文章编号：1000-3673（2016）08-2406-10 中图分类号：TM 734 文献标志码：A 学科代码：470·40

电力系统状态估计欺诈性数据攻击及防御综述

朱杰，张葛祥，王涛，赵俊博
（西南交通大学 电气工程学院，四川省 成都市 610031）

Overview of Fraudulent Data Attack on Power System State Estimation and Defense Mechanism

ZHU Jie, ZHANG Gexiang, WANG Tao, ZHAO Junbo
(School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, Sichuan Province, China)

ABSTRACT: Aiming to distort power system state estimation by efficiently bypassing traditional bad data detection and identification algorithms, fraudulent data pose a great threat to safe and reliable operations of power systems. Therefore, more attention should be paid to investigate data security vulnerabilities of real power systems and formulate corresponding defense mechanism during process of constructing secure smart grids. For this reason, basic principles of fraudulent data and their impacts on power systems are firstly discussed. Secondly, according to feasible ways of constructing fraudulent data, their manipulation methods are classified into 2 categories: manipulating data collection and corrupting data communication. Thirdly, according to their capabilities, defense mechanisms are classified into 3 types: detection, identification and containment. Then merits and demerits of these defense mechanisms are discussed. Finally, some issues in urgent solution need about fraudulent data attacks and defense mechanisms are pointed out.

KEY WORDS: state estimation; fraudulent data; attack strategies; data security vulnerabilities; defense mechanism

摘要：电力系统状态估计欺诈性数据能够有效躲避传统不良数据检测和辨识，对电力系统的安全可靠运行产生巨大威胁，因此，研究实际电力系统中存在的数据安全漏洞，并制定相应的防御措施是建设安全智能电网进程中不容忽视的问题。文章首先介绍了构建电力系统状态估计欺诈性数据的基本原理，并分析了其对电力系统的影响。再者，根据构建欺诈性数据的可行性途径，将构建欺诈性数据的方式分为操纵数据采集和破坏数据通信 2 类。之后，根据现有防御措施的防御能力，将欺诈性数据的防御措施分为检测、辨识和遏制 3 类，并评述了各类欺诈性数据防御措施的优缺点。最后，指出了欺诈性数据攻击及防御研究中亟待解决的一些问题。

关键词：状态估计；欺诈性数据；攻击策略；数据安全漏洞；防御措施

DOI：10.13335/j.1000-3673.pst.2016.08.023

0 引言

电力系统安全可靠运行是国民经济持续健康发展的重要保障。因此，对电力系统运行状态进行实时监控至关重要。通过对 SCADA 系统实时采集的量测数据进行滤波，电力系统状态估计[1]能够推断出表征电力系统实时运行状态的状态变量，为能量管理系统做出潮流优化、电网实时建模及应急分析等控制决策提供数据支持[2]。显然，量测数据的可靠性直接关系控制指令的准确性。因此，在状态估计过程中，采用不良数据检测和辨识算法剔除量测量中的单个或多个不良数据[3-12]，是确保量测数据安全性的关键。2009 年以前，对量测数据安全性的研究皆局限于保护其免受随机错误的影响，或从通信网络角度关注数据的完整性和有效性[13]，并未考虑黑客精心构建的欺诈性数据对量测数据安全性的影响。

2009 年，Liu Y.等人首次提出电力系统状态估计欺诈性数据的概念，其研究表明：通过获取电力系统网络参数和拓扑结构，并具备操纵特定量测数据的能力时，黑客可以恶意构建针对传统不良数据检测和辨识算法漏洞的欺诈性数据，从而蓄意操纵状态估计结果，威胁电力系统的安全可靠运行[14]。考虑电力系统向着开放型的智能化方向发展，SCADA 系统中逐步融入的先进设备和通信技术必然加剧电力系统的数据安全风险。因此，研究实际电力系统中的数据安全漏洞，并制定相应的防御措施是建设智能电网进程中不可忽视的问题[15-17]。

基于上述背景，本文首次系统性归纳和总结了近年来电力系统状态估计欺诈性数据攻击及防御

基金项目：国家自然科学基金资助项目(61170016，61373047)。
Project Supported by National Nature Science Foundation of China (NSFC) (61170016, 61373047).

研究现状。首先介绍了构建电力系统状态估计欺诈性数据的基本原理，并分析了其对电力系统的影响；再者，根据构建欺诈性数据的可行性途径，将构建欺诈性数据的方式分为操纵数据采集和破坏数据通信 2 类。之后，根据现有防御方法的防御能力，将欺诈性数据防御方法分为检测、辨识和遏制 3 类，并评述了现有欺诈性数据防御措施的优缺点；最后，指出了电力系统状态估计欺诈性数据攻击及防御研究中亟待解决的一些问题，意在为建设智能电网进程中迫切需要关注和解决的课题提供指引。

1　电力系统状态估计欺诈性数据及其影响

1.1　电力系统状态估计欺诈性数据

最大标准化残差(largest normalized residual，LNR)检验是不良数据检测的经典方法。在交流状态估计模型下，设黑客在量测数据中注入欺诈性数据，构建攻击向量 $\boldsymbol{a}$，引起的状态误差向量为 $\boldsymbol{c}$。此时，残差可用公式(1)表示如下。

$$\begin{aligned} r_a &= \|(\boldsymbol{z}+\boldsymbol{a})-h(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 = \\ &\|(\boldsymbol{z}-h(\hat{\boldsymbol{x}}))+(\boldsymbol{a}+h(\hat{\boldsymbol{x}})-h(\hat{\boldsymbol{x}}+\boldsymbol{c}))\|_2 \le \\ &\|\boldsymbol{z}-h(\hat{\boldsymbol{x}})\|_2+\|\boldsymbol{a}+h(\hat{\boldsymbol{x}})-h(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 = \\ &r+\tau_a \end{aligned} \tag{1}$$

对于直流状态估计模型，记常数雅克比矩阵为 $\boldsymbol{H}$，则公式(1)的线性表达如公式(2)所示。

$$\begin{aligned} r_a &= \|(\boldsymbol{z}+\boldsymbol{a})-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 = \\ &\|(\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}})+(\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c})\|_2 \le \\ &\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\|_2+\|\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\|_2 = \\ &r+\tau_a \end{aligned} \tag{2}$$

公式(1)和(2)中：$\boldsymbol{z}$ 为量测数据构成的列向量；$\hat{\boldsymbol{x}}$ 为状态变量构成的列向量；$h(\cdot)$ 表示状态变量与量测数据之间的非线性关系；r_a 和 r 分别表示有无欺诈性数据时 LNR 检验的残差值；τ_a 表示欺诈性数据引起的残差增量。令 $\tau_0 = r+\tau_a$ 为无欺诈性数据时 LNR 检验的阈值，则在交流[18]和直流[14]状态估计模型下构建欺诈性数据的方法可分别用公式(3)和(4)表示。

$$\|\boldsymbol{a}+h(\hat{\boldsymbol{x}})-h(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 < r_a-\tau_a-\|\boldsymbol{z}-h(\hat{\boldsymbol{x}})\|_2 \tag{3}$$

$$\|\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\|_2 < r_a-\tau_a-\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\|_2 \tag{4}$$

当公式(3)和(4)成立时，有 $r_a<\tau_0$，此时欺诈性数据的注入并未触发 LNR 检验，可有效躲避传统不良数据检测和辨识。

显然，SCADA 系统中逐步融入的智能电表、智能继电器、相量测量单元(phasor measurement unit，PMU)等先进设备和通信技术正加剧黑客获取电网信息的风险[19-24]。据此，黑客甚至可通过侵入量测终端单元、数据传输通道和控制中心[25]等方式准确获悉电力系统网络参数和拓扑结构，把握电力系统实时运行状态，以操纵特定量测数据为手段，在特殊条件下构建针对交流[18]和直流[14]状态估计模型的攻击向量，分别如公式(5)和(6)所示。

$$\boldsymbol{a} = h(\hat{\boldsymbol{x}}+\boldsymbol{c})-h(\hat{\boldsymbol{x}}) \tag{5}$$

$$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} \tag{6}$$

需要说明的是，基于公式(3)和(4)构建的攻击向量仅满足 $r_a<\tau_0$，但 $\tau_a\neq 0$，研究中将其称为非完美型欺诈性数据；而基于公式(5)和(6)构建的攻击向量不仅满足 $r_a<\tau_0$，且有 $\tau_a=0$，因此将其称为完美型欺诈性数据。

1.2　电力系统状态估计欺诈性数据的影响

状态估计结果直接用于潮流优化，对电力系统的发电控制和经济调度产生直接的影响。因此，欺诈性数据的注入必然破坏潮流优化，进而通过发电控制指令干扰电力经济调度，引起负荷重分配[26-30]。据此，黑客可进行电力投资，通过电能买卖获取经济收益，扰乱电力市场的经济秩序[31-41]。图 1 给出了电力系统状态估计欺诈性数据攻击和防御关系图，由图 1 可知，完善传统不良数据检测和辨识算法固有的数据安全漏洞是防御欺诈性数据的核心。

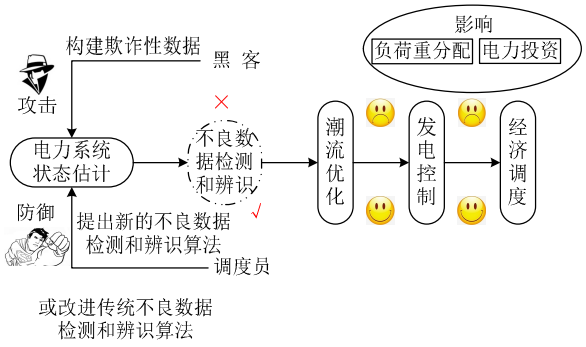

图 1　电力系统状态估计欺诈性数据攻击及防御关系图

Fig. 1　Relation schema of fraudulent data attack on power system state estimation and the defense mechanisms

2　电力系统状态估计欺诈性数据攻击

根据量测数据的采集、传输及处理过程，黑客可通过 3 种途径构建欺诈性数据：操纵数据采集，干扰数据通信，破坏控制中心数据融合；鉴于数据中心均配置严密的安全防御措施，破坏控制中心数据融合而构建欺诈性数据的攻击方式往往难以实现[25]。因此，现阶段的研究论文都仅仅着眼于采用操纵量测数据采集和破坏数据通信的方式构建欺诈性数据。

2.1　操纵数据采集构建欺诈性数据

操纵数据采集构建欺诈性数据时，黑客对电力

系统实时运行状态、网络参数、拓扑结构的熟悉程度以及操纵量测数据的能力大小，决定其构建欺诈性数据的类型。现阶段，研究所涉及的 2 类欺诈性数据有基于公式(3)(4)构建的非完美型欺诈性数据和基于公式(5)(6)构建的完美型欺诈性数据。

2.1.1 非完美型欺诈性数据攻击

在实际电力系统中，对特定量测数据和状态变量的物理保护等原因，限制了黑客操纵特定量测数据和攻击特定状态变量；同时，开关断路器状态、变压器抽头位置及输电线路导纳的实时变化，也使黑客对电力系统的网络参数和拓扑结构信息的获取具有滞后性。由此，黑客有时仅能构建非完美型欺诈性数据。

文献[42]提出攻击评估模型，用以验证黑客在攻击能力受限时构建欺诈性数据的可行性，若完美型欺诈性数据攻击存在，则该模型输出相应的攻击策略。然而，在此种情况下构建完美型欺诈性数据往往是不可行的。此时，构建非完美型欺诈性数据应在非零残差增量的引入不触发不良数据检测的前提下实现。以此前提为指引，文献[43]研究在仅获悉不良数据检测阈值的条件下，黑客通过观察系统正常运行时的误差范围，操纵量测数据构建欺诈性数据的方法。文献[44]采用等效标准化广义特征值法，求解使均方误差增量最大化的攻击策略。文献[45]则对非完美型欺诈性数据引起残差增量的取值范围进行了研究，有 $0 \le \tau_a \le \cos\gamma \cdot \|\boldsymbol{a}\|_2$，$\gamma$ 表示真实雅克比转置矩阵的零空间与非精确雅克比矩阵像空间之间的夹角。特别的，当仅获悉电力系统拓扑结构和关键支路导纳参数，且关键支路所连接子系统间的状态变量偏差相等时[46]，或仅获悉含潮流量测支路的网络参数，且潮流量测支路两端节点的状态变量偏差相等时[47]，黑客均可构建完美型欺诈性数据。更为特殊的情况下，在仅获悉关键支路拓扑结构和网络参数时，黑客可通过篡改关键支路中的支路潮流量测数据和端点注入功率量测数据，使潮流局部平衡，从而操纵不含参考节点子区域的运行状态[48]。

如上所述，在攻击能力受限时，黑客构建完美型欺诈性数据的难度较大，其核心问题在于其无法准确获取电力系统的雅克比矩阵。为了克服该问题，文献[49]将相互独立的负荷作为状态变量，采用独立元分析直接求解表征量测数据与状态变量之间关系的等效雅克比矩阵；由于等效雅克比矩阵关联的状态变量为相互独立的负荷，故此时欺诈性数据的攻击对象仅局限于负荷。为克服该缺点，文献[50]采用主元分析法将传统状态变量映射到新的低维空间下，削弱传统状态变量之间的相关性，求解低维空间下的等效雅克比矩阵。

2.1.2 完美型欺诈性数据攻击

黑客准确获悉电力系统网络参数、拓扑结构，把握电力系统实时运行状态，且能够操纵足够数目和特定位置的量测数据，是构建完美型欺诈性数据的充分条件。站在黑客角度来看，可通过对量测数据进行风险评估，并据此搜寻最优攻击策略，从而极大限度降低攻击成本。

1）量测数据风险评估。

设在 $\boldsymbol{a}$ 的第 k 个量测数据中注入的欺诈性数据为 a_k，若使 a_k 有效躲避不良数据检测和辨识，则必须在与 a_k 相关的量测数据中同时注入欺诈性数据[14]。攻击第 k 个量测数据时，共需操纵的量测数据总数定义为第 k 个量测数据的安全指数，记为 α_k，用以评估第 k 个量测数据应对欺诈性数据攻击的能力。文献[51]和文献[52]分别在量测数据未被保护和部分被保护条件下，研究 α_k 的求解问题。由于求解 α_k 属 NP-难问题[52-54]，故该研究仅界定了 α_k 的取值范围。文献[53]和文献[54]在此基础上，分别将 α_k 的求解问题近似等效为标准化最小分割问题和线性规划问题，但也仅仅是间接求取量测数据未被保护和部分被保护条件下 α_k 的次优解。

2）最优攻击策略。

构建欺诈性数据需付出的最小代价称为最优攻击策略。研究中，将成功构建欺诈性数据时，操纵量测数据的最少数目作为最优攻击策略的衡量指标[55]。求解最优攻击策略同属 NP-难问题[55-58]。因此，文献[55]将求解过程近似等效为加权线性规划问题，通过标准线性规划获取最优攻击策略的先验性结果，以此为参考，设定加权线性规划的权重矩阵。研究表明：先验加权线性规划求得的近似最优策略显著优于线性规划求解结果，但对于大系统而言，权重矩阵的确定和串行计算无疑降低了该方法的求解效率。为提高计算效率，文献[56]采用区域分割法将大系统分割为相互重叠的子系统，通过搜索算法求得各子系统的最优解，组合各系统的解近似获取全局最优攻击策略；理论上讲，分布式并行计算提高了计算效率，但将其用于求解大系统中的最优攻击策略时，组合结果后获得的攻击策略可能会在很大程度上偏离真实的最优攻击策略。为克服该缺陷，文献[57]和[58]分别采用正交匹配追踪算法和交替方向乘子法近似求解最优攻击策略，降低求解过程所需的迭代次数，进一步优化了求解结

果。文献[59]则采用适用于大系统的超图分割算法，保证计算效率的同时，求解的最优攻击策略更接近真实情况。

2.2　破坏数据通信构建欺诈性数据

根据量测数据的通信过程，本文将破坏数据通信构建欺诈性数据的方式分为 3 类：破坏量测终端与数据中心之间的数据通信、破坏分布式系统之间的数据通信以及破坏 PMU 终端的数据通信。

2.2.1　破坏量测终端与数据中心之间的数据通信

文献[60]提出通信数据干扰矩阵，将其用于篡改或增删变电站量测终端采集的原始数据信息，使独立传输到数据中心的通信数据偏离原始值。然而，实际电力系统中的数据通信是多路传输的，即变电站终端传感器采集的信息传输到数据中心的过程中可能会经过其他变电站，基于该实际，文献[61]研究了黑客能够完全操纵某变电站量测终端传输的数据信息时，向通信系统中注入欺诈性数据的方法。

2.2.2　破坏分布式系统之间的数据通信

文献[62-63]研究黑客具备操纵某分布式子系统能力时，通过篡改与该分布式子系统进行通信的数据，构建欺诈性数据的方法。该方法构建的欺诈性数据可使状态变量很大程度偏离电力系统的状态真实值[62]，甚至导致状态估计结果不收敛，造成电力系统瘫痪[63]。

2.2.3　破坏 PMU 终端的数据通信

全球定位系统(global positioning system，GPS)传送信号时，无加密和认证机制的固有漏洞使电力系统无法识别在 GPS 传送信号中伪造的通信数据。据此，文献[64]采用攻击 GPS 设备的方式，抹除 PMU 量测数据中的时间同步信息，使数据中心质疑 PMU 采集的量测数据，造成量测数据不可用。文献[65]则利用 PMU 传输数据的周期性和通信数据的固有长度及时序信息，推断数据中心和 PMU 配置点等通信主体的身份和位置，获得数据传输通道及其相关性等信息，而后通过黑客技术监控目标位置，攻击相关数据传输通道中的通信数据(如：篡改和抹除数据、延迟数据传输时间、限制信息传输等)，使控制中心接收到的数据组在时间上不再同步，同样导致量测数据不可用。

3　电力系统状态估计欺诈性数据防御

现阶段，尚无相关论文专门对电力系统状态估计欺诈性数据防御方法做分类。本文结合现有研究成果，将防御措施分为检测、辨识和遏制 3 类。前两者分别着眼于检测欺诈性数据的存在、辨识欺诈性数据的位置；而欺诈性数据的遏制则着眼于采用电力系统物理保护法、量测信息重叠法等措施，从根本上消除黑客构建欺诈性数据的可能性。表 1 总结了近年来 2 种途径所构建欺诈性数据的检测、辨识和遏制方法，并指出各自优缺点。下文将分别做综述介绍。

3.1　操纵数据采集构建欺诈性数据的防御

3.1.1　操纵数据采集构建欺诈性数据的检测

与完美型欺诈性数据不同，非完美型欺诈性数据的注入会引起部分量测数据残差的异常变化。据此，文献[66]提出∞-范数检验法，检测量测残差的局部异常。需要说明的是，∞-范数检验设定的阈值大小对检测精度的影响较大，应用中易出现漏检。考虑 LNR 检验阈值与电力系统规模大小呈正相关，文献[67]将全局电力系统进行自适应分块，为各子系统设定较小的检验阈值，将超过设定阈值的子系统标记为可疑区域，并对可疑区域进一步分割，最终锁定欺诈性数据所在区域。由于自适应分块后的各子系统相互不重叠，因此，自适应分块检验法无法检测连接支路上存在的欺诈性数据。为弥补该不足，文献[43]将各子系统进一步扩展，将连接支路和相邻节点纳入子系统中，确保全局系统被多个相互重叠的子系统分割，从而可以检测系统中任何区域存在的欺诈性数据。

完美型欺诈性数据发生时，量测向量会由服从均值为 $\mathbf{0}$ 的高斯分布变为服从均值为 $\boldsymbol{a}$ 的高斯分布。据此，文献[68]和文献[69]分别提出广义似然比检验和广义累积和检验，根据欺诈性数据出现前后高斯分布密度函数值的差异是否超过检验阈值，判定欺诈性数据是否存在。在此基础上，文献[70]进一步提出了自适应累积和检验，采用递归方式求解高斯分布密度函数值，使得检测速度更快、精度更高。文献[71-72]提出状态和检测法，依据系统状态的运行规律和历史数据库，预测状态变量的分布规律，同时实现了检测欺诈性数据和系统异常的作用。鉴于欺诈性数据的出现会破坏电压特性曲线的固有的正弦波特性，文献[73]将$|V_i|\cos\theta_i$和$|V_i|\sin\theta_i$(V_i和θ_i分别表示节点i的电压幅值和相角)作为卡尔曼滤波算法的初始值，通过估计电压特性曲线是否出现异常，判定系统中是否存在欺诈性数据。文献[74]采用主元分析法将量测数据映射到新的低维空间，消除量测数据之间的相关性，使正常和被操纵量测数据在低维空间中相互分离，从而在低维空间中快速检测欺诈性数据。

表 1 电力系统状态估计欺诈性数据防御措施

Tab. 1 Defense mechanisms of fraudulent data attack on power system state estimation

防御对象	防御分类	防御思路	相关文献	防御方法的优点	防御方法的缺点
操纵数据采集构建的欺诈性数据	检测	∞-范数检验	[66]	可有效检测非完美型欺诈性数据；	阈值的设定对检测精度影响大，易出现误检，且无法检测完美型欺诈性数据；
		自适应分块检验	[43,67]	检测精度较高；	无法检测完美型欺诈性数据；
		广义似然比检验 广义累积和检验	[68] [69]	可有效检测非完美型和完美型欺诈性数据；	计算复杂度高，检测速度慢，不适用于大系统；
		自适应累积和检验	[70]	可在线快速检测非完美型和非完美型欺诈性数据，且检测精度较高；	对于大系统，计算耗时；
		状态和检验	[71,72]	拥有检测系统异常的作用；	对于大系统和动态系统，检测灵敏度有所降低；
		电压特性曲线检验	[73]	可快速检测非完美型和完美型欺诈性数据；	非欺诈性数据引起的异常波动会影响系统的检测结果；
		主元分析检验	[74]	检测速度快；	通信数据丢失会导致检测结果出错；
	辨识	无功潮流残差检验	[75]	有效辨识支路潮流中的欺诈性数据；	大系统的辨识速度慢，且仅能够辨识支路潮流中存在的欺诈性数据；
		低秩矩阵填充及恢复	[76]	有效辨识量测数据中的欺诈性数据；	大系统的计算复杂度较高，辨识速度慢；
		信任度检验	[77]	有效隔离欺诈性数据；	欺诈性数据所在区域的供电可靠性降低；
	遏制	量测数据保护法	[78-82,71-72]	最简单，有效遏制欺诈性数据；	加密设备投资过高；
		网络参数动态调节法	[83-85]	有效遏制欺诈性数据；	D-FACTS 设备未普及，使防御方法应用受限；
		拓扑结构动态调节法	[86]	无需设备投资，可有效遏制欺诈性数据；	限制电力系统全局输电能力；
		拓扑结构重构法	[46]	系统的安全性相对提高；	未消除系统被攻击的可能；
		量测信息重叠法	[87]	防御成本较低，从根本上遏制欺诈性数据；	不适用于量测冗余度较低的电力系统，计算复杂度较高；
破坏数据通信构建的欺诈性数据	检测	可信度检验	[62-63]	有效隔离欺诈性数据；	可疑区域的供电可靠性降低，且仅适用于检测分布式系统间存在的欺诈性数据；
	辨识	批验证数据通道滤波	[88]	有效辨识特定位置的欺诈性数据；	仅适用于辨识量测终端与数据中心间数据通道中的欺诈性数据，且仅能辨识含相同相邻节点传感器量测终端中存在的欺诈性数据；
		多项式数据通道滤波	[89]	能辨识所有传感器量测终端出现的欺诈性数据；	仅适用于辨识量测终端与数据中心间数据通道中存在的欺诈性数据，且计算复杂度较高；
		交叉层防御	[64]	欺诈性数据的辨识定位较为准确；	仅适用于辨识 PMU 终端存在的欺诈性数据，且设备投资成本较高；
	遏制	数据包加密和随机串联	[65]	可用于遏制各类破坏数据通信构建的欺诈性数据；	对系统的通信能力和数据处理能力要求较高；

3.1.2 操纵数据采集构建欺诈性数据的辨识

分布式发电技术的日趋成熟，使未来电力系统的电压幅值因更易受到监控而难以成为黑客的攻击对象。据此，文献[75]将与电压幅值相关的支路无功潮流残差作为检测指标，由于支路无功潮流残差仅与自身支路的有功和无功潮流相关，因此，可通过支路无功潮流残差是否超过检测阈值，辨识支路潮流量测中是否存在欺诈性数据。显然，无功潮流残差检验仅能辨识支路潮流量测中的欺诈性数据。为弥补该缺陷，文献[76]利用量测数据的低秩性和欺诈性数据的稀疏性，将欺诈性数据的辨识问题转化为量测数据低秩矩阵的恢复和填充问题，采用拉格朗日乘子法和矩阵分解法高效求解量测数据和欺诈性数据，有效辨识欺诈性数据。文献[77]则通过分布式子系统之间状态估计偏差确定分布式子系统间的信任度，通过滤除信任度较低的子系统传输的信息，有效辨识欺诈性数据。

3.1.3 操纵数据采集构建欺诈性数据的遏制

1）电力系统物理保护法。

将能够确保系统可观测性，包含最少量测数据的集合称为基本量测集[78]。文献[79]和文献[80]分别采用量测矩阵搜索算法和 Steiner 树约简算法确定加密设备的安装位置及数目，使基本量测集免于黑客操纵。据此，调度中心可通过基本量测集获取状态估计结果[81]。当电力系统各节点都可通过支路连接被保护节点[82]，或黑客无法操纵的量测数据不能保证系统可观测性时，欺诈性数据是无法构建的。据此，文献[71-72]提出量测保护集搜索算法，

在基本量测集中进一步添加量测数据，使未被保护的量测数据无法保证系统可观测性，有效弥补文献[79-80]无法应对电力系统拓扑结构变化而导致量测数据保护法失效的不足。显然，加密设备的高额投资限制了量测数据保护法的应用。

在实际电力系统中，分布式柔性交流输电(distributed flexible AC transmission system，D-FACTS)设备可动态调节电力系统的网络参数[83]。据此，文献[84]提出多套使输电线路损失功率波动较小的D-FACTS设备参数设定方案，并组建方案库。电力系统运行过程中，调度中心从方案库中随机选定参数设定方案，并将该方案下求解的状态变量预期值与实际值对比，遏制欺诈性数据。文献[85]在此基础上，改进了D-FACTS设备参数方案库的组建过程，使系统能够返回到前一时刻的运行状态，通过返回后的量测数据对比，量化欺诈性数据。显然，D-FACTS设备的配置现状和高额投资，同样限制了网络参数动态调节法的应用。

文献[86]提出拓扑结构动态调节法，用以遏制欺诈性数据。电力系统运行过程中，调度员依次逐条断开由输电线路集构成的非环形扩展树中的输电线路，组建黑客无法获悉的动态拓扑结构，有效遏制欺诈性数据。与量测数据保护法和网络参数动态调节法相比，拓扑结构动态调节法虽然更加经济，但也在一定程度上限制了电力系统的全局输电能力。

2）量测信息重叠法。

文献[46]将欺诈性数据引起的状态偏差作为衡量指标，评估特定拓扑结构的电力系统遏制欺诈性数据的能力，为构建安全的电网结构提供参考。需要指出的是，该方法只在一定程度上相对提高了电力系统的安全性，并未消除系统受到欺诈性数据攻击的可能。据此，文献[87]提出量测信息重叠法，将电力系统动态随机分割为2个相互重叠的子系统，分别构建雅克比矩阵衍生矩阵 $\boldsymbol{B}_1$ 和 $\boldsymbol{B}_2$，使二者满足 $\mathrm{rank}([\boldsymbol{B}_1\ \boldsymbol{B}_2]^{\mathrm{T}})=m$ (m 为量测数据总个数)，从根本上遏制欺诈性数据。

3.2　破坏数据通信构建欺诈性数据的防御

3.2.1　破坏数据通信构建欺诈性数据的检测

文献[62]利用分布式状态估计迭代求解过程的收敛特性，实现了对分布式系统通信过程中的异常数据的检测。在此基础上，文献[63]计算每次迭代过程中分布式系统传输数据的均方偏差与总均方偏差的比值，将其作为分布式系统每次传输数据的可信度，通过隔离可信度较低的可疑区域，降低欺诈性数据的影响。

3.2.2　破坏数据通信构建欺诈性数据的辨识

文献[88]提出批验证数据通道滤波法，对含相同相邻节点的传感器在同一时刻传输信息的同一性进行批验证，若同一性无法被满足，则滤除该信息，从而有效辨识和滤除欺诈性数据。由上述机理可知，批验证数据通道滤波法仅能够识别含相同相邻节点传感器中存在的欺诈性数据。为弥补该不足，文献[89]提出多项式数据通道滤波法，实现对传输通道中各传感器节点传输信息真伪的辨识。

文献[64]提出了交叉层防御机制，综合考察来自物理层的被攻击先验概率和高级层的被攻击位置判定信息，辨识被攻击的PMU。

3.2.3　破坏数据通信构建欺诈性数据的遏制

数据包加密技术可以有效遏制黑客掌握数据的内容信息，但却无法阻止黑客掌握数据包的长度和时序信息。据此，文献[65]进一步提出数据包随机串联技术，阻止黑客获取量测数据的长度和时序信息，从而有效遏制破坏数据通信而构建的欺诈性数据攻击。

4　结论

本文系统性综述了近年来电力系统状态估计欺诈性数据攻击及防御研究现状，并提炼了防御措施在应用中的优缺点。目的在于指出电力系统中的隐蔽性数据安全漏洞，介绍相关防御措施，为建设智能电网进程中需要关注的问题提供方向性指引。考虑电力系统的实际运行状态和发展趋势，电力系统状态估计欺诈性数据攻击及防御课题仍存在诸多问题值得深入研究，具体如下：

1）实际电力系统中数据安全漏洞的探索。

现阶段，电力系统状态估计欺诈性数据攻击及防御的研究论文大多都是基于直流静态状态估计模型开展的。考虑交流状态估计算法存在迭代过程，欺诈性数据在每次迭代的过程中均有可能被检测出来[90]。因此，将直流状态估计模型下构建欺诈性数据的思路用于交流状态估计模型时，系统受到的影响较小[91]；换句话说，在交流状态估计模型中构建欺诈性数据时，黑客需要掌控更全面的信息[92-93]；但这并非说明交流状态估计模型可以有效遏制欺诈性数据，如最新提出的通过干扰数据中心的数据融合而构建的不可辨识型欺诈性数据[94]、栽赃型欺诈性数据[95-96]以及拓扑结构欺诈性数据[97-98]都在很大程度上威胁交流状态估计模型的安全。而在开放型的智能电网中，通过侵入智能电网

的基础设施[99]，黑客可轻易获取家居及企业新能源的发电量等相关参数，甚至直接操纵终端的分布式电源[100-101]或间歇性切换网络拓扑[102-103]构建针对交流动态状态估计模型的欺诈性数据。因此，探索实际电力系统中的数据安全漏洞，分析其对电力系统运行与控制的影响，并构建防御系统，是更好服务于建设安全电力系统的必要环节。

2）综合型欺诈性数据防御系统的构建。

现阶段，欺诈性数据防御研究都只着眼于检测、辨识或遏制单一途径注入的欺诈性数据，且研究中假设欺诈性数据是单次注入的。而在未来的智能电网中，黑客可以通过量测终端单元、数据传输通道，甚至侵入数据中心等多种途径，动态连续注入混合型欺诈性数据，拖慢防御算法的处理效率，甚至导致防御算法失效。因此，未来欺诈性数据的防御措施研究不仅需要提高算法的效率，还需要着眼于从根本上遏制多途径动态连续注入的混合型欺诈性数据，构建综合型欺诈性数据防御系统。为此，可通过引入可信计算，保证量测数据来源的可靠性，阻止含欺诈性数据的量测量参与状态求解；或在量测终端、数据传输通道、控制中心等数据采集、传输和处理的各个环节构建安全环境，从根本上杜绝篡改量测数据行为的发生。除此之外，从本质层面看，加权最小二乘法缺乏鲁棒性的固有特性是电力系统状态估计欺诈性数据得以成功构建的重要原因；而欺诈性数据不具备正常量测数据固有的时空关联性也为构建欺诈性数据防御系统提供了一点启发，据此，将鲁棒性状态估计算法与挖掘量测数据时空关联性相结合，同样是电力系统状态估计欺诈性数据防御研究中值得关注的课题。

参考文献

[1] Schweppe F C，Wildes J，Rom D B．Power system static-state estimation：Part I，II & III[J]．IEEE Transactions on Power Apparatus and Systems，1970，89(1)：120-135．

[2] Wu F F．Power system state estimation：a survey[J]．International Journal of Electrical Power & Energy Systems，1990，12(2)：80-87．

[3] Monticelli A，Garcia A．Reliable bad data processing for real-time state estimation[J]．IEEE Transactions on Power Apparatus and Systems，1983，102(5)：1126-1139．

[4] Cutsem T V，Pavella M R，Mili L．Hypothesis testing identification: a new method for bad data analysis in power system state estimation[J]．IEEE Transactions on Power Apparatus and Systems，1984，103 (11)：3239-3252．

[5] Monticelli A，Wu F F，Multiple M Y．Bad data identification for state estimation by combinatorial optimization[J]．IEEE Transactions on Power Delivery，1986，1(3)：361-369．

[6] Cutsem T V，Pavella M R，Mili L．Bad data identification methods in power system state estimation：a comparative study[J]．IEEE Transactions on Power Apparatus and Systems，1985，104(11)：3037-3049．

[7] Cheniae M G，Mili L，Rousseeuw J．Identification of multiple interacting bad data via power system decomposition[J]．IEEE Transactions on Power Systems，1996，11(3)：1555-1563．

[8] 吴军基，杨伟，葛成，等．基于 GSA 的肘形判据用于电力系统不良数据辨识[J]．中国电机工程学报，2007，26(22)：23-28．
Wu Junji，Yang Wei，Ge Cheng．Application of GSA-based elbow judgment on bad-data detection of power system[J]．Power System Protection and Control，2007，26(22)：23-28(in Chinese)．

[9] 卢志刚，王浩锐，孙继凯．基于灵敏度分析的数据最优筛选与不良数据辨识[J]．电网技术，2011，35(2)：38-42．
Lu Zhigang，Wang Haorui，Sun Jikai．Optimal data screening and bad data identification based on sensitive analysis[J]．Power System Technology，2011，35(2)：38-42(in Chinese)．

[10] 卢志刚，程慧琳，冯磊，等．基于证据融合理论的多不良数据辨识[J]．电网技术，2012，36(1)：123-128．
Lu Zhigang，Cheng Huilin，Feng Lei，et al．Multi bad data identification based on evidence fusion theory[J]．Power System Technology，2012，36 (1)：123-128(in Chinese)．

[11] 陈艳波，何光宇，周京阳，等．基于改进转移潮流法的拓扑错误辨识方法[J]．电网技术，2012，36(3)：95-100．
Chen Yanbo，He Guangyu，Zhou Jingyang，et al．An improved power flow transfer approach with enhanced ability to identify topology error and bad data[J]．Power System Technology，2012，36(3)：95-100(in Chinese)．

[12] 刘健，蔡明威，张志华，等．基于可信度的电缆配电网不良数据辨识与修正[J]．电力自动化设备，2014，34(2)：57-72．
Liu Jian，Cai Mingwei，Zhang Zhihua，et al．Bad data identification and correction based on confidence level for cable power distribution system[J]．Electric Power Automation Equipment，2014，34(2)：57-72(in Chinese)．

[13] 杨清宇，杨洁，马训鸣．电力系统中假数据注入攻击研究[J]．微电机与计算机，2011，28(12)：175-179．
Yang Qingyu，Yang Jie，Ma Xunming．Research on false data injection attacks in power systems[J]．Microelectronics and Computer，2011，28(12)：175-179(in Chinese)．

[14] 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，2011，14(1)：13．

[15] Sridhar S，Hahn A，Govindarasu M．Cyber–physical system security for the electric power grid[J]．Proceedings of the IEEE，2012，100(1)：210-224．

[16] Liu J，Xiao Y，Li S，et al．Cyber security and privacy issues in smart grids[J]．IEEE Communications Surveys & Tutorials，2012，14(4)：981-997．

[17] Wang W，Lu Z．Cyber security in the smart grid: survey and challenges[J]．Computer Networks，2013，57(5)：1344-1371．

[18] 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．

[19] Huang Y F，Werner S，Huang J，et al．State estimation in electric power grids：meeting new challenges presented by the requirements of the future grid[J]．IEEE Signal Processing Magazine，2012，29(5)：33-43．

[20] Locke G，Gallagher P D．NIST framework and roadmap for smart grid interoperability standards，release 1.0[EB/OL]．2010-01-25 [2015-09-26]．Available：http://www.nist.gov/smartgrid/upload/FinalSGDoc2010019-corr010411-2.pdf．

[21] 林宇锋，钟金，吴复立．智能电网技术体系探讨[J]．电网技术，

2009，33(12)：9-16.
Lin Yufeng，Zhong Jin，Felix Wu. Discussion on smart grid supporting technologies[J]. Power System Technology，2009，33(12)：9-16(in Chinese).

[22] 苗新，张恺，田世明，等. 支撑智能电网的信息通信体系[J]. 电网技术，2009，33(17)：8-13.
Miao Xin，Zhang Kai，Tian Shiming，et al. Information communication system supporting smart grid[J]. Power System Technology，2009，33(17)：8-13(in Chinese).

[23] 雷煜卿，李建岐，侯宝素. 面向智能电网的配用电通信网络研究[J]. 电网技术，2011，35(12)：14-19.
Lei Yuqing，Li Jianqi，Hou Baosu. Power distribution and utilization communication network for smart grid[J]. Power System Technology，2011，35(12)：14-19(in Chinese).

[24] 苏盛，吴长江，马钧，等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术，2014，38(11)：3115-3120.
Su Sheng，Wu Changjiang，Ma Jun，et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]. Power System Technology，2014，38(11)：3115-3120(in Chinese).

[25] Giani A，Sastry S，Johansson K H，et al. The VIKING project：an initiative on resilient control of power networks[C]//2009 International Symposium on Resilient Control Systems. Idaho Falls，Idaho：IEEE，2009：31-35.

[26] Mohsenian-Rad A H，Leon-Garcia A. Distributed internet-based load altering attacks against smart power grids[J]. IEEE Transactions on Smart Grid，2011，2(4)：667-674.

[27] Yuan Y，Li Z，Ren K. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid，2011，2(2)：382-390.

[28] Yuan Y，Li Z，Ren K. Quantitative analysis of load redistribution attacks in power systems[J]. IEEE Transactions on Parallel and Distributed Systems，2012，23(9)：1731-1738.

[29] Liu X，Li Z. Local load redistribution attacks in power systems with incomplete network information[J]. IEEE Transactions on Smart Grid，2014，5(4)：1665-1676.

[30] Liu X，Bao Z，Lu D，et al. Modeling of local false data injection attacks with reduced network information[J]. IEEE Transactions on Smart Grid，2015，6(4)：1686-1696.

[31] Xie L，Mo Y，Sinopoli B. False data injection attacks in electricity markets[C]//2010 IEEE International Conference on Smart Grid Communications. Gaithersburg，MD：IEEE，2010：226-231.

[32] Xie L，Mo Y，Sinopoli B. Integrity data attacks in power market operations[J]. IEEE Transactions on Smart Grid，2011，2(4)：659-666.

[33] Jia L，Thomas R J，Tong L. Malicious data attack on real-time electricity market[C]//2011 IEEE International Conference on Acoustics，Speech and Signal Processing. Prague，Czech：IEEE，2011：5952-5955.

[34] Jia L，Thomas R J，Tong L. Impacts of malicious data on real-time price of electricity market operations[C]//2012 Hawaii International Conference on System Science. Maui，HI：IEEE，2012：1907-1914.

[35] Esmalifalak M，Han Z，Song L. Effect of stealthy bad data injection on network congestion in market based power system[C]//2012 IEEE Wireless Communications and Networking Conference. Shanghai：IEEE，2012：2468-2472.

[36] Choi D H，Xie L. Malicious ramp-induced temporal data attack in power market with look-ahead dispatch[C]//2012 IEEE International Conference on Smart Grid Communications. Tainan，China：IEEE，2012：330-335.

[37] Esmalifalak M，Shi G，Han Z，et al. Bad data injection attack and defense in electricity market using game theory study[J]. IEEE Transactions on Smart Grid，2013，4(1)：160-169.

[38] Bi S，Zhang Y J. False-data injection attack to control real-time price in electricity market[C]//2013 IEEE Global Communications Conference. Atlanta，GA：IEEE，2013：772-777.

[39] Lin J，Yu W，Yang X. On false data injection attack against Multistep Electricity Price in electricity market in smart grid[C]//2013 IEEE Global Communications Conference. Atlanta，GA：IEEE，2013：760-765.

[40] Rahman M A，Al-Shaer E，Kavasseri R G. A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids[C]//2014 ACM/IEEE International Conference on Cyber-Physical Systems. Berlin，Germany：IEEE，2014：175-186.

[41] Lin J，Yu W，Yang X. Towards multistep electricity prices in smart grid electricity markets[J]. IEEE Transactions on Parallel and Distributed Systems，2016，27(1)：286-302.

[42] Rahman M A，Al-Shaer E，Rahman M A. A formal model for verifying stealthy attacks on state estimation in power grids[C]//2013 IEEE International Conference on Smart Grid Communications. Vancouver，BC：IEEE，2013：414-419.

[43] Wang D，Guan X，Liu T，et al. Extended distributed state estimation：a detection method against tolerable false data injection attacks in smart grids[J]. Energies，2014，7(3)：1517-1538.

[44] Kosut O，Jia L，Thomas R J，et al. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid，2011，2(4)：645-658.

[45] Teixeira A，Amin S，Sandberg H，et al. Cyber security analysis of state estimators in electric power systems[C]//2010 IEEE Conference on Decision and Control. Atlanta，GA：IEEE，2010：5991-5998.

[46] Rahman M A，Mohsenian-Rad H. False data injection attacks with incomplete information against smart power grids[C]//2012 IEEE Global Communications Conference. Tampa，FL：IEEE，2012：3153-3158.

[47] Bi S，Zhang Y J. Mitigating false-data injection attacks on DC state estimation using covert topological information[C]//2013 Global Communications Conference. Atlanta，GA：IEEE，2013：766-771.

[48] Bi S，Zhang Y J. Using covert topological information for defense against malicious attacks on DC state estimation[J]. IEEE Journal on Selected Areas in Communications，2014，32(7)：1471-1485.

[49] Esmalifalak M，Nguyen H，Zheng R，et al. Stealth false data injection using independent component analysis in smart grid[C]//2011 IEEE International Conference on Smart Grid Communications. Brussels，Belgium：IEEE，2011：244-248.

[50] Yu Z H，Chin W L. Blind false data injection attack using PCA approximation method in smart grid[J]. IEEE Transactions on Smart Grid，2015，6(3)：1219-1226.

[51] Dán G，Sandberg H. Stealth attacks and protection schemes for state estimators in power systems[C]//2010 IEEE International Conference on Smart Grid Communications. Gaithersburg，MD：IEEE，2010：214-219.

[52] Teixeira A，Dán G，Sandberg H，et al. A cyber security study of a SCADA energy management system：Stealthy deception attacks on the state estimator[J]. IFAC Proceedings Volumes，2011，44(1)：11271-11277.

[53] Hendrickx J M，Johansson K H，Jungers R M，et al. Efficient computations of a security index for false data attacks in power networks[J]. IEEE Transactions on Automatic Control，2014，59(12)：3194-3208.

[54] Sou K C，Sandberg H，Johansson K H. On the exact solution to a smart grid cyber-security analysis problem[J]. IEEE Transactions on Smart Grid，2013，4(2)：856-865.

[55] 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.

[56] Yang Q，Yang J，Yu W，et al. On a hierarchical false data injection attack on power system state estimation[C]//2011 IEEE Global Telecommunications Conference. Houston，TX：IEEE，2011：1-5.

[57] Zhang C，Ren Z，Zhang A，et al. Malicious data injection attack against power system state estimation based on orthogonal matching pursuit[C]//2013 Asian Control Conference. Istanbul，Turkey：IEEE，2013：1-6.

[58] Ozay M，Esnaola I，Vural F T Y，et al. Sparse attack construction and state estimation in the smart grid：centralized and distributed models[J]. IEEE Journal on Selected Areas in Communications，2013，31(7)：1306-1318.

[59] Yamaguchi Y，Ogawa A，Takeda A，et al. Cyber security analysis of power networks by hypergraph cut algorithms[J]. IEEE Transactions on Smart Grid，2015，6(5)：2189-2199.

[60] Bishop A N，Savkin A V. On false-data attacks in robust multi-sensor-based estimation[C]//2011 9th IEEE International Conference on Control and Automation. Santiago，Chile：IEEE，2011：10-17.

[61] Vuković O，Sou K C，Dán G，et al. Network-aware mitigation of data integrity attacks on power system state estimation[J]. IEEE Journal on Selected Areas in Communications，2012，30(6)：1108-1118.

[62] Vuković O，Dán G. On the security of distributed power system state estimation under targeted attacks[C]//2013 Proceedings of the 28th Annual ACM Symposium on Applied Computing. Coimbra，Portugal：ACM，2013：666-672.

[63] Vuković O，Dán G. Security of fully distributed power system state estimation：detection and mitigation of data integrity attacks[J]. IEEE Journal on Selected Areas in Communications，2014，32(7)：1500-1508.

[64] Fan Y，Zhang Z，Trinkle M，et al. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids[J]. IEEE Transactions on Smart Grid，2015，6(6)：2659-2668.

[65] Sikdar B，Chow J H. Defending synchrophasor data networks against traffic analysis attacks[J]. IEEE Transactions on Smart Grid，2011，2(4)：819-826.

[66] Kosut O，Jia L，Thomas R J，et al. Limiting false data attacks on power system state estimation[C]//2010 Annual Conference on Information Sciences and Systems. Princeton，NJ：IEEE，2010：1-6.

[67] 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. Budapest，Hungary：IEEE，2013：4483-4487.

[68] Kosut O，Jia L，Thomas R J，et al. On malicious data attacks on power system state estimation[C]//2010 International Universities Power Engineering Conference. Cardiff，Wales：IEEE，2010：1-6.

[69] Li S，Yilmaz Y，Wang X. Quickest detection of false data injection attack in wide-area smart grids[J]. IEEE Transactions on Smart Grid，2015，6(6)：2725-2735.

[70] 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.

[71] Li Y，Wang Y. State summation for detecting false data attack on smart grid[J]. International Journal of Electrical Power & Energy Systems，2014，57：156-163.

[72] 王以良. 智能电网虚假数据攻击检测及防范研究[D]. 北京：华北电力大学，2014.

[73] 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.

[74] Esmalifalak M，Liu L，Nguyen N，et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal，DOI：10.1109/JSYST.2014.2341597.

[75] Sou K C，Sandberg H，Johansson K H. Data attack isolation in power networks using secure voltage magnitude measurements[J]. IEEE Transactions on Smart Grid，2014，5(1)：14-28.

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

[77] Matei I，Baras J S，Srinivasan V. Trust-based multi-agent filtering for increased smart grid security[C]//2012 Mediterranean Conference on Control & Automation. Barcelona，Spain：IEEE，2012：716-721.

[78] Bi S，Zhang Y J. Defending mechanisms against false-data injection attacks in the power system state estimation[C]//2011 IEEE GLOBECOM Workshops. Houston，TX：IEEE，2011：1162-1167.

[79] Giani A，Bitar E，Garcia M，et al. Smart grid data integrity attacks[J]. IEEE Transactions on Smart Grid，2013，4(3)：1244-1253.

[80] Bi S，Zhang Y J. Graphical methods for defense against false-data injection attacks on power system state estimation[J]. IEEE Transactions on Smart Grid，2014，5(3)：1216-1227.

[81] Bobba R B，Rogers K M，Wang Q，et al. Detecting false data injection attacks on DC state estimation[C]//2010 Preprints of the First Workshop on Secure Control Systems. Stockholm，Sweden：CPSWEEK，2010：1-9.

[82] Zheng S，Jiang T，Baras J S. Robust state estimation under false data injection in distributed sensor networks[C]//2010 IEEE Global Telecommunications Conference. Miami，FL：IEEE，2010：1-5.

[83] Rogers K M. Power system control with distributed flexible ac transmission system devices[D]. University of Illinois at Urbana-Champaign，2009.

[84] Morrow K L，Heine E，Rogers K M，et al. Topology perturbation for detecting malicious data injection[C]//2012 Hawaii International Conference on System Science. Maui，HI：IEEE，2012：2104-2113.

[85] Kuntz K，Smith M，Wedeward K，Collins M. Detecting，locating，& quantifying false data injections utilizing grid topology through optimized D-FACTS device placement[C]//2014 North American Power Symposium. Pullman，WA：IEEE，2014：1-6.

[86] Wang S，Ren W. Stealthy false data injection attacks against state estimation in power systems: Switching network topologies[C]//2014 American Control Conference. Portland，OR：IEEE，2014：1572-1577.

[87] Talebi M，Wang J，Qu Z. Secure power systems against malicious cyber-physical data attacks: protection and identification[J]. World Academy of Science，Engineering and Technology，2012，6(6)：112-119.

[88] Euodial A，Beryl Princess P J. EFBV: En-route filtering based batch verification scheme for false data injection attack in wireless sensor networks[C]//2013 IEEE International Conference on Green High Performance Computing. Nagercoil，India：IEEE，2013：1-5.

[89] Yang X，Lin J，Yu W，et al. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems[J]. IEEE Transactions on Computers，2015，64(1)：4-18.

[90] Jia L，Thomas R J，Tong L. On the nonlinearity effects on malicious data attack on power system[C]//2012 IEEE Power and Energy Society General Meeting. San Diego，CA：IEEE，2012：1-8.

[91] Rahman M A，Mohsenian-Rad H. False data injection attacks against nonlinear state estimation in smart power grids[C]//2013 IEEE Power and Energy Society General Meeting. Vancouver，BC：IEEE，2013：1-5.

[92] Niu R，Huie L. System state estimation in the presence of false information injection[C]//2012 IEEE Statistical Signal Processing Workshop. Ann Arbor，MI：IEEE, 2012：385-388.

[93] Kosut O. Malicious data attacks against dynamic state estimation in the presence of random noise[C]//2013 IEEE Global Conference on Signal and Information Processing. Austin，TX：IEEE，2013：261-264.

[94] Qin Z，Li Q，Chuah M C. Defending against unidentifiable attacks in electric power grids[J]. IEEE Transactions on Parallel and Distributed Systems，2013，24(10)：1961-1971.

[95] Kim J，Tong L，Thomas R J. Data framing attack on state estimation[J]. IEEE Journal on Selected Areas in Communications，2014，32(7)：1460-1470.

[96] Kim J，Tong L，Thomas R J. Subspace methods for data attack on state estimation：a data driven approach[J]. IEEE Transactions on Signal Processing，2015，63(5)：1102-1114.

[97] 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.

[98] Chakhchoukh Y，Ishii H. Coordinated cyber-attacks on the measurement function in hybrid state estimation[J]. IEEE Transactions on Power Systems，2015，30(5)：2487-2497.

[99] Liu X，Zhu P，Zhang Y，et al. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure[J]. IEEE Transactions on Smart Grid，2015，6(5)：2435-2443.

[100] Chen P Y，Yang S，McCann J，et al. Detection of false data injection attacks in smart-grid systems[J]. IEEE Communications Magazine，2015，53(2)：206-213.

[101] Srikantha P，Kundur D. A DER attack-mitigation differential game for smart grid security analysis[J]. IEEE Transactions on Smart Grid，2016，7(3)：1476-1485.

[102] Liu S，Mashayekh S，Kundur D，et al. A framework for modeling cyber-physical switching attacks in smart grid[J]. IEEE Transactions on Emerging Topics in Computing，2013，1(2)：273-285.

[103] Farraj A，Hammad E，Al Daoud 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.

收稿日期：2015-09-28。

作者简介：

朱杰

朱杰(1990)，男，博士研究生，研究方向为电力系统网络安全、电力系统状态估计和智能电网，E-mail：jiezhu2013@163.com；

张葛祥(1974)，男，教授，博士生导师，研究方向为智能电网、电气信息与控制和模式识别，E-mail：zhgxdyan@126.com；

王涛(1987)，女，博士研究生，研究方向为电力系统故障诊断和智能电网；

赵俊博(1989)，男，博士研究生，研究方向电力系统状态估计和电力系统运行与控制。

（责任编辑　李兰欣）