# 基于拓扑篡改的电力市场虚假数据注入攻击方案

王胜锋，丁 洲，吴劲松，邱爱兵
（南通大学 电气工程学院，江苏 南通 226019）

**摘要**：从攻击者的角度出发，在直流状态估计框架下提出了一种基于拓扑篡改的虚假数据注入攻击（FDIA）方案。首先，通过分析攻击后由网络拓扑处理器计算所得拓扑结构与传感器测量结果的一致性以及对比攻击前、后的残差，给出可以躲避拓扑误差处理检测以及残差检测的隐蔽攻击定义；然后，基于上述定义以及攻击向量列空间的隐蔽条件，提出一种FDIA方案，通过求解凸规划问题实现在保证隐蔽性的同时获得最大发电收益；最后，基于标准IEEE 9节点及14节点系统对所提方案的有效性进行验证。结果表明，与现有FDIA方案相比，所提将拓扑篡改与FDIA相结合的攻击方案具有更强的隐蔽性且获利更大。

**关键词**：虚假数据注入攻击；网络拓扑；拓扑篡改；电力市场；状态估计
**中图分类号**：TM 761 **文献标志码**：A DOI：10.16081/j.epae.202106004

## 0 引言

随着电力系统通信智能化的快速发展，现代电力系统已发展成为由信息网和电力网深度融合而成的典型电力信息物理融合系统（CPPS）[1-2]。2019年10月16日，《泛在电力物联网白皮书2019》的发布标志着我国CPPS的建设正在加速推进[3]。与此同时，随着《关于进一步深化电力体制改革的若干意见》的发布，我国电力体制改革稳步推进，逐步开始建设电力市场[4]。能量管理系统（EMS）、市场管理系统（MMS）是实现信息层（现场传感器测量和通信网络）与物理系统和市场运营深度融合的关键。网络拓扑处理器（NTP）和状态估计是EMS的核心功能。NTP根据断路器/开关的状态数据构建系统拓扑，EMS使用NTP生成的网络拓扑结构，根据传感器测量的节点注入功率和线路流过功率估计节点电压幅值以及电压相角，MMS则使用EMS估计所得数据进行电价计算以及运营决策等操作[5]。

电网拓扑的一致性、完整性是监控中心确保电力系统安全经济运行的基本前提[6]。然而，在上述融合过程中，由于通信网络具有开放性、脆弱性，会导致NTP面临各种类型的网络攻击。此外，MMS计算的节点边际价格（LMP）与电力系统的实际运行状态密切相关，这使得准确的状态估计至关重要。网络攻击者可通过修改量测值来改变拓扑结构及状态估计结果，进而影响电力市场，这给电力市场带来了隐患[7]。虚假数据注入攻击（FDIA）是典型的针对状态估计的网络攻击，此类攻击具有隐蔽性、复杂性、破坏性大等特点[8]。由于LMP是根据实际系统运行的状态估计结果计算确定，攻击者可发起FDIA来操纵节点电价并获利。因此，建立直观的攻击模型并系统地分析FDIA对实时电力市场的影响，有助于电力系统监控中心、运营商采取相应的防御措施。

为此，有关电力市场FDIA的研究受到了广泛关注[9-17]。文献[9]首次通过虚拟竞标研究了FDIA对电力市场运营中的状态估计可能产生的经济影响；文献[10]根据市场收入评估所提的数据攻击方案；文献[11]研究了不同的不良数据模型对LMP的影响；文献[12]提出攻击者能使用FDIA及伪造的双边合同从日前市场与实时市场之间的LMP差异中获利；文献[13]提出了一种攻击者无需电网拓扑或参数信息就可通过电表测量的实时数据流发起的在线攻击方案。值得指出的是，上述研究均假设电力系统的网络拓扑结构未受到攻击，而事实上攻击者可轻易地通过篡改传感器测量的开关状态离散数据，在不被监控中心的拓扑误差处理（TEP）检测的情况下，误导监控中心认为电力系统在与现实不同的拓扑结构下运行，这具有更强的隐蔽性、破坏性[17]。文献[5，14-16]探索了拓扑攻击对电力市场的影响，其中文献[14]提出了一个分析框架，用于评估在线路阻塞情况下网络拓扑偏差对LMP的影响；特别地，文献[15]提出了线路增加攻击、线路断开攻击、线路交换攻击3种拓扑攻击框架，并根据3种攻击方案提出一种统一的最优攻击模型，通过直接误导监控中心的决策过程以影响电力系统的经济运行和安全性。

受上述研究工作的启发，本文针对线路断开攻击研究了一种更为具体的针对电力市场的攻击方

**收稿日期**：2020-12-18；**修回日期**：2021-04-08
**基金项目**：国家自然科学基金资助项目（61473159，61973209）；江苏省六大人才高峰项目（XYDXX-091）；南通市民生科技重点项目（MS22020030）
Project supported by the National Natural Science Foundation of China（61473159，61973209），the Six Talent Peaks Project of Jiangsu Province（XYDXX-091） and Nantong Key Science and Technology Program for People's Livelihood（MS22020030）

案，通过在状态估计框架下研究线路断开隐蔽攻击方案并分析其对电力市场的影响，以更全面地发现电力市场潜在的经济风险。与现有FDIA方案不同的是，本文所提FDIA方案考虑了攻击易被忽略的拓扑结构数据，并构造了比现有FDIA方案收益更高且更隐蔽的攻击策略。具体而言，本文从攻击者的角度出发，提出了一种基于拓扑篡改的电力市场FDIA方案。通过篡改传感器传输的离散的网络数据以及连续的模拟量数据分析拓扑攻击对电力市场的影响。主要内容及创新点如下：①为了保证攻击后拓扑结构与传感器测量的连续数据的一致性及隐蔽性，给出了躲避残差检测以及TEP检测的隐蔽攻击的定义；②根据上述隐蔽攻击定义及隐蔽攻击向量的代数条件，提出一种能在发电机节点获得最大收益的同时通过残差检测以及TEP检测的攻击方案，并可通过求解凸规划问题实现该方案；③算例仿真结果表明，在拓扑攻击的基础上，当攻击者篡改的传感器数量越多，所提攻击方案获得的收益越高。

## 1 电力市场模型

在以美国为代表的放松管制的电力市场中，节点电价由区域输电组织(RTO)决定。实时LMP是所有市场参与者的结算价格。本节介绍了包含网络拓扑信息的量测模型、状态估计、实时市场中的事前市场和事后市场模型，并给出了LMP的计算形式。

### 1.1 量测模型

现代电网通过大量远程终端单元(RTU)或相量测量单元(PMU)等传感和感知设备获取电网数据，并将其传输至监控中心。从信号特征角度而言，这些数据可分为以下2类：一类是各种断路器以及开关状态的二进制数据$s\in\{0,1\}$，这些二进制数据构成了电网的拓扑结构，可以采用有向图$g=(\nu,\varepsilon)$表示，其中$\nu$为节点集合，$\varepsilon$为连接线路集合；另一类是由节点注入功率和线路潮流等组成的模拟量，这些模拟量与电力系统的状态和拓扑结构$g$有关，可用式(1)所示交流潮流模型表示[5]。

$$z=h(\boldsymbol{x},g)+\boldsymbol{w} \tag{1}$$

式中：$z$为由节点注入功率和线路潮流传感器测量的有功、无功功率组成的向量；$\boldsymbol{x}$为由所有节点电压相角、幅值组成的电力系统状态向量；$h$为包含$\boldsymbol{x}$和$g$的非线性函数；$\boldsymbol{w}$为加性测量噪声。

目前，实际工程中应用的LMP都是基于直流潮流模型计算所得[14]。基于直流潮流模型计算LMP的优势在于：可以利用线性规划法进行求解，其计算速度明显优于交流模型，适合在线应用[9]。将非线性函数$h$在稳定点附近进行线性化，即做如下假设：①电压相角都很小；②忽略电网损耗；③电压幅值都接近于额定值。则可得直流潮流模型为：

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{w} \tag{2}$$

式中：由于在直流意义下不存在无功功率，$\boldsymbol{z}\in\mathbf{R}^m$仅由节点注入功率和线路潮流测量的有功功率组成，$m$为观测量数量；$\boldsymbol{x}\in\mathbf{R}^n$为由所有节点电压相角组成的状态向量，$n$为状态变量数量；$\boldsymbol{H}\in\mathbf{R}^{m\times n}$为测量矩阵；$\boldsymbol{w}\in\mathbf{R}^m$为方差是$Q$的高斯噪声。

测量矩阵$\boldsymbol{H}$依赖于网络拓扑$g$，但是$\boldsymbol{H}$不与$g$显式相关，为了便于表示，在直流潮流模型中用$\boldsymbol{H}$表示拓扑结构。根据式(2)，线路$ij$的潮流$z_{ij}=B_{ij}(x_i-x_j)$，其中$B_{ij}$为线路$ij$的电纳，$x_i$、$x_j$分别为节点$i$、$j$的电压相角，$\boldsymbol{H}$中对应的行向量$\boldsymbol{h}_i$为：

$$\boldsymbol{h}_i=[0,\cdots,0,B_{ij},0,\cdots,0,-B_{ij},0,\cdots,0] \tag{3}$$

如果$z_{ij}$为1条断开线路的潮流测量，则$z_{ij}=0$，$\boldsymbol{H}$中对应行向量的各元素均为0。

线路潮流$\boldsymbol{z}_{\mathrm{f}}$与节点注入功率$\boldsymbol{z}_{\mathrm{in}}$存在如下关系：

$$\boldsymbol{z}_{\mathrm{f}}=\boldsymbol{S}\boldsymbol{z}_{\mathrm{in}} \tag{4}$$

式中：$\boldsymbol{S}\subset\boldsymbol{H}$为功率传输分布因子矩阵，表示线路潮流对节点注入功率的灵敏程度[14]。

### 1.2 状态估计

监控中心进行以网络和传感器数据为输入的广义状态估计(GSE)。基于交流潮流模型(式(1))的状态估计示意图见图1。图中，$(s,z)$为GSE的输入；$\hat{\boldsymbol{x}}$为电力系统状态的非线性最小二乘估计，如式(5)所示，可通过迭代算法进行求解；在未受攻击时有$\hat{g}=g$。

$$\hat{\boldsymbol{x}}=\mathrm{argmin}\left[(z-h(\boldsymbol{x},\hat{g}))^{\mathrm{T}}(z-h(\boldsymbol{x},\hat{g}))\right] \tag{5}$$

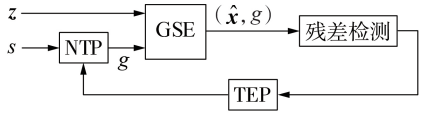



**图1 基于交流潮流模型的状态估计示意图**

Fig.1 Schematic diagram of state estimation based on AC power flow model

进一步地，考虑简化后的直流潮流模型式(2)，最小二乘估计则退化为线性估计，如式(6)所示。

$$\hat{\boldsymbol{x}}=(\hat{\boldsymbol{H}}^{\mathrm{T}}\hat{\boldsymbol{H}})^{-1}\hat{\boldsymbol{H}}^{\mathrm{T}}\boldsymbol{z} \tag{6}$$

式中：$\hat{\boldsymbol{H}}$为$\hat{g}$的测量矩阵，在无攻击时有$\hat{\boldsymbol{H}}=\boldsymbol{H}$。

根据式(6)可得：

$$\hat{\boldsymbol{z}}=\hat{\boldsymbol{H}}\hat{\boldsymbol{x}}=\boldsymbol{K}\boldsymbol{z} \tag{7}$$

式中：$\boldsymbol{K}=\hat{\boldsymbol{H}}(\hat{\boldsymbol{H}}^{\mathrm{T}}\hat{\boldsymbol{H}})^{-1}\hat{\boldsymbol{H}}^{\mathrm{T}}$。

定义测量残差$\boldsymbol{r}$如式(8)所示。

$$\boldsymbol{r}=\boldsymbol{z}-\hat{\boldsymbol{z}}=(\boldsymbol{I}-\boldsymbol{K})\boldsymbol{z} \tag{8}$$

式中：$\boldsymbol{I}$为与矩阵$\boldsymbol{K}$同维度的单位矩阵。

监控中心通过比较$\boldsymbol{r}$的范数与阈值$\gamma$大小进行异常检测，逻辑一般为：

$$\begin{cases}\|\boldsymbol{r}\|>\gamma & \text{报警}\\ \|\boldsymbol{r}\|\leqslant\gamma & \text{正常}\end{cases} \tag{9}$$

### 1.3 事前市场模型

事前市场通常在实时前10~15 min进行一次安

全约束经济调度（SCED），用于确定在预期负荷 $L^*_{\mathrm{d},j}$ 下的最优发电 $P^*_{\mathrm{g},i}$。事前市场中的SCED问题可以由式（10）表示，其结果是向每个市场参与者发出的调度命令[9,14]。

$$\begin{cases}\min\limits_{P^*_{\mathrm{g},i}} \sum\limits_{i=1}^{I} C_i(P^*_{\mathrm{g},i}) \\ \text{s.t.} \quad \sum\limits_{i=1}^{I} P^*_{\mathrm{g},i} = \sum\limits_{j=1}^{J} L^*_{\mathrm{d},j} \\ \qquad P_l^{\min} \leqslant P^*_l \leqslant P_l^{\max} \quad l=1,2,\cdots,L \\ \qquad P^{\min}_{\mathrm{g},i} \leqslant P^*_{\mathrm{g},i} \leqslant P^{\max}_{\mathrm{g},i} \quad i=1,2,\cdots,I\end{cases} \tag{10}$$

式中：$C_i(P^*_{\mathrm{g},i})$为发电机节点$i$的发电成本函数，$C_i(P^*_{\mathrm{g},i})=a_i(P^*_{\mathrm{g},i})^2+b_iP^*_{\mathrm{g},i}+c_i$，$a_i$、$b_i$、$c_i$为发电机节点$i$的发电成本系数；$P^{\min}_{\mathrm{g},i}$、$P^{\max}_{\mathrm{g},i}$分别为发电机节点$i$的最小、最大发电功率；$P^*_l$为线路$l$的最优潮流；$P_l^{\min}$、$P_l^{\max}$分别为线路$l$允许传输的最小、最大功率；$I$为发电机节点数量；$J$为负荷节点数量；$L$为线路数量。

### 1.4　事后市场模型

由于实时运行状态与事前市场调度的最优状态不同，RTO将基于状态估计数据计算LMP进行出清结算。首先定义式（11）所示阻塞集$\hat{C}$。

$$\hat{C}=\left\{l:\hat{P}_l>P_l^{\max}\right\} \tag{11}$$

式中：$\hat{P}_l$为线路$l$的潮流估计值。

为了获得用于结算的LMP，事后市场在实际系统状态附近的较小范围内求解SCED[9]，见式（12）。

$$\begin{cases}\min\limits_{\Delta P_{\mathrm{g},i}} \sum\limits_{i=1}^{I} C_i(\Delta P_{\mathrm{g},i}+\hat{P}_{\mathrm{g},i}) \\ \text{s.t.} \quad \sum\limits_{i=1}^{I} \Delta P_{\mathrm{g},i} = 0 \\ \qquad \Delta P^{\min}_{\mathrm{g},i} \leqslant \Delta P_{\mathrm{g},i} \leqslant \Delta P^{\max}_{\mathrm{g},i} \quad i=1,2,\cdots,I \\ \qquad \Delta P_l \leqslant 0 \quad l\in\hat{C}\end{cases} \tag{12}$$

式中：$\hat{P}_{\mathrm{g},i}$为系统估计的发电机节点$i$的发电功率；$\Delta P_{\mathrm{g},i}$为发电机节点$i$增加的边际发电量；$\Delta P_l$为线路$l$增加的边际潮流；$\Delta P^{\max}_{\mathrm{g},i}$、$\Delta P^{\min}_{\mathrm{g},i}$分别为发电机节点$i$增加边际发电量的上、下限，通常取$\Delta P^{\max}_{\mathrm{g},i}=0.1\,\mathrm{MW\cdot h}$，$\Delta P^{\min}_{\mathrm{g},i}=-2\,\mathrm{MW\cdot h}$，

利用拉格朗日乘子法求解式（12）可得相应的拉格朗日算子$\lambda$、$\mu_{i,\max}$、$\mu_{i,\min}$、$\eta_l$[9]，因此节点$f$的LMP矩阵形式为：

$$\lambda_f=\lambda-\boldsymbol{S}_f^{\mathrm{T}}\boldsymbol{\eta} \tag{13}$$

式中：$\lambda_f$为节点$f$的LMP[12]；$\boldsymbol{\eta}=[\eta_1,\eta_2,\cdots,\eta_L]^{\mathrm{T}}$；$\boldsymbol{S}_f$为矩阵$\boldsymbol{S}$的第$f$列向量。

由上述LMP的计算过程可以看出，节点注入功率以及线路潮流的估计结果决定了LMP式（13），因此状态估计在市场价格制定中至关重要。为了出清实时市场，发电机节点$i$获得的收益为$\lambda_i(\hat{P}_{\mathrm{g},i}-P^*_{\mathrm{g},i})$，消费客户在负荷节点$j$支付的费用为$\lambda_j(\hat{L}_{\mathrm{d},j}-L^*_{\mathrm{d},j})$，$\hat{L}_{\mathrm{d},j}$为节点$j$的负荷估计值。

## 2　基于拓扑篡改的FDIA

### 2.1　攻击模型及攻击目标

假设恶意第三方想要通过破坏一定数量的传感器来攻击系统并向监控中心发送虚假测量结果而从市场中获利。为了分析极端情况下FDIA对电力系统的影响，通常假设攻击者有如下能力[15-17]。

1）攻击者知道系统的拓扑矩阵、线路参数、状态估计方案以及数据检测方法，即攻击者知道系统模型并能在发起攻击前获取$(s,z)$的所有数据。

2）攻击者可篡改传感器数据，包括传输到NTP的断路器/开关的离散数据、传输到状态估计的数据。这与现有大多有关FDIA的研究中假设拓扑网络数据不受攻击不同。将拓扑$g$篡改为$g'$的模型为：

$$\begin{cases}s'=s+b\\ z'=z+\boldsymbol{\Gamma a}\end{cases} \tag{14}$$

式中：$g'$为篡改相应的网络数据$s'$后对应的系统拓扑；$b\in\{0,1\}$为添加到网络数据$s$中的篡改值；$\boldsymbol{a}\in\mathbf{R}^m$为添加到传感器数据$z$中的攻击向量；$\boldsymbol{\Gamma}=\mathrm{diag}(\gamma_1,\gamma_2,\cdots,\gamma_m)$为可行攻击向量空间，当且仅当$\gamma_i=1$时表示第$i$台传感器的数据被篡改，$\boldsymbol{\Gamma}$完全反映了攻击者的能力。

3）假设直流模型式（2）中的测量矩阵$\boldsymbol{H}$为满秩矩阵，即无论是否存在攻击，系统都是可观的[5]。这就要求攻击者不能通过剧烈的系统改变来误导监控中心，从而避免引起监控中心的过多关注。

攻击者的目标是将拓扑$g=(\nu,\varepsilon)$篡改为不同的目标拓扑$g'=(\nu,\varepsilon')$。为了改变网络的拓扑结构，攻击者发起了一次中间人攻击，攻击者拦截$(s,z)$并篡改部分传感器数据，然后将篡改后的$(s',z')$发送给监控中心。攻击后的状态估计示意图见图2。

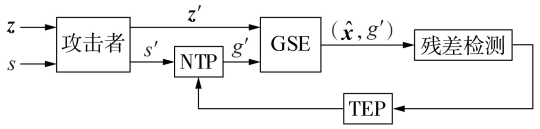



**图2　攻击后的状态估计示意图**

Fig.2　Schematic diagram of state estimation after attack

由图2可看出，当发生攻击后，GSE接收到篡改后的数据$(s',z')$并进行状态估计，残差检测基于状态估计结果进行数据一致性检验，若测量数据和估计结果不一致，则GSE会报警。当然系统允许一定的误报率，如果攻击被检测的概率不大于系统所允许的误报率，则此类攻击无法被检测到。为此给出如下定义。

定义1：如果攻击被检测的概率不大于系统的误报率，则将$g$篡改为$g'$的攻击$\boldsymbol{a}$不可检测。

在无噪声的情况下，攻击不可检测问题可视为一个确定性问题。此时若对于每个测量值$z$都存在相应的状态向量$\boldsymbol{x}'$使$z+\boldsymbol{\Gamma a}=h(\boldsymbol{x}',g)$，则$(s',z+\boldsymbol{\Gamma a})$

将拓扑从$g$篡改为$g'$是不可检测的。

相比于非线性模型，直流模型下攻击不可检测条件可通过一个简单的代数形式给出。对于直流模型式(2)，当发生攻击后，GSE接收到攻击后的测量数据$(s',z')$，对应的拓扑状态信息$s'$的测量矩阵可表示为$\boldsymbol{H}'$。在不考虑噪声的情况下，TEP检测等同于检测接收到的传感器数据是否在测量矩阵的列空间中。因此，不可检测攻击可由下述定义表示。

定义2：如果攻击向量$\boldsymbol{a}$满足式(15)，则将$g$篡改为$g'$的攻击可以躲避TEP检测。

$$z+\boldsymbol{\Gamma a}\in C_{\mathrm{col}}(\boldsymbol{H}')\quad \forall z\in C_{\mathrm{col}}(\boldsymbol{H}) \tag{15}$$

式中：$C_{\mathrm{col}}(\boldsymbol{H})$、$C_{\mathrm{col}}(\boldsymbol{H}')$分别为$\boldsymbol{H}$、$\boldsymbol{H}'$的列空间。

根据式(8)和式(14)中的模拟数据$z'=z+\boldsymbol{\Gamma a}$，可以得到攻击后状态估计的残差$\boldsymbol{r}_a$为：

$$\begin{aligned}\boldsymbol{r}_a&=z'-\hat{z}'=z+\boldsymbol{\Gamma a}-\boldsymbol{K}_a(z+\boldsymbol{\Gamma a})=\\&z-\boldsymbol{K}z+\boldsymbol{K}z-\boldsymbol{K}_a z+\boldsymbol{\Gamma a}-\boldsymbol{K}_a\boldsymbol{\Gamma a}=\\&\boldsymbol{r}+(\boldsymbol{K}-\boldsymbol{K}_a)z+(\boldsymbol{I}-\boldsymbol{K}_a)\boldsymbol{\Gamma a}\end{aligned} \tag{16}$$

式中：$\boldsymbol{K}_a=\hat{\boldsymbol{H}}'(\hat{\boldsymbol{H}}'^{\mathrm{T}}\hat{\boldsymbol{H}}')^{-1}\hat{\boldsymbol{H}}'^{\mathrm{T}}$，$\hat{\boldsymbol{H}}'$为攻击后的$\boldsymbol{H}'$。

根据式(16)，$\left\|(\boldsymbol{K}_a-\boldsymbol{K})z+(\boldsymbol{I}-\boldsymbol{K}_a)\boldsymbol{\Gamma}\right\|_2$越小，则残差检测将越难检测到攻击。给出以下$\delta$隐蔽攻击的定义。

定义3：若$\boldsymbol{a}$满足$\left\|(\boldsymbol{K}_a-\boldsymbol{K})z+(\boldsymbol{I}-\boldsymbol{K}_a)\boldsymbol{\Gamma}\right\|_2<\delta$，则将该攻击称为$\delta$隐蔽攻击。

### 2.2 攻击方案

本节首先给出一个将$g$篡改为$g'$且躲避TEP检测的充要条件。

引理1：在可行攻击向量空间$\boldsymbol{\Gamma}$的子空间中存在TEP无法检测的攻击的充要条件为$C_{\mathrm{col}}(\boldsymbol{H})\subset C_{\mathrm{col}}(\boldsymbol{H}',\boldsymbol{\Gamma})$[5]，$C_{\mathrm{col}}(\boldsymbol{H}',\boldsymbol{\Gamma})$为以$\boldsymbol{H}'$与$\boldsymbol{\Gamma}$为基组成的矩阵空间。

引理1考虑的是无噪声情况，文献[5]也证明了在有噪声的情况下引理1仍成立。

在正常情况下，实时阶段的估计发电量应与日前阶段的最优调度相匹配，根据式(7)，对于发电机节点$i$有：

$$\begin{aligned}\hat{P}'_{\mathrm{g},i}-P^*_{\mathrm{g},i}&=\boldsymbol{K}_{a,i}(z+\boldsymbol{\Gamma a})-\boldsymbol{K}_i z=\\&\boldsymbol{K}_{a,i}z+\boldsymbol{K}_{a,i}\boldsymbol{\Gamma a}-\boldsymbol{K}_i z=\\&(\boldsymbol{K}_{a,i}-\boldsymbol{K}_i)z+\boldsymbol{K}_{a,i}\boldsymbol{\Gamma a}\end{aligned} \tag{17}$$

式中：$\boldsymbol{K}_i$为矩阵$\boldsymbol{K}$中对应于发电机节点$i$的行向量；$\boldsymbol{K}_{a,i}$为拓扑篡改后矩阵$\boldsymbol{K}_a$中对应于发电机节点$i$的行向量；$\hat{P}'_{\mathrm{g},i}$为攻击后发电机节点$i$的注入功率估计值，是攻击后$\hat{z}'$的一部分。

因此，攻击者希望从发电机中获取收益。根据1.4节以及式(17)，可得攻击向量总收益$\rho$为：

$$\rho=\sum_{i=1}^{I}\lambda_i(\hat{P}'_{\mathrm{g},i}-P^*_{\mathrm{g},i})=\sum_{i=1}^{I}\lambda_i[(\boldsymbol{K}_{a,i}-\boldsymbol{K}_i)z+\boldsymbol{K}_{a,i}\boldsymbol{\Gamma a}] \tag{18}$$

根据2.1节的定义1—3和式(18)，针对实时电力市场的基于拓扑篡改的FDIA问题攻击策略可以描述为如下凸优化问题：

$$\begin{cases}\max\limits_{\boldsymbol{a},s}\ \sum\limits_{i=1}^{I}\lambda_i[(\boldsymbol{K}_{a,i}-\boldsymbol{K}_i)z+\boldsymbol{K}_{a,i}\boldsymbol{\Gamma a}]\\ \text{s.t.}\ \ \left\|(\boldsymbol{K}_a-\boldsymbol{K})z+(\boldsymbol{I}-\boldsymbol{K}_a)\boldsymbol{\Gamma a}\right\|_2<\delta\\ \quad C_{\mathrm{col}}(\boldsymbol{H})\subset C_{\mathrm{col}}(\boldsymbol{H}',\boldsymbol{\Gamma})\end{cases} \tag{19}$$

由式(19)易知，目标函数、约束条件均为凸，上述优化问题是一个凸优化问题，KKT条件是求解其最优解的充分必要条件。攻击策略的目标函数是连续的，且$\boldsymbol{a}$的可行域是非空的，因此优化问题存在最优解。凸性规划问题目前有很多种求解算法，如拉格朗日乘子法、对偶内点法、遗传算法等。本文采用MATLAB中的Global Optimization Toolbox进行求解。

从式(17)—(19)中可看出，本文所提基于拓扑篡改的FDIA方案使测量矩阵$\boldsymbol{H}'$、$\boldsymbol{K}_{a,i}$分别发生变化，这会影响发电收益；式(19)中不等式约束保证了残差隐蔽及能躲避TEP检测，这确保了攻击不被检测。

## 3 仿真结果

以标准IEEE 9节点与14节点系统为例，基于MATLAB平台中的MATPOWER以及Global Optimization Toolbox求解器进行仿真，分析基于拓扑篡改的FDIA对电力市场的影响。

IEEE 9节点系统的拓扑结构见附录A图A1，其由3台发电机、9个节点、9条支路组成。假设在网络中部署9个断路器收集所有线路的数字信息，在每条线路上部署9台传感器测量线路潮流，并在9个节点处部署传感器测量节点注入功率。系统中共有18台传感器。所有参数均使用MATPOWER中标准IEEE 9节点系统的默认值，且不考虑阻塞情况。

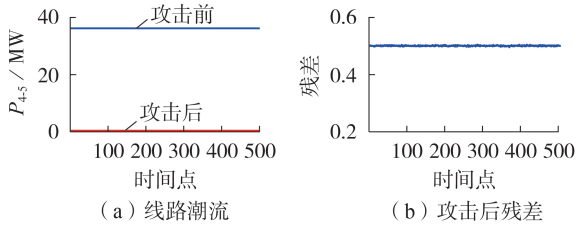
假设攻击者篡改线路4-5的拓扑数据使线路4-5断开，即拓扑篡改的目标线路为4-5。这使得$\boldsymbol{H}'$中与线路4-5、节点4、节点5相关的元素与$\boldsymbol{H}$不一致，其他元素都不变。当$\boldsymbol{\Gamma}$中与线路4-5相关的列元素不为0时，则满足引理1。为了全面验证本文所提方案，考虑不同数量的传感器遭受FDIA。为了在保持隐蔽性的同时保证收益的最大化，根据攻击策略式(19)求解攻击向量如表1所示。

**表1 不同数量传感器被攻击时的攻击向量**

Table 1 Attack vectors with different numbers of sensors under attack

| 遭攻击传感器数量/台 | 攻击向量 |
|---|---|
| 12 | [98,-355,-5,0.435,-5,0.4,4,-4,0.4,3,-3,98,61,-40] |
| 14 | [93,-35,-64,577,7,-7,50,-42,42,93,50,57,98] |
| 16 | [98,-35,-20,9920,99,-2,-73,98,-27,27,97,98,97,92,-56,77,-74] |

线路4-5在不同时间点遭攻击前、后线路潮流$P_{4\text{-}5}$见图3(a)。从图中可看出，攻击后线路4-5无潮流通过，这表明拓扑篡改起到了攻击效果。16台传感器遭攻击后的残差见图3(b)，12、14台传感器遭攻击后的残差结果与图3(b)类似，限于篇幅不再赘述。从图3(b)中可看出，遭攻击后的残差小于报警值0.6。IEEE 9节点系统遭攻击后的最大收益见图4。由图可知，遭攻击的传感器越多，系统收益越大。上述结果表明本文所提攻击方案在成功实现盈利的同时保持了隐蔽性。




（a）线路潮流　　（b）攻击后残差

**图3　IEEE 9节点系统遭攻击前、后的仿真效果**

Fig.3　Simulative results of IEEE 9-bus system before and after attack

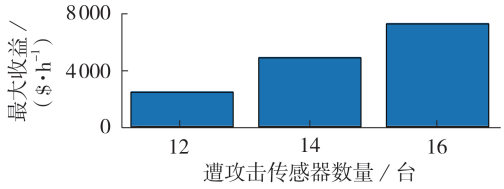



**图4　IEEE 9节点系统遭攻击后的最大收益**

Fig.4　Maximum benefit of IEEE 9-bus system after attack

IEEE 14节点系统的拓扑结构见附录A图A2，其包括5台发电机、14个节点、20条支路。假设系统通过20个断路器测量所有线路上的数字信息，安装34台传感器测量线路潮流以及节点注入功率，且设置如下2种攻击情景。

Case 1：攻击者篡改线路4-5的拓扑数据使线路4-5断开，且考虑不同数量的传感器遭受攻击。

Case 2：攻击者篡改线路3-4、4-5、6-12的拓扑数据，使这3条线路断开，且考虑不同数量的传感器遭受攻击。

攻击策略与IEEE 9节点系统相同，Case 1的幅值结果见附录A图A3、A4。图A3(a)为线路4-5遭攻击前、后线路潮流$P_{4\text{-}5}$结果，可见基于拓扑的攻击成功使线路断开；图A3(b)为遭攻击后的残差，可见残差始终在阈值0.6之内；图A4为攻击不同数量传感器时的系统最大收益，可见攻击的传感器越多，收益越大。上述结果表明本文所提攻击方案可以在保持盈利的同时保证隐蔽性。

为了突出本文攻击方案的效果，将Case 2与文献[13]中无拓扑篡改的针对模拟量量测的FDIA进行对比，Case 2的残差以及线路潮流仿真结果均与上述算例相同，限于篇幅不再赘述。

本文攻击方案Case 2与现有攻击方案[13]的最大收益对比见图5。由图可知，本文攻击方案的收益更大。现有攻击方案并未考虑躲避TEP检测，这意味着一旦存在拓扑篡改情况，则无法满足TEP隐蔽条件$C_{\text{col}}(\boldsymbol{H})\subset C_{\text{col}}(\boldsymbol{H}',\boldsymbol{\Gamma})$。TEP检测值见图6。由图可知，现有攻击方案躲避不了TEP检测，这意味着本文攻击方案更隐蔽。综合图5和图6可知，与现有无拓扑篡改的攻击方案相比，本文所提攻击方案更隐蔽且盈利更多。

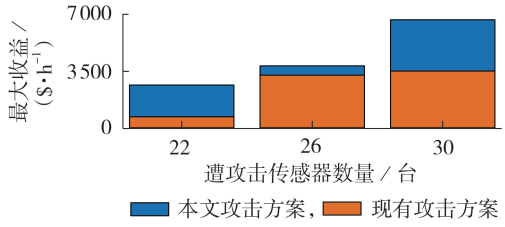



**图5　本文攻击方案与现有攻击方案的最大收益对比**

Fig.5　Comparison of maximum benefit between proposed attack scheme and existing attack scheme

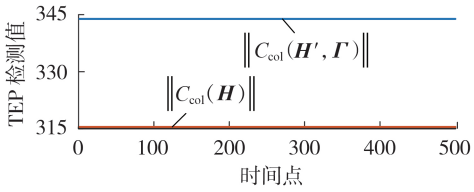



**图6　TEP检测值**

Fig.6　TEP detection values

## 4　结论

本文提出了一种基于拓扑篡改的电力市场FDIA方案。通过篡改传感器离散的开关量数据以及连续的模拟量数据，给出了可以躲避监控中心TEP检测的充分必要条件以及躲避残差检测的定义，基于此通过分析发电机节点的最大化收益以及隐蔽条件将攻击策略描述为一类易于求解的凸规划问题。研究结果表明：基于拓扑篡改的FDIA更难防范，监控中心不仅需要防范常见的针对传输模拟数据传感器的攻击，还需重点防范针对传输离散量的传感器的攻击，可通过增加冗余传感器以提高系统的安全性。在非线性状态估计框架下研究不同的拓扑结构篡改方式对电力市场的影响将是未来的研究方向。

附录见本刊网络版(http://www.epae.cn)。

**参考文献：**

[1] 阳育德，蓝水岚，覃智君，等. 电力信息物理融合系统的网络-物理协同攻击[J]. 电力自动化设备，2020，40(2)：97-103.
YANG Yude，LAN Shuilan，QIN Zhijun，et al. Coordinated cyber-physical attacks of cyber-physical power system[J]. Electric

Power Automation Equipment,2020,40(2):97-103.
[2] 陈柯任,文福拴,赵俊华,等. 考虑物理-信息虚拟连接的电力信息物理融合系统的脆弱性评估[J]. 电力自动化设备,2017,37(12):67-72,79.
CHEN Keren,WEN Fushuan,ZHAO Junhua,et al. Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections[J]. Electric Power Automation Equipment,2017,37(12):67-72,79.
[3] 刘东,盛万兴,王云,等. 电网信息物理系统的关键技术及其进展[J]. 中国电机工程学报,2015,35(14):3522-3531.
LIU Dong,SHENG Wanxing,WANG Yun,et al. Key technologies and trends of cyber physical system for power grid[J]. Proceedings of the CSEE,2015,35(14):3522-3531.
[4] 娄素华,吕梦璇,王永灿,等. 考虑投资风险的含风电系统电源投资扩展规划研究[J]. 中国电机工程学报,2019,39(7):1944-1955.
LOU Suhua,LÜ Mengxuan,WANG Yongcan,et al. Generation investment expansion planning for wind power accommodation considering investment risk[J]. Proceedings of the CSEE,2019,39(7):1944-1955.
[5] KIM J,TONG L. On topology attack of a smart grid:undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications,2013,31(7):1294-1305.
[6] ZHOU Y Q,CISNEROS-SALDANA J,XIE L. False analog data injection attack towards topology errors:formulation and feasibility analysis[C]//2018 IEEE Power & Energy Society General Meeting(PESGM). Portland,OR,USA:IEEE,2018:1-5.
[7] CHE L,LIU X,LI Z,et al. False data injection attacks induced sequential outages in power systems[J]. IEEE Transactions on Power Systems,2019,34(2):1513-1523.
[8] 田继伟,王布宏,尚福特,等. 基于数据驱动的稀疏虚假数据注入攻击[J]. 电力自动化设备,2017,37(12):52-59.
TIAN Jiwei,WANG Buhong,SHANG Fute,et al. Sparse false data injection attacks based on data driven[J]. Electric Power Automation Equipment,2017,37(12):52-59.
[9] XIE L,MO Y L,SINOPOLI B. Integrity data attacks in power market operations[J]. IEEE Transactions on Smart Grid,2011,2(4):659-666.
[10] KOSUT O,JIA L Y,THOMAS R J,et al. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid,2011,2(4):645-658.
[11] JIA L Y,KIM J,THOMAS R J,et al. Impact of data quality on real-time locational marginal price[J]. IEEE Transactions on Power Systems,2014,29(2):627-636.
[12] MOSLEMI R,MESBAHI A,VELNI J M. Design of robust profitable false data injection attacks in multi-settlement electricity markets[J]. IET Generation,Transmission & Distribution,2018,12(6):1263-1270.
[13] TAN S,SONG W Z,STEWART M,et al. Online data integrity attacks against real-time electrical market in smart grid[J]. IEEE Transactions on Smart Grid,2018,9(1):313-322.
[14] CHOI D H,XIE L. Impact of power system network topology errors on real-time locational marginal price[J]. Journal of Modern Power Systems & Clean Energy,2017,5(5):797-809.
[15] LIANG G Q,WELLER S R,ZHAO J H,et al. A framework for cyber-topology attacks:line-switching and new attack scenarios[J]. IEEE Transactions on Smart Grid,2019,10(2):1704-1712.
[16] LIANG G Q,WELLER S R,LUO F J,et al. Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism[J]. IEEE Transactions on Smart Grid,2018,9(4):3820-3829.
[17] 张殷,肖先勇,李长松. 基于攻击者视角的电力信息物理融合系统脆弱性分析[J]. 电力自动化设备,2018,38(10):81-88.
ZHANG Yin,XIAO Xianyong,LI Changsong. Vulnerability analysis of cyber physical power system from attacker's perspective[J]. Electric Power Automation Equipment,2018,38(10):81-88.

**作者简介:**

王胜锋

王胜锋(1979—),男,江苏海安人,讲师,硕士,主要研究方向为故障诊断与容错控制及其在电力系统中的应用(**E-mail**:wangsf@ntu.edu.cn);

丁 洲(1994—),男,江苏南通人,硕士,研究方向为智能电网网络攻击与网络安全(**E-mail**:ntudz17@163.com);

邱爱兵(1982—),男,江苏海安人,教授,博士,通信作者,研究方向为故障诊断与容错控制及其在智能建筑和电网中的应用(**E-mail**:aibqiu@ntu.edu.cn)。

(编辑 陆丹)

## False data injection attack scheme of electricity market based on topology tampering

WANG Shengfeng,DING Zhou,WU Jingsong,QIU Aibing

(School of Electrical Engineering,Nantong University,Nantong 226019,China)

**Abstract**:From the attacker's point of view,a FDIA(False Data Injection Attack) scheme based on topology tampering is proposed under the framework of DC state estimation. Firstly,by analyzing the consistency between the topology structure calculated by the network topology processor after the attack and measured by the sensor,and comparing the residuals before and after the attack,the definition of stealthy attack which can avoid the topology error processing detection and residual detection is given. Then,based on the above definition and the concealment condition of the attack vector column space,a FDIA scheme is proposed to achieve the maximum generation benefits while ensuring concealment by solving the convex programming problem. Finally,the effectiveness of the proposed scheme is verified based on standard IEEE 9-bus and 14-bus systems. The results show that,compared with the existing FDIA schemes,the proposed attack scheme combining topology tampering with FDIA is more concealable and more profitable.

**Key words**:false data injection attack;network topology;topology tampering;electricity market;state estimation

# 附录 A

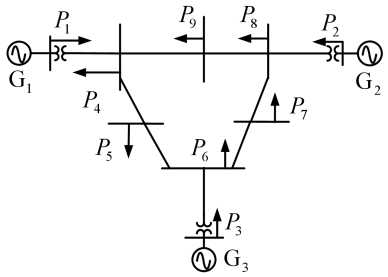



图 A1 IEEE 9 节点系统拓扑结构
Fig.A1 Topology structure of IEEE 9-bus system

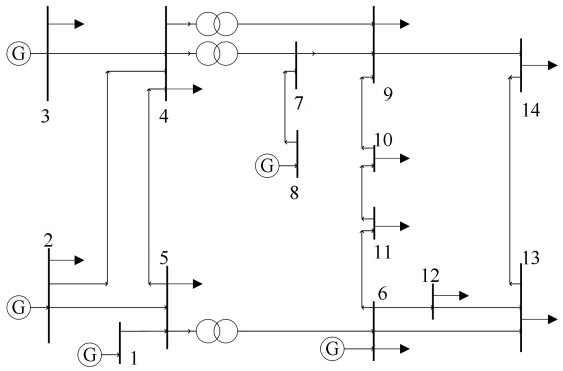



图 A2 IEEE 14 节点系统拓扑结构
Fig.A2 Topology structure of IEEE 14-bus system

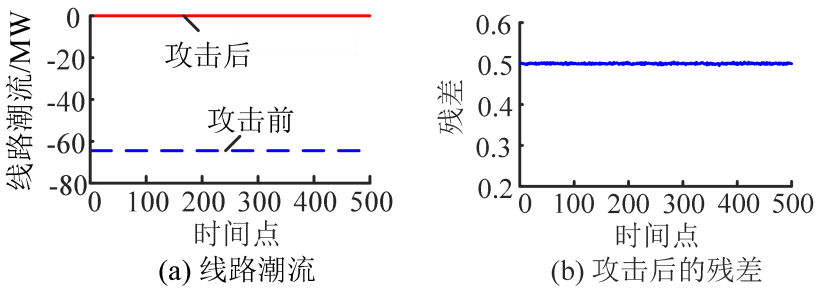



图 A3 IEEE 14 节点系统攻击前、后的仿真结果
Fig.A3 Simulative results of IEEE 14-bus system before and after attack

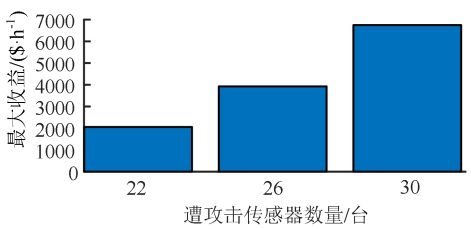



图 A4 攻击后 IEEE 14 节点系统的最大收益
Fig.A4 Maximum benefit of IEEE 14-bus system after attack