电力信息物理系统跨域攻击协同防御架构及机制研究

张 涛[1],费稼轩[1],王 琦[2*],邵志鹏[1],蔡星浦[2]
(1. 国网智能电网研究院电网数字化技术研究所,北京 100190;2. 东南大学电气工程学院,江苏南京 210096)

摘 要: 我国电力基础设施已经发展成为具有高度信息化、自动化、智能化特征的信息物理融合系统. 信息-物理交互在显著提升电力供给效率和性能的同时,也引入了新型网络安全威胁,通过发生于信息域并明确作用于物理域的跨域攻击,可造成电力基础设施系统性瘫痪,继而引发大面积停电事故,而当前孤立的信息侧或物理侧防御体系难以有效应对跨域攻击威胁. 本文介绍了电力系统面临的信息物理跨域攻击威胁现状,分析了传统防御方法面对跨域攻击时存在的不足,提出了一种信息物理协同的跨域攻击防御架构,在针对跨域攻击传播的不同阶段,从感知、辨识、阻断三个角度设计了防御方法,通过算例验证了所提信息物理协同防御架构能够有效保障电力系统安全稳定运行.

关键词: 电力信息物理系统;信息物理协同;跨域攻击;协同防御;知识-数据驱动;电力系统安全
基金项目: 国家自然科学基金(No.52261145704)
中图分类号: TN915.08 **文献标识码:** A **文章编号:** 0372-2112(2024)04-1205-14
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20231001

Research of Architecture and Mechanism of Coordinative Defense Methods for Cross-Domain Attacks of Cyber Physical System

ZHANG Tao[1], FEI Jia-xuan[1], WANG Qi[2*], SHAO Zhi-peng[1], CAI Xing-pu[2]
(1. *Grid Digital Technology Institute*, *State Grid Smart Grid Research Institute*, *Beijing* 100190, *China*;
2. *School of Electrical Engineering*, *Southeast University*, *Nanjing*, *Jiangsu* 210096, *China*)

Abstract: The electric power infrastructure of China has developed into a highly informationized, automated, and intelligent cyber physical integration system. The interaction of cyber and physical not only significantly improves the efficiency and performance of power supply, but also introduces new network security threat. Cross-domain attacks that occurring in the cyber domain and acting on the physical domain can cause the systematic breakdown of power infrastructure and then lead to large-scale power outages. However, the current isolated cyber side or physical side defense system is difficult to effectively deal with these cross-domain attack threats. This paper introduces the current situation of information and physical cross domain attack threats faced by the power system, elaborates on the shortcomings of traditional defense methods in facing cross domain attacks, proposes a cross domain attack defense architecture based on information and physical collaboration, and designs defense methods from the perspectives of perception, identification, and blocking on the attack time scale. Through example design, it is proven that the proposed information and physical collaboration defense architecture can ensure the safe and stable operation of the power system.

Key words: cyber physical power system; information-physical collaboration; cross-domain attack; coordinated defense; knowledge-data driven; power system safety
Foundation Item(s): National Natural Science Foundation of China (No.52261145704)

1 引言

电力作为国家关键基础设施,承担着为我国经济社会运行提供安全可靠电力供应的重要使命. 随着先进信息通信技术的广泛应用,电力系统的运行控制高度依赖智能化测控设备、通信网络和软件系统[1,2]. 当前,我国电力基础设施已经发展成为具有高度信息化、

收稿日期:2023-10-26;修回日期:2024-03-08;责任编辑:宋甲英
*通讯作者:王琦

自动化、智能化特征的信息物理融合系统. 信息侧作为通信、计算、控制的支撑性组成部分,在电力信息物理系统(Cyber Physical System,CPS)安全可靠运行中有重要的地位,其故障可能会降低电网运行控制可靠性的问题不容忽视[3]. 通过发生于信息域并明确作用于物理域目标的信息物理跨域攻击,可造成电力基础设施系统性瘫痪,继而引发大面积停电事故,危及国家安全[4,5].

近年来陆续发生了多起由网络攻击导致的电力系统安全事故. 2015年,乌克兰电力系统受到网络攻击,造成大面积停电事故,这也被认为是第一例由网络攻击导致电力系统大停电事件. 2018年,美国联邦调查局的报告表明,网络攻击实施者已经成功获取其国内工控系统权限,窃取了工作站和数据采集监控系统的机密文档,并获得直接开合开关的能力. 2019年3月委内瑞拉电网发生数次大停电事故,有报道认为是由网络软杀伤和军事硬摧毁协同配合的"电力战"造成. 上述事件表明,电力基础设施已经成为跨域攻击的首要目标之一,其不仅在地理和网络空间上广泛分布从而存在防范难度,而且在知识架构上相互交叉需要信息与物理的深度融合. 现实中网络攻击乃至"电力战"带来的严重后果应引起重视和警惕,必须加强防范意识,并对其防御理论与方法进行深入研究.

传统互联网信息领域的网络攻击行为通常是通过非法窃取或操纵信息以获得经济、政治等利益,而电力信息物理系统的跨域攻击行为意在影响电网正常运行状态的安全稳定运行[6~8],并造成大面积停电,从而影响社会生产生活. 因此,针对跨域攻击的防御也与传统单一网络空间的防御有所不同,应当更加注重电力系统物理侧业务功能的安全防护和事故后恢复.

我国电力物理系统运行安全稳定的研究已较为成熟,并已在实际应用中形成完整体系. 前期电力基础设施通过建立互联网、信息网、控制网三道纵深边界隔离防护体系,有效抵御了来自互联网的传统攻击威胁. 在电力信息安全领域则通常存在以下三点认知:(1)我国电力监控系统采用"安全分区、网络专用、横向隔离、纵向认证"的防护原则,确保了二次系统的安全边界完整,从而增加了防御攻击成功的概率;(2)部分电力系统关键测控和保护装备采用本地控制,降低了网络攻击风险;(3)我国电网现有的安全稳定三道防线理念,能够应对网络攻击造成单一元件故障从而引发的后果[9].

但随着能源互联网加快建设,电力系统规模化和信息化程度提高,电力基础设施通过更开放的网络以及更大规模的电力测控终端,对电气设备与用户负荷实施广域量测与控制;而各类针对工业控制网络的恶意攻击手段也呈现多样化和专业化,具有"针对性强、隐蔽高、传导性快"特征的信息物理跨域攻击威胁,对当前电力信息安全防护体系提出了挑战[10,11].

(1)非受控环境下海量异构终端防御难度大. 智能电网建设推进过程中,多类型负荷、储能和分布式能源的并网伴随着大量非传统电力信息设备(如分布式量测装置、监控终端等)的广泛接入,承担物理空间量测与控制功能的测控终端多处于非可控环境且自身防护薄弱,海量电力终端跨域攻击感知与自主防御技术难度大.

(2)开放网络跨域攻击识别难度大. 电力量测数据和调控指令通过公专融合网络进行传输,以安全边界为主的防护思路无法完全适用,电力网络公专混联、业务复杂,攻击路径隐蔽且特征不明,公专融合网络下跨域攻击识别及低时延指令级保护技术难度大.

(3)强实时条件下跨域连锁故障抑制难度大. 目前我国电网仍处于坚强电网建设过渡时期,大电网耦合特性复杂,电网一次网架与二次系统之间的结构性矛盾尚存. 电力系统耦合互动、实时运行,攻击传导性强,极易导致系统故障,跨域攻击行为实时阻断及连锁故障抑制难度大.

针对电力系统跨域攻击风险,有必要基于信息侧与物理侧协同分析,挖掘潜在的攻击威胁,以构建更加坚固的网络安全防线. 本文首先分析信息物理跨域攻击与传统防御方法的优缺点,指出当前防御架构在应对跨域攻击方面的局限性. 接着,提出信息物理协同安全防御方法,并构建相应的安全防御体系架构. 在此基础上,针对体系架构的各个阶段,提出具体的防御措施,包括基于信息物理关联状态分析的跨域攻击协同感知方法、知识-数据融合驱动的跨域攻击协同辨识方法以及信息物理协同优化的跨域攻击紧急阻断方法. 最后,通过算例分析验证所提方法的有效性.

2 信息物理跨域攻击与传统防御方法分析

我国电网物理侧配置了成熟的安全稳定防御体系,通过对物理系统运行状态实时监测和预防紧急控制措施,应对由各类偶发因素造成的设备故障,确保系统受扰后保持稳定,不发生大停电事故. 通常情况下,信息侧偶发性扰动(延时、中断等)不容易造成物理侧故障,而通过信息侧实施的跨域攻击则可能突破两侧的防护措施,破坏物理侧安全稳定. 因此针对跨域攻击的研究需要考虑信息物理耦合,对跨域攻击过程和影响后果进行深入分析. 本节将对电力系统跨域攻击的建模和评估方法进行总结,并从辨识与防御两个角度,指出当前方法所存在的局限性.

2.1　电力信息物理系统跨域攻击建模和评估

电力信息物理系统跨域攻击建模主要包括攻击方法模型和攻击后果模型. 其中,攻击方法建模包括以下三点.(1)保密性攻击:非法获取电力系统信息侧和物理侧数据. 其攻击方法与流程的建模可借鉴信息安全领域研究,建模对象主要是攻击路径和状态转移概率,建模方法有攻击树/图、贝叶斯方法、Petri网等[12]. (2)完整性攻击:非法篡改电力信息物理系统数据,从而使调度中心获取错误系统状态而发生误操作[13~15]. 此攻击行为所篡改的信息是否能躲过监控系统辨识在很大程度上决定了该类攻击的有效性. 因此攻击者掌握的资源约多、权限越高,完整性攻击成功实施的可能性越大,故完整性攻击常以保密性攻击为前提. (3)可用性攻击:阻断系统接收数据信息,如拒绝服务攻击、延时攻击等,力图造成信息缺失或异常. 此类攻击对攻击者掌握的资源和权限要求较低,攻击发动较为容易.

跨域攻击后果主要包括:(1)信息系统功能被降低甚至破坏,如系统通信被阻碍、系统的运行状态被获知等;(2)电力系统的检测保护机制实效,物理系统产生实际损失,如系统稳定性被削弱、频率电压越限等[16]. 目前针对电力CPS攻击向量建模的研究通常局限于物理侧业务,而忽视攻击过程中电力CPS的整体状态变化. 信息-物理侧的割裂使得现有基于攻击建模的系列研究缺乏现实的多阶段交互攻防过程[17].

2.2　电力信息物理系统跨域攻击辨识

电力CPS跨域安全事件辨识的目的是判断系统中是否出现异常事件,即判断系统状态正常与否,辨识方法可分为图1所示的基于偏差和基于特征.(1)基于偏差的辨识方法:选择与攻击强相关的系统量测、控制信号或网络通道状态等进行监控,当检测到运行中这些变量值偏离正常范围达到一定阈值时认为出现攻击. 常用的偏差量包括:(a)统计分布偏差:基于采集信息的统计规律和物理模型,设定正常模式范围以检测攻击事件[18];(b)控制效果偏差:基于控制反馈的效果偏差检测网络攻击事件[19];(c)预测偏差:基于电力CPS预测状态和实际状态的对比结果以检测异常[20]. (2)基于特征的辨识方法:基于系统正常运行和受攻击状态下的特征比对结果,判断是否出现攻击. 主要方法有:(a)基于系统物理模型,通过对系统运行机理的分析确定系统正常运行的状态特征[21];(b)基于数据驱动方法,基于数据提取形成的攻击事件特征库,分析正常事件、普通故障和攻击事件的特征[20~23].

现有依赖单侧数据信息的异常辨识的方法可能在实际应用时出现误检、漏检,而信息-物理侧关联辨识的研究尚不充分. 单侧信息检测方法难以区分监控信号

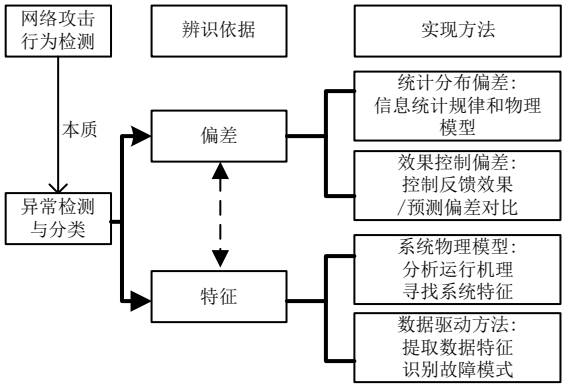

图1　现有电力CPS安全事件检测方法

所传递的信息,无法辨别故障与攻击行为. 因此,有必要开展信息物理融合的事件辨识方法研究,通过双侧数据的耦合关联弥补单侧检测能力的缺陷.

2.3　电力信息物理系统跨域攻击防御

电力CPS的网络安全防御需同时保证信息和物理双侧安全. 当前研究侧重发挥本侧内部的安全防护能力,或通过耦合关联利用另一侧信息协助保护本侧安全(主要是物理侧). 现有电力CPS网络安全防御手段总结如图2所示,(1)信息侧主要包括事前预防和事后应对两类:(a)通过认证、加密、隔离等常规手段或可信计算、区块链等新兴手段实施信息侧防御[24,25];(b)如果网络攻击已经越过信息侧并开始影响物理侧,通过隔离攻击设备或调整控制策略,包括针对DoS攻击可采取追踪溯源、重构网络等事后应对措施.(2)物理侧包括资源调配和数据校正方法:(a)通过在攻击前、攻击中、攻击后部署冗余资源,保障攻击后系统的安稳运行[26];(b)数据校正方法主要作用于攻击后段,对异常数据和控制信号进行校正,从而达到预期的控制效果. 根据对象的不同,可分为针对态势感知预测校正和控制策略校正[3,27,28].

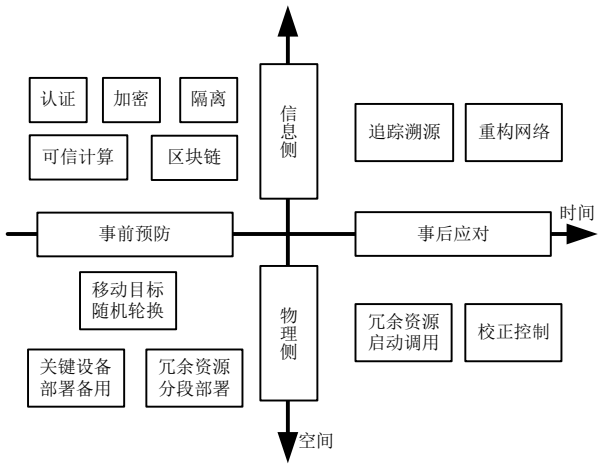

图2　现有电力CPS网络安全防御手段总结

目前研究侧重被动防御方法,在跨域攻击方式快速更新的背景下容易出现漏洞. 与发现攻击后封堵查杀式的被动保护相比,主动保护以增强系统自身安全性和弹性为宗旨,在网络安全威胁仍在萌芽阶段时进行主动防护,对未知的攻击方式也有一定防御能力. 另一方面,现有研究中常常仅考虑如物理侧配置冗余设备增加信息篡改难度的单向利用,在防御方法中的信息-物理侧双向交互过程有待研究[29].

3 电力基础设施信息物理协同安全防御架构与方法

针对传统防御手段在应对信息物理跨域攻击方面的局限性,本节将探讨并构建信息物理协同安全防御架构与策略. 首先,以乌克兰电网大规模停电事件为背景,分析信息物理协同防御的紧迫性;其次,依托电网安全稳定三道防线,构建包含多道防线的信息物理协同安全防御体系;最后,在时间维度上,从感知、辨识、阻断三个方面设计相应的防御方法,提出基于信息物理关联状态分析的跨域攻击协同感知策略、知识-数据融合驱动的跨域攻击协同辨识策略以及信息物理协同优化的跨域攻击紧急阻断策略.

3.1 信息物理协同防御应对跨域攻击的必要性

以乌克兰电网大规模停电事件为例,探讨信息物理协同防御的重要性. 此次电网停电源于跨域攻击,攻击者疑似具备电力业务专业知识. 其攻击过程可分为以下三个步骤:首先,在事发前潜伏于系统中搜集情报;其次,恶意伪造操作指令,导致发电厂跳闸;最后,协同发起 DDoS 攻击,使远程通信中断,进而加剧攻击影响.

乌克兰电网跨域攻击实例表明,电力 CPS 网络攻击通常从信息侧渗透,继而在物理侧利用系统业务流程漏洞和物理约束进行破坏. 这一特点使得 CPS 攻击显著区别于普通互联网攻击,从而对电力 CPS 网络安全防御提出了更高要求[30],以构建时空协同的安全防御新体系为例,需关注以下问题.

(1)协同信息物理空间资源. 信息物理协同防御能够提升识别潜在攻击目标的精确度,从而防止防御资源的低效或无效配置. 以图 3 所展示的乌克兰 BalckEnergy 事件部分过程为例,假设攻击者利用已获得的权限规避事前攻击感知,并导致控制装置产生误动. 当攻击成功入侵后,现行的电力物理侧保护策略会将攻击误判为合法指令并执行. 若因为信息侧和物理侧的时空差异性,无法识别出指令异常,导致本次故障被认为是偶然误动,则可能为未来大规模攻击埋下隐患. 实际上,远程下发控制指令和偶然误动导致的故障虽然均属于小概率事件,但它们之间可能存在关联. 因此,通过双侧信息协同分析可以揭示这种关联并发掘潜在攻击事件.

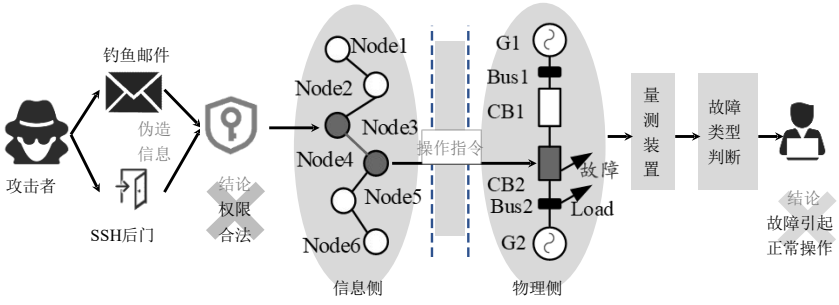

图 3 乌克兰 BlackEnergy 事件单侧辨识结果:信息侧和物理侧均得到错误结论

(2)在上述事件中,攻击过程呈现出“潜伏(事前)-试探(稳态)-生效(暂态)”的特点,跨越了多个时间尺度. 因此,为应对此类攻击,有必要拓展信息-物理防御深度. 在物理侧的规划与部署阶段,应重视网络安全防御,构建全面覆盖电网 CPS 全过程的多重防御体系,这将有助于在各个阶段发现并阻断攻击途径,为前期防御措施提供有力支持.

基于上述分析,本文构建信息物理协同的电力基础设施网络安全防御体系. 首先,将电力 CPS 的防御阶段进行分解,构建相应的协同防御体系架构;接着,对关键环节进行深入分析,提出具体防御方法.

3.2 信息物理协同安全防御架构

在电网安全稳定三道防线基础上,构建包含多道防线的信息物理协同安全防御体系. 该体系的总体架构如下:首先,在攻击入侵之前,优化配置保护资源;其次,在攻击潜伏阶段,系统通过协同感知识别异常;最后,在攻击导致故障之后,实施故障溯因和紧急恢复控制. 针对攻击的各个阶段,均采取相应的信息物理协同措施和保护方案,如图 4 所示.

(1)保护资源优化配置. 在遭受攻击入侵之前,保护资源的配置状态对攻击者的攻击手段的成功与否具有显著影响. 通过优化资源配置,提升关键区域与设备

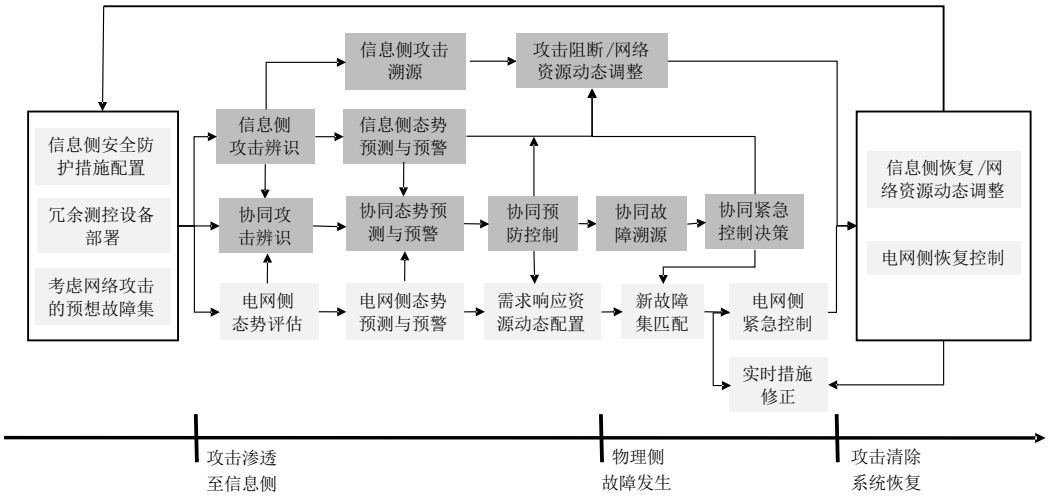

图4　信息物理协同防御体系整体架构

在网络防御方面的性能,可以预先降低网络安全风险,减小遭受攻击的可能性. 具体措施包括信息侧安全防护措施的优化配置、冗余测控设备的优化部署等.

(2)稳态攻击感知. 在攻击开始渗透但尚未对电力物理系统的稳定状态产生影响时,进行的攻击检测方法. 目前,入侵检测系统主要依赖单一信息侧数据进行检测,重点关注验证信息行为的合法性,但对分析信息行为的合理性关注不足. 以图5所示场景为例,信息系统的数据流量和业务进程会受到不同负荷状态下系统对物理状态采样频率的影响.

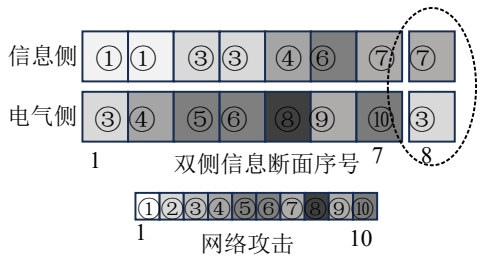

图5　电力CPS双侧状态关联典型场景

借助社会工程学技巧,攻击者可以获取必要的攻击知识,对工程故障展开攻击,从而在一定程度上掌控信息侧的变化. 如图5中的攻击断面8所示,在保持权限和协议合法的前提下,攻击者将信息侧状态维持在历史数据状态的上下限之间,从而导致传统信息检测方法出现漏检. 然而,通过双侧数据综合分析,可知在断面8所对应的物理侧状态下,其信息侧状态实为异常断面数据. 因此,鉴于电力CPS的信息物理耦合特性,运用信息物理协同的攻击感知方法有望为入侵检测系统提供有益的补充,以便发现刻意设计的隐蔽攻击行为.

(3)跨域攻击辨识. 当攻击已经发生且对电力系统状态产生影响时,静态攻击感知无法确保所有攻击行为都能在信息层面被发现并拦截,这意味着网络攻击仍可能引发工程故障. 目前,一般采用“三道防线”策略来对抗单一或多重故障,通过电网故障诊断流程确定故障类型及故障元件并予以隔离. 在网络攻击场景下,量测数据和控制指令可能被攻击者篡改. 如图5所示的案例所示,同时考虑信息侧和物理侧有助于有效识别和追踪故障. 因此,有必要利用双侧数据的耦合关联关系以弥补单侧检测能力的不足,开展双侧协同的事件溯源方法研究. 在构建纵深防御体系时,引入信息物理协同的故障溯源环节可为后续采取针对性紧急措施提供支持.

(4)攻击紧急阻断. 当攻击已经发生并导致物理侧出现故障时,电力系统常规的实时故障诊断过程通常首先提取故障特征,并通过事先制定预想故障集查找紧急控制措施. 然而,在网络攻击情况下,一些传统意义上的“小概率”故障场景发生概率可能会增加,但这些场景并未被纳入原有的预想故障集中. 因此,应在现有故障集基础上,考虑网络攻击的影响,对预想故障集进行补充. 此外,提前制定的紧急控制策略的实施效果取决于相关通信路径和设备的正常可靠运行. 因此,在应对网络攻击导致的故障时,需要考虑策略相关通信路径的实时性和物理设备的可靠性.

在图4所示的整体架构中,下文从感知、辨识、阻断三个方面设计相应的防御方法.

3.3　跨域攻击感知——基于信息物理关联状态分析的跨域攻击协同感知方法

为获取电网运行状态相关数据以实施有效的跨域攻击,攻击者在获得系统权限后,需要潜伏以进行信息收集,直至达到预期目标. 当攻击行为并未造成明显的状态异常时,以单一信息数据为支撑的网络安全感知方法难以发现潜伏的跨域攻击行为. 然而,当信息侧与

物理侧耦合后,双边关联得到加强,因此通过信息物理关联状态分析以感知潜在的网络攻击.

孤立森林算法是常用的异常感知算法,其核心理念是根据数据集构建一棵二叉树,通过对数据集的每一维属性随机设定值,将数据划分至两个空间域,并在划分后的空间内重复该过程,直至树的高度达到预设值或划分出的空间仅包含单一数据.在各类数据中,由于异常数据数量较正常数据稀少,数据特征相似性弱,其对应的路径较短,迅速被孤立.鉴于孤立森林算法高效、低复杂度的特点,该问题适用该算法.在森林属性选择方面,研究了不同工况下的双侧运行数据.信息侧数据包括延时、传输数据量、链路利用率和进程CPU占用率;物理侧数据涵盖节点电压、线路潮流;其他告警信息包括稳控装置软压板状态(投、退)等.

针对电力CPS双侧数据,本文在原有孤立森林模型基础上,提出了一种改进方法.该方法首先遵循无监督学习和集成学习原则,通过有放回抽样历史数据集训练,构建出相互独立的隔离树.接着,通过无放回抽样构建多个子森林感知模型,形成主森林感知模型.鉴于不同类型电力系统运行规划和运行状态分布具有各自独立的特征,随机抽样所得子森林模型对特定系统的适应度存在差异,可能导致检测效果偏差.因此,本文提出基于错误样本反馈,根据训练中错判样本反馈调整子森林模型权重比例.在具体案例中,减小偏差较大的子森林模型权重,增加准确性较高的子森林模型权重,实现主森林模型与系统的高度适配,优化子森林权值得到对特定系统适应度较高的动态权值集成孤立森林.改进孤立森林的具体构建流程如图6所示.

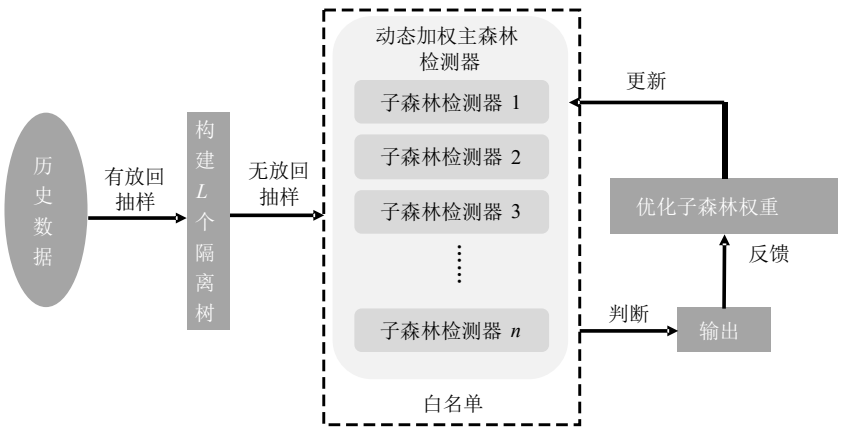

图6 动态权值集成孤立森林构建流程

3.4 跨域攻击辨识——知识-数据融合驱动的跨域攻击协同辨识方法

当前电网信息侧的网络安全管理平台主要依赖流量和日志变化,而物理侧的事件感知系统则主要基于SCADA(Supervisory Control And Data Acquisition)和WAMS(Wide Area Measurement System)状态,这两种系统相对独立,在应对针对性强的跨域攻击时,仅依靠单侧信息难以有效识别事件属性.为防止伪造指令或信号造成更大范围的影响,亟需迅速辨识当前指令或信号是由于物理侧自然故障所致,还是网络攻击引发的.因此提出知识-数据融合驱动的跨域攻击协同辨识方法,如图7所示.

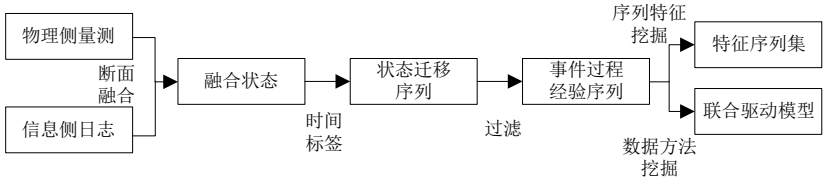

图7 信息物理协同的暂态故障溯因流程

信息侧数据主要包括流量、日志记录等离散化事件描述数据,电网侧数据主要包括电气量测(连续)、开关量信号(离散)等状态描述数据,且通常具备全网同步时钟.在进行信息侧与物理侧数据的融合分析之前,需解决断面时钟同步问题和异构数据映射关联问题.首先,分析信息侧异常检测和报警信号汇集时间的构成及典型分布,确定影响信号汇集时间动态变化的因素及合理分布范围;考虑设备及通信网络运行状态变化对信号汇集时间的影响,进行动态评估;接着,分析信息侧与物理侧事件/量测数据的时序关联特征,构建信息物理数据虚拟时钟,生成电网信息物理同步断面,如图8所示.

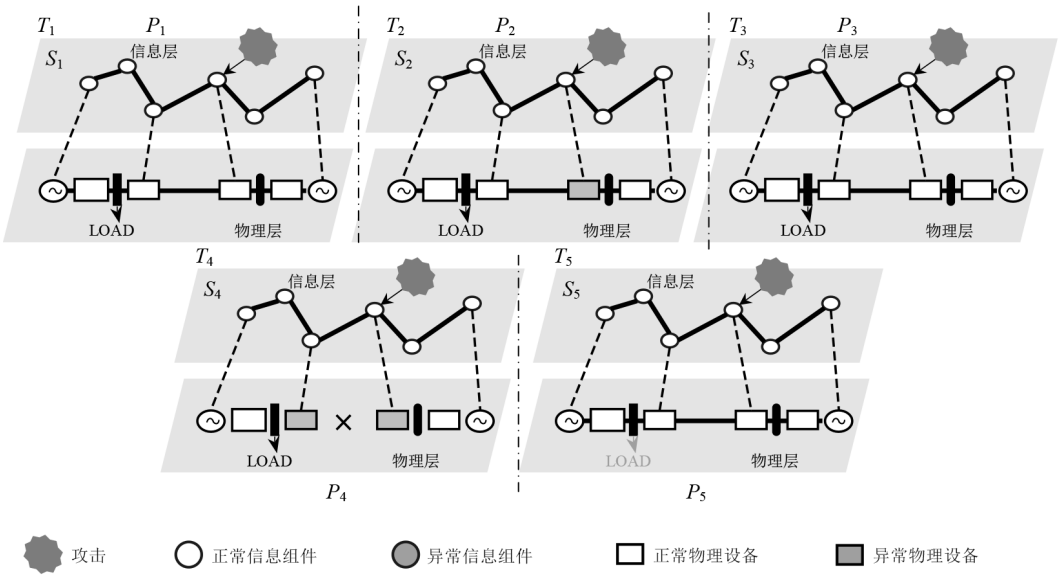

图8　信息物理同时特征断面

针对事件、报警信号以及状态量测等多源异构数据,研究其时空关联特性,从而构建电力CPS基础数据的时空映射关系. 进一步地,基于信息物理交互影响机理与网络攻击跨空间传播机理,挖掘双侧数据关联关系. 通过分析受人为规则定义的指令行为与受电力本质约束的物理响应的关联关系,提取系统典型状态下的正常互动模式,以实现异常检测. 基于正常互动模式频繁集的异常检测方法有信息物理交互机理支持,辨识结果可信可解释,但难以保证模型全面性和灵活性;数据驱动方法能够通过样本进行频繁集的泛化挖掘,但存在样本依赖性强和缺乏可解释性等问题. 所以采用知识-数据融合驱动模式对信息物理事件频繁集进行挖掘,形成事件协同辨识,如图9所示.

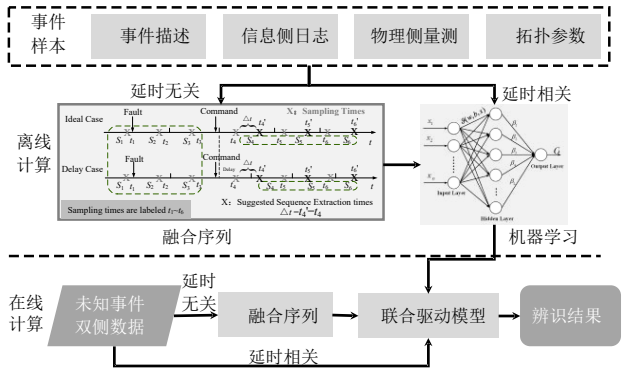

图9　数据-知识联合驱动攻击辨识模型

3.5　跨域攻击阻断——信息物理协同优化的跨域攻击紧急阻断方法

当跨域攻击已经造成电网物理侧故障时,传统的以预想故障集为基础的紧急控制策略只能应对偶发性故障,而无法应对蓄意攻击. 为及时有效地阻断攻击影响,需要建立包含信息侧攻击和物理侧故障的信息物理预想故障集. 因此,本文提出了信息物理协同优化的跨域攻击紧急阻断方法,包括计及网络攻击的预想故障集生成方法和信息物理协同的双层自适应紧急控制方法,具体控制策略如图10所示. 首先,对CPS初始状态进行关联建模[31],在跨域攻击发生后,根据攻击影响和突发事件修正系统状态,从而建立新的CPS模型. 进一步分析既定紧急控制策略的可用性,若可行,则执行原策略;若不可行,则通过信息物理双层优化,得到替代控制策略并执行,确保一次系统的安全稳定运行.

4　算例分析

基于第3节提出的信息物理协同防御架构和方法,本节通过算例分析验证方法的可行性和有效性. 本节所有算例均基于OPAL-RT公司技术和OPNET(OPtimized Network Engineering Tool)构建的电力CPS实时仿真平台建模和仿真[32,33],在OPAL-RT平台中搭建电力系统模型,在OPNET中搭建相应的通信系统模型,并构建自动攻击脚本以模拟跨域攻击行为.

4.1　跨域攻击感知算例分析

针对第3.3节提出的基于信息物理关联状态分析的跨域攻击协同感知方法进行仿真验证. 基于实时仿真平台构建攻击者获得系统权限后潜伏以进行信息收集的场景. 采用如图11所示的IEEE 14节点标准系统及其信息系统进行测试,物理侧负荷水平为[0.8,1.2]范围内波动的正态分布,信息侧则根据线路负载水平调整采样频率,如图12所示. 所采集信息侧数据包括通

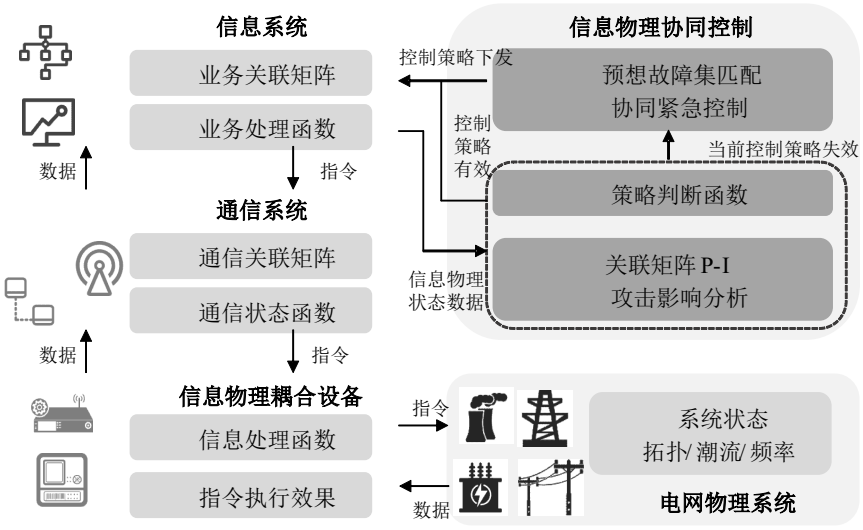

图 10 信息物理协同优化的跨域攻击紧急阻断方法

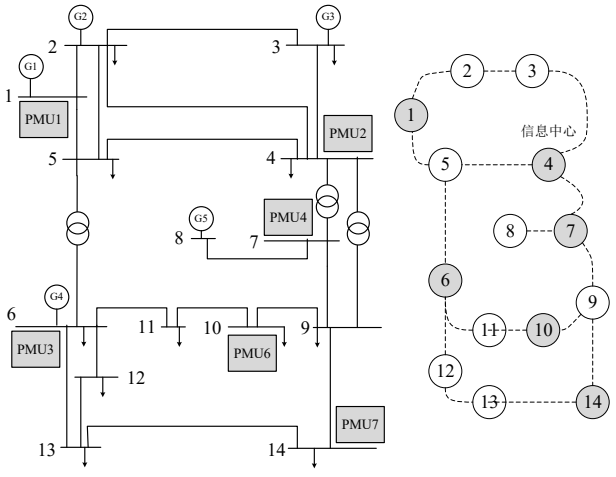

图 11 IEEE 14 节点系统物理系统和信息系统拓扑

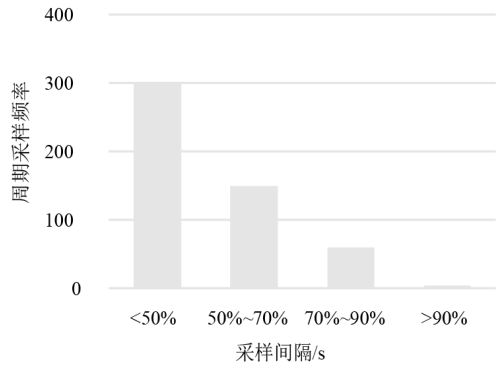

图 12 信息侧相关数据

信流量、链路延迟，节点资源占用率，物理侧数据包括系统潮流数据，样本共 80 维. 通过自动仿真生成 1 200 组样本，其中 200 组为攻击场景. 通过采用曲线下的面积值与定义的 F_n 指标，对异常检测算法的性能进行评估，定义检测出的异常样本与判断为异常样本的比值为 N_p，定义检测出的异常样本与实际异常样本总数的比值为 N_r，定义指标 $F_n=2\left[N_pN_r/\left(N_p+N_r\right)\right]$.

图 13 展示了基于信息物理状态关联的孤立森林算法与其他异常检测算法的性能对比，包括基于信息单侧数据的孤立森林算法、局部离群因子（Local Outlier Factor，LOF）算法以及一分类支持向量机（One Class SVM，OCSVM）算法. 从图 13 中可以看出，基于信息单侧数据的算法在挖掘隐蔽恶意攻击方面的能力较为有限. 在基于双侧信息的三种方法中，LOF 算法和 OCSVM 对于信息侧变化有限攻击的挖掘效果均不如改进后的孤立森林模型. 在计算时间方面，OCSVM 不适用于高维度数据集，孤立森林方法的训练时间最短，此处所提训练时间仅涵盖初始主森林的形成，未包括后续的动态权值优化时间. 在检测计算速度方面，孤立森林算法具有线性时间复杂度，子森林集成的方法适用于含有海量数据的数据集. 通常情况下，树的数量与算法的稳定性呈正相关，树独立生成的特性使其能够提高大规模分布式系统的运算速度.

图 14 给出了经过长时间仿真之后，动态权值集成孤立森林算法与原有孤立森林模型的曲线下面积值和 F_n 指标结果，结果显示本文所提方法更能适应复杂的、时变的电力 CPS 运行状况.

4.2 跨域攻击辨识算例分析

针对知识-数据融合驱动的跨域攻击协同辨识方法进行验证. 以图 15 所示的电力系统距离保护业务开展测试. 设置系统中除平衡节点外任意节点发生不平衡功率扰动事件概率相同，扰动大小和持续时间分别服从[0.1，1.2]的均匀分布和 N(0.1，0.03)的正态分布，算例场景分为网络攻击场景、单相接地短路和正常运行

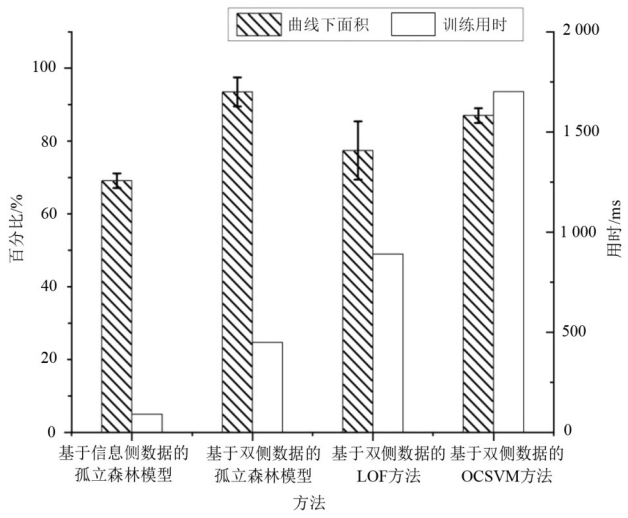

图 13　不同方法结果对比

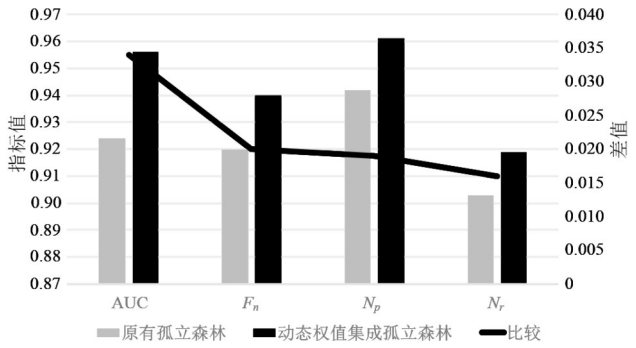

图 14　动态权值集成孤立森林算法与原有孤立森林模型在长时间仿真内检测结果

三类,共24个场景事件.

在仿真过程中,各个场景以系统达到并重新恢复稳定状态为一次仿真的起点和终点. 系统每秒对同步量测数据进行200次采集,攻击时间稍短于采样间隔0.005 s.共仿真获得916组样本,具体内容如图16所示. 物理侧同步相量数据包括离散的相电压和相电流. 每次事件记录约包含4 000个时刻的数据,对应约20 s的仿真时间.

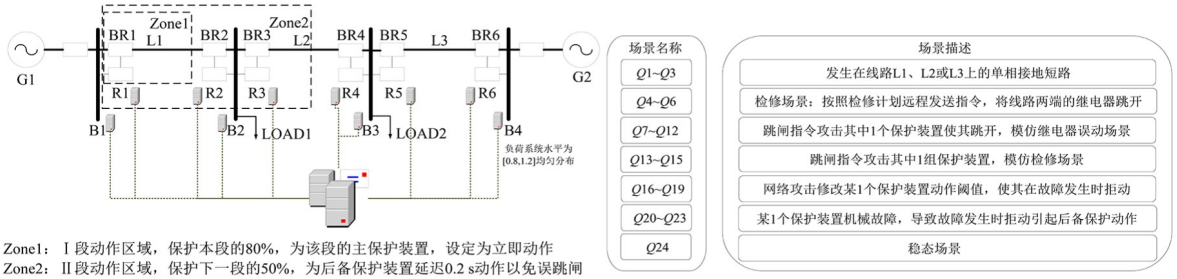

图 15　测试系统架构,各算例场景名称与相应描述

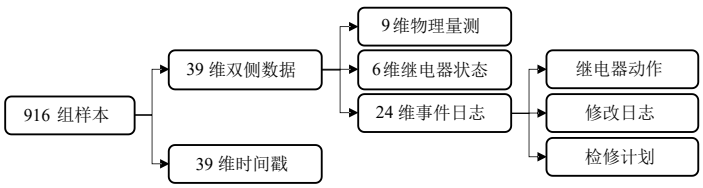

图 16　算例结果

本文方法的整体辨识结果如表1所示. 三种不同模型的辨识比较结果如图17所示,实验表明联合驱动模型的辨识效果明显优于纯数据驱动模型与纯序列驱动模型,且辨识时间几乎相同.

本文探讨的联合驱动模型辨识结果的假阳性率是衡量模型性能的关键指标之一. 将攻击事件误判为自然故障的情况,其后果尤为严重. 因此,在训练模型的过程中,以不漏检任何网络攻击事件为最低标准,从而获得非攻击事件辨识的假阳性率,如图18所示. $Q1$~$Q3$的特例中,大部分被错误分类到继电器机械故障场景,$Q4$和$Q6$的特例被辨识为针对两侧继电器的虚假指令攻击. 电力CPS系统的动态变化和数据的偏差均有可能导致假阳性.

表 1　基于特征序列匹配方法辨识准确率

场景类别	准确率/%
所有场景	91.6
网络攻击	85.2
自然故障	96.0
未知	2.0
不确定	6.4

4.3　跨域攻击阻断算例分析

针对信息物理协同优化的跨域攻击紧急阻断方法开展验证. 以IEEE 14节点系统为例生成预想故障集. 遍历电力系统攻击成功状态空间,分别计算网络攻击

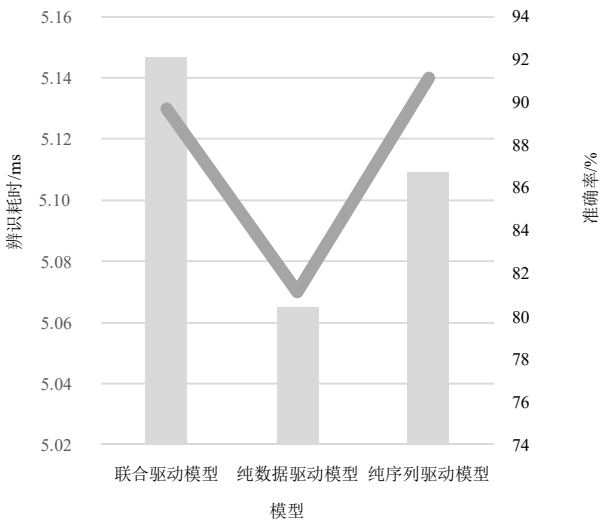

图17 联合驱动、纯数据驱动、纯序列驱动模型验证结果

成功后系统损失的负荷量,将攻击类型、成功的线路和电力系统损失的非零负荷量加入预想故障集分别如图19所示,IEEE 14节点预想故障集后果如图20所示.

在所搭建的CPS仿真模型中,控制信息从负控中心站(命名为MS)经不同切负荷子站(命名为SS)到达执行站(命名为ES)的总体通信时延. 例如,主站向子站SS1下达切负荷指令,该指令通过2 M光纤传输到子站,再通过就近变电站中的光纤转换器转成分路信号,传输给子站下面管理的执行站ES2、ES3等. 攻击场景为DoS攻击导致通信链路不可用,验证在攻击状况下本论文所提信息物理协同自适应策略调整方法的有效性. 系统对应的二次设备层和通信层简化网络如图21所示,包含1个主站(MS)、4个子站(SS)、11个执行站(ES)和14个通信节点.

	攻击场景	非攻击场景
攻击场景	487	0
非攻击场景	5	424

场景名称	假阳性率
$Q1$~$Q3$	3.0%/3.1%/3.1%
$Q4$	2.8%
$Q5$	全部分类正确
$Q6$	2.7%

图18 非攻击事件辨识的假阳性率结果

序号	攻击方式	攻击导致脱网节点/线路
1~17	紧急状态下DoS攻击使安控装置拒动	节点:(1),(4),(9),(14) (13) (4) (10) (5) (12) (11) (4) (1,6) (4,13) (8,3) (10,3) (7,9),(12,13)
18~21	跳闸指令重放攻击	线路:(6-11),(6-13),(7-9),(9-14)

图19 考虑网络攻击预想故障集

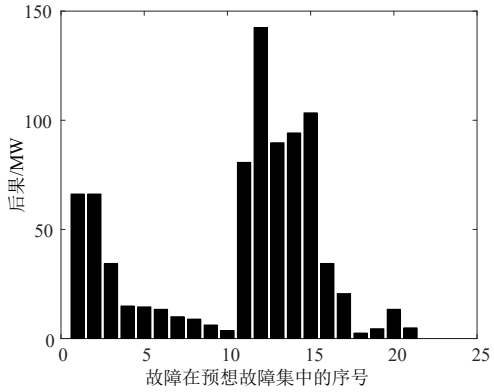

图20 IEEE 14节点预想故障集后果

根据相关标准,故障发生,策略匹配到动作指令到达整个过程需要在300 ms以内完成[33,34]. 基于关联矩阵采用混成计算方法,建立系统信息和指令上传下达矩阵.

场景1:无网络攻击,信息按照ES10-SS3-MS顺序上传,指令按照MS-SS4-ES4顺序下达.

场景2:DoS攻击导致通信链路7-9堵塞,系统无策略调整能力,攻击的影响为$C'(7,9)=C(7,9)+C7-9=+\infty$. 频率继续下降到49.90 Hz后触发后续动作,切除节点9负荷10 MW,指令下发路径为MS-ES5.

场景3:DoS攻击导致通信链路7-9堵塞,触发系统策略调整模块. 第一次优化,物理目标不变,指令经过9-10-11-6-5-4-7到达SS4,经校核,延时不符合业务要求. 第二次优化,切除目标改为节点6负荷6 MW,指令经过MS-SS1-ES7,策略优化过程耗时约20 ms,重新规划的信息下发路径耗时比既定策略耗时多24 ms. 各场景根据关联特性矩阵计算得到的动作延时情况如图22所示.

分析得到各场景动作延时,负荷损失情况和系统频率变化如图23所示. 在联合仿真平台分别仿真三种场景,结果如图24所示. 在常规故障时,电力系统的三道防线可

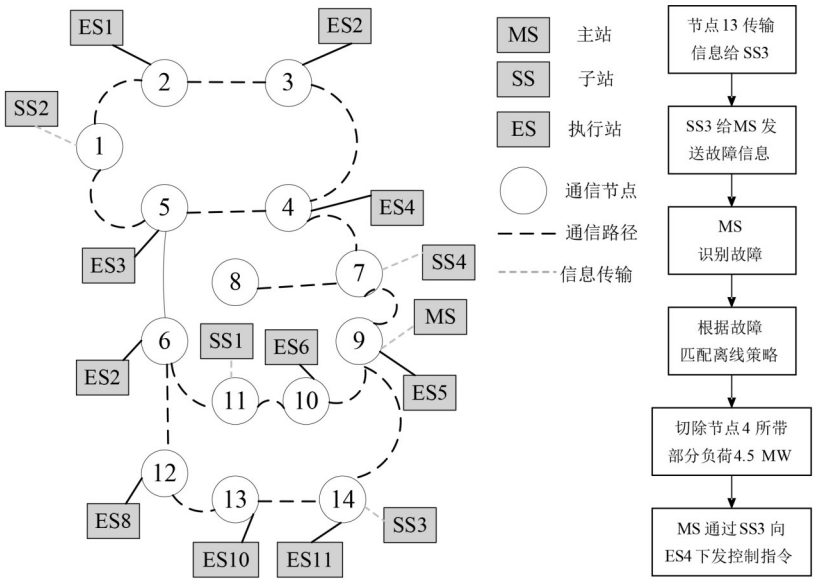

图21　通信网络拓扑和安全稳定控制系统各站的位置以及安全稳定防御系统动作顺序

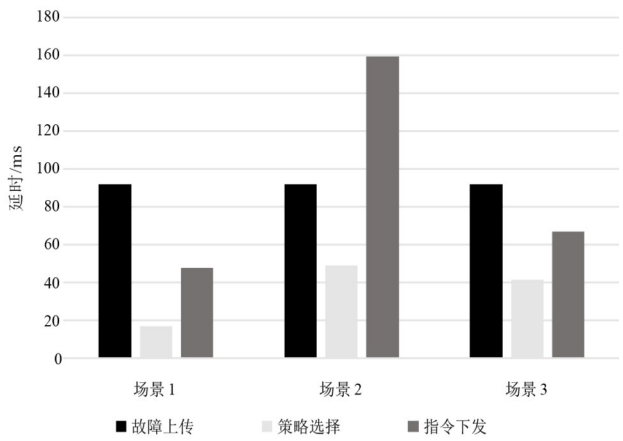

图22　不同场景下故障上传、策略选择、指令下发延时情况

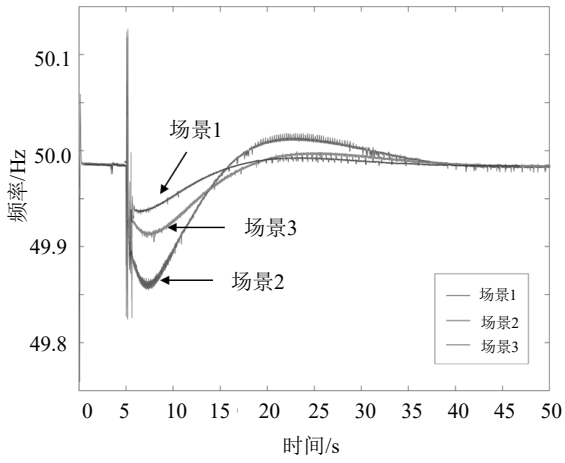

图24　各场景下系统频率变化

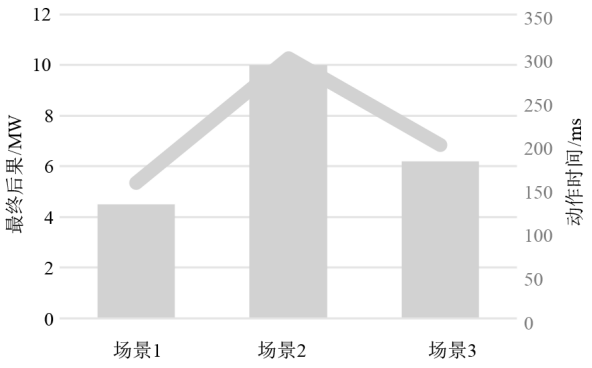

图23　不同场景下最终后果、动作时间、频率最低点对比结果

以较好地恢复电网频率. 当有DoS攻击造成控制指令延时,系统频率没有恢复却不断跌落,触发了后续的切负荷指令执行,使得负荷减载量变大,频率跌落更加严重,若后续的攻击仍被堵塞则后果将更加严重.

5　结论与展望

本文分析了信息物理协同防御应对跨域攻击的必要性,构建了电力信息物理协同安全防御架构,并提出了基于信息物理关联状态分析的跨域攻击协同感知方法、知识-数据融合驱动的跨域攻击协同辨识方法和信息物理协同优化的跨域攻击紧急阻断方法等技术. 在后续研究中,信息物理系统跨域攻击的深层次传播机理亟待深入挖掘与探讨. 通过对传播机理的探究,能为电力信息物理系统防御跨域攻击提供更优质的防御策略设计理念. 此外,需进一步研究更广泛场景下信息物理系统的攻击威胁,以提升电力系统在面对未知攻击时的抵御能力. 同时,本文所提架构的实际应用依赖于电力监控系统、网络安全管理平台、通信管理系统等多个系统平台,需要从管理机制、数据业务接口等方面推动数据和业务的充分融合与协同.

参考文献

[1] YU X H, XUE Y S. Smart grids: A cyber-physical systems perspective[J]. Proceedings of the IEEE, 2016, 104(5): 1058-1070.

[2] 张涛, 赵东艳, 薛峰, 等. 电力系统智能终端信息安全防护技术研究框架[J]. 电力系统自动化, 2019, 43(19): 1-8, 67.
ZHANG T, ZHAO D Y, XUE F, et al. Research framework of cyber-security protection technologies for smart terminals in power system[J]. Automation of Electric Power Systems, 2019, 43(19): 1-8, 67. (in Chinese)

[3] 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(3): 3-14.
XU F Y, XUE A C, CHANG N C, et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems, 2021, 45(3): 3-14. (in Chinese)

[4] 蔡晔, 刘放, 曹一家, 等. 电力信息物理系统低代价多阶段高危攻击策略研究[J]. 电力系统自动化, 2021, 45(20): 1-8.
CAI Y, LIU F, CAO Y J, et al. Research on low-cost multi-stage high-risk attack strategy for power cyber-physical system[J]. Automation of Electric Power Systems, 2021, 45(20): 1-8. (in Chinese)

[5] 李满礼, 倪明, 颜云松, 等. 面向恶意攻击的安全稳定控制系统信息物理协调防御方法[J]. 电力系统自动化, 2021, 45(18): 113-121.
LI M L, NI M, YAN Y S, et al. Cyber-physical coordinated defense method against malicious attacks for security and stability control system[J]. Automation of Electric Power Systems, 2021, 45(18): 113-121. (in Chinese)

[6] 刘依晗, 王宇飞. 新型电力系统中跨域连锁故障的演化机理与主动防御探索[J]. 中国电力, 2022, 55(2): 62-72, 81.
LIU Y H, WANG Y F. Exploring the evolution mechanism and active defense of cross-domain cascading failures in new type power system[J]. Electric Power, 2022, 55(2): 62-72, 81. (in Chinese)

[7] 王宇飞, 邱健, 李俊娥. 考虑攻击损益的电网CPS场站级跨空间连锁故障早期预警方法[J]. 中国电力, 2020, 53(1): 92-99.
WANG Y F, QIU J, LI J E. A station level early warning method of cascading failures across space based on attack gain and cost principle in GCPS[J]. Electric Power, 2020, 53(1): 92-99. (in Chinese)

[8] 章锐, 费稼轩, 石聪聪, 等. 特定攻击场景下源网荷系统恶意攻击关联分析方法[J]. 中国电力, 2019, 52(10): 1-10.
ZHANG R, FEI J X, SHI C C, et al. Malicious attack correlation analysis method of source-grid-load system under specific attack scenarios[J]. Electric Power, 2019, 52(10): 1-10. (in Chinese)

[9] 汤涌. 基于响应的电力系统广域安全稳定控制[J]. 中国电机工程学报, 2014, 34(29): 5041-5050.
TANG Y. Response-based wide area control for power system security and stability[J]. Proceedings of the CSEE, 2014, 34(29): 5041-5050. (in Chinese)

[10] 王琦, 李梦雅, 汤奕, 等. 电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J]. 电力系统自动化, 2019, 43(9): 9-21.
WANG Q, LI M Y, TANG Y, et al. A review on research of cyber-attacks and defense in cyber physical power systems part one modelling and evaluation[J]. Automation of Electric Power Systems, 2019, 43(9): 9-21. (in Chinese)

[11] 胡向东, 吕高飞, 白银. 基于优化支持向量回归的工业互联网安全态势预测方法[J]. 电子学报, 2023, 51(2): 446-454.
HU X D, LÜ G F, BAI Y. A method of security situation prediction for industrial Internet based on optimized support vector regression[J]. Acta Electronica Sinica, 2023, 51(2): 446-454. (in Chinese)

[12] XIANG D M, LIN S, WANG X H, et al. Checking missing-data errors in cyber-physical systems based on the merged process of petri nets[J]. IEEE Transactions on Industrial Informatics, 2023, 19(3): 3047-3056.

[13] 安宇, 刘东, 陈飞, 等. 考虑信息攻击的配电网信息物理运行风险分析[J]. 电网技术, 2019, 43(7): 2345-2352.
AN Y, LIU D, CHEN F, et al. Risk analysis of cyber physical distribution network operation considering cyber attack[J]. Power System Technology, 2019, 43(7): 2345-2352. (in Chinese)

[14] XU Y. A review of cyber security risks of power systems: From static to dynamic false data attacks[J]. Protection and Control of Modern Power Systems, 2020, 5: 19.

[15] CHE L, LIU X, LI Z Y. Mitigating false data attacks induced overloads using a corrective dispatch scheme[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 3081-3091.

[16] 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(3): 15-23.
CHEN L D, LIU N. False data injection attack and its detection method for interactive demand response[J]. Automation of Electric Power Systems, 2021, 45(3): 15-23. (in

Chinese)

[17] 刘权莹, 李俊娥, 倪明, 等. 电网信息物理系统态势感知: 现状与研究构想[J]. 电力系统自动化, 2019, 43(19): 9-21, 51.
LIU Q Y, LI J E, NI M, et al. Situation awareness of grid cyber-physical system: Current status and research ideas [J]. Automation of Electric Power Systems, 2019, 43(19): 9-21, 51. (in Chinese)

[18] 陈碧云, 李弘斌, 李滨. 伪量测建模与AUKF在配电网虚假数据注入攻击辨识中的应用[J]. 电网技术, 2019, 43(9): 3226-3236.
CHEN B Y, LI H B, LI B. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network[J]. Power System Technology, 2019, 43(9): 3226-3236. (in Chinese)

[19] LIN H, SLAGELL A, KALBARCZYK Z T, et al. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids[J]. IEEE Transactions on Smart Grid, 2018, 9(1): 163-178.

[20] 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.

[21] 曹翔, 张阳, 宋林川, 等. 基于深度报文检测和安全增强的正向隔离装置设计及实现[J]. 电力系统自动化, 2019, 43(2): 162-167.
CAO X, ZHANG Y, SONG L C, et al. Design and implementation of forward isolation device based on deep packet inspection and security enhancement[J]. Automation of Electric Power Systems, 2019, 43(2): 162-167. (in Chinese)

[22] WANG H Z, RUAN J Q, WANG G B, et al. Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(11): 4766-4778.

[23] 李元诚, 曾婧. 基于改进卷积神经网络的电网假数据注入攻击检测方法[J]. 电力系统自动化, 2019, 43(20): 97-104.
LI Y C, ZENG J. Detection method of false data injection attack on power grid based on improved convolutional neural network[J]. Automation of Electric Power Systems, 2019, 43(20): 97-104. (in Chinese)

[24] ZHENG P L, XU Q Q, LUO X P, et al. Aeolus: Distributed execution of permissioned blockchain transactions via state sharding[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 9227-9238.

[25] POLITOU E, CASINO F, ALEPIS E, et al. Blockchain mutability: Challenges and proposed solutions[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9 (4): 1972-1986.

[26] SANJAB A, SAAD W. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.

[27] 刘亮, 苏盛, 曹一家, 等. 基于Kalman滤波的持续卫星时间同步攻击防护方法[J]. 电力系统自动化, 2020, 44 (10): 119-126.
LIU L, SU S, CAO Y J, et al. Kalman filtering based protection method of sustained satellite time synchronization attack[J]. Automation of Electric Power Systems, 2020, 44(10): 119-126. (in Chinese)

[28] CHLELA M, MASCARELLA D, JOÓS G, et al. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4702-4711.

[29] 汤奕, 李梦雅, 王琦, 等. 电力信息物理系统网络攻击与防御研究综述(二)检测与保护[J]. 电力系统自动化, 2019, 43(10): 1-9, 18.
TANG Y, LI M Y, WANG Q, et al. A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection[J]. Automation of Electric Power Systems, 2019, 43(10): 1-9, 18. (in Chinese)

[30] 费稼轩, 裴培, 张明, 等. 电网工控网络攻击场景中的层次关联分析方法[J]. 南京理工大学学报, 2020, 44(6): 715-723.
FEI J X, PEI P, ZHANG M, et al. Hierarchical association analysis method in industrial control cyber attack scenario of power grid[J]. Journal of Nanjing University of Science and Technology, 2020, 44(6): 715-723. (in Chinese)

[31] 薛禹胜, 李满礼, 罗剑波, 等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化, 2018, 42(2): 11-19.
XUE Y S, LI M L, LUO J B, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11-19. (in Chinese)

[32] 汤奕, 王琦, 郜伟, 等. 基于OPAL-RT和OPNET的电力信息物理系统实时仿真[J]. 电力系统自动化, 2016, 40 (23): 15-21, 92.
TANG Y, WANG Q, TAI W, et al. Real-time simulation

of cyber-physical power system based on OPAL-RT and OPNET[J]. Automation of Electric Power Systems, 2016, 40(23): 15-21, 92. (in Chinese)

[33] YANG Z W, LIU H, BI T S, et al. Bad data detection algorithm for PMU based on spectral clustering[J]. Journal of Modern Power Systems and Clean Energy, 2020, 8(3): 473-483.

[34] 蔡星浦, 王琦, 黄建业, 等. 电力系统网络攻击信息物理双层协同紧急控制方法[J]. 全球能源互联网, 2020, 3(6): 560-568.
CAI X P, WANG Q, HUANG J Y, et al. Double-layered cyber-physical cooperative emergency control-strategy-adjustment method to prevent power-system cyber attacks [J]. Journal of Global Energy Interconnection, 2020, 3(6): 560-568. (in Chinese)

作者简介

张 涛 男, 1976 年 10 月出生于陕西榆林. 现为国网智能电网研究院有限公司电网数字化技术研究所副所长. 主要研究方向为电力网络和数据安全.

费稼轩 男, 1984 年 11 月出生于江苏江阴市. 现为国网智能电网研究院电网数字化技术研究所业务安全研究室高级专家. 主要研究方向为电力网络和数据安全.

王 琦 男, 1989 年 4 月出生于江苏南通市. 现为东南大学电气工程学院副教授. 主要研究方向为电网信息物理系统和电力系统网络安全. 中国电子学会会员编号:E190035063M.
E-mail: wangqi@seu. edu. cn

邵志鹏 男, 1984 年 5 月出生于江苏南京市. 现为国网智能电网研究院电网数字化技术研究所业务安全研究室主任. 主要研究方向为电力网络和数据安全.

蔡星浦 男, 1996 年 3 月出生于浙江宁波市. 东南大学电气工程学院硕士学位. 现为国网浙江省电力有限公司杭州供电公司员工. 主要研究方向为电网信息物理系统.