DOI: 10.7667/PSPC152000

一种基于状态估计的新型窃电方法及对策研究

王 昕[1,2]，田 猛[3]，赵艳峰[1,2]，赵 旭[1,2]，魏 龄[1,2]，蒋婷婷[1,2]，王先培[3]

(1.南方电网电能计量重点实验室，云南 昆明 650217；2.云南电网有限责任公司电力科学研究院，云南 昆明 650217；3.武汉大学电子信息学院，湖北 武汉 430072)

摘要：随着科学技术的不断发展，窃电手段逐渐趋向于智能化，也更加的隐蔽。研究了一种基于状态估计的新型窃电方法-虚假数据注入。首先，在传统的虚假数据注入模型基础之上，得到了标准的 L0 范数优化模型，消除了变量系数对虚假数据注入向量精度的影响。然后，基于脆弱性指标提出设置 PMU 的方法提高窃电成本和难度。最后在 IEEE 标准测试系统上对提出的标准的 L0 范数优化模型和保护策略进行了测试。结果表明提出的标准 L0 范数优化模型可以得到更精确的虚假数据注入向量，基于脆弱性指标设置 PMU 可以有效提高非法用户的窃电成本。

关键词：窃电；虚假数据注入；L0 范数优化模型；保护策略；PMU

A new kind of electricity theft based on state estimation and countermeasure

WANG Xin[1,2], TIAN Meng[3], ZHAO Yanfeng[1,2], ZHAO Xu[1,2], WEI Ling[1,2], JIANG Tingting[1,2], WANG Xianpei[3]

(1. Key Laboratory of CSG for Electric Power Measurement, Kunming 650217, China; 2. Yunnan Electric Power Research Institute, Kunming 650217, China; 3. School of Electronic Information, Wuhan University, Wuhan 430072, China)

Abstract: With the development of science and technology, electricity theft tends to be more intelligent and covert. A new kind of electricity theft based on the state estimation, namely false data injection, is analyzed. First, a standard L0-norm optimization model is proposed based on the classic false data injection model. The effects of variable factors on the solution accuracy are eliminated with this standard model. Furthermore, in order to increase the cost and difficulty of the electricity theft, the placement of PMUs based on the vulnerability index is proposed. Finally, the standard L0-norm optimization model and the countermeasure are tested on the IEEE Power Flow Test Cases. The results show that the proposed standard L0-norm optimization model can obtain more accurate false data injection vector, and setting the PMUs based on the vulnerability index can increase the electricity theft cost of illegal users effectively.

Key words: electricity theft; false data injection; L0-norm optimization model; countermeasure; PMU

0 引言

当前，由于缺乏较为先进的计量措施和科学经营手段，窃电已经成为一个全球性的难题，导致电力系统的管理线损高居不下，每年电力企业都会在电力营销方面损失高额的利润，也扰乱了供用电市场，给电力企业和国民生活等带来了极大的负面影响[1-2]。以 2014 年广东电网为例，广东全省共查处窃电案件累计 3964 起，补交电费及追缴违约金合计 5223.12 万元[3]。因此，窃电现象得到了全球电力企业的广泛关注。

常见的窃电手段包括欠压法窃电、欠流法窃电、移相法窃电、扩差法窃电和无表法窃电五大类[4]。针对这些窃电手段，传统的防窃电方法包括使用具有防伪及防撬功能的铅封、对智能电能表编程器加设密码、采用专用计量箱锁和采用专用计量箱计量柜等[5]。这些防窃电措施大都是从一些具体的设备装置出发，针对一种或几种窃电手段进行防窃电。虽然都实现了一定的防窃电功能，但是仍然有一定的局限性，部分技术存在一些缺陷，比如防撬铅封技术含量较低，容易伪造。在此背景下，一些新的防窃电方法和智能防窃电系统应运而生[5]。文献[6]利用当前远程集抄海量数据，提出基于距离的离群点检测法的窃电判定算法。文献[7]将遗传算法与支

基金项目：云南电网公司重点项目(YN2014-2-001)

持向量机相结合，提出了一种利用供电企业积累的大量历史用电数据的防窃电方法。由于文献[7]采用 C 类支持向量机进行分类，存在学习时间过长和需要事先对大量样本进行分类的问题，因此文献[8]进一步地提出采用 One-class 支持向量机分类算法的方案解决人工分类的问题，提高了检测的准确性和效率。文献[9]提出一种基于状态估计理论的防窃电方法，该方法利用状态估计理论中不良数据检测方法定位窃电用户，充分考虑各个用户之间的关联性。

总的说来，随着先进的信息通信技术在电力系统中的大规模使用，防窃电技术越来越趋向于智能化，提高了窃电检测精度和效率，但是开放式的网络环境和信息通信系统自身的故障、缺陷和漏洞使得电力系统面临信息安全问题，尽管已经提出了多种安全标准[10]，新型窃电方式仍层出不穷，也越来越隐秘。文献[11-12]针对电力系统状态估计中不良数据检测的漏洞提出了虚假数据注入(False data injection，FDI)方式，当非法用户掌握电力系统的全部电气参数和拓扑结构参数时，通过构造与电力系统观测矩阵 $\boldsymbol{H}$ 列向量成线性组合关系的虚假数据注入向量，非法用户可以成功地绕过状态估计中的不良数据检测，进而修改电力系统的测量值和状态变量，达到获取经济利益等非法目的。FDI 为非法用户提供了一种新的窃电方案，对电力市场具有很强的负面影响[13-14]。

当前FDI研究已经引起了国内外的广泛关注[15-18]，本文在文献[11-12]的基础上，首次得到了测量值注入虚假数据时标准 L0 范数优化表达式，提高了虚假数据注入向量的精度，并提出了保护重要测量值的防窃电方法，最后在 IEEE 标准测试系统上对模型进行了验证。

1 虚假数据注入基本原理

假设电力系统的母线数量为 N，测量点数量为 m。状态变量一般是母线的电压幅值和电压相角，参考点的相角设置为 0，则状态变量的数量为 $n=2N-1$，满足 $m>n$，用 $\boldsymbol{x}=\left[x_1,x_2,\cdots,x_n\right]^{\mathrm{T}}$ 表示。测量值一般是母线的注入有功功率和无功功率、支路有功功率和无功功率或者母线电压幅值，用 $\boldsymbol{z}=\left[z_1,z_2,\cdots,z_m\right]^{\mathrm{T}}$ 表示。测量值和状态变量之间满足基尔霍夫定律，为非线性关系。

对于一个正常运行的电力系统，由于电力系统母线电压在额定电压附近，并且支路两端相角差很小，对于超高压电力网，线路电阻比电抗小得多。因此，作如下假设，所有母线的电压幅值相等并且均为 1，忽略线路电阻，则测量值中不存在无功功率，状态变量只有电压相角[19]。此时，测量值和状态变量之间满足线性关系，得到如式(1)所示的直流潮流方程。

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e}\quad \boldsymbol{e}\sim \mathrm{N}\left(0,\boldsymbol{\Sigma}_{\mathrm{e}}\right) \tag{1}$$

其中，$\boldsymbol{z}$ 表示测量值，为母线的注入有功功率和支路有功功率；$\boldsymbol{H}$ 表示电力系统的测量雅克比矩阵，与电力系统的连接关系和电气参数相关；$\boldsymbol{x}$ 表示状态变量，为母线电压相角；$\boldsymbol{e}=\left[e_1,e_2,\cdots,e_m\right]^{\mathrm{T}}$ 表示测量误差，并且 $\boldsymbol{e}\sim \mathrm{N}\left(0,\boldsymbol{\Sigma}_{\mathrm{e}}\right)$，$\boldsymbol{\Sigma}_{\mathrm{e}}=\mathrm{diag}\left[\sigma_1^2,\sigma_2^2,\cdots,\sigma_m^2\right]$。同时要求 $m>n$，状态变量 $\boldsymbol{x}$ 的估计值 $\hat{\boldsymbol{x}}$ 可以用等式(2)确定[20]。

$$\hat{\boldsymbol{x}}=\arg\min_{x}\left[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\right]^{\boldsymbol{T}}\boldsymbol{\Sigma}_{\mathrm{e}}^{-1}\left[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\right] \tag{2}$$

加权最小二乘法(WLS)是应用最为广泛的求解方法[21]，通过求解等式(2)，得到直流潮流方程下状态变量的估计值。

$$\hat{\boldsymbol{x}}=\left(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{\Sigma}_{\mathrm{e}}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{\Sigma}_{\mathrm{e}}^{-1}\boldsymbol{z} \tag{3}$$

目前不良数据检测的方法主要基于残差，残差的表达式如式(4)所示。

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}} \tag{4}$$

若 $\|\boldsymbol{r}\|>\tau$，则表示测量数据中至少存在一个不良数据，其中 τ 表示判断阈值。由于 $\boldsymbol{r}^2\sim\chi^2\left(m-n\right)$，阈值 τ 可以根据显著性水平 α 来确定。

若用 $\boldsymbol{a}=\left[a_1,a_2,\cdots,a_m\right]^{\mathrm{T}}$ 表示非法用户在测量值中注入的虚假数据向量，则实际的测量数据为 $\boldsymbol{z}_{\mathrm{bad}}=\boldsymbol{z}+\boldsymbol{a}$，$\boldsymbol{c}=\left[c_1,c_2,\cdots,c_n\right]^{\mathrm{T}}$ 表示由于虚假数据的注入在状态变量中引入的误差向量，估计的状态变量为 $\boldsymbol{x}_{\mathrm{bad}}=\hat{\boldsymbol{x}}+\boldsymbol{c}$。文献[11-12]指出，当 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$ 时，非法用户可以成功的避开虚假数据检测。此时有

$$\begin{aligned}\|\boldsymbol{r}\|=\left\|\boldsymbol{z}_{\mathrm{bad}}-\boldsymbol{H}\boldsymbol{x}_{\mathrm{bad}}\right\|=\left\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right)\right\|=\\ \left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\right\|=\left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\right\|\end{aligned} \tag{5}$$

显然，当 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$ 时，采用基于残差的不良数据检测方法无法发现测量数据中的虚假数据，非法用户可以将测量值和状态变量修改为任意值，获取非法的经济利益。

2 新型防窃电方法及对策分析

2.1 最小虚假数据注入向量求解方法

对于非法用户而言，为了降低窃电成本，待修改的测量装置的数量要尽可能的少，即是虚假数据注入向量 $\boldsymbol{a}$ 中非零元素个数要尽可能的少。一个向量的 L0 范数表示该向量中非零元素的个数，因此可以用虚假数据注入向量 $\boldsymbol{a}$ 的 L0 范数表示非法用

户的窃电代价，L0 范数越大，表示虚假数据注入代价越大，反之，若 L0 范数越小，向量越稀疏，表示虚假数据注入成本越小。因此，非法用户的窃电行为可以用式(6)表示[16]。

$$\begin{aligned}&\min \left\|\boldsymbol{Hc}\right\|_0\\&\text{s.t. } \boldsymbol{a}(k)=1\end{aligned} \tag{6}$$

式中：k 表示非法用户期望修改的计量装置的编号；$\boldsymbol{a}(k)=1$ 表示对第 k 个测量装置注入的虚假数据进行归一化处理，若期望注入的虚假数据为 $\boldsymbol{a}(k)=a_k$。$\boldsymbol{c}^*$ 表示问题(6)的解，则注入的虚假数据为 $\boldsymbol{a}^*=a_k\boldsymbol{Hc}^*$。因此通过求解式(6)可以得到最优的窃电方式，以最低的成本将测量值修改为任意的值。由于式(6)是一个 NP-hard 问题，不可能在一个多项式时间内得到最优解[17]，但可得到近似的次优解，目前研究者已经提出了许多次优解求解算法，如凸松弛技术[16]和最小割集算法[17]。

由于凸优化问题已经有一套完整的求解方法，因此将问题(6)通过凸松弛技术转化为凸优化问题，可以直接采用已有的凸优化问题的求解方法，减小了算法的复杂度。L1 范数是 L0 范数的最优凸近似，因此一般将等式(6)直接转化为 L1 范数的最优问题，如式(7)所示。

$$\begin{aligned}&\min \left\|\boldsymbol{Hc}\right\|_1\\&\text{s.t. } \boldsymbol{a}(k)=1\end{aligned} \tag{7}$$

目标函数中，状态变量 $\boldsymbol{c}$ 存在系数观测矩阵 $\boldsymbol{H}$，文献[18]指出该系数对求解精度有重要影响，通过消除系数 $\boldsymbol{H}$ 可以提高虚假数据注入向量的精度。文献[12]的定理 3.2 表明，$\boldsymbol{a}=\boldsymbol{Hc}$ 当且仅当 $\boldsymbol{Ba}=0$ 成立，其中，$\boldsymbol{B}=\boldsymbol{H}(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{I}$。问题(7)可以进一步的转化为

$$\begin{aligned}&\min \left\|\boldsymbol{a}\right\|_1\\&\text{s.t. } \boldsymbol{Ba}=0\\&\quad\ \boldsymbol{a}(k)=1\end{aligned} \tag{8}$$

用 $\boldsymbol{b}_i$ 表示 $\boldsymbol{B}$ 的第 $\boldsymbol{i}$ 列，$\boldsymbol{B}_i$ 表示移除 $\boldsymbol{B}$ 的第 i 列后剩余的矩阵，$\boldsymbol{a}_i$ 表示向量 $\boldsymbol{a}$ 移除第 i 行之后剩余的变量。问题(8)可以转化为

$$\begin{aligned}&\min \left\|\boldsymbol{a}_i\right\|_1+1\\&\text{s.t. } \boldsymbol{B}_i\boldsymbol{a}_i=-\boldsymbol{b}_i\end{aligned} \tag{9}$$

等价于

$$\begin{aligned}&\min \left\|\boldsymbol{a}_i\right\|_1\\&\text{s.t. } \boldsymbol{B}_i\boldsymbol{a}_i=-\boldsymbol{b}_i\end{aligned} \tag{10}$$

问题(7)和问题(10)是典型的凸优化问题，可以转化为线性规划问题，得到次优虚假数据注入向量。以问题(10)为例，未知向量 $\boldsymbol{a}_i$ 由 $\boldsymbol{a}_i=\boldsymbol{u}-\boldsymbol{v}$ 代替，其中，$\boldsymbol{u},\boldsymbol{v}\in\boldsymbol{R}^n$，并且都为非负向量。$\boldsymbol{u}$ 拥有 $\boldsymbol{a}_i$ 中所有的正元，$\boldsymbol{v}$ 拥有 $\boldsymbol{a}_i$ 中所有的负元。通过这种替换，可以用 $\boldsymbol{z}=\left[\boldsymbol{u}^{\mathrm{T}},\boldsymbol{v}^{\mathrm{T}}\right]^{\mathrm{T}}\in\boldsymbol{R}^{2n}$ 表示拼接向量，则有 $\left\|\boldsymbol{a}_i\right\|_1=1^{\mathrm{T}}(\boldsymbol{u}+\boldsymbol{v})=1^{\mathrm{T}}\boldsymbol{z}$，以及 $\boldsymbol{B}_i\boldsymbol{a}_i=\boldsymbol{B}_i(\boldsymbol{u}-\boldsymbol{v})=\left[\boldsymbol{B}_i,-\boldsymbol{B}_i\right]\boldsymbol{z}$，问题(10)可以转化为如问题(11)所示优化问题。

$$\begin{aligned}&\min 1^{\mathrm{T}}\boldsymbol{z}\\&\text{s.t. }\left[\boldsymbol{B}_i,-\boldsymbol{B}_i\right]\boldsymbol{z}=-\boldsymbol{b}_i\end{aligned} \tag{11}$$

优化问题(11)不再是一个 L1 范数最小化的问题，而是一个典型的线性规划问题，可以采用如内点法、单纯性法和同伦法等方法求解。

2.2 基于保护重要测量装置的防窃电方法

电力系统同步相量测量装置(PMU)采用 GPS 授时，安装在母线上时，同时提供精确的相角和电压幅值测量值，可以用于状态估计中的不良数据检测[22]。文献[23]指出通过设置基本测量 PMU 可以完全防止虚假数据注入，但是该方法要求的基本测量 PMU 数量较大，至少要与母线的数量相等，比如对于一个具有 300 个节点的电力系统而言，要求 PMU 的最低数量为 300 个，因此该方法的成本较高。为了成功攻击编号为 k 的测量点，要求攻击者额外攻击其他测量点，构成攻击向量。攻击向量的 L0 范数越大，表明攻击者需要攻击更多的测量点，攻击成本更高，反之，攻击向量的 L0 范数越小，表明攻击成本越低。基于以上分析，由于完全防止虚假数据注入的成本较高，提出采用增加窃电成本的保护策略，即是增加攻击向量的 L0 范数。

基于攻击向量的 L0 范数，定义如式(12)所示的脆弱性指标。

$$V_k=\sum_{k=1,2,\cdots,m} I\left(\left\|\boldsymbol{a}_k^*\right\|_0<\beta\right) \tag{12}$$

式中：k 表示测量点编号；β 表示脆弱度阈值，表征了容易发生窃电的测量点数量；$I(.)$表示指示函数。若脆弱性指标 V_k 越大，则电力网络中的脆弱节点越多，表明窃电者可以以低于管理者期望的难度发动攻击；反之，若脆弱性指标 V_k 越小，则电力网络中的脆弱节点越少，需要更高的成本窃电。

当集合 $\boldsymbol{S}$ 中的母线受到保护时，用 $\boldsymbol{H}^s$ 表示受保护的 PMU 对应的测量雅克比矩阵的行向量构成的矩阵，则有 $\boldsymbol{H}^s\boldsymbol{c}=0$ 成立。假设 PMU 安装在第 k 个母线上，$\boldsymbol{H}^k$ 表示观测矩阵 $\boldsymbol{H}$ 的第 k 行，若要成功窃电，则有式(13)成立[22]。

$$\begin{bmatrix}\boldsymbol{H}^s\\\boldsymbol{H}^k\end{bmatrix}\boldsymbol{c}=0 \tag{13}$$

在第 k 个测量点上安装 PMU 后，假设最优虚假数据注入向量对应的误差为 $\boldsymbol{c}_k^*$，最优虚假数据注入向量为 $\boldsymbol{a}_k^*$，此时对应的脆弱性指标 V_k^{PMU}，未安装 PMU 之前对应的脆弱性指标为 V_k。显然，如果

$V_k^{\mathrm{PMU}} < V_k$，表明电力网络中的脆弱节点减少，应对窃电的能力增强。因此，安装 PMU 时的目标是使得脆弱性指标最小，直至$V_k^{\mathrm{PMU}} = 0$。

为此，本文提出如下基于 PMU 的防窃电策略。

步骤 1：初始化脆弱度阈值$\beta = \beta_{\mathrm{PMU}}$，PMU 设置母线编号集合$\boldsymbol{P} = \varnothing$，初始化 PMU 母线放置编号$k = 1$。

步骤 2：按照公式(11)和(13)计算虚假数据注入向量，对系统中的测量点进行遍历攻击，计算在脆弱度阈值β_{PMU}下电力网络的脆弱性指标V_k^{PMU}，如果脆弱性指标$V_k^{\mathrm{PMU}} = 0$，$\boldsymbol{P} = \boldsymbol{P} \cup k$，转到步骤 4；否则执行步骤 3。

步骤 3：记录值最小的脆弱性指标V_k^{PMU}对应的母线编号i，将 PMU 设置在母线i上，更新 PMU 设置的母线集合，$\boldsymbol{P} = \boldsymbol{P} \cup k$。$k = k + 1$，执行步骤 2。

步骤 4：算法结束，输出 PMU 设置集合$\boldsymbol{P}$，将 PMU 放置在集合$\boldsymbol{P}$对应的母线上可以使得$V_k^{\mathrm{PMU}} = 0$。

3 仿真与分析

本文主要以 IEEE 标准测试系统为测试用例，假设每个母线上有一个测量点，每条支路的入口端和出口端各设置一个测量点。比如对于 IEEE 14 节点系统，除去参考节点后，则总共有$n = 13$个状态变量，$m = 54$个测量值，各个测量点的编号根据 Matpowe4.1 工具箱确定。

利用 CVX 优化工具箱直接求解优化模型(7)和优化模型(10)，并以 IEEE 14、IEEE30、IEEE 57 和 IEEE 118 节点系统为例，比较采用两种优化模型时虚假数据注入向量的稀疏度，如表 1 所示。

表 1 不同测试系统下虚假数据注入向量的L0范数

Table 1 L0norm of FDI in different test systems

模型类别	IEEE 14	IEEE 30	IEEE 57	IEEE 118
模型(7)	0.777 8	0.803 6	0.695 9	0.830 6
模型(10)	0.925 9	1.0	0.935 5	0.940 8

以IEEE 14节点测试系统为例，对测试网络的测量值遍历地注入虚假数据，得到各个测量值在模型(7)和模型(10)时对应的虚假数据注入向量L0范数的分布图，如图1所示。模型(10)中有0.925 9比例的虚假数据注入向量比模型(7)更稀疏，而模型(7)中有0.777 8比例的虚假数据注入向量比模型(10)更稀疏。表明通过求解优化问题(10)可以得到比问题(7)更稀疏的解，意味着非法用户可以采用代价更低的攻击手段，对电力系统的危害也更大。

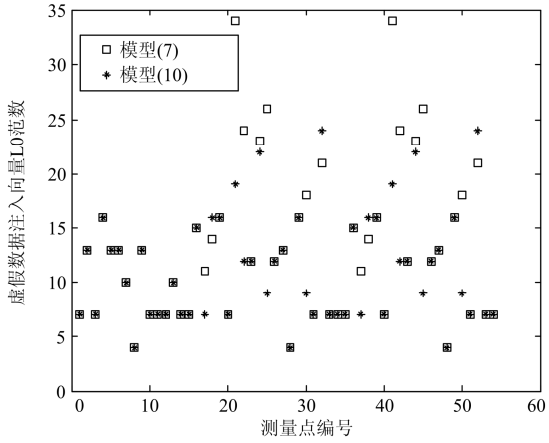

图1 IEEE 14节点测试系统中L0范数的分布图

Fig. 1 Distribution of L0-norm in IEEE 14 bus system

在脆弱度阈值$\beta = 6$时，根据脆弱性指标V_k的定义，仍然以 IEEE 14、IEEE30、IEEE 57 和 IEEE 118 节点系统为例，得到未设置 PMU 时各个网络相应的脆弱性指标V_k，如表 2 所示。由表 2 知，在相同的脆弱度阈值$\beta = 6$下，不同测试网络对应的脆弱性指标V_k不相等，表明窃电时窃电者付出的最小代价不一样。并且脆弱性指标V_k与电力网络的结构相关，与网络规模无关，大规模电力网络的脆弱性指标V_k可能小于小规模网络，比如 IEEE57 节点系统的节点规模大于 IEEE 30 节点测试系统，但是脆弱性指标更低，表明脆弱节点较少。针对 IEEE 14 节点系统，脆弱度阈值$\beta = 6$时，脆弱性指标$V_k = 3$，由图 1 知，对应的测量点为节点注入功率 P_8和支路潮流 $P_{7\text{-}8}$和 $P_{8\text{-}7}$，下标表示母线编号，这些节点对应的虚假数据注入向量的 L0 范数较小，攻击者从这些节点窃电代价更低。

表 2 不同测试系统下对应的脆弱性指标V_k

Table 2 Vulnerability index V_k in different test systems

测试网络	IEEE 14	IEEE 30	IEEE 57	IEEE 118
V_k	3	9	3	25

以 IEEE 14 节点系统为例，考虑在不同脆弱度阈值β时脆弱性指标V_k，结合图 1，得到脆弱性指标如表 3 所示。由表 3 知，不同的脆弱度阈值β对应的脆弱性指标V_k不同，随着脆弱度阈值β的增加，脆弱性指标V_k也逐渐增加。脆弱度阈值β越大，表明管理者期望网络防窃电的能力越强，因此在未实施保护措施时，网络中的脆弱节点数也越多。

设置脆弱度阈值$\beta = 6$，以 IEEE 14、IEEE30、IEEE 57 和 IEEE 118 为例，验证本文提出的 PMU 放置策略，以达到防窃电的目的，得到使得脆弱性指标$V_k = 0$时各个网络需要设置的 PMU 数量，如表

4 所示。由表知，与文献[23]设置基本测量 PMU 的保护策略相比，在脆弱度阈值 $\beta=6$ 时，不同测试网络对应的保护 PMU 数量远小于节点数量，降低了保护成本。

表 3 不同脆弱度阈值对应的脆弱性指标

Table 3 Vulnerability index corresponding to the vulnerability threshold

β	5	10	15	30
V_k	3	25	41	52

表 4 不同测试网络 PMU 设置数量

Table 4 Number of PMUs in different test systems

测试网络	IEEE 14	IEEE 30	IEEE 57	IEEE 118
PMU数量	2	6	2	18

以IEEE 14节点测试系统为例，得到消除脆弱度阈值 $\beta=6$ 意义下的脆弱节点后的各个测量点对应的L0范数分布图，如图2所示。图中，L0范数为零，表明无法从该测量点窃电。根据本文的算法，在 IEEE 14节点系统的母线1和母线7上设置PMU，由图2知，网络中不存在虚假数据向量的L0范数小于脆弱度阈值 $\beta=6$ 的测量点，消除了脆弱度阈值 $\beta=6$ 意义下的脆弱点，提高了整个网络防窃电的能力。

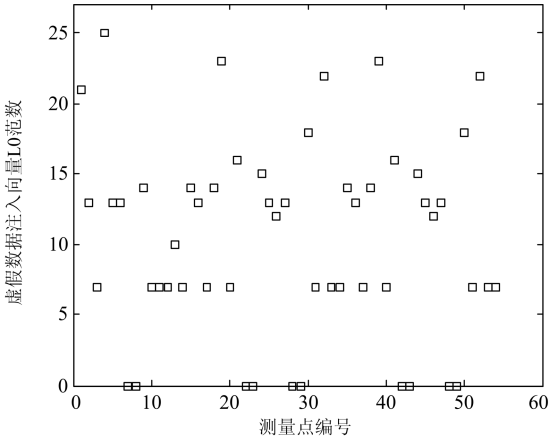

图 2 IEEE 14节点系统设置PMU后L0范数分布图

Fig. 2 Distribution of L0-norm in IEEE 14 bus system with PMUs

4 总结

由于窃电严重影响了电力企业的经济效益，扰乱了用电市场，目前，采用多种手段防窃电，在一定程度上降低了窃电带来的经济损失。但是，随着科学技术的不断进步，窃电也逐渐的趋向于智能化，也更加的隐蔽。本文研究了一类基于状态估计的窃电方法-虚假数据注入，该种窃电方法利用传统估计理论中不良数据检测的漏洞，可以任意的修改测量值而不被发现。为了应对 FDI，本文采用设置 PMU 的方法提高窃电者的窃电代价，最后在 IEEE 标准测试系统上进行验证，表明该种窃电方法在转化为标准的 L0 范数优化形式后，可以得到比传统模型更精确的虚假数据注入向量，设置合适的 PMU 可以有效的提高窃电者的代价。

参考文献

[1] SMITH T B. Electricity theft: a comparative analysis[J]. Energy Policy, 2004, 32(18): 2067-2076.

[2] 赵兵, 吕英杰, 邹和平. 一种新型防窃电装置的设计[J]. 电力系统保护与控制, 2009, 37(23): 116-118, 184.
ZHAO Bing, LÜ Yingjie, ZOU Heping. Design of a new anti-stealing electricity[J]. Power System Protection and Control, 2009, 37(23): 116-118, 184.

[3] 龙金光. 2014 年广东查处窃电案 3964 起[EB/OL] // http://epaper.southcn.com/nfdaily/html/2015-04/13/content_7417490.htm.

[4] 程海花, 李晓明, 黄军高, 等. 窃电检测在电能量计量计费系统中的应用[J]. 电力系统及其自动化学报, 2001, 13(6): 53-57.
CHENG Haihua, LI Xiaoming, HUANG Jungao, et al. Applying of detecting the theft of electricity in the power energy billing system[J]. Proceedings of the CSU-EPSA, 2001, 13(6): 53-57.

[5] 王月志, 郑安刚, 邹和平, 等. 智能防窃电技术的研究[J]. 沈阳工程学院学报(自然科学版), 2013, 9(4): 319-322.
WANG Yuezhi, ZHENG Angang, ZOU Heping, et al. Research on intelligent technology for anti-electricity-theft[J]. Journal of Shenyang Institute of Engineering (Natural Science), 2013, 9(4): 319-322.

[6] 程超, 张汉敬, 景志敏, 等. 基于离群点算法和用电信息采集系统的反窃电研究[J]. 电力系统保护与控制, 2015, 43(17): 69-74.
CHENG Chao, ZHANG Hanjing, JING Zhimin, et al. Study on the anti-electricity stealing based on outlier algorithm and the electricity information acquisition system[J]. Power System Protection and Control, 2015, 43(17): 69-74.

[7] NAGI J, YAP K S, TIONG S K, et al. Detection of abnormalities and electricity theft using genetic support vector machines[C] // TENCON 2008-2008 IEEE Region 10 Conference. IEEE, 2008: 1-6.

[8] 简富俊, 曹敏, 王磊, 等. 基于 SVM 的 AMI 环境下用电异常检测研究[J]. 电测与仪表, 2014, 51(6): 64-69.
JIAN Fujun, CAO Min, WANG Lei, et al. SVM based energy consumption abnormality detection in AMI

system[J]. Electrical Measurement & Instrumentation, 2014, 51(6): 64-69.

[9] HUANG S C, LO Y L, LU C N. Non-technical loss detection using state estimation and analysis of variance[J]. IEEE Transactions on Power Systems, 2013, 28(3): 2959-2966.

[10] 丁心志, 李慧杰, 杨慧霞, 等. 基于 IEC/TC57 国际标准体系现状分析研究与展望[J]. 电力系统保护与控制, 2014, 42(21): 145-154.
DING Xinzhi, LI Huijie, YANG Huixia, et al. Present situation analysis and prospect for international standards system based on IEC/TC 57[J]. Power System Protection and Control, 2014, 42(21): 145-154.

[11] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[C] // Proceedings of the 16th ACM conference on Computer and communications security. ACM, Chicago, November 9-13, 2009: 21-32.

[12] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 13.

[13] XIE L, MO Y, SINOPOLI B. Integrity data attacks in power market operations[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 659-666.

[14] JIA L, THOMAS R J, TONG L. Malicious data attack on real-time electricity market[C] // Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on. IEEE, 2011: 5952-5955.

[15] LI Y, WANG Y. State summation for detecting false data attack on smart grid[J]. International Journal of Electrical Power & Energy Systems, 2014, 57(5): 156-163.

[16] SANDBERG H, TEIXEIRA A, JOHANSSON K H. On security indices for state estimators in power networks[C] // First Workshop on Secure Control Systems (SCS), Stockholm, 2010.

[17] SOU K C, SANDBERG H, JOHANSSON K H. Electric power network security analysis via minimum cut relaxation[C] // Decision and Control and European Control Conference (CDC-ECC), Orlando, December 12-15, 2011 50th IEEE Conference on. IEEE, 2011: 4054-4059.

[18] KIM T T, POOR H V. Strategic protection against data injection attacks on power grids[J]. IEEE Transactions on Smart Grid, 2011, 2(2): 326-333.

[19] 赵娟, 申旭辉, 吴丽华, 等. 结合直流潮流模型的电网断面热稳定极限快速评估方法[J]. 电力系统保护与控制, 2015, 43(3): 97-101.
ZHAO Juan, SHEN Xuhui, WU Lihua, et al. Fast evaluation method on thermal stability limit of power grid cross-section with DC power flow model[J]. Power System Protection and Control, 2015, 43(3): 97-101.

[20] 黄知超, 谢霞, 王斌. 结合模糊综合评判与决策的电力系统状态估计[J]. 电力系统保护与控制, 2015, 43(7): 65-69.
HUANG Zhichao, XIE Xia, WANG Bin. Power system state estimation combined with fuzzy comprehensive evaluation and decision-making[J]. Power System Protection and Control, 2015, 43(7): 65-69.

[21] 王茂海, 齐霞. 输电线路电阻参数误差对无功状态估计结果的影响分析[J]. 电力系统保护与控制, 2015, 43(23): 143-147.
WANG Maohai, QI Xia. Analysis of transmission line resistance parameter's impacts on reactive power estimation results[J]. Power System Protection and Control, 2015, 43(23): 143-147.

[22] CHEN J, ABUR A. Placement of PMUs to enable bad data detection in state estimation[J]. IEEE Transactions on Power Systems, 2006, 21(4): 1608-1615.

[23] 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, CPSWEEK. 2010.

收稿日期：2015-11-15； 修回日期：2016-03-01

作者简介：

王 昕(1969-)，女，本科，高级工程师，研究方向为电能计量；E-mail: wx3128@126.com

田 猛(1989-)，男，通信作者，博士，研究方向为大电网安全和信息安全；E-mail: mengtian@whu.edu.cn

王先培(1963-)，男，博士，教授，研究方向为大电网安全和信息安全。E-mail: xpwang@whu.edu.cn

(编辑 姜新丽)