面向电力信息物理系统的虚假数据注入攻击研究综述

王 琦[1] 邰 伟[1] 汤 奕[1] 倪 明[2,3,4]

摘 要 随着电力信息通信技术的发展与应用, 电力流与信息流深度融合, 共同实现对系统的全景状态感知与控制决策, 电力系统转变成典型的信息物理系统 (Cyber physical system, CPS). 开放的通信环境与复杂的信息物理耦合交互过程, 使得信息安全风险成为影响电力系统安全稳定运行的重要因素. 其中, 虚假数据注入攻击 (False data injection attack, FDIA) 通过破坏网络数据完整性以干扰控制决策, 是一种典型的网络攻击方式. 本文针对面向电力 CPS 的虚假数据注入的攻击过程和防御手段进行了分析与总结. 从攻击者视角分析了 FDIA 的攻击目标、策略及后果; 从防御者视角总结了保护与检测环节中的各类方法; 最后基于联合仿真技术, 提出了针对虚假数据攻防过程建模和评估的电力 CPS 联合攻防平台.

关键词 信息物理系统, 虚假数据注入, 安全监控, 联合仿真

引用格式 王琦, 邰伟, 汤奕, 倪明. 面向电力信息物理系统的虚假数据注入攻击研究综述. 自动化学报, 2019, **45**(1): 72−83

DOI 10.16383/j.aas.2018.c180369

A Review on False Data Injection Attack Toward Cyber-physical Power System

WANG Qi[1] TAI Wei[1] TANG Yi[1] NI Ming[2,3,4]

Abstract With the development and application of information communication technology, the power flow and the information flow are becoming deeply integrated in order to achieve panoramic state awareness and control decision. Therefore the power system has been transformed into a typical cyber-physical system (CPS). Considering the open communication environment and complex cyber physical coupling mechanism, the information risk has become an important issue posing severe threats to the secure operation of power systems. False data injection attack (FDIA), as a typical attack mode destroying data integrity, can interfere with the control decision. In this paper, the attack process and defense method of false data injection are analyzed and summarized. Firstly, from the perspective of attackers, the goals, strategies and consequences of FDIA are comprehensively discussed. Then, from the perspective of defenders, the protection and detection countermeasures are discussed. Finally the co-simulation technology is utilized to construct associated attack-defense platform of cyber-physical power system (CPPS), which is aimed at modeling and assessment of the attack and defense processes of false data injection.

Key words Cyber physical system (CPS), false data injection, security supervisory and control, co-simulation

Citation Wang Qi, Tai Wei, Tang Yi, Ni Ming. A review on false data injection attack toward cyber-physical power system. *Acta Automatica Sinica*, 2019, **45**(1): 72−83

随着智能电网建设的不断推进, 先进的感知、计算、通信与控制技术在电力系统中得到深入应用[1−2]. 传统电力系统逐渐与信息控制设备和通信传感网络深度融合, 形成电力信息物理系统 (Cyber physical system, CPS)[3−5]. 在促进电力资源高效配置、实时分析、科学决策的同时, 通信网络和信息设备中的安全漏洞也带来了潜在威胁[6−7].

电力通信网络作为电力工控系统的专用网络, 具有安全分区、网络专用、横向隔离、纵向认证的特点, 长期以来被认为具备较强的安全性和可靠性[8]. 因此与相对健壮的电力一次系统相比, 针对电力信息通信系统的安全防护研究起步较晚. 目前针对电力系统网络攻击实例的研究表明, 由于规划和运行管理漏洞的存在, 物理隔离并不能保证电力 CPS 的绝对安全[9−10]. 作为针对基础工控设施的新型攻击方式, 网络攻击已成为电力系统安全稳定运行不容忽视的威胁, 其攻击机理、防御手段及相应的系统安全态势评估方法亟待深入研究[11−12].

收稿日期 2018-05-30 录用日期 2018-09-05
Manuscript received May 30, 2018; accepted September 5, 2018
国家重点研究发展计划 (2017YFB0903000), 国家自然科学基金 (51577030, 51707032), 国家电网公司总部科技项目 (针对网络攻击的电网信息物理系统协同运行态势感知与主动防御方法研究) 资助
Supported by National Key Research and Development Program of China (2017YFB0903000), National Natural Science Foundation of China (51577030, 51707032), and the Project of State Grid Corporation of China (Research on Cooperative Situation Awareness and Active Defense Method of Cyber Physical Power System for Cyber Attack)
本文责任编委 孙秋野
Recommended by Associate Editor SUN Qiu-Ye
1. 东南大学电气工程学院 南京 210096 2. 南瑞集团 (国网电力科学研究院) 有限公司 南京 211000 3. 国电南瑞科技股份有限公司 南京 211000 4. 智能电网保护和运行控制国家重点实验室 南京 211000
1. School of Electrical Engineering, Southeast University, Nanjing 210096 2. NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211000 3. NARI Technology Co. Ltd., Nanjing 211000 4. State Key Laboratory of Smart Grid Protection and Control, Nanjing 211000

针对电力 CPS 的网络攻击可按攻击目标分为破坏信息可用性、完整性和保密性[13]. 其中, 虚假数据注入攻击 (False data injection attack, FDIA) 作为通过篡改测控数据以破坏电网信息完整性的攻击方式, 具有较强的可达性、隐蔽性与干扰性, 能够影响上层控制中心的分析决策, 造成严重后果, 是对电力系统威胁程度较高的攻击方式之一. 近年来世界范围内发生了多起大规模电力网络安全事故, 其中不乏利用数据篡改机制进行攻击的场景. 以乌克兰电网遭受的攻击为例, 攻击者向控制监控与数据采集 (Supervisory control and data acquisition, SCADA) 系统注入虚假数据和删改原有数据, 从而使得操作员与控制设备失去对系统的可观可控性, 故障大规模扩散且难以恢复[14−16].

传统 FDIA 的作用原理是利用状态估计器中不良数据辨识方法的局限性, 恶意篡改元件的量测值, 使控制中心误判电网当前状态, 继而造成电力系统安稳控制措施误动或拒动, 从而影响电力系统安全稳定运行[17−18]. 随着电力信息物理耦合程度的提升, FDIA 的涵义也进一步拓展, 从广义上讲, 以破坏电网稳定性或获取经济利益为目的, 通过恶意篡改电力信息设备中的测控数据而实施的攻击, 都可视为面向电力 CPS 的 FDIA.

本文归纳和分析了针对电力 CPS 的虚假数据注入攻击和防御过程中的关键问题与研究现状, 旨在揭示电力 CPS 网络安全漏洞, 分析潜在攻击途径, 继而构建有效防御方式. 在信息与电力层面分析攻防构建方式与作用效果, 并基于联合仿真技术提出了电力 CPS 网络安全攻防平台, 以实现虚假数据注入攻防交互过程的建模、仿真和分析.

1　FDIA 原理与建模方法

电力信息系统主要包括发电侧的发电厂监控信息系统、电网侧的 SCADA 系统、能量管理系统 (Energy management system, EMS)、电力市场运营管理系统和电能量计量系统, 以及用户侧的需求侧管理系统等, 如图 1 所示. 攻击者可能采用 FDIA 对上述系统中的电力生产、输配与市场信息进行篡改, 最终干扰电力应用业务[19]. 以图 1 中针对 SCADA 的 FDIA 为例, 攻击者可以通过量测单元、通信网络与控制设备等多途径注入虚假数据, 继而对电力业务实施后续攻击.

从数据流动方向追溯, 电力 CPS 涵盖了量测、通信、存储、处理、执行等多过程数据对象, 其一般应用入侵检测系统和防火墙等安全监视设备以保证数据的完整性, 如图 2 所示. 然而在实际电力紧急控

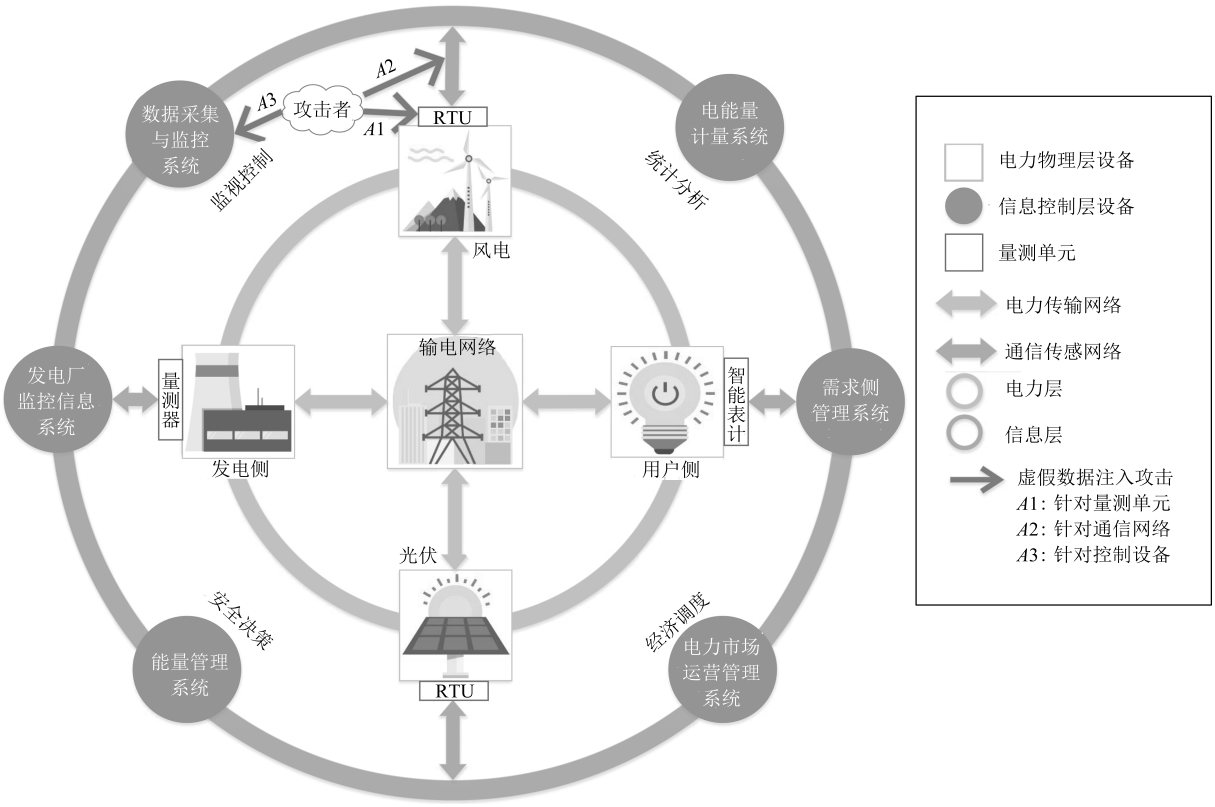

图 1　电力 CPS 结构图

Fig. 1　The framework of cyber physical power systems

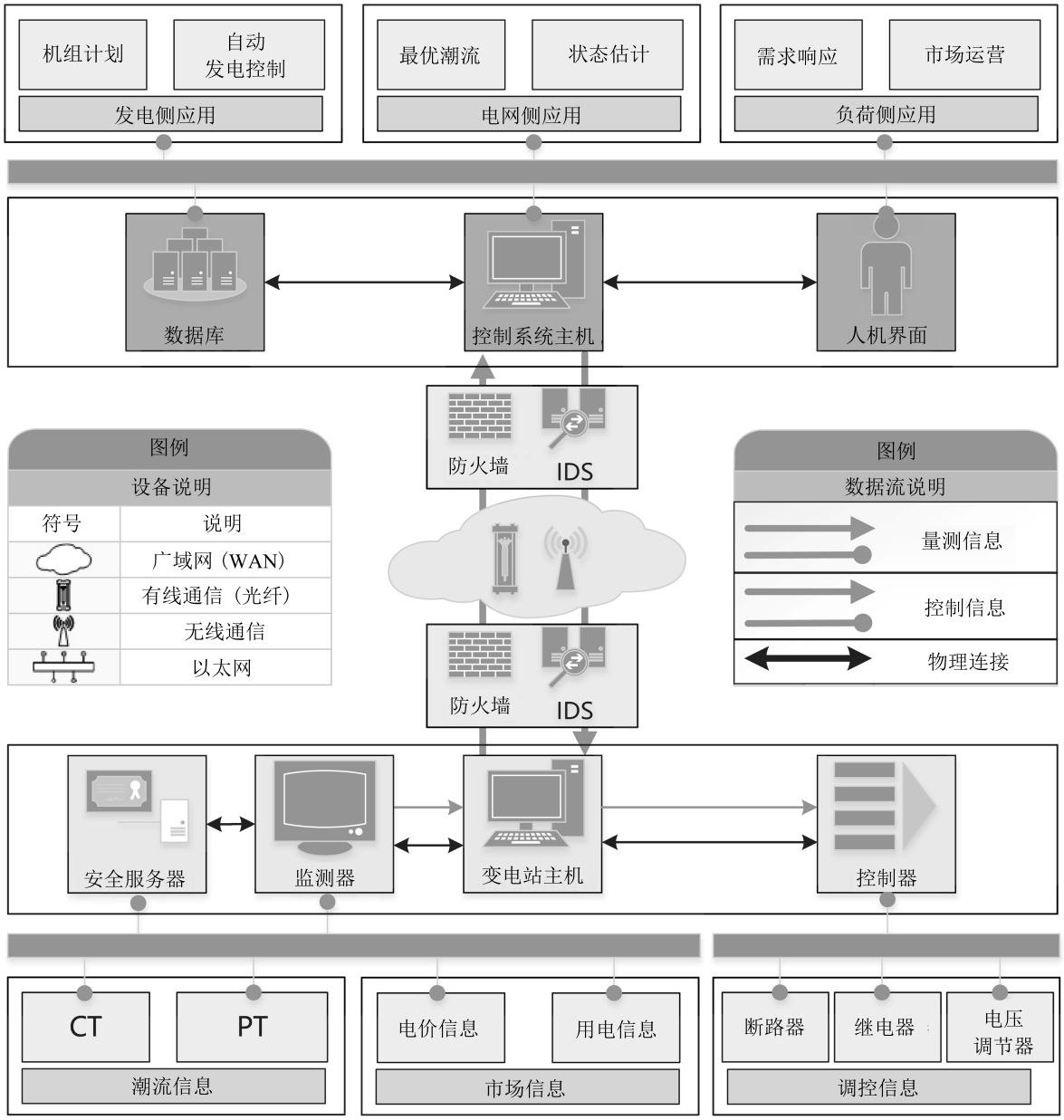

图 2 电力 CPS 安全监控架构

Fig. 2 The security supervisory and control architecture of CPPS

制业务的数据传输过程中, 由于快速响应需求, 相应的加密与检测环节的漏洞给 FDIA 提供了入侵路径.

1.1 面向电力 CPS 的 FDIA 过程分析

1.1.1 针对通信传感网络的 FDIA 过程

针对通信传感网络进行入侵以获得电力 CPS 信息侧可达性是 FDIA 的第一步, 入侵进程通常在数据采集与传输过程中实现. 依据入侵原理, 主要可以分为交互作用和植入系统等方式, 其中交互作用包括伪装、旁路控制、中间人和截听重放等攻击手段, 植入系统包括病毒木马、陷阱门和服务欺骗等攻击手段.

在数据采集过程中, 主要可以通过远程终端单元 (Remote terminal unit, RTU)、同步相量测量单元 (Phasor measurement unit, PMU) 和各类智能用户表计进行入侵. 攻击者需要利用设备加密认证机制的固有漏洞以实现数据篡改, 目前大部分攻击研究针对传统量测终端 RTU 进行入侵[20]. 文献 [21] 将 PMU 作为目标攻击量测单元, 攻击者利用 PMU 中的 GPS 漏洞进行时间同步攻击, 由于 GPS 信号没有任何加密或授权机制, 攻击者可以伪

造 GPS 信号以淹没正确数据. 文献 [22] 将智能电表作为攻击目标, 基于有色 petri 网建立了智能电表的威胁模型, 分析其中信息流的脆弱性.

为构建针对数据传输过程的入侵, 攻击者通过在量测单元到控制中心之间部署中间人等方式实现对通信传输过程的旁路控制, 从而在通信网中注入错误数据. 文献 [23] 通过劫持并扭曲传感器的输出, 从而篡改量测矩阵, 破坏状态估计器的完整性. 文献 [24] 分析了灰洞攻击对量测数据的影响, 通过在数据传输过程中丢弃 PMU 数据包, 造成系统可观性下降, 继而导致控制决策失误.

攻击者成功将错误数据注入到信息层后, 基于对电力系统运行、控制和保护业务的充分了解, 可以操纵电力物理过程[25].

1.1.2　针对电力控制系统的 FDIA 过程

电力系统控制中的量测数据通过传感器传输给控制系统 (例如 EMS) 中的状态估计器, 估计出系统的实时状态. 传感器量测数据不是完全准确的, 由于设备故障、传感器的偏移、错误连接、通信干扰等偶然因素会引起不良数据, 导致状态估计结果受到污染. 不良数据检测辨识方法的目的即为去除此类偶然随机不良数据, 目前成熟的算法主要是通过最大标准残差 (Largest normalized residual, LNR) 方法来检测. 与随机自然误差相比, 如果攻击者熟悉电力系统拓扑及状态估计算法, 那么精心设计的虚假数据可以满足线路拓扑与潮流约束, 避开不良数据辨识, 提升成功率.

状态估计算法可以分为静态和动态两种算法, 静态状态估计主要基于低采样频率的 RTU, 对系统某个时间断面的静态参数进行估计[26]; 相对于静态状态估计, 动态状态估计主要基于高采样频率的 PMU, 通常采取分布式并行算法, 依据滤波算法与系统历史信息, 对系统连续断面的状态信息与动态参数进行估计[27]. 对攻击者来说, 成功的关键在于利用已有的系统拓扑知识与攻击资源, 针对系统静态或动态状态估计算法, 设计最优的虚假数据向量, 两种情形下攻击者均需要综合攻击隐蔽性、攻击代价与量测冗余度, 确定成功实施攻击所需破坏的最少传感器量测值. 相对于静态状态估计, 针对动态算法的 FDIA 所需先验知识更加复杂, 攻击者需要依据攻击向量的时间相关性, 建立连续控制模型, 进行潜伏攻击, 提前获取系统状态变化特征, 以逃避基于历史数据的时间滤波检测算法, 但由于动态状态估计本身的不精确性, 给攻击者提供了较大的向量篡改范围.

1.2　虚假数据构建方法

由于系统量测信息需要遵循潮流规律, 篡改单一量测量难以躲过不良数据辨识环节, 攻击者需同时修改相关量测量以实施成功的 FDIA. 因此攻击构建目标之一就是寻找到最少需要被篡改的量测量. 如图 3 所示, 为了篡改线路 2-3 的潮流, 可以通过同时篡改节点 3 的电压和与节点 3 相邻线路节点的量测值来实现. 本文定义该最少量测量集合为目标篡改量测量的最小相关空间. 因此在攻击某一电力元件时, 需要对该元件最小相关空间的所有元件进行协同攻击, 保证该范围中的状态信息互洽, 符合系统潮流规律, 以满足状态估计约束.

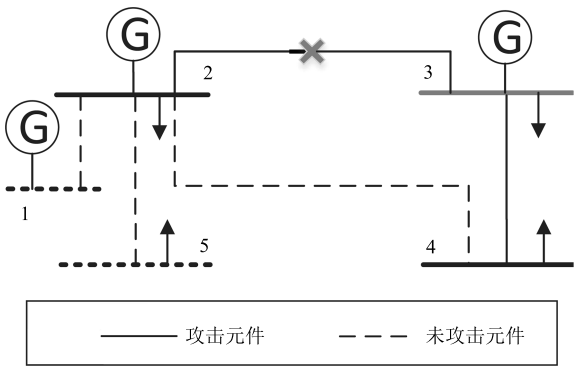

图 3　FDIA 最优攻击区域选取

Fig. 3　The optimal attack area of the FDIA

除了上述条件, 由于电力系统的运行特性, 数据篡改还需要满足以下约束条件:

1) 零注入节点不能作最小相关空间边界节点;

2) 平衡节点电压不能被攻击;

3) 系统各节点篡改后的量测值应满足历史数据预测特性、发电机实际特性等限制条件的要求;

4) 对存在冗余量测装置的区域, 攻击者需要篡改该区域内所有量测装置的数据.

理想情况下, 攻击者设法取得足够的权限, 准确获取系统完整信息, 包括实时状态量、电网拓扑及线路参数等信息, 同时可操纵一定数量的量测装置. 在此场景下, 攻击者可针对攻击策略的隐蔽性与后果进行有效评估, 从而实现最优的攻击过程[28]. 如果攻击者只能够掌握系统部分信息, 为成功构建 FDIA, 需要对部分未知信息进行估计, 尽可能缩小篡改后状态估计的残差. 该条件下攻击者可以通过主成分分析法或 Lagrange 最优乘子法等方法构建最优策略, 针对部分信息完善的区域进行局部攻击[29].

目前多数研究为简化问题的复杂度, 通常基于静态状态估计算法与完全信息情形. 在掌握部分信息与攻击资源的情形下, 如何构造攻击向量, 对电网造成最严重后果, 属于多项式复杂程度的非确定性问题, 需要进一步研究平衡计算资源和时间的攻击算法优化策略.

1.3 FDIA 影响后果分析

针对不同电力业务, FDIA 对系统影响主要包括经济调度与安全控制等方面[30].

1.3.1 经济调度后果

在以经济利益为目的的 FDIA 中, 攻击者的目标包括降低电网企业的经济效益和提高自身的不正当经济利益.

以安全约束经济调度 (Security constrained economic dispatch, SCED) 为目标说明 FDIA 对电网经济效益的破坏. SCED 作为生产调度算法, 综合考虑了机组燃料类型、能耗、机组启停费用、网损、污染物排放及电网安全等因素, 从而实现系统能耗最优或生产成本最优[31]. 攻击者通过对系统机组出力计划或负荷预测数据进行篡改, 从而导致系统对负荷平衡、机组运行和电网安全等约束条件产生误判, 最终增加系统能耗与设备损耗.

以获取经济利益为目标, 攻击者可以伪造线路阻塞级别, 通过电力市场的电价差或窃电行为来获利. 在文献 [32] 中, 攻击者利用恶意数据检测算法的缺陷, 针对 IEEE14 节点系统, 伪造两条线路堵塞进行虚拟竞价, 最终获得了 \$6.0/MWh 的经济套利. 文献 [33] 提出了电力系统的电价模型, 以 IEEE14 节点系统为例, 仿真得出由拓扑修改与量测修改导致的节点边际电价偏移值分别在 15 % 和 5 % 左右, 前者通过重构价格区间, 比后者篡改状态估计对电价的影响更为严重.

1.3.2 安全控制后果

在电力系统安全控制方面, 攻击后果可分为对系统可观可控性的影响和对安全稳定性的影响.

如果 FDIA 未能躲避不良数据检测, 那么被篡改的量测量将被作为不良数据剔除, 从而造成系统某区域不可观, 导致电力系统调度控制中心无法及时掌握不可观区域的实际运行状态, 从而引发系统后续运行风险[34−35].

当 FDIA 成功干扰量测估计值, 控制中心基于攻击者伪造的假象误以为电力系统进入紧急状态, 实行切机切负荷等保护措施. 电力系统拓扑结构发生变化, 可能引起连锁反应, 导致电力系统中其他输电线路真正过负荷, 扩大故障范围, 甚至引起严重的电力系统事故[36]. 在文献 [37] 中, 攻击者通过在正常的 PMU 数据中渗入大量错误数据, 导致误控制动作甚至停电事故. 在文献 [38] 中, 攻击者以重放攻击的形式注入虚假 PMU 测量数据, 从而屏蔽传输线真实故障信息, 引起系统潮流失稳和连锁故障.

对于攻击者来说, 依据注入的虚假数据类型, 会对电力系统造成不同的影响. 通过伪造节点电压幅值越限, 可能导致甩负荷甚至系统电压崩溃; 通过伪造线路过负荷, 可能导致线路故障和电力拓扑结构的变化; 如果攻击者同时掌握电力调度算法和电力市场交易信息, 则可通过发动 FDIA 扰乱电力市场的正常秩序, 获得不正当的经济利益.

2 FDIA 防御机理与建模方法

传统的信息安全模型主要考虑预警、保护、检测、响应、恢复和反击等环节. 针对电力网络安全, 需要针对电力 CPS 多层架构进行专门分析, 在信息层从传输通道、边界防护、主机和终端安全、数据安全等方面进行防御[39−40]; 在物理层从线路、设备、网络结构等方面进行防御. 电力 CPS 中包含大量电力一次设备、通信设备和信息处理控制设备, 由于电力一次设备侧是时变连续系统, 而信息侧为离散系统, 信息变化由事件触发, 因此两者时空特性和描述方法存在着本质不同.

在时间维度, 以电力业务数据分析为例, 由于数据的来源和业务重要度不同, 因而数据的采样频率和延时需求不同, 对不同来源和时间尺度的量测数据需要进行冗余性和合理性核查, 挖掘数据之间的相互关系, 进行互校核剔除错误数据, 提升数据质量, 形成多时间尺度的信息安全防御机制.

在空间维度, 一方面要保证信息空间的保密性、完整性与可用性, 另一方面要保证电力空间电压、频率、负荷供应等指标的稳定性. 需要通过风险由信息到物理的跨空间传播机制, 建立两者运行特征的关联匹配规则, 进行协同防御.

基于以上方法, 在时间上建立覆盖暂态、稳态和中长期动态全过程的防御体系, 在空间上建立包含电力层、信息层与耦合层的多层防御架构, 从而建立时空多维的协同防御模型. 电力 CPS 网络安全防护过程, 是一个不断演进的动态过程, 需要通过周期性的安全管理、实施、部署与评估等循环过程.

如图 4 所示, 针对电力 CPS 的组织结构, 根据数据传输过程, 攻击者首先在信息层获取对节点设备或通信线路的接入甚至控制权限, 继而在电力层设计数据篡改方式, 最大化物理攻击后果. 在此基础上, 可以总结针对各攻击手段的防御方法. 其中信息层防御手段的基本原理是依据信息安全知识对数据协议、逻辑的正确性进行辨识; 电力层防御手段的原理是基于电力专业知识对数据内容的合理性进行辨识. 两者的交汇之处在控制应用设备, 作为信息基础设施的最高层, 包含了数据库和高层业务应用程序, 涵盖面向物理电网的量测与指令数据流. 在信息层注入的虚假数据都会汇集在控制应用中, 因此依据电力知识保证数据内容的正确性是阻止虚假数据破坏物理电网的最后一道防线. 电力层防御是电力 CPS 整体防御过程的关键, 防御手段主要包含保护

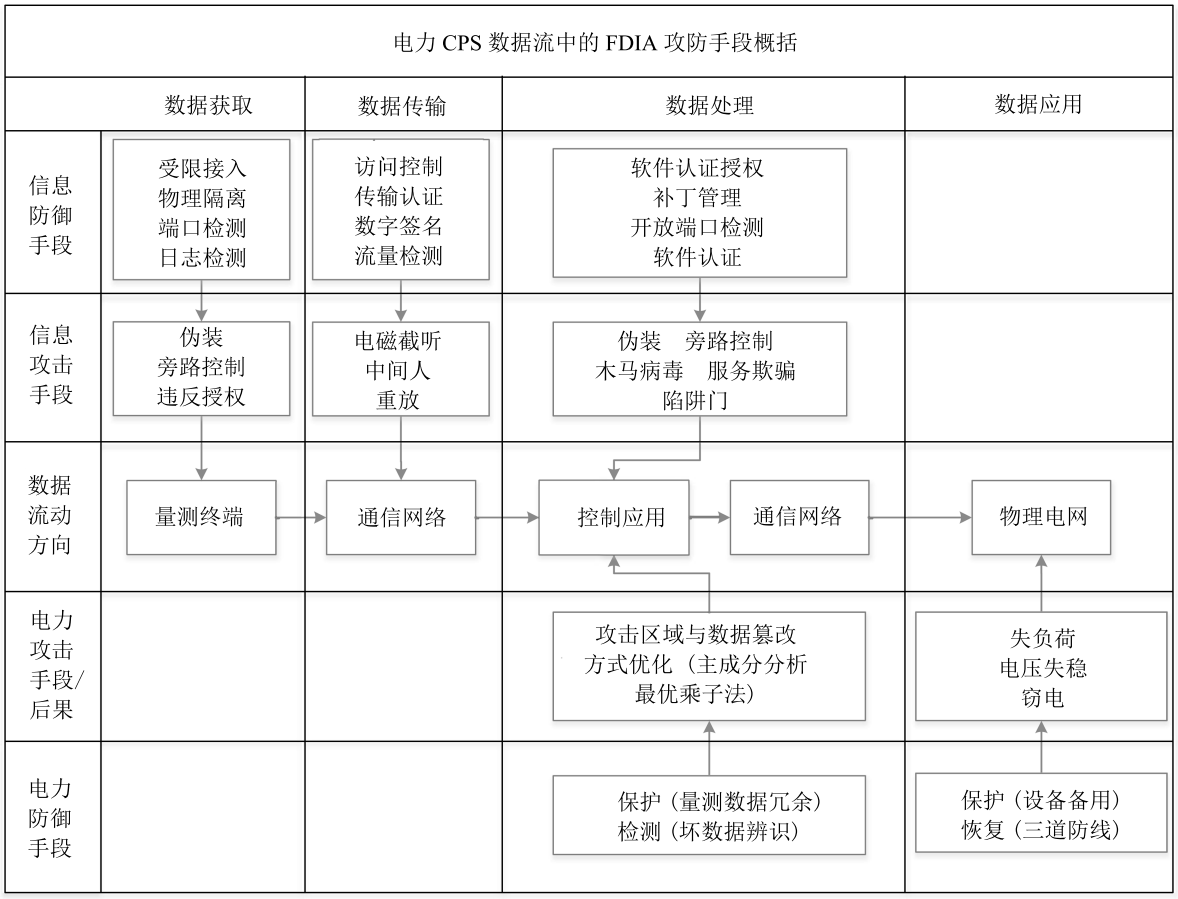

图 4　电力 CPS 数据流中的 FDIA 攻防手段概括

Fig. 4　The attack-defense means of FDIA aimed at the data flow in CPPS

与检测环节, 保护方法侧重于对攻击前的保护资源规划, 检测方法侧重于对攻击后的攻击行为辨识. 两类环节通常应用在攻击初始阶段, 如果布置得当可将攻击消除在萌芽阶段, 最小化攻击影响, 因而在整体防御过程中处于重要地位, 是本文重点研究的防御环节.

2.1　面向 FDIA 的检测方法

2.1.1　基于状态估计的检测方法

如果攻击者对电网信息和电力保护算法有充分的了解, 可以构建出能够逃避现有基于最小二乘状态估计的不良数据辨识检测算法. 基于该类数据篡改的特征, 目前的检测方法针对原有状态估计算法进行了改进, 增强了对人为恶意数据的辨识能力. 改进后的方法主要包括残差检测法、量测突变量检测法和量测相关性检测方法等[41−43]. 此外, 考虑到检测阈值受系统规模影响较大, 针对大系统可以将全局系统进行分块, 按各子系统实际参数设定不同阈值检测[44−45].

该类方法的优点是利用了成熟算法, 检测速度快, 能够较好反映电力系统特性; 但检测阈值的设定对检测精度影响大, 易出现漏检和误检.

2.1.2　基于轨迹预测的检测方法

基于状态估计的检测方法主要用于静态分析, 针对某个时间点的攻击行为进行检测. 在电力系统连续动态运行过程中, 多重状态量之间存在着较强的时空关系. 因此可以考虑利用历史数据进行轨迹分析, 对电网当前状态进行预测, 并与当前实际量测量对比, 分析其中可能受到攻击的区域. 基于轨迹预测的检测方法主要包括统计一致性检验、基于广义似然比的序贯检测和传感器轨迹预测等[46−48].

该类方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, 通过运行轨迹进行匹配, 可以有效检测各种类型的虚假数据, 但计算复杂度高, 检测速度慢, 不适用于复杂系统.

2.1.3　基于人工智能的检测方法

在传统的数学建模研究方法之外, 近年来提出了基于人工智能的 FDIA 检测方法, 主要有基于神经网络、深度学习和模糊聚类的研究方法[49−50].

文献 [49] 利用深度学习检测算法, 辅助检测传

统状态估计无法识别的坏数据, 在 IEEE118 节点系统中, 针对 1 300 组测试数据进行检测, 真正类率和负正类率分别为 96.43 % 和 95.89 %. 由于电力系统结构的复杂性和攻击特征的多元性, 复杂多维的攻击特征库与系统故障集之间的关联关系通常难以用传统解析方法构建, 而深度学习方法可以通过海量数据库进行训练, 有效地揭示攻击特征模式库, 对攻击行为进行分类检测. 从模糊聚类的角度出发, 以迭代自组织数据分析技术为基础, 并融合运用数据挖掘中的聚类分析方法和模糊集方法, 判断虚假数据[50].

人工智能方法的显著优点在于强大的计算能力和清晰的框架. 然而, 由于电力系统运行机理的复杂性, 该类方法的可解释性通常较差.

2.2 面向 FDIA 的保护方法

在电网安全规划中, 分析电网中重要和脆弱的区域, 对电网关键设备进行保护, 是防止系统被入侵的重要手段. 其中, 直接保护方法包括物理隔离、通道加密、增加防火墙等. 间接保护方法主要通过部署冗余量测装置, 增强系统的量测冗余度. 该类防御方法最重要的研究点为如何定位并保护重要的量测节点.

由于电网海量的测控数据和复杂的运行方式, 不同组合类型的攻击对电力系统运行方式的影响计算量十分庞大, 因此采用实时决策, 实时控制的方式难以满足对决策时间的要求. 需要采用离线决策, 在线匹配的思想, 攻击前在离线静态分析阶段, 采用规划的思想进行关键区域定位, 分析攻击–故障映射关系, 从而预先确定决策表; 在在线匹配决策阶段, 采用博弈的思想进行攻防行为预判分析, 过滤出可能的攻击方式, 确定最优防御策略.

2.2.1 电网关键区域识别规划方法

规划方法是在系统潮流和其他电气约束条件下, 考虑元件故障对系统整体安全性的影响, 从而识别系统中的关键区域进行保护. 按优化目标分类, 可以分为对系统整体稳定裕度、发电成本、负荷供应等目标的最优求解. 按约束条件分类, 规划方法可分为直流潮流线性规划和交流潮流非线性规划, 其中混合整数线性规划 (Mixed integer linear programming, MILP) 模型是判断电力系统关键区域最常用的方法. 文献 [51] 提出了双层 MILP 模型, 分析了保持系统整体稳定所需的最少保护量测量. 文献 [52] 为了防御针对智能电网的价格修改攻击, 提出了双层 MILP 模型, 并采用启发式算法计算关键节点. 规划方法一般适用于对保护资源的离线优化配置.

2.2.2 电网关键区域攻防博弈方法

规划方法适合从整体性的角度分析电网中的重点防御部署, 该方法多数停留在静态攻防策略求解层面, 以系统中最薄弱或最重要的区域作为攻防对象, 实际上由于攻防双方资源的有限性, 无法对电网所有区域进行攻防, 双方都会基于对方可能的选择, 优化自身的攻防资源部署, 形成了双人动态博弈过程.

现有的研究主要可以分为针对经济指标和安全指标的攻防过程. 从经济指标的角度, 文献 [53] 以市场电价为回报函数, 提出了斯塔克尔伯格博弈过程, 在一个领导的防御方和多个跟随的攻击方中, 分析双方不同地位的影响. 从安全指标的角度, 文献 [54−55] 应用多阶段混合博弈, 研究针对线路的 n-k 攻击, 其中前者运用状态转移矩阵表征攻防双方的预判行动, 后者采取考虑时间因素的马尔科夫模型来模拟双方互相影响的情形, 以最小负荷减载量化攻击后果, 得出了各线路的重要程度和攻防概率. 文献 [56] 将安全指标与经济指标结合, 攻击者针对电力控制网络的入侵, 控制变压器, 引起线路断线, 针对攻击引起的负荷损失和发电机跳闸, 将其量化为攻击者的经济收益, 并且与攻击成本进行权衡, 而防御者通过发电机出力的再调度措施减少攻击损失.

3 联合仿真技术在 FDIA 中的应用

在电力 CPS 环境中, 对 FDIA 的研究需要分析物理环境、通信环境与控制设备间的关联特性[57]. 由于信息物理耦合程度高、机理复杂, 面向 FDIA 的检测、定位和保护措施难度较大. 为了对攻击进行全周期过程分析, 可以利用电力 CPS 联合仿真技术, 构建攻击场景, 模拟攻击复现、故障定位、安全分析和故障恢复等过程.

3.1 联合仿真平台整体研究现状

3.1.1 联合仿真平台方案

近年来, 国内外各研究机构提出了多种联合仿真方案, 在平台架构、时间同步、计算精度和应用场景等方面各有不同[58−59]. 针对面向电力 CPS 的网络攻击而言, 主要包括拒绝服务攻击、中间人攻击、FDIA 等攻击策略和入侵检测、故障定位、安全评估等防御方法的仿真场景. 表 1 列出了近年来较为成熟的电力 CPS 网络安全攻防平台.

目前将电力 CPS 联合仿真技术应用于网络攻击的相关研究中, 重点是介绍通用平台的搭建过程及电力 CPS 的宏观特征, 例如多仿真器组成联合仿真平台时的数据交互和时间同步方法, 尚缺乏对于包含 FDIA 在内的网络攻击过程的详细建模和分析

表 1 电力 CPS 网络安全攻防平台研究现状

Table 1 Researches of CPPS associated attack-defense platforms

组成结构	攻击场景	防御方法	验证效果
MATLAB, OPNET[60]	信息传输故障	基于多维尺度和局部异常因子的检测方法	实现 CPS 各区域故障的统一识别与定位
Digsilent, OMNET++, MATLAB[61]	针对 EMS 的 FDIA	检测和事后恢复方法	构建了脆弱性和攻击影响的综合评估框架
PSLF, NS2[62]	针对 PMU 状态估计器的 FDIA	基于状态变量时效性的检测方法	验证了状态估计器对单链路和路由器故障、拥塞的鲁棒性
MATLAB, OPNET, C++[63]	针对广域阻尼控制系统的拒绝服务、中间人等攻击	无	分析归纳了延迟、无序、错误数据的端到端信息特征
Simulink, OPNET[64]	目的为延迟和污染通信数据的分布式拒绝服务攻击	无	观察了网络攻击对故障附近发电机响应的影响
RTDS, Python, AutoIt[65]	面向广域监控系统应用的电力 CPS 突发事件和网络攻击行为	基于数据挖掘的入侵异常检测方法	验证了电力系统应对攻击的脆弱性评估、异常检测与故障检测能力

功能[66]. 本文提出一种面向 FDIA 的电力 CPS 实时联合仿真平台架构, 能够模拟 FDIA 的攻击路径及相应的检测手段和保护策略.

3.1.2 基于硬件在环的网络实时联合攻防平台

方案总体框架如图 5 所示. 以 OPNET 仿真的通信网络作为纽带, 连接了 RT-LAB 仿真的电力系统网络、ARM 平台开发的主站系统、硬件测控装置和网络安全测试装置. 其中硬件测控终端是执行单元, 网络安全测试平台负责对系统整体安全性能进行评估, 主站系统负责实现各模块的同步分析与控制. $A1 \sim A3$ 三种攻击方式分别代表针对量测终端、通信网络和主站系统的入侵攻击过程.

为了使平台能够适应网络攻击仿真需求, 需对电力信息设备进行完整地协议建模和漏洞分析. 在传统的电力 CPS 仿真中, 针对通信部分的研究主要考虑数据传输延时对物理电网的影响, 缺乏对网络安全架构的建模. 在本平台中, 对于网络攻击类应用, 利用 OPNET 和硬件设备, 扩展了网络攻击元件库, 并建立安全评估模块分析攻防结果, 从而针对攻击的复现、传播、溯源、防御和评估等环节进行仿真模拟.

OPNET 作为通用的商业化通信仿真软件, 涵盖了大部分常见通信元件, 但对部分电力专用通信协议和设备缺乏支持. 因此采用数模混合仿真的形式, 对通用元件进行数字模拟, 具有建模速度快, 经济性好, 参数调整方便的优点; 对于网络安全测试设备, 采用硬件装置进行模拟, 复现攻击渗透、入侵检测等真实网络攻击场景, 通过 OPNET 的系统在环 (System in the loop, SITL) 元件进行连接, 从而真实反映设备特性. 综合采用两种方法, 组成半实物协同仿真, 具有直观性、广泛性、灵活性和整体性等优点, 从而搭建电力 CPS 网络攻击专用验证环境.

3.2 FDIA 中验证环境搭建

如图 6 所示, 为了在平台中构建攻防场景, 从信息层攻防角度, 需要选取脆弱性高的目标进行渗透, 将虚假报文注入到通信网络中, 再通过身份认证、机密性与完整性保障等措施进行防御; 从物理层攻防角度, 需要基于电力知识设计攻击向量, 再从保护、检测与恢复等步骤对 FDIA 进行多阶段防御, 最小化攻击影响; 在此基础上, 构建网络安全评估模块, 对攻防交互场景进行安全裕度评估, 验证对信息通信性能和电力系统稳定性的影响.

3.2.1 多种形式 FDIA 的实验复现策略

在 OPNET 通信仿真环境中, 可以通过渗透通信节点和网络路由协议来构建 FDIA.

针对通信节点的入侵, 主要利用目标主机软件缺陷或协议漏洞, 向其发送恶意报文. 比较典型的方式有旁路控制, 攻击者通过监听客户端节点发起的请求, 然后伪造主站发送虚假数据指令给客户端, 可以误导其执行虚假指令.

针对路由协议的入侵过程需要考虑整体网络拓扑, 以开放式最短路径优先 (Open shortest path first, OSPF) 协议为例, 其由两个互相关联的主要部分组成: 呼叫协议和可靠泛洪机制. 呼叫协议检测邻居并维护邻接关系, 可靠泛洪算法可以确保统一域中的所有的 OSPF 路由器始终具有一致的链路状态数据库. 如果攻击者越过了加密机制, 通过伪造泛洪报文, 可以篡改路由表, 造成指令目的地址的错误下发.

3.2.2 网络安全防御系统的构建

为了抵御攻击风险, 利用 OPNET 中的网络安全元件, 建立相应的网络安全防御系统, 主要组成部

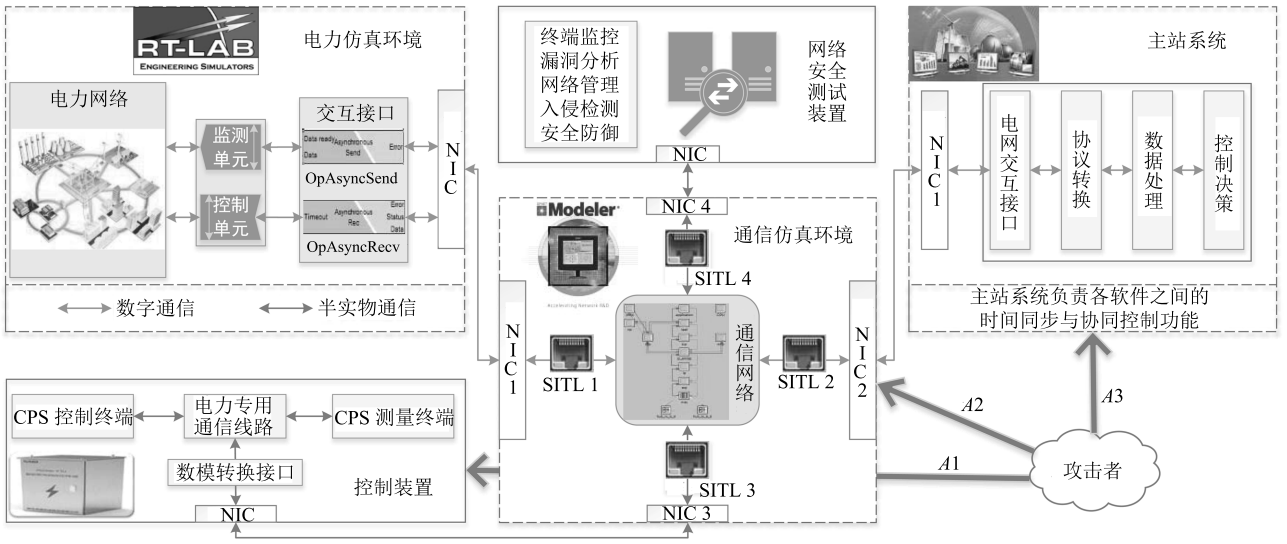

图 5 电力 CPS 网络联合攻防平台框架

Fig. 5 The framework of the CPPS associated attack-defense platform

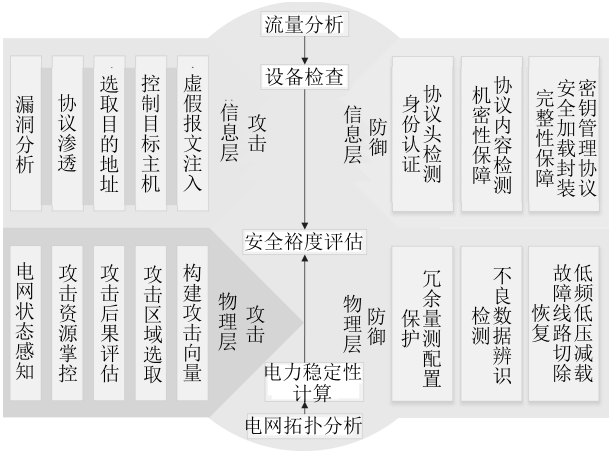

图 6 FDIA 协同攻防框架

Fig. 6 The synergetic attack-defense framework of FDIA

分为风险防御模块和安全评估模块.

在风险防御模块中, 通过认证、机密性和数据完整三重形式保护公有或私有 IP 网络中的传送数据. 该模块通过协议头来验证数据源身份, 保证数据完整性, 并防止相同报文不断重播; 通过安全加载封装和互联网密钥管理协议提供对数据内容机密性保障和数据流机密性保障.

在安全评估模块中, 主要利用 OPNET 中的 Cyber effects 元件, 实现感染设备检查、流量统计、已知感染清除、控制转发速率等功能, 从而评估网络性能、安全性和可靠性, 对抗网络威胁. 该模块通过测量故障或被攻击环境下离散网络组件的稳定性, 针对多种业务, 对端到端时延、丢包率、吞吐量、误码率、重传次数、重传时延等属性进行评估, 综合得出网络整体安全裕度[67]. 在此基础上, 可以释放恶意应用程序导致的用户负载, 强化关键网络或数据中心的稳定性, 从而增强对 FDIA 的抵御能力.

3.2.3 物理侧安全防护复现过程

在物理侧, 面对含虚假信息的电网测控数据, 可以建立保护、检测和恢复模块, 最小化攻击影响.

从保护的角度, 在 RT-LAB 中的电网模型, 一方面, 设置冗余量测单元, 从而增强量测冗余度; 另一方面适时调整网络拓扑结构和参数, 保障电网信息隐蔽性. 从检测的角度, 在主站系统中建立数据合理性辨识模块, 依据状态估计算法, 建立异常检测模型. 从恢复的角度, 此时物理电网已经遭受到 FDIA 影响, 存在故障风险. 在 RT-LAB 中建立控制恢复模块, 故障发生后快速切除故障支路. 如果系统失步或母线长期低频低压, 通过失步解列、低频低压减载等措施阻止故障范围扩散, 尽快恢复对被停负荷的供电.

4 结束语

本文从攻击入侵方法、攻击条件、攻击影响等攻击过程和保护、检测等防御环节进行理论分析, 介绍了面向电力 CPS 的 FDIA 攻防机理. 阐述了针对 FDIA 的联合攻防平台构建过程, 介绍了平台框架、攻击复现原理以及网络安全防御系统. 从理论探索到实验验证, 针对 FDIA 进行了多角度、多目标的协同分析.

随着源网荷广泛互动, 海量数据的交换共享, 电源侧、电网侧和供电侧的信息系统均会受到 FDIA 影响, 从而威胁电力系统监视控制、统计分析、经济调度和安全决策等多方面的功能. 因此本文认为面向电力 CPS 的 FDIA 的后续研究方向主要包括: 1)

研究电力 CPS 的信息侧漏洞分析和入侵检测过程; 2) 研究电力 CPS 各空间状态特征的数据检测算法; 3) 考虑信息物理耦合关系, 分析信息篡改与物理故障的关联关系, 研究信息物理协同防御机制.

References

1 Zhao Jun-Hua, Wen Fu-Shuan, Xue Yu-Sheng, Li Xue, Dong Zhao-Yang. Cyber physical power systems: architecture, implementation techniques and challenges. *Automation of Electric Power Systems*, 2010, **34**(16): 1−7
(赵俊华, 文福拴, 薛禹胜, 李雪, 董朝阳. 电力 CPS 的架构及其实现技术与挑战. 电力系统自动化, 2010, **34**(16): 1−7)

2 Ma Zhao, Zhou Xiao-Xin, Shang Yu-Wei, Sheng Wan-Xing. Exploring the concept, key technologies and development model of energy internet. *Power System Technology*, 2015, **39**(11): 3014−3022
(马钊, 周孝信, 尚宇炜, 盛万兴. 能源互联网概念、关键技术及发展模式探索. 电网技术, 2015, **39**(11): 3014−3022)

3 Mo Y L, Kim T H J, Brancik K, Dickinson D, Lee H, Perrig A, et al. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 2012, **100**(1): 195−209

4 He H B, Yan J. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory and Applications*, 2016, **1**(1): 13−27

5 Liu Dong, Sheng Wan-Xing, Wang Yun, Lu Yi-Ming, Sun Chen. Key technologies and trends of cyber physical system for power grid. *Proceedings of the CSEE*, 2015, **35**(14): 3522−3531
(刘东, 盛万兴, 王云, 陆一鸣, 孙辰. 电网信息物理系统的关键技术及其进展. 中国电机工程学报, 2015, **35**(14): 3522−3531)

6 Vellaithurai C, Srivastava A, Zonouz S, Berthier R. CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Transactions on Smart Grid*, 2015, **6**(2): 566−575

7 Wang W Y, Lu Z. Cyber security in the smart grid: survey and challenges. *Computer Networks*, 2013, **57**(5): 1344−1371

8 Miao Xin, Zhang Kai, Tian Shi-Ming, Li Jian-Qi, Yin Shu-Gang, Zhao Zi-Yan. Information communication system supporting smart grid. *Power System Technology*, 2009, **33**(17): 8−13
(苗新, 张恺, 田世明, 李建歧, 殷树刚, 赵子岩. 支撑智能电网的信息通信体系. 电网技术, 2009, **33**(17): 8−13)

9 Liu S, Mashayekh S, Kundur D, Zourntos T, Butler-Purry K. A framework for modeling cyber-physical switching attacks in smart grid. *IEEE Transactions on Emerging Topics in Computing*, 2013, **1**(2): 273−285

10 Ye Xia-Ming, Wen Fu-Shuan, Shang Jin-Cheng, He Yang. Propagation mechanism of cyber physical security risks in power systems. *Power System Technology*, 2015, **39**(11): 3072−3079
(叶夏明, 文福拴, 尚金成, 何洋. 电力系统中信息物理安全风险传播机制. 电网技术, 2015, **39**(11): 3072−3079)

11 Hahn A, Govindarasu M. Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2011, **2**(4): 835−843

12 Tian Ji-Wei, Wang Bu-Hong, Li Xia. State-preserving topology attacks and its impact on economic operation of smart grid. *Power System Protection and Control*, 2018, **46**(1): 50−56
(田继伟, 王布宏, 李夏. 智能电网状态维持拓扑攻击及其对经济运行的影响. 电力系统保护与控制, 2018, **46**(1): 50−56)

13 Tang Yi, Chen Qian, Li Meng-Ya, Wang Qi, Ni Ming, Liang Yun. Overview on cyber-attacks against cyber physical power system. *Automation of Electric Power Systems*, 2016, **40**(17): 59−69
(汤奕, 陈倩, 李梦雅, 王琦, 倪明, 梁云. 电力信息物理融合系统环境中的网络攻击研究综述. 电力系统自动化, 2016, **40**(17): 59−69)

14 Liang G Q, Weller S R, Zhao J H, Luo F J, Dong Z Y. The 2015 Ukraine blackout: implications for false data injection attacks. *IEEE Transactions on Power Systems*, 2017, **32**(4): 3317−3318

15 Li Zhong-Wei, Tong Wei-Ming, Jin Xian-Ji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel. *Automation of Electric Power Systems*, 2016, **40**(8): 147−151
(李中伟, 佟为明, 金显吉. 智能电网信息安全防御体系与信息安全测试系统构建: 乌克兰和以色列国家电网遭受网络攻击事件的思考与启示. 电力系统自动化, 2016, **40**(8): 147−151)

16 Zhao Jun-Hua, Liang Gao-Qi, Wen Fu-Shuan, Dong Zhao-Yang. Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks. *Automation of Electric Power Systems*, 2016, **40**(7): 149−151
(赵俊华, 梁高琪, 文福拴, 董朝阳. 乌克兰事件的启示: 防范针对电网的虚假数据注入攻击. 电力系统自动化, 2016, **40**(7): 149−151)

17 Ni Ming, Yan Jie, Bo Rui, Tang Yi. Power system cyber attack and its defense. *Automation of Electric Power Systems*, 2016, **40**(5): 148−151
(倪明, 颜诘, 柏瑞, 汤奕. 电力系统防恶意信息攻击的思考. 电力系统自动化, 2016, **40**(5): 148−151)

18 Wei Zhi-Nong, Chen He-Sheng, Ni Ming, Sun Guo-Qiang, Sun Yong-Hui, Li Chao. Definition, construction and defense of false data in cyber physical system. *Automation of Electric Power Systems*, 2016, **40**(17): 70−78
(卫志农, 陈和升, 倪明, 孙国强, 孙永辉, 厉超. 电力信息物理系统中恶性数据定义、构建与防御挑战. 电力系统自动化, 2016, **40**(17): 70−78)

19 Tang Yi, Wang Qi, Ni Ming, Liang Yun. Analysis of cyber attacks in cyber physical power system. *Automation of Electric Power Systems*, 2016, **40**(6): 148−151
(汤奕, 王琦, 倪明, 梁云. 电力信息物理融合系统中的网络攻击分析. 电力系统自动化, 2016, **40**(6): 148−151)

20 Zhu Jie, Zhang Ge-Xiang, Wang Tao, Zhao Jun-Bo. Overview of fraudulent data attack on power system state estimation and defense mechanism. *Power System Technology*, 2016, **40**(8): 2406−2415
(朱杰, 张葛祥, 王涛, 赵俊博. 电力系统状态估计欺诈性数据攻击及防御综述. 电网技术, 2016, **40**(8): 2406−2415)

21 Fan Y W, Zhang Z H, Trinkle M, Dimitrovski A D, Song J B, Li H S. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart Grids. *IEEE Transactions on Smart Grid*, 2015, **6**(6): 2659−2668

22 Liu X X, Zhu P D, Zhang Y, Chen K. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Transactions on Smart Grid*, 2015, **6**(5): 2435−2443

23 Bishop A N, Savkin A V. On false-data attacks in robust multi-sensor-based estimation. In: Proceedings of the 9th IEEE International Conference on Control and Automation. Santiago, Chile: IEEE, 2011. 10−17

24 Pal S, Sikdar B, Chow J H. An online mechanism for detection of gray-hole attacks on PMU data. *IEEE Transactions on Smart Grid*, 2018, **9**(4): 2498−2507

25 Ji Xing-Pei, Wang Bo, Dong Zhao-Yang, Chen Guo, Liu Di-Chen, Wei Da-Qian, et al. Vulnerability evaluation and link addition protection strategy research of electrical cyber-physical interdependent networks. *Power System Technology*, 2016, **40**(6): 1867−1873
(冀星沛, 王波, 董朝阳, 陈果, 刘涤尘, 魏大千, 等. 电力信息–物理相互依存网络脆弱性评估及加边保护策略. 电网技术, 2016, **40**(6): 1867−1873)

26 Li Qiang, Zhou Jing-Yang, Yu Er-Keng, Liu Shu-Chun, Wang Lei. Hybrid algorithm for power system state estimation based on PMU measurement and SCADA measurement. *Automation of Electric Power Systems*, 2005, **29**(19): 31−35
(李强, 周京阳, 于尔铿, 刘树春, 王磊. 基于混合量测的电力系统状态估计混合算法. 电力系统自动化, 2005, **29**(19): 31−35)

27 Mo Y L, Sinopoli B. False data injection attacks in control systems. In: Proceedings of the 1st Workshop on Secure Control Systems. Stockholm, Sweden: Springer, 2010.

28 Wang Yu-Fei, Gao Kun-Lun, Zhao Ting, Qiu Jian. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. *Proceedings of the CSEE*, 2016, **36**(6): 1490−1499
(王宇飞, 高昆仑, 赵婷, 邱健. 基于改进攻击图的电力信息物理系统跨空间连锁故障危害评估. 中国电机工程学报, 2016, **36**(6): 1490−1499)

29 Tian Meng, Wang Xian-Pei, Dong Zheng-Cheng, Zhu Guo-Wei, Dai Dang-Dang, Zhao Le. Injected attack strategy for false data based on Lagrange multipliers method. *Automation of Electric Power Systems*, 2017, **41**(11): 26−32
(田猛, 王先培, 董政呈, 朱国威, 代荡荡, 赵乐. 基于拉格朗日乘子法的虚假数据攻击策略. 电力系统自动化, 2017, **41**(11): 26−32)

30 Su Sheng, Wu Chang-Jiang, Ma Jun, Zeng Xiang-Jun. Attacker′s perspective based analysis on cyber attack mode to cyber-physical system. *Power System Technology*, 2014, **38**(11): 3115−3120
(苏盛, 吴长江, 马钧, 曾祥君. 基于攻击方视角的电力 CPS 网络攻击模式分析. 电网技术, 2014, **38**(11): 3115−3120)

31 Zhu Ze-Lei, Zhou Jing-Yang, Pan Yi, Yan Cui-Hui, Cui Hui, Li Wei-Gang. Security constrained economic dispatch considering balance of electric power and energy. *Proceedings of the CSEE*, 2013, **33**(10): 168−176
(朱泽磊, 周京阳, 潘毅, 闫翠会, 崔晖, 李伟刚. 考虑电力电量平衡的安全约束经济调度. 中国电机工程学报, 2013, **33**(10): 168−176)

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

33 Jia L Y, Kim J, Thomas R J, Tong L. Impact of data quality on real-time locational marginal price. *IEEE Transactions on Power Systems*, 2014, **29**(2): 627−636

34 Mousavian S, Valenzuela J, Wang J H. A probabilistic risk mitigation model for cyber-attacks to PMU networks. *IEEE Transactions on Power Systems*, 2015, **30**(1): 156−165

35 Zhao J B, Zhang G X, La Scala M, Wang Z Y. Enhanced robustness of state estimator to bad data processing through multi-innovation analysis. *IEEE Transactions on Industrial Informatics*, 2017, **13**(4): 1610−1619

36 Wang Xian-Pei, Zhu Guo-Wei, He Rui-Juan, Tian Meng, Dong Zheng-Cheng, Dai Dang-Dang, et al. Survey of cascading failures in cyber physical power system based on complex network theory. *Power System Technology*, 2017, **41**(9): 2947−2956
(王先培, 朱国威, 贺瑞娟, 田猛, 董政呈, 代荡荡, 等. 复杂网络理论在电力 CPS 连锁故障研究中的应用综述. 电网技术, 2017, **41**(9): 2947−2956)

37 Liu R, Vellaithurai C, Biswas S S, Gamage T T, Srivastava A K. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid*, 2015, **6**(5): 2444−2453

38 Deng R L, Zhuang P, Liang H. CCPA: coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Transactions on Smart Grid*, 2017, **8**(5): 2420−2430

39 Bo Z Q, Lin X N, Wang Q P, Yi Y H, Zhou F Q. Developments of power system protection and control. *Protection and Control of Modern Power Systems*, 2016, **1**: Article No. 7

40 Smart Grid Interoperability Panel Cyber Security Working Group. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. Technical Standard, NIST Special Publication, 2010, 154

41 Hu Z S, Wang Y, Tian X X, Yang X L, Meng D J, Fan R S. False data injection attacks identification for smart grids. In: Proceedings of the 3rd International Conference on Technological Advances in Electrical, Electronics and Computer Engineering. Beirut, Lebanon: IEEE, 2015. 139−143

42 Bobba R B, Rogers K M, Wang Q Y, Khurana H, Nahrstedt K, Overbye T J. Detecting false data injection attacks on DC state estimation. In: Proceedings of the 1st Workshop on Secure Control Systems. Urbana-Champaign, USA, 2010. 1−9

43 Chakhchoukh Y, Ishii H. Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations. *IEEE Transactions on Power Systems*, 2016, **31**(6): 4395−4405

44 Gu Y, Liu T, Wang D, Guan X H, Xu Z B. Bad data detection method for smart grids based on distributed state estimation. In: Proceedings of the 2013 IEEE International Conference on Communications. Budapest, Hungary: IEEE, 2013. 4483−4487

45 Wang D, Guan X H, Liu T, Gu Y, Shen C, Xu Z B. Extended distributed state estimation: a detection method against tolerable false data injection attacks in smart grids. *Energies*, 2014, **7**(3): 1517−1538

46 Zhao J B, Zhang G X, La Scala M, Dong Z Y, Chen C, Wang J H. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Transactions on Smart Grid*, 2017, **8**(4): 1580−1590

47 Li S, Yılmaz Y, Wang X D. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Transactions on Smart Grid*, 2015, **6**(6): 2725−2735

48 Khalid H M, Peng J C H. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. *IEEE Transactions on Smart Grid*, 2017, **8**(2): 697−707

49 He Y B, Mendis G J, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, 2017, **8**(5): 2505−2516

50 Ozay M, Esnaola I, Tunay F, Vural Y, Kulkarni S R, Poor H V. Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems*, 2016, **27**(8): 1773−1786

51 Liu X, Li Z, Member S, Li Z, Member S. Optimal protection strategy against false data injection attacks in power systems. *IEEE Transactions on Smart Grid*, 2017, **8**(4): 1802−1810

52 Mishra S, Li X, Pan T Y, Kuhnle A, Thai M T, Seo J. Price modification attack and protection scheme in smart grid. *IEEE Transactions on Smart Grid*, 2017, **8**(4): 1864−1875

53 Sanjab A, Saad W. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. *IEEE Transactions on Smart Grid*, 2016, **7**(4): 2038−2049

54 Wei L F, Sarwat A I, Saad W, Biswas S. Stochastic games for power grid protection against coordinated cyber-physical attacks. *IEEE Transactions on Smart Grid*, 2018, **9**(2): 684−694

55 Ma C Y T, Yau D K Y, Lou X, Rao N S V. Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Transactions on Power Systems*, 2013, **28**(2): 1676−1686

56 Wang C, Hou Y H, Ten C W. Determination of Nash Equilibrium based on plausible attack-defense dynamics. *IEEE Transactions on Power Systems*, 2017, **32**(5): 3670−3680

57 Tang Yi, Wang Qi, Tai Wei, Chen Bin, Ni Ming. Real-time simulation of cyber-physical power system based on OPAL-RT and OPNET. *Automation of Electric Power Systems*, 2016, **40**(23): 15−21, 92
(汤奕, 王琦, 邰伟, 陈彬, 倪明. 基于 OPAL-RT 和 OPNET 的电力信息物理系统实时仿真. 电力系统自动化, 2016, **40**(23): 15−21, 92)

58 Wang Yun, Liu Dong, Weng Jia-Ming, Yan Guang-Sheng, Yong Jun, Dai Hui. The research of power CPS modeling and simulation verification platform. *Proceedings of the CSEE*, 2018, **38**(1): 130−136
(王云, 刘东, 翁嘉明, 严光升, 雍军, 戴晖. 电网信息物理系统建模与仿真验证平台研究. 中国电机工程学报, 2018, **38**(1): 130−136)

59 Li Xia, Li Yong, Cao Yi-Jia, Shi Xing-Yu. Wide-area damping control strategy of interconnected power grid based on cyber physical system. *Power System Protection and Control*, 2017, **45**(21): 35−42
(李霞, 李勇, 曹一家, 施星宇. 基于信息物理系统融合的广域互联电网阻尼控制策略. 电力系统保护与控制, 2017, **45**(21): 35−42)

60 Zhang Zhi-Peng, Li Yong, Cao Yi-Jia, Shi Xing-Yu, Hu Wei, Zhao Qing-Zhou. A local outlier factor fault identification algorithm based on the co-simulation between cyber and power system for distribution network. *Automation of Electric Power Systems*, 2016, **40**(17): 44−50
(张志鹏, 李勇, 曹一家, 施星宇, 胡伟, 赵庆周. 通信和电网联合仿真的配电网局部异常因子故障辨识算法. 电力系统自动化, 2016, **40**(17): 44−50)

61 Pan K K, Teixeira A, López C D, Palensky P. Co-simulation for cyber security analysis: data attacks against energy management system. In: Proceedings of the 2007 IEEE International Conference on Smart Grid Communications. Dresden, Germany: IEEE, 2017. 253−258

62 Lin H, Deng Y, Shukla S, Thorp J, Mili L. Cyber security impacts on all-PMU state estimator — a case study on co-simulation platform GECO. In: Proceedings of the 3rd IEEE International Conference on Smart Grid Communications. Tainan, China: IEEE, 2012. 587−592

63 Cao Y J, Shi X Y, Li Y, Tan Y, Shahidehpour M, Shi S L. A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations. *IEEE Transactions on Smart Grid*, 2018, **9**(5): 4893−4905

64 Sadi M A H, Ali M H, Dasgupta D, Abercrombie R K, Kher S. Co-simulation platform for characterizing cyber attacks in cyber physical systems. In: Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence. Cape Town, South Africa: IEEE, 2015. 1244−1251

65 Adhikari U, Morris T, Pan S Y. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining. *IEEE Transactions on Smart Grid*, 2017, **8**(6): 2744−2753

66 Tang Y, Tai W, Liu Z J, Li M Y, Wang Q, Liang Y, et al. A hardware-in-the-loop based co-simulation platform of cyber-physical power systems for wide area protection applications. *Applied Sciences*, 2017, **7**(12): Article No. 1279

67 Jia Chi-Qian, Feng Dong-Qin. Industrial control system devices security assessment with multi-objective decision. *Acta Automatica Sinica*, 2016, **42**(5): 706−714
(贾驰千, 冯冬芹. 基于多目标决策的工控系统设备安全评估方法研究. 自动化学报, 2016, **42**(5): 706−714)

王 琦 博士, 东南大学电气工程学院讲师. 主要研究方向为电力信息物理系统和电力系统稳定分析与控制. 本文通信作者. E-mail: wangqi@seu.edu.cn
(**WANG Qi** Ph. D., lecturer at the School of Electrical Engineering, Southeast University. His research interest covers cyber physical power systems, and power system stability analysis and control. Corresponding author of this paper.)

邰 伟 东南大学电气工程学硕士研究生. 主要研究方向为电力信息物理系统网络攻击. E-mail: taiwei@seu.edu.cn
(**TAI Wei** Master student at the School of Electrical Engineering, Southeast University. His research interest covers cyber-attacks against cyber physical power systems.)

汤 奕 博士, 东南大学电气工程学院副教授. 主要研究方向为电力系统稳定分析与控制和电力信息物理融合系统.
E-mail: tangyi@seu.edu.cn
(**TANG Yi** Ph. D., associate professor at the School of Electrical Engineering, Southeast University. His research interest covers power system stability analysis and control, and cyber physical power systems.)

倪 明 博士, 南瑞集团有限公司研究员级高级工程师. 主要研究方向为电力系统规划, 分析与控制.
E-mail: ni-ming@sgepri.sgcc.com.cn
(**NI Ming** Ph. D., professor status high level engineer at NARI Group Corporation. His research interest covers planning, analysis and control of power system.)