**Smart Grid** 智能电网, 2017, 7(3), 153-160
Published Online June 2017 in Hans. http://www.hanspub.org/journal/sg
https://doi.org/10.12677/sg.2017.73017

Hans汉斯

# Model Building and Analysis of Minimal False-Data Attack Vector Launched on Power System

**Jiaqi Ruan[1], Jianchun Peng[1], Huaizhi Wang[1], Hui Jiang[2]**

[1]College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen Guangdong
[2]College of Optoelectronic Engineering, Shenzhen University, Shenzhen Guangdong
Email: jcpeng@szu.edu.cn

Received: May 20th, 2017; accepted: Jun. 4th, 2017; published: Jun. 7th, 2017

## Abstract

**A model for building minimal false-data attack vector launched on power systems is proposed in this paper. It is based on a local looped sub-network. The model's objective function is minimizing the changes in bus injection powers. The model's constraints include that the values of border state variables remain unchanged; a line congestion occurs and bus power balance equations. It is thus an optimization problem. Adding the attack vector produced by this model to actual measurements from the local looped sub-network gives a false-data attack to the power system. In this way, all bus power balance equations are still satisfied for the whole grid. As a result, the false-data attack naturally avoids the check from power system state estimation software. The false line congestion will lead the security correction system to action that will place the power system on a true not secure state, achieving the aim of an attack. Simulation results show that the attack vector produced by the proposed model is not only effective but easy to achieve.**

## Keywords

**Smart Grid, False-Data Attack, Attack Vector, State Estimation, SCADA**

# 电力系统最小虚假数据攻击向量的建模与分析

**阮嘉祺[1]，彭建春[1]，王怀智[1]，江　辉[2]**

[1]深圳大学机电与控制工程学院，广东　深圳
[2]深圳大学光电工程学院，广东　深圳
Email: jcpeng@szu.edu.cn

收稿日期：2017年5月20日；录用日期：2017年6月4日；发布日期：2017年6月7日

文章引用: 阮嘉祺, 彭建春, 王怀智, 江辉. 电力系统最小虚假数据攻击向量的建模与分析[J]. 智能电网, 2017, 7(3): 153-160. https://doi.org/10.12677/sg.2017.73017

## 摘　要

**本文提出了一种电力系统最小虚假数据攻击向量的建模方法。这种方法以被攻击电网的局部子环网为对象，以其节点注入功率的改变量最小为目标函数，以边界节点状态量不变和出现线路阻塞以及节点功率平衡为约束条件，建立虚假数据攻击向量的数学模型。用这种方法得到的攻击向量篡改局部电网检测数据后，全电网仍然满足节点功率平衡约束、自然躲过传统状态估计的检测，且虚假线路阻塞经过安全校正系统的调节会使电网陷入真正不安全状态，从而达到攻击目的。仿真结果表明，本文方法生成的攻击向量不仅有效、而且易于获取。**

## 关键词

**智能电网，虚假数据攻击，攻击向量，状态估计，监测控制与数据获取**



## 1. 引言

由线路和变压器等构成的电力网是连接发电机和负荷用户的桥梁，其安全性和可靠性是直接影响电源连续供电和用户连续用电的关键因素。

为确保电力网安全可靠运行，布置在电力网各处的测量仪表需要对注入节点的有功功率和无功功率大小、线路传输的有功功率和无功功率大小等重要数据进行连续不断检测。它们通过 SCADA 系统传送至电网控制中心，再通过状态估计系统剔除不良数据才能得到可信的电力网运行状态数据(如节点电压幅值和相位) [1] [2] [3]。基于这些可信的运行状态数据，控制中心才能实施最优潮流分析、经济调度决策、安全校正控制等[4]，确保整个电力系统安全可靠运行。

黑客通过篡改检测数据攻击电网的目的，轻则使电网控制中心得到虚假数据而从中获利(如篡改关口表有功功率大小)，重则使电网控制中心收到虚假的阻塞信息、使安全校正系统自动响应、导致系统陷入真实的阻塞状况或更严重的停电事故[5]。如 2015 年 12 月 23 日乌克兰发生大规模的停电事故，被认为是第一起网络攻击直接导致停电事故的案例[6]。由于电网控制中心的状态估计系统对不良数据有过滤作用，一般随机性不良数据都无法躲过该系统的过滤作用[7] [8]。因此，黑客通过篡改检测数据发起的攻击能否成功，关键是这些虚假数据能否躲过状态估计系统的过滤。

Liu Y.等人在 2009 年提出了电力系统状态估计欺诈性数据的概念[9]，即攻击者可以通过检测方法的漏洞，蓄意改变状态估计结果，使电力系统无法安全可靠的运行。2011 年 Yuan Y.等人提出了负荷再分配的攻击模型[10]，随后 Qin Z.等人在 2012 年提出了无法被辨识的攻击的概念[11]，并构建了该方法的攻击模型。为躲过状态估计系统对虚假不良数据的过滤作用，通常攻击向量的建模要在全电网结构和参数已知的条件下进行，这增大了攻击向量建模的难度[5]。实际上，基于全电网结构和参数的建模方法，使模型呈现为含 0 或 1 范数的大规模复杂问题、难以求解[12]。因此，研究信息量需求小且易于求解的攻击向量建模方法，是降低发起虚假数据攻击代价的关键。

本文提出了一种电力系统最小虚假数据攻击向量的建模方法。这种方法以被攻击电网的局部子网为

对象建模，需要的信息量很小。本文模型中通过引入虚假数据攻击导致线路输电阻塞的约束，使电网控制中心的安全校正系统产生响应，达到严重影响电网安全可靠运行的目的。这种攻击向量模型以满足节点功率平衡方程约束为条件，巧妙躲过电网控制中心状态估计系统的过滤作用，因此是一种小代价、高效能的攻击向量模型。

## 2. 攻击向量和虚假数据

针对直流潮流的情况，用 $\boldsymbol{z}$ 表示 SCADA 系统采集的电力系统量测量(包括节点注入有功功率和线路有功功率、是 $m$ 维列向量)，用 $\boldsymbol{x}$ 和 $\hat{\boldsymbol{x}}$ 分别表示系统的状态量及其状态估计值(节点电压幅值和相位、是 $n$ 维列向量)，用 $\boldsymbol{H}\hat{\boldsymbol{x}}$ 表示直流潮流下量测量的估计值( $\boldsymbol{H}$ 是直流潮流下量测量方程组的雅可比矩阵)，用 $\boldsymbol{e}$ 表示测量误差向量。则有量测量方程：

$$\boldsymbol{z}=\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{e} \tag{1}$$

定义残差 $\boldsymbol{r}$ 为

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}\right) \tag{2}$$

式(2)中 $\boldsymbol{h}\left(\hat{\boldsymbol{x}}\right)$ 表示直流潮流下量测量方程组，电力系统状态估计就是找出使 $\left\|\boldsymbol{r}\right\|_2$ 最小的 $\boldsymbol{x}$ 的估计值 $\hat{\boldsymbol{x}}$。这运用最小二乘解即可求得。

正常情况下，残差 $\boldsymbol{r}$ 由测量噪声引起且非常小，它远远小于统计学卡方分布的允许误差门坎值 $\chi^2_{k,\alpha}$ (其中 $k=m-n$ 是自由度、$\alpha$ 是显著性水平如 0.05)，这是量测量未受不良数据侵扰的标志。若构造一个与 $\boldsymbol{z}$ 同维的向量 $\boldsymbol{a}$、让量测量由 $\boldsymbol{z}$ 变成 $\boldsymbol{z}+\boldsymbol{a}$、且仍然使残差 $\boldsymbol{r}$ 小于统计学卡方分布的允许误差门坎值 $\chi^2_{k,\alpha}$ (即躲过状态估计系统的过滤作用)，则是一个成功的虚假数据攻击。称 $\boldsymbol{a}$ 为攻击向量、$\boldsymbol{z}+\boldsymbol{a}$ 为虚假量测量或虚假数据。因此，发起一个虚假数据攻击的关键，在于构建一个能够躲过状态估计系统过滤作用的攻击向量 $\boldsymbol{a}$。上述分析虽基于直流潮流(为简明)，但也适用交流潮流的情况。若添加攻击向量 $\boldsymbol{a}$ 的虚假数据 $\boldsymbol{z}+\boldsymbol{a}$ 对应的最小二乘解残差 $\boldsymbol{r}_a$ 与不添加 $\boldsymbol{a}$ 时的最小二乘解残差 $\boldsymbol{r}$ 相等，则称虚假数据 $\boldsymbol{z}+\boldsymbol{a}$ 为完美欺诈性数据[3]。

## 3. 最小虚假数据攻击向量的建模

生成一个攻击向量必须基于电网的拓扑结构和参数。对黑客而言，掌握电网某个局部的拓扑结构和参数比掌握其全部信息要容易得多、简单得多。为此，下面以受攻击电网的一个局部子环网为对象来分析。

将受攻击的电力网划分成局部子环网(有 $n$ 个节点)和外网两个部分，如图 1 所示。外网中两者的边界节点编号为 $j_1, j_2, \cdots, j_n$。局部子环网中节点的编号为 $h_1, h_2, \cdots, h_m$，其中局部子环网的节点数大于边界节点数( $m>n$ )。若改变局部子环网中各节点注入功率的分布、如叠加一个攻击向量 $\boldsymbol{a}$，同时确保这些边界节点的电压和局部子环网注入外网的功率不变(由局部子环网的环形结构保障)、确保局部子网的节点注入功率满足电路规律，则 $\boldsymbol{z}+\boldsymbol{a}$ 就是一个有效的虚假数据攻击。

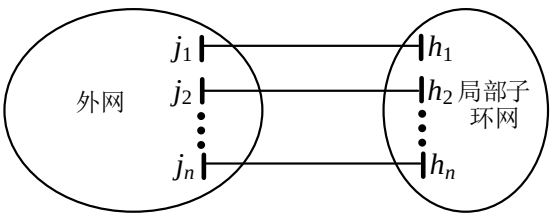


**Figure 1.** Local sub-network and external network
**图 1.** 局部子环网和外网

按上述思路，可构建出如下的攻击向量模型：

$$\min f = \sum_{h\in\Omega_s}\Delta P_h^2 \tag{3}$$

$$\text{s.t. } P_{i0}+\Delta P_i = V_i\sum_{j=1}^{n}V_j\begin{pmatrix}G_{ij}\cos\theta_{ij}\\+B_{ij}\sin\theta_{ij}\end{pmatrix} \tag{4}$$

$$Q_{i0}+\Delta Q_i = V_i\sum_{j=1}^{n}V_j\begin{pmatrix}G_{ij}\sin\theta_{ij}\\-B_{ij}\cos\theta_{ij}\end{pmatrix} \tag{5}$$

$$P_{ll'} \geq P_{ll'}^{\bar{U}} \tag{6}$$

$$V_h^{\bar{L}} \leq V_h \leq V_h^{\bar{U}} \tag{7}$$

$$P_h^{\bar{L}} \leq P_{h0}+\Delta P_h \leq P_h^{\bar{U}} \tag{8}$$

$$Q_h^{\bar{L}} \leq Q_{h0}+\Delta Q_h \leq Q_h^{\bar{U}} \tag{9}$$

$$-\tau P_h \leq \Delta P_h \leq \tau P_h \tag{10}$$

$$V_j = V_{j0} \tag{11}$$

$$\theta_j = \theta_{j0} \tag{12}$$

$$\Delta P_j = 0 \tag{13}$$

$$\Delta Q_j = 0 \tag{14}$$

$$i\in\Omega, h\in\Omega_S, j\in\Omega_E$$

其中：$ll'$ 是虚假数据攻击欲达到的输电阻塞线路、$l$ 和 $l'$ 是它的两个节点编号，通常取局部子环网中容易发生阻塞的一条线路。$\Omega_S=\{h_1,h_2,\cdots,h_m\}$ 是局部子环网的节点编号集合，$\Omega_E=\{j_1,j_2,\cdots,j_n\}$ 是外网中边界节点编号的集合，$\Omega=\Omega_S\bigcup\Omega_E$。上标 $\bar{L}$ 和 $\bar{U}$ 分别表示变量的下界和上界。$G_{ij}$ 和 $B_{ij}$ 分别是局部子环网与外网边界节点构成的电网的节点导纳矩阵中元素的实部和虚部。下标 0 表示实际测量值。

式(3)是目标函数，即最小化局部子环网节点注入功率增量的平方和、使攻击向量的模长尽可能小。式(4)和(5)是节点功率平衡约束。式(6)是线路阻塞约束，引入它、使虚假数据攻击达到使安全校正系统自动响应、导致系统陷入真实的阻塞状况或更严重的停电事故。式(7)~(10)是局部子环网变量的上限和下限约束，$\tau$ 是给定的局部子环网节点注入功率增量的允许百分数(如 10%，参照当前真实负荷和各节点可能出现的最大负荷确定)。式(11)~(14)是外网中边界节点变量的约束，是使外网边界节点的电压和注入功率保持不变、从而使外网节点功率平衡方程仍然成立。

求解上述模型，得到的局部子环网内电表测量值增量 $\boldsymbol{a}=\left[\Delta P_{x_i},\cdots,\Delta Q_{x_i},\cdots,\Delta P_{x_{i-j}},\cdots,\Delta Q_{x_{i-j}},\cdots\right]^{\mathrm{T}}$ 就是攻击向量，其中 $\Delta P_{x_i}$、$\Delta Q_{x_i}$ 是局部子环网内节点注入功率的增量，$\Delta P_{x_{i-j}}$、$\Delta Q_{x_{i-j}}$ 是局部子环网内线路潮流的增量。将它在 SCADA 系统中叠加到测量数据 $\boldsymbol{z}=\left[P_{x_i},\cdots,Q_{x_i},\cdots,P_{x_{i-j}},\cdots,Q_{x_{i-j}},\cdots\right]^{\mathrm{T}}$ 上、并送到电网控制中心，就成功地发射了一次虚假数据攻击。因为，该攻击向量的构造确保将它叠加到原有检测值上后仍然使电网各节点满足功率平衡约束、成功躲过状态估计软件的过滤作用。

## 4. 仿真与分析

为了验证上述模型的可行性，采用 IEEE 14 节点系统和 IEEE 30 节点系统构建攻击向量并进行仿真与分析，通过鲁棒状态估计方法对该攻击模型作状态估计和残差检验[13]。

① 对图 2 所示 IEEE 14 节点系统，其结构和运行参数取自文献[14]。取图 3 所示节点 1 至 5 的局部子环网建立数学模型，并将由文献[15]给定参数决定的其运行状态参数作为 SCADA 系统的测量数据。表 1 和表 2 给出了仿真计算结果。

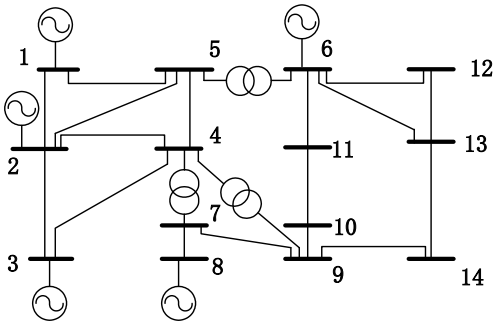


**Figure 2.** IEEE 14-bus system
**图 2.** IEEE 14 节点系统

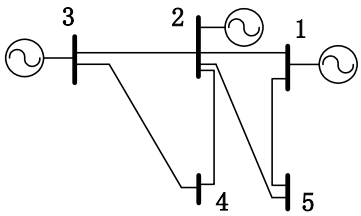


**Figure 3.** Local sub-network 1
**图 3.** 局部子环网一

**Table 1.** Attack vector at different line congestion
**表 1.** 设置不同线路阻塞时的攻击向量

| 阻塞线路 | 攻击向量 $\boldsymbol{a}$ | 模长 |
|---|---|---|
| 1-2 | [0.0020 −0.2029 0.0084 −0.0073 −0.0059 −0.4874 0.1329 −0.0723] | **0.5493** |
| 1-5 | [0.1754 −0.3164 0.4636 −0.1284 0.0538 −0.6680 0.1775 −0.1124] | 0.9249 |
| 2-3 | [−0.0958 −0.1971 −0.2471 0.0601 −0.0419 −0.5242 0.1498 −0.0714] | 0.6456 |
| 2-5 | [−0.0776 −0.2056 −0.1992 0.0473 −0.0354 −0.5353 0.1516 −0.0743] | 0.6376 |
| 3-4 | [−0.0541 −0.1858 −0.1383 0.0316 −0.0261 −0.4756 0.1331 −0.0668] | 0.5537 |

**Table 2.** Comparison of residual before and after attack
**表 2.** 攻击前后残差的对比

| 阻塞线路 | 攻击前残差 $\boldsymbol{r}$ | 攻击后残差 $\boldsymbol{r}_a$ |
|---|---|---|
| 1-2 | 0.26316 | 0.26878 |
| 1-5 | 0.26316 | 0.27682 |
| 2-3 | 0.26316 | 0.26735 |
| 2-5 | 0.26316 | 0.26788 |
| 3-4 | 0.26316 | 0.26748 |
| 攻击后最大残差: | ~ | 0.27682 |

表 1 给出了设置不同线路阻塞时的攻击向量 $\boldsymbol{a}=[\Delta P_3,\Delta Q_3,\Delta P_{1\text{-}2},\Delta P_{2\text{-}3},\Delta P_{4\text{-}2},\Delta Q_{1\text{-}2},\Delta Q_{2\text{-}3},\Delta Q_{4\text{-}2}]$。可见，设置线路 1-2 出现阻塞(加剧攻击效果)建模时，得到的攻击向量模长为 0.5493、最小，由此发起虚假数据攻击将更不易被运行调度人员发觉(因为改变真实测量值的幅度最小)。因此称之为最小虚假数据攻击。此外，本例中攻击者在 14 个节点中只选取 5 个节点的子环网进行攻击。更具体地，对于一共有 32 个量测电表的电网，只需篡改 8 个电表的数据便可实现攻击。因此，这是一种攻击代价小(数据容易获取且攻击向量易于构建)、易于实现的虚假数据攻击。

表 2 给出了表 1 的攻击向量作用下的残差。按统计学理论，此时的自由度 $k=32-27=5$、选择显著性水平为 0.05，查表得到卡方分布的检测门槛值 $\chi^2_{5,0.05}=11.07$。表 2 中攻击前的残差为 0.26316、攻击后的最大残差为 0.27682，都远小于门槛值 $\chi^2_{5,0.05}=11.07$。这表明，按本方模型构建的攻击向量的确能躲过状态估计系统的过滤作用、从而产生有效攻击。同时攻击后的残差与攻击前的残差近似相等，表明发起该攻击的虚假数据属于完美欺诈性数据。

② 对图 4 所示 IEEE 30 节点系统，其结构和运行参数取自文献[14]。取图 5 所示节点 1 至 7 的局部子环网建立数学模型，并将由文献[15]给定参数决定的其运行状态参数作为 SCADA 系统的测量数据。表 3 和表 4 给出了仿真计算结果。

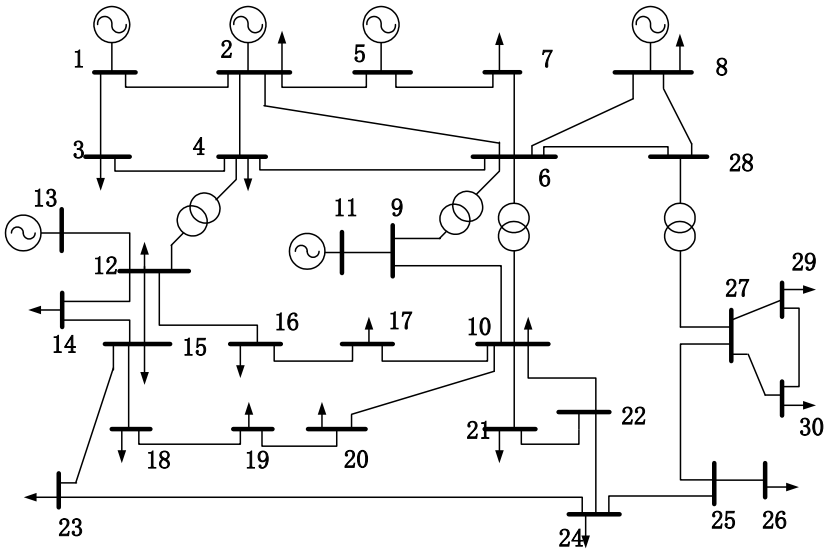


**Figure 4.** IEEE 30-bus system
**图 4.** IEEE 30 节点系统

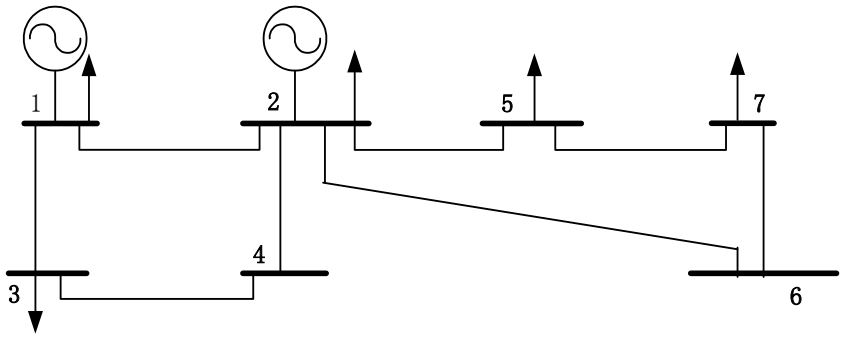


**Figure 5.** Local sub-network 2
**图 5.** 局部子环网二

**Table 3.** Attack vector at different line congestion
**表 3.** 设置不同线路阻塞时的攻击向量

| 阻塞线路 | 攻击向量 $\boldsymbol{a}=[\Delta P_2,\Delta P_3,\Delta Q_2,\Delta Q_3,\Delta P_{1\text{-}3},\Delta P_{2\text{-}4},\Delta P_{2\text{-}5},\Delta P_{2\text{-}6},\Delta P_{3\text{-}4},\Delta P_{5\text{-}7},\Delta Q_{1\text{-}3},\Delta Q_{2\text{-}4},\Delta Q_{2\text{-}5},\Delta Q_{2\text{-}6},\Delta Q_{3\text{-}4},\Delta Q_{5\text{-}7}]$ | | | | | | | | 模长 |
|---|---|---|---|---|---|---|---|---|---|
| 1-2 | [0.0042 | 0.0023 | 0.8784 | 0.1817 | −0.0012 | 0.0017 | −0.0118 | 0.0025 | 0.9302 |
| | −0.0015 | −0.0071 | −0.1993 | 0.0290 | 0.0965 | 0.0281 | −0.0284 | −0.0950] | |
| 1-3 | [0.0067 | 0.0023 | 0.1137 | 0.5898 | 0.0203 | −0.0118 | 0.0027 | −0.0158 | 0.8059 |
| | 0.0122 | 0.0082 | −0.3982 | −0.1492 | −0.2383 | −0.1447 | 0.1513 | 0.0787] | |
| 2-4 | [−1.9775 | 1.6902 | 3.1012 | 0.1683 | −0.9319 | −0.7510 | −0.6072 | −0.7435 | 4.5725 |
| | 0.7794 | −0.5569 | −0.5011 | 0.3425 | −0.0981 | 0.3134 | −0.2607 | 0.8238] | |
| 2-5 | [0.0041 | 0.0032 | −1.2260 | 0.2557 | 0.0153 | −0.0165 | 0.0302 | −0.0213 | 1.3902 |
| | 0.0173 | 0.0246 | −0.0722 | −0.1761 | −0.4050 | −0.1708 | 0.1793 | 0.3157] | |
| 2-6 | [−3.0189 | 2.5687 | 4.1307 | 0.0463 | −1.3916 | −1.1158 | −0.9410 | −1.1071 | 6.4297 |
| | 1.1896 | −0.8653 | −0.3774 | 0.5072 | 0.6258 | 0.4647 | −0.2905 | −0.1273] | |
| 3-4 | [3.5133 | −2.5919 | 0.8965 | 2.8430 | 1.7655 | 1.3489 | 0.8399 | 1.3243 | 6.4053 |
| | −1.1700 | 0.9886 | −0.6492 | −0.3877 | 0.1596 | −0.3379 | 0.9337 | −1.3247] | |
| 5-7 | [0.0002 | 0.0002 | −0.1757 | 0.0583 | 0.0028 | −0.0029 | 0.0043 | −0.0037 | **0.2126** |
| | 0.0027 | 0.0040 | 0.0263 | −0.0314 | −0.0700 | −0.0304 | 0.0310 | 0.0489] | |

**Table 4.** Comparison of residual before and after attack
**表 4.** 攻击前后残差的对比

| 阻塞线路 | 攻击前残差 $\boldsymbol{r}$ | 攻击后残差 $\boldsymbol{r}_a$ |
|---|---|---|
| 1-2 | $1.5382\times10^{-4}$ | $1.0581\times10^{-4}$ |
| 1-3 | $1.5382\times10^{-4}$ | $1.0565\times10^{-4}$ |
| 2-4 | $1.5382\times10^{-4}$ | $1.0440\times10^{-4}$ |
| 2-5 | $1.5382\times10^{-4}$ | $1.0545\times10^{-4}$ |
| 2-6 | $1.5382\times10^{-4}$ | $1.0415\times10^{-4}$ |
| 3-4 | $1.5382\times10^{-4}$ | $1.1116\times10^{-4}$ |
| 5-7 | $1.5382\times10^{-4}$ | $1.0564\times10^{-4}$ |
| 攻击后最大残差: | ~ | $1.1116\times10^{-4}$ |

表 3 给出了设置不同线路阻塞时的攻击向量 $\boldsymbol{a}=[\Delta P_2,\Delta P_3,\Delta Q_2,\Delta Q_3,\Delta P_{1\text{-}3},\Delta P_{2\text{-}4},\Delta P_{2\text{-}5},\Delta P_{2\text{-}6},\Delta P_{3\text{-}4},\Delta P_{5\text{-}7},\Delta Q_{1\text{-}3},\Delta Q_{2\text{-}4},\Delta Q_{2\text{-}5},\Delta Q_{2\text{-}6},\Delta Q_{3\text{-}4},\Delta Q_{5\text{-}7}]$。可见，设置线路 5-7 出现阻塞(加剧攻击效果)建模时，得到的攻击向量模长为 0.2126、最小，由此发起虚假数据攻击将更不易被运行调度人员发觉(因为改变真实测量值的幅度最小)。因此称之为最小虚假数据攻击。而设置线路 2-4、2-5、2-6 阻塞时，模长非常大，因此需要篡改的电表量测值幅度很大，不宜作为攻击向量。此外，本例中攻击者在 30 个节点中只选取 7 个节点的子环网进行攻击。更具体地，对于一共有 78 个量测电表的电网，只需篡改 16 个电表的数据便可实现攻击。因此，这是一种攻击代价小(数据容易获取且攻击向量易于构建)、易于实现的虚假数据攻击。

表 4 给出了表 3 的攻击向量作用下的残差。按统计学理论，此时的自由度 $k=78-59=19$、选择显著性水平为 0.05，查表得到卡方分布的检测门槛值 $\chi^2_{19,0.05}=30.144$。表 2 中攻击前的残差为 $1.5382\times10^{-4}$、攻击后的最大残差为 $1.1116\times10^{-4}$，都远小于门槛值 $\chi^2_{19,0.05}=30.144$。这表明，按本方模型构建的攻击向量的确能躲过状态估计系统的过滤作用、从而产生有效攻击。同时攻击后的最大残差比攻击前小了 27%，表明发起该攻击的虚假数据属于完美欺诈性数据。

## 5. 结论

本文构建攻击向量的方法从受攻击电网的局部子环网出发建模，需要掌握的电网信息量少、易于实现。在本文方法得到的攻击向量作用下，状态估计的残差值远小于卡方分布的允许误差，并且与攻击前的残差值变化不大，因此能有效躲过电力系统状态估计软件的过滤作用，形成有效的虚假数据攻击。模型中通过引入虚假数据攻击导致线路输电阻塞的约束，使电网控制中心的安全校正系统产生响应，达到严重影响电网安全可靠运行的目的。此外，本文方法得到的攻击向量模长小，因此是一种最小虚假数据攻击。这种攻击能躲过传统电力系统状态估计的过滤作用，应对该类攻击的检测手段和方法有待深入研究。

## 基金项目

国家自然科学基金资助(编号 51477104)；深圳市科技研发资金资助(编号 GJHZ20150313093836007)；深圳市战略新兴产业发展专项资金资助(编号 JCYJ20150525092941041)。

## 参考文献 (References)

[1] Schweppe, F.C. and Wildes, J. (1970) Power System Static-State Estimation, Part I: Exact Model. *IEEE Transactions on Power Apparatus & Systems*, **89**, 120-125. https://doi.org/10.1109/TPAS.1970.292678

[2] 于尔铿. 电力系统状态估计[M]. 北京: 水利电力出版社, 1985.

[3] 朱杰, 张葛祥, 王涛, 等. 电力系统状态估计欺诈性数据攻击及防御综述[J]. 电网技术, 2016, 40(8): 2406-2415.

[4] 周京阳, 于尔铿. 能量管理系统(EMS) [J]. 电力系统自动化, 1997(5): 75-78.

[5] Liang, J., Sankar, L. and Kosut, O. (2015) Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation.

[6] 郭庆来, 辛蜀骏, 王剑辉, 等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化, 2016(5): 145-147.

[7] Van Cutsem, T., Ribbens-Pavella, M. and Mili, L. (1985) Bad Data Identification Methods in Power System State Estimation—A Comparative Study. *IEEE Transactions on Power Apparatus & Systems*, **104**, 3037-3049. https://doi.org/10.1109/TPAS.1985.318945

[8] Monticelli, A., Wu, F.F. and Yen, M. (1986) Multiple Bad Data Identification for State Estimation by Combinatorial Optimization. *IEEE Power Engineering Review*, **6**, 73-74. https://doi.org/10.1109/MPER.1986.5527891

[9] Liu, Y., Ning, P. and Reiter, M.K. (2009) False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Transactions on Information & System Security*, **14**, 21-32. https://doi.org/10.1145/1653662.1653666

[10] Yuan, Y., Li, Z. and Ren, K. (2011) Modeling Load Redistribution Attacks in Power Systems. *IEEE Transactions on Smart Grid*, **2**, 382-390. https://doi.org/10.1109/TSG.2011.2123925

[11] Qin, Z., Li, Q. and Chuah, M.C. (2012) Defending against Unidentifiable Attacks in Electric Power Grids. *IEEE Transactions on Parallel & Distributed Systems*, **99**, 1-11.

[12] Sou, K.C., Sandberg, H. and Johansson, K.H. (2012) On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem. *IEEE Transactions on Smart Grid*, **4**, 856-865. https://doi.org/10.1109/TSG.2012.2230199

[13] Mili, L., Cheniae, M.G., Vichare, N.S., *et al*. (1996) Robust State Estimation Based on Projection Statistics [of Power Systems]. *IEEE Transactions on Power Systems*, **11**, 1118-1127. https://doi.org/10.1109/59.496203

[14] Power System Test Case Archive Univ. Washington, Dept. Elect. Eng., 2007.

[15] Zimmerman, R.D., Murillo-SáNchez, C.E. and Thomas, R.J. (2011) MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Transactions on Power Systems*, **26**, 12-19. https://doi.org/10.1109/TPWRS.2010.2051168