岳东. 网络环境下不确定时滞系统鲁棒H_∞控制[J]. 自动化学报，2007，33(10)：1093 – 1096.
Peng C, Yue D. Robust H_∞ control of uncertain time-delay systems in network environment[J]. Acta Automatica Sinica, 2007, 33(10):

1093 – 1096.

[18] 周映江，李训铭，梁华. 不确定时滞网络控制系统的状态反馈控制[J]. 控制理论与应用，2010，27(2)：221 – 225.
Zhou Y J，Li X M，Liang H. State feedback control for uncertain networked control systems with time delays[J]. Control Theory and Application，2010，27(2)：221 – 225.

[19] 彭晨，岳东，彭丽萍. 网络控制中基于 LMI 的次优化允许等价时滞界研究[J]. 系统仿真学报，2007，19(2)：369 – 371，387.
Peng C，Yue D，Peng L P. Research on LMI-based suboptimal admissible equivalent delay bounds in network control[J]. Journal of Systems Simulation，2007，19(2)：369 – 371，387.

[20] 杨洪玖，徐豪，张金会. 不完全信息拒绝服务攻击下基于预测控制的信息物理系统稳定性分析[J]. 信息与控制，2018，47(1)：75 – 80，89.
Yang H J，Xu H，Zhang J H. Stability analysis of information physics system based on predictive control under incomplete information denial of service attack[J]. Information and Control，2018，47(1)：75 – 80，89.

[21] Monticelli A. State estimation in electric power systems[M]. Berlin，Germany：Springer-Verlag，1999.

作者简介

彭华晔(1996 –)，男，硕士生. 研究领域为网络安全控制.

彭　晨(1972 –)，男，博士，教授，博士生导师. 研究领域为网络化安全控制，时滞控制.

(上接第 521 页)

[75] Farraj A，Hammad E，Daoud A A，et al. A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems[J]. IEEE Transactions on Smart Grid，2016，7(4)：1846 – 1855.

[76] Li Y，Quevedo D E，Dey S，et al. A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems[J]. IEEE Transactions on Signal and Information Processing over Networks，2017，3(1)：1 – 11.

[77] Attiah A，Chatterjee M，Zou C C. A game theoretic approach to model cyber attack and defense strategies[C]//2018 IEEE International Conference on Communications (ICC). Piscateway，NJ，USA：IEEE，2018：1 – 7.

[78] Zhang R，Zhu Q，Hayel Y. A bi-level game approach to attack-aware cyber insurance of computer networks[J]. IEEE Journal on Selected Areas in Communications，2017，35(3)：779 – 794.

[79] Liu Y，Xin H，Qu Z，et al. An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks[J]. IEEE Transactions on Smart Grid，2016，7(6)：2923 – 2932.

[80] Ashok A，Govindarasu M，Wang J. Cyber-physical attack-resilient wide-area monitoring，protection，and control for the power grid[J]. Proceedings of the IEEE，2017，105(7)：1389 – 1407.

[81] Pajic M，Weimer J，Bezzo N，et al. Design and implementation of attack-resilient cyber physical systems：With a focus on attack-resilient state estimators[J]. IEEE Control Systems Magazine，2017，37(2)：66 – 81.

作者简介

丁　达(1996 –)，男，硕士生. 研究领域为信息物理系统，网络控制系统.

曹　杰(1969 –)，男，博士，教授，博士生导师. 研究领域为商务智能，电子商务推荐系统，数据挖掘基础理论，电子商务平台支撑技术.