文章编号：2095-2163(2022)06-0121-06 中图分类号：TM711 文献标志码：A

电力 CPS 中的虚假数据注入攻击

鲁 杰[1]，杨 超[1]，杜刃刃[2]，伍 虹[1]
（1 贵州大学 电气工程学院，贵阳 550025；2 贵州电网有限责任公司贵安供电局，贵阳 550000）

摘 要：随着智能化、信息化的加速发展，信息网络技术已经应用到电力工业的各个方面，形成电力信息物理系统。电力能源是一种关乎国计民生的重要资源，对国民经济的健康稳步发展具有重要意义。然而，信息层与物理层相融合，在为电力工业带来智能化便利的同时，面临的网络安全风险也随之升高，虚假数据注入攻击便是电力信息物理系统面临的安全隐患之一。在新时代建设坚强智能电网的背景下，考虑电网安全问题尤为突出。为此本文从电力信息物理系统的物理层面出发，归纳整理了发电、输电、配电、用电四个环节中存在的虚假数据注入攻击问题，以便深入了解每个环节面临的安全风险，从而有针对性地研究相应的保护防御措施。

关键词：信息物理系统；网络攻击；虚假数据注入攻击；坚强智能电网

False data injection attack in power CPS

LU Jie[1], YANG Chao[1], DU Renren[2], WU Hong[1]
(1 College of Electrical Engineering, Guizhou University, Guiyang 550025, China;
2 Gui′an Power Supply Bureau, Guizhou Power Grid Co., Ltd., Guiyang 550000, China)

【Abstract】With the accelerated development of intelligence and informatization, information network technology has been applied into all aspects of power industry, therefore power information physical system has been formed. Electric energy is an important resource related to the national economy and the people´s livelihood, which is of great significance to the healthy and steady development of the national economy. However, the integration of information layer and physical layer not only brings intelligent convenience to the power industry, but also increases the network security risk. False data injection attack is one of the security hidden dangers faced by the power information physical system. In the context of building a strong smart grid in the new era, considering the security of power grid is particularly prominent. Therefore, starting from the physical level of power information physical system, this paper summarizes the false data injection attack problems in the four links such as power generation, transmission, distribution and power consumption, so as to have an in-depth understanding of security risks faced by each link, pointedly study the corresponding protection and defense measures.

【Key words】information physics system; network attack; false data injection attack; strong smart grid

0 引 言

随着 3C 技术的飞速发展，如今物理世界与网络世界的交互越来越频繁、耦合程度越来越深，由此发展成信息物理系统[1]（Cyber-Physical Systems，CPS）。CPS 的本质是信息网络与物理世界相融合，发展成一系列复杂、多学科、有物理意识的下一代工程系统[2]，其应用领域十分广泛，如交通、能源、医疗、军事、移动教育等。在这些应用领域中，信息物理系统与电力工业相结合，发展成为一种典型的 CPS 系统—电力 CPS，不仅发展得十分迅速，而且有着广泛应用和可观前景。

电力能源是一种关乎国计民生的重要资源，保障电力的可靠供应对国民经济的健康稳步发展有着重大作用。然而，信息层与物理层相融合，在为电力工业带来智能化便利的同时，其面临的网络安全风险也不断增加。同时，在新时代建设坚强智能电网的背景下，电网安全问题尤为突出，网络攻击就是重大的安全隐患之一。由于电网与信息网络的紧密联系，信息网络存在的安全风险也可能渗透到电网物理层，严重威胁电网安全稳定运行。多年以来，由于网络攻击等原因给电网运行造成了严重的事故，对国家的经济发展也带来过重大损失。作为网络攻击的方式之一，虚假数据注入（False Data Injection，FDI）攻击对电力 CPS 的危害不容忽视，因而研究电力 CPS 中的虚假数据注入攻击具有重要意义。

基金项目：贵州省科学技术基金（黔科合基础[2019]1100）。

作者简介：鲁 杰（1997-），男，硕士研究生，主要研究方向：智能电网虚假数据注入攻击检测；杨 超（1971-），女，副教授，主要研究方向：配电网规划及电能质量管理；杜刃刃（1992-），男，硕士，副职调度监控员，主要研究方向：负荷识别；伍 虹（1998-），男，硕士研究生，主要研究方向：智能电网信息安全。

收稿日期：2021-12-11

本文从电力信息物理系统的物理层面出发,归纳整理了发电、输电、配电、用电四个环节中存在的虚假数据注入攻击问题,以利于深入了解每个环节面临的安全风险,从而有针对性地研究相应的保护防御措施。

1 电力信息物理系统

电力 CPS 是一个多维异构系统,具有 CPS 的复杂性与异构性,其体系结构[3]如图 1 所示。整个系统利用先进的计算机技术、通信技术以及控制技术,对系统的关键变量和状态进行实时监测监控,涵盖了电力系统中发、输、变、配及用电等重要环节,并将监测信息及时传送至控制中心进行科学分析,最后由控制中心下达精准的操作控制指令,实现系统整体性能最优化和系统安全稳定运行,保障能源的可靠供应。

除了具有一般 CPS 的基本特性之外,电力 CPS 还具备一些独有特性[2]:高可靠性、高可预测性、高可持续性、高安全性和高互操作性等。这是因为电力系统外部存在很多不确定性和各种干扰,给维持系统稳定和调节电压、频率带来了极大的挑战,从而要求系统中的元件能够实时协同工作,以保证系统安全、稳定、可靠。在电力 CPS 中,系统更加地智能化,同时因其开放程度提高而面临的安全问题也更加突出,为抵御风险,保持网络稳定性、功能的连通性和动态依赖性比任何其他工程网络都更为重要,必须严格地执行时间临界控制并保持稳定,才能在面临不确定性和扰动时也同样得到不间断的能源供应。

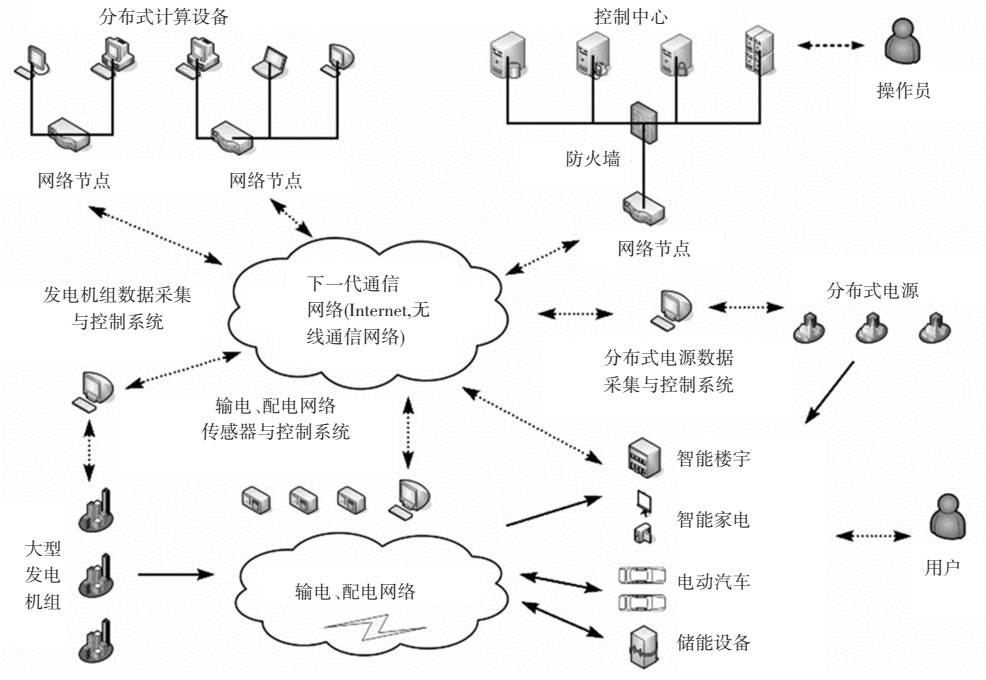

图 1 电力信息物理系统结构图

Fig. 1 Structure diagram of power information physical system

2 虚假数据注入攻击原理

2009 年,Liu 等人[4]首次提出 FDI 攻击的概念,指出攻击者在了解电力系统配置等相关信息的情况下,可以向实际测量结果中注入恶意虚假数据,且能成功绕过现有的任何不良数据检测技术而不被发现。这是因为现有的不良数据检测技术都依赖于同一个假设:“当出现错误的量测数据时,观测到的测量值与其对应的估计值之差的平方会出现明显的变化”。然而,精心构造 FDI 攻击,可以篡改测量值而不违反上述假设,从而躲避检测不被发现。

为更加透彻了解 FDI 攻击,利用电力系统直流状态估计模型来阐述其基本原理。

假设有 m 个量测量 $z_1,z_2,\cdots,z_m$,n 个状态变量 $x_1,x_2,\cdots,x_n$,则直流状态估计下量测量与状态变量之间的关系式可表示为:

$$\boldsymbol{z} = \boldsymbol{Hx} + \boldsymbol{e} \tag{1}$$

其中,$\boldsymbol{H}$ 为 $m \times n$ 的雅克比矩阵,$\boldsymbol{e}$ 为 m 维量测误差向量。

系统残差表示为:

$$r = \| z - H\hat{x} \|_2 < \tau \tag{2}$$

其中，τ 为检测阈值。

在没有 FDI 攻击的正常情况下，式(2)所表示的残差方程成立，表明系统没有不良数据出现。

在发生 FDI 攻击时，假定与量测 z 同维数的攻击向量为 $a = [a_1, a_2, \cdots, a_m]^T$，攻击发生后，量测值变为 $z_a = z + a$；若 $c = [c_1, c_2, \cdots, c_n]^T$ 为由攻击所引起的状态变量误差向量，则状态估计向量为 $\hat{x}_a = \hat{x} + c$。系统残差公式变为：

$$r_a = \| z_a - H\hat{x}_a \|_2 = \| (z + a) - H(\hat{x} + c) \|_2 = \| (z - H\hat{x}) + (a - Hc) \|_2 \tag{3}$$

当注入攻击向量 $a = Hc$ 时，得到式(4)：

$$r_a = \| z_a - H\hat{x}_a \|_2 = \| z - H\hat{x} \|_2 = r \tag{4}$$

由此可见，在这种 FDI 攻击下仍有 $r_a = r$，使式(2)成立，意味着系统在受到恶意攻击之后仍能躲避不良数据检测技术而不被发现，从而对系统安全产生严重威胁。

3　电力 CPS 中的虚假数据注入攻击

本节着眼于电力 CPS 中发、输、配、用电 4 个环节，归纳整理每一环节中存在的一些虚假数据注入攻击。

3.1　发电侧的攻击

电力 CPS 中，常见的攻击形式有篡改自动发电控制(automatic generation control，AGC)系统的采集数据和破坏数据传输等。AGC 是一个高度自动化、只需少量人工监督和干预的闭环控制系统，包含经济调度控制和负荷频率控制。通过调节控制发电机出力、维持发电与负荷的实时平衡、完成区域间按计划进行功率交换，AGC 可以维持系统功率平衡和频率稳定，实现发电计划追踪、区域调节控制等。AGC 要实现系统状态监测与控制指令下发等诸多功能，离不开网络通信设施与遥测数据，因而，网络攻击对其运行效果会产生直接的影响。

在针对 AGC 的 FDI 攻击中，攻击者的主要攻击对象有 3 类：功率和频率量测、仅功率量测和区域控制偏差[5]。Ashok 等人[6]考虑了 2 种基于数据完整性的秘密攻击模型：缩放攻击与斜坡攻击。其中，缩放攻击会立即导致系统频率偏离正常工作频率，其攻击矢量涉及基于缩放攻击参数的联络线功率流测量值的缩放，然后计算出相应的恶意频率测量值。斜坡攻击的攻击向量包括基于斜坡攻击参数按规律变化到联络线功率测量值的时变斜坡信号，并计算相应的恶意频率测量，以引起系统频率的缓慢偏移。Huang 等人[7]介绍了 3 种典型的攻击模型：

(1)重放攻击。实施此种攻击前，在一段时间内，攻击者记录正常操作条件下的测量值；在实施该攻击的过程中，攻击者将之前记录的测量值注入到传感器中，用以取代当前传感器的实际测量值，并传送至控制中心。

(2)噪声注入攻击。在这种攻击模式下，通用传感器向实际测量值添加一个有界随机值，再将其传输给控制中心。

(3)失稳攻击。在失稳攻击中，假定区域自动发电控制系统中有传感器受损，该受损传感器传输了一组测量序列，这个序列可看作是实际测量序列的过滤版本，如此失稳攻击包括将这个过滤版本序列注入系统，使原始系统变得不稳定。

Sridhar 等人[8]探讨了智能攻击对 AGC 的潜在影响，并提出了一个将攻击弹性控制应用于电力系统的通用框架，该框架采用基于异常的 IDS 和缓解措施，以在攻击期间保持系统稳定性，作为智能攻击检测和缓解的组成部分。Alhalali 等人[9]设计了一种以传感器为攻击目标的攻击模型，其攻击向量对量测变量表现为附加干扰，从而得到一个具有冗余度量和攻击的 AGC 模型。Law 等人[10]提出了一种智能电网安全的博弈论方法，使用随机(马尔可夫)安全博弈对攻击者-防御者的交互进行建模，并指定了一个非正式的风险模型，将博弈和风险模型应用于自动发电控制，讨论了基于这种模型下的攻击。Wu 等人[11]介绍了共振攻击，这是一种简单而强大的 LFC 发电系统攻击类型。在共振攻击中，攻击者巧妙地根据共振源、例如频率变化率修改发电厂的输入，以产生 LFC 发电系统的反馈，从而使发电厂的状态迅速变得不稳定。该攻击具有非常低的计算成本和通信成本，很容易在类似智能电子设备这种资源有限的设备中发起此种攻击。Tan 等人[12]重点讨论了针对 AGC 所需传感器数据的 FDI 攻击，并推导了一个攻击影响模型，进而分析了一种最优攻击，该最优攻击可以通过一种有效的线性规划算法来进行计算。这种攻击由一系列 FDI 组成，该 FDI 可将中断补救措施开始之前的剩余时间减至最少，从而使电网能够在最短的时间内进行反击。攻击者可以根据窃听的传感器数据和一些系统常数秘密学习攻击影响模型，并利用学习的模型来计算最佳攻

击。

3.2 输电侧的攻击

FDI 攻击作为网络攻击的形式之一,攻击者如果了解输电侧系统配置等相关信息的情况下,可以向 SCADA 系统中的实际测量结果注入恶意虚假数据,且能成功绕过现有的任何不良数据检测技术而不被发现。这种攻击经过了攻击者的精心策划,具有极高的隐蔽性,是系统运行中客观存在的潜在威胁,甚至会造成大停电事故。

Anwar 等人[13]在任何电力系统拓扑结构和电气参数未知的情况下,仅利用具有高斯噪声的测量数据就成功地构造出 FDI 攻击向量,并提出了一种有利于攻击者规避粗误差问题和构造隐形攻击的技术。Deka 等人[14]设计了一种隐蔽数据攻击模型,攻击者通过破坏电网中测量装置的量测值,从而使一组关键状态变量产生误差,并且这种误差不能被检测到。为了防止这种隐蔽攻击,研究中假设在攻击者受资源约束和不受资源约束两种情况下,提出了一种贪婪保护算法。

Li 等人[15]针对 FDI 攻击绕过坏数据检测模块,分析了防护策略,并讨论了稀疏攻击和安全度量的寻找方法,构建了利用状态变量分布检测虚假数据的检测器。Liu 等人[16]提出一种新的攻击模型,这种攻击不需要获取全部区域的信息,只用了解到想要攻击的局部目标区域信息即可成功发起攻击,且不会被现有的不良数据检测技术发现。Liu 等人[17]提出一种有效策略来确定最优攻击区域,并介绍了智能电网网络安全研究的一个新前沿:通过获取较少的网络信息来确定可行的攻击区域。Yu 等人[18]提出了一种盲假数据攻击模型,攻击者在这种攻击模型中没有获取电网拓扑相关知识,并在直流潮流模型和交流潮流模型中验证了这种攻击的有效性。Kim 等人[19]提出了 2 种攻击策略。第一种策略是通过在系统子空间中隐藏攻击向量来直接影响系统状态;第二种策略误导坏数据检测机制,从而删除未受攻击的数据。研究提出的子空间方法从测量中学习系统运行子空间并据此发起攻击,在完全测量模型和部分测量模型下,得到了不可见子空间攻击存在的条件。Zhang 等人[20]在综合风电场 SCADA/EMS 系统架构中,考虑了涉及网络组件或网络的网络攻击场景,采用 2 个贝叶斯攻击图模型来表示网络攻击成功的过程,并对风电场 SCADA/EMS 系统的成功网络攻击频率进行了估计,通过仿真结果表明,随着风电场 SCADA/EMS 系统攻击成功率和攻击者技能水平的提高,系统整体可靠性降低。Zhao 等人[21]面对非线性电力系统状态估计问题,通过引入攻击矢量松弛误差,并确定了松弛误差的上界,在考虑单状态变量攻击和多状态变量攻击两种情况下,提出了一种不完美的虚假数据注入攻击模型及其相应的预测辅助实现方法。最后仿真结果表明该方法对非线性模型和直流模型都有很好的效果。Hug 等人[22]针对 SCADA 系统进行交流状态估计时因坏数据检测模块存在漏洞而有潜在的虚假数据注入网络攻击问题,介绍了一种新的分析技术,该技术可以利用系统的物理特性作为保护而使电力系统免受此类攻击。Anwar 等人[23]定义攻击目标能源系统效率和攻击目标能源系统稳定性两种不同的攻击策略。Deng 等人[24]提出一种基于有限输电线电纳信息的 FDI 攻击,攻击者在知道与总线相关的每条输电线路的电纳信息时,可以发动 FDI 攻击来修改总线状态变量。

3.3 配电侧的攻击

随着传统配电网向主动配电网转变的速度越来越快,配电侧面临的信息网络安全风险日益增加。配电侧的主要功能是把优质的电能输送至用户端,这一过程中主要有 3 个场景容易遭受到恶意攻击:AMI 系统、配电自动化设备和分布式电源管理。

除了在上述攻击场景中,针对配电网状态估计的 FDI 攻击研究,Isozaki 等人[25]考虑了多个光伏系统接入时网络攻击对配电系统电压调节的影响,此外,研究了试图降低具有过电压保护功能的光伏系统输出功率的攻击。Deng 等人[26]针对配电系统的状态估计,提出了一个实用的 FDI 攻击模型,攻击者可以基于潮流或注入量测来近似系统状态,从而不需要付出很高的代价就可以获取系统状态。实验表明这种攻击即使是在近似的系统状态下,也更有可能破坏状态估计而不被检测到。魏书珩等人[27]提出一种针对三相不平衡配电网状态估计的 FDI 攻击方法,并在 2 种运行场景下进行仿真,结果表明这种攻击方法能够成功避开坏数据检测模块,达到篡改状态估计结果的。Liu 等人[28]针对智能量测终端注入病毒进行数据篡改,通过影响公共数据中心造成能量管理及预测系统混乱的配电侧攻击。

3.4 用电侧的攻击

在用电侧,由于传统的分时电价和阶梯电价机制存在突出的缺陷,无法精确统计、充分反映短时间内电力用户的负荷需求变化,为此引入实时电价(Real-Time Price,RTP)机制。实时电价在定价时

以小时或分钟来划分时段，短时间内能够精确反映电力供应商电价与电力用户负荷需求之间的弹性关系，同时具备高节能性和能源利用率。实时电价机制的引入，在带来优势的同时，也存在着潜在的安全威胁，用电侧本身具有用电行为多样化等特点，是一个复杂的环境，其面临的网络攻击风险更加严峻。

有一种针对用电侧实时电价的新型 FDI 攻击：实时电价攻击（Real-Time Price Attacks，RTPA）。该攻击以截获并伪造实时电价信号为手段，增加电力用户总负荷需求为途径，进而破坏整个电力市场的发电-用电平衡。Dayaratne 等人[29]提出了一种新的 FDI 攻击，该攻击针对需求响应注入虚假数据，能够获得更低的电力成本，并评估了攻击者如何使用有针对性的战略数据完整性攻击，以达到基于实时定价方案获得经济利益的目的。TAN 等人[30]采用控制理论的方法研究了缩放攻击和延迟攻击对实时电价系统稳定性的影响，得出结论：为了使 RTP 系统不稳定，攻击者有必要在缩放攻击中降低消费者的价格，或者在延迟攻击中降低消费者价格的一半以上。Giraldo 等人[31]在已有研究的基础上考虑了一个更现实的攻击模型。该模型中，攻击者可以在价格信号中注入微小的变化，以此增加产生和消耗能量之间的差异，这种模型不受缩放或延迟攻击的限制，但可以生成任意的定价信号。Jia 等人[32]假设攻击者可以访问有限的量测装置，并且有能力根据这些装置仪器的观测值构建数据攻击。在此基础上，采用基于电网状态空间上实时 LMPs 的几何表征，引入一个几何框架，考虑几种不同的观测场景，模拟攻击者不同级别的攻击，并得到最优数据攻击的上界和下界。王小山等人[33]提出一种新的电价策略，这种电价策略可以抵御时延攻击，为电力供应商与电力用户之间建立动态模型。邹逢飞[34]针对 RTPA 定义了户内能源管理系统（HEMS），并提出 2 种防御策略：一是基于双人零行列式的防御策略，该策略与 HEMS 相结合可以削减电力用户的期望负荷需求；二是基于多人零行列式的防御策略，该策略中有电力供应商参与博弈，不仅可以优化 HEMS 的行为状态选择，而且削减电力用户期望负荷需求的效果比第一种策略更好。陈刘东等人[35]通过分析需求侧 FDI 攻击的脆弱性，针对互动需求响应的 FDI 攻击，运用启发式算法求解主从博弈问题，从而采用主从博弈来构建攻击模型。Raman 等人[36]表明攻击者可以利用虚假通信信息来操纵用户行为，从而对系统稳定性造成极大的影响。

4　结束语

通过历年电网遭遇网络攻击的相关事件，网络攻击对电网的影响引起高度关注。简要介绍了电力 CPS 和虚假数据注入攻击原理，着重从电力 CPS 发、输、配、用电四个环节出发，归纳整理各个环节存在的 FDI 攻击，以便深入了解不同环节所面临的攻击形式，为研究有针对性的防御保护措施提供有益参考，从而加快了建设坚强智能电网的工作步伐。

参考文献

[1] 汤奕，王琦，倪明，等. 电力信息物理融合系统中的网络攻击分析[J]. 电力系统自动化，2016，40(06)：148-151.

[2] 孙帝. 电力信息物理系统虚假数据注入攻击检测研究[D]. 南宁：广西大学，2021.

[3] 赵俊华，文福拴，薛禹胜，等. 电力 CPS 的架构及其实现技术与挑战[J]. 电力系统自动化，2010，34(16)：1-7.

[4] LIU Yao，NING Peng，REITER M K. False data injection attacks against state estimation in electric power grids [J]. Acm Transactions on Information & System Security，2009，14(1)：21-32.

[5] 徐飞阳，薛安成，常乃超，等. 电力系统自动发电控制网络攻击与防御研究现状与展望[J]. 电力系统自动化，2021，45(03)：3-14.

[6] ASHOK A，SRIDHAR S，MCKINNON A D，et al. Testbed-based performance evaluation of attack resilient control for AGC [C] //IEEE 2016 Resilience Week. Chicago，USA：IEEE，2016：125-129.

[7] HUANG T，SATCHIDANANDAN B，KUMAR P R，et al. An online detection framework for cyber attacks on automatic generation control [J]. IEEE Transactions on Power Systems，2018，33(6)：6816-6827.

[8] SRIDHAR S，GOVINDARASU M. Model-based attack detection and mitigation for automatic generation control [J]. IEEE Transactions on Smart Grid，2014，5(2)：580-591.

[9] ALHALALI S，NIELSEN C，EL-SHATSHAT R. Mitigation of cyber-physical attacks in multi-area automatic generation control [J]. International Journal of Electrical Power & Energy Systems，2019，112：362-369.

[10] LAW Y W，ALPCAN T，PALANISWAMI M. Security games for risk minimization in automatic generation control [J]. IEEE Transactions on Power Systems，2015，30 (1)：223-232.

[11] WU Yongdong，WEI Zhuo，WENG Jian，et al. Resonance attacks on load frequency control of smart grids[J]. IEEE Transactions on Smart Grid，2018，9(5)：4490-4502.

[12] TAN Rui，NGUYEN H H，EDDY Y F，et al. Modeling and mitigating impact of false data injection attacks on automatic generation control[J]. IEEE Transactions on Information Forensics and Security，2017，12(7)：1609-1624.

[13] ANWAR A，MAHMOOD A N. Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors[C] // 2016 IEEE Power and Energy Society General Meeting(PESGM). Boston，USA：IEEE，2016：1-5.

[14] DEKA D，BALDICK R，VISHWANATH S. Data attack on

strategic buses in the power grid: design and protection[C] // 2014 IEEE PES General Meeting | Conference & Exposition. National Harbor, MD, USA:IEEE,2014:1-5.
[15] LI Yuancheng, WANG Yiliang. State summation for detecting false data attack on smart grid [J]. International Journal of Electrical Power & Energy Systems, 2014(57): 156-163.
[16] LIU Xuan, LI Zuyi. Local load redistribution attacks in power systems with incomplete network information [J]. IEEE Transactions on Smart Grid, 2014, 5(4): 1665-166.
[17] LIU Xuan, BAO Zhen, LU Dan, et al. Modeling of local false data injection attacks with reduced network information[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686-1696.
[18] YU Zonghan, CHIN Wenlong. Blind false data injection attack using PCA approximation method in smart grid [J]. IEEE Transactions on Smart Grid, 2015, 6(3): 1219-1226.
[19] KIM J, TONG Lang, 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.
[20] ZHANG Yichi, XIANG Yingmeng, WANG Lingfeng. Power system reliability assessment incorporating cyber attacks against wind farm energy management systems[J]. IEEE Transactions on Smart Grid, 2017, 8(5):2343-2357.
[21] ZHAO Junbo, ZHANG Gexiang, DONG Zhaoyang, et al. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation[J]. IEEE Transactions on Smart Grid, 2016, 7(1): 6-8.
[22] 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.
[23] ANWAR A, MAHMOOD A N, AHMED M. False data injection attack targeting the LTC transformers to disrupt smart grid operation[M]//TIAN J, JING J, SRIVATSA M. International Conference on Security and Privacy in Communication Networks. SecureComm 2014. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham:Springer, 2015,153: 252-266.
[24] DENG Ruilong, LIANG Hao. False data injection attacks with limited susceptance information and new countermeasures in smart grid[J]. IEEE Transactions on Industrial Informatics, 2019, 15(3): 1619-1628.
[25] ISOZAKI Y, YOSHIZAWA S, FUJIMOTO Y, et al. Detection of cyber attacks against voltage control in distribution power grids with PVs[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 1824-1835.
[26] DENG Ruilong, ZHUANG Peng, LIANG Hao. False data injection attacks against state estimation in power distribution systems[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 2871-2881.
[27] 魏书珩, 徐俊俊, 吴在军,等. 针对三相不平衡配电网状态估计的虚假数据注入攻击方法[J]. 高电压技术, 2021, 47(07): 2367-2377.
[28] LIU Xiaoxue, ZHU Peidong, ZHANG Yan, 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.
[29] DAYARATNE T, RUDOLPH C, LIEBMAN A, et al. High impact false data injection attack against real-time pricing insmart grids[C] //2019 IEEE PES Innovative Smart Grid Technologies Europe(ISGT-Europe). Bucharest, Romania:IEEE,2019:1-5.
[30] TAN Rui, KRISHNA V B, YAU D K Y, et al. Integrity attacks on real-time pricing in electric power grids[J]. ACM Transactions on Information & System Security, 2015, 18(2): 5.
[31] GIRALDO J, CARDENAS A, QUIJANO N. Integrity attackson real-time pricing in smart grids: impact and countermeasures[J]. IEEE Transaction on Smart Grid, 2016, 81(4): 1-9.
[32] JIA Liyan, THOMAS R J, TONG Ling. Impacts of malicious data on real-rime price of electricity market operations[C]//2012 45th Hawaii International Conference on System Sciences. Maui, HI, USA:IEEE Computer Society, 2012: 1907 - 1914.
[33] 王小山, 石志强, 任建军,等. 智能电网中实时电价的抗时延攻击策略[J]. 北京邮电大学学报, 2015, 38(S1): 116-120.
[34] 邹逢飞. 基于零行列式的实时电价攻击防御策略研究[D]. 长沙:长沙理工大学, 2018.
[35] 陈刘东, 刘念. 面向互动需求响应的虚假数据注入攻击及其检测方法[J]. 电力系统自动化, 2021, 45(03): 15-23.
[36] RAMAN G, PENG J C, RAHWAN T. Manipulating residents' behavior to attack the urban power distribution system[J]. IEEE Transactions on Industrial Informatics , 2019 , 15(10): 5575-5587.

(上接第 120 页)

[4] LOZANO-PEREZ T. Spatial planning: A configuration space approach[J]. IEEE Transactions on Computers, 1983,C-32(2): 108-120.
[5] 贾庆轩,陈钢,孙汉旭,等. 基于 A*算法的空间机械臂避障路径规划[J]. 机械工程学报,2010,46(13):109-115.
[6] Lavalle S M. Rapidly-exploring random trees:A new tool for path pl-anning [J]. Algorithmic & Computational Robotics New Directions,1998:293-308.
[7] 姜力,周扬,孙奎,等. 七自由度冗余机械臂避障控制[J]. 光学精密工程,2013,21(07):1795-1802.
[8] 齐志刚,黄攀峰,刘正雄,等. 空间冗余机械臂路径规划方法研究[J]. 自动化学报,2019,45(06):1103-1110.
[9] SAKATA H, NG T, MACK B. Collision avoidance system concept for mobile servicing system[C]// Proceedings IROS'91: IEEE/RSJ International Workshop on Intelligent Robots and Systems'91. Osaka, Japan:IEEE, 1991: 1641-1646.
[10] 徐文福,刘宇,强文义,等. 自由漂浮空间机器人的笛卡尔连续路径规划[J]. 控制与决策,2008,23(03):278-282.