AI 告警降噪技术下电力网络安全防护路径探究

孙婧
吉林电力股份有限公司白城发电公司
DOI:10.12238/acair.v2i4.10301

[摘　要] 为强化电力网络安全防护效能,实现防护的智能化、集成化与高效化,减少故障发生概率,控制使用成本与运维成本,构建电力网络运维管理新生态。文章运用文献资料研究、案例分析等方法,以AI告警降噪技术为切入点,通过概括技术特点,总结技术优势,扭转既有观念。通过算法选择、思路梳理,实现技术整合、流程再造,形成搭建电力网络安全防护新平台。AI告警降噪技术凭借高自动化、高精准度等优势,切合了电力网络安全防护的基本要求。
[关键词] 电力网络；安全防护；AI告警降噪；技术应用；方法路径
中图分类号：G250.72　文献标识码：A

Exploration of Power Network Security Protection Path under AI Alarm Noise Reduction Technology

Jing Sun
Jilin Electric Power Co., Ltd.

[Abstract] In order to strengthen the effectiveness of power network security protection, achieve intelligent, integrated and efficient protection, reduce the probability of failure, control the cost of use and operation and maintenance, and build a new ecology of power network operation and maintenance management. The article uses literature research, case analysis and other methods, taking AI alarm noise reduction technology as the starting point, summarizing the technical characteristics and advantages, and reversing existing concepts. By selecting algorithms and organizing ideas, technology integration and process reengineering are achieved, forming a new platform for building power network security protection. AI alarm noise reduction technology, with its advantages of high automation and high precision, meets the basic requirements of power network security protection.
[Key words] power network; Security protection; AI alarm noise reduction; Technology application; Method Path

前言

根据相关统计部门公布的数据,截至2023年12月底,国内220千伏及以上输电线路建设总长度超过92万公里,全口径发电装机容量达到29.2亿千瓦。着眼电力资源持续输出和稳定供应的总体要求,技术团队通过引入AI告警降噪技术等防护方案,实现电力网络风险隐患的准确识别与高效处置,强化电力网络安全防护能力,确保电力网络自我纠偏能力。

1 AI告警降噪技术特性分析

梳理AI告警降噪技术基本原理与主要特点,引导技术团队掌握底层逻辑,为后续安全防护体系的搭建、防护路径的完善提供便利条件,确保技术应用的针对性与有效性。

1.1 AI告警降噪技术基本原理

AI告警降噪技术体系成熟,涵盖数据收集与预处理、特征提取与选择、模型构建与训练、预警分类与降噪等流程,确保风险隐患识别能力和准确预警,辅助工作团队完成风险处置,保证电力网络运行的稳定性。具体来看,从各种监控系统、传感器等来源收集大量的告警数据[1]。这些数据包含了不同类型的告警信息,可能存在格式不一致、噪声干扰等问题,对数据进行清洗,去除重复、错误或不完整的数据记录。对数据进行标准化处理,将不同格式的数据统一转化为适合分析的格式。将时间戳统一格式,将告警级别进行标准化分类等,为后续的模型训练和分析奠定基础。从预处理后的告警数据中提取有价值的特征。这些特征可以包括告警的类型、频率、时间间隔、来源设备、相关的网络协议信息等。例如,对于网络攻击告警,可能提取攻击的类型、攻击源的IP地址特征、攻击发生的时间频率等作为关键特征。基于提取和选择的特征,选择合适的机器学习或深度学习

模型。常见的模型包括决策树、支持向量机、神经网络等。例如,在处理较为复杂的网络告警数据时,卷积神经网络可以有效地捕捉告警数据中的时空特征,而对于简单的告警分类场景,训练好的模型对新收到的告警数据进行分类。将告警分为真实有效的告警和噪声告警。例如,模型可以根据告警的特征判断某个网络端口扫描告警是来自正常的网络维护行为还是潜在的恶意扫描。

1.2 AI告警铸造技术主要特点

1.2.1高度自动化

AI告警降噪技术能够自动处理大量的告警数据,无需人工手动逐个分析。它可以在短时间内对海量的告警信息进行分类和处理,大大提高了告警处理的效率。例如,在大型数据中心的监控中,每天可能产生数以万计的告警,通过AI告警降噪技术,可以快速准确地筛选出有价值的告警,节省了大量的人力和时间成本。

1.2.2精准度高

基于先进的机器学习和深度学习算法,AI告警降噪技术能够准确地识别告警中的噪声。通过对大量数据的学习和训练,模型可以捕捉到告警数据中的细微模式和规律,从而更精准地判断告警的真实性。相比传统的基于规则的告警过滤方法,AI技术能够适应更复杂的环境和变化,减少误判和漏判的情况。例如,在应对新型网络攻击时,传统方法可能由于缺乏相应的规则而无法准确识别告警,而AI模型可以通过学习新的攻击特征来准确判断告警的有效性。

1.2.3适应性强

AI告警降噪技术可以适应不同类型的系统和环境。无论是网络安全监控、电力系统监控还是工业控制系统监控等,它都可以根据不同领域的告警数据特点进行调整和优化[2]。例如,在电力系统中,告警数据可能与电网运行状态、设备故障等相关,AI模型可以针对电力系统的特定数据模式和故障类型进行训练,从而有效地处理电力告警中的噪声问题；在工业控制系统中,由于系统的复杂性和实时性要求,AI告警降噪技术可以通过不断学习和更新模型来适应不断变化的生产环境和告警类型。

2 AI告警降噪技术在电力网络安全防护中的作用分析

概括AI告警降噪技术与电力网络安全防护内在关联,细化技术方案的实用价值、经济价值,消除错误认知,补齐机制短板,推动安全防护体系转型升级。

2.1提高安全事件响应速度

传统的告警方式可能会产生大量的误报和冗余信息,导致安全人员在处理告警时浪费大量时间在筛选信息上。AI告警降噪技术能够快速准确地过滤掉噪声告警,使安全人员能够迅速聚焦于真正的安全事件,及时采取相应的措施。例如,当电力网络遭受恶意攻击时,如针对电力调度系统的入侵尝试,经过降噪处理后的告警能够使安全团队在最短时间内启动应急响应,减少攻击可能造成的损失。

2.2增强安全防护的精准性

通过对电力网络长期运行产生的告警数据进行学习和分析,AI 告警降噪技术可以识别出不同类型安全威胁的特征模式。这有助于更精准地判断告警的性质,例如,对于变电站内设备的异常告警,可以区分是正常的设备老化磨损引起的小波动还是可能导致大面积停电的严重故障隐患相关的告警,从而提高安全防护措施的针对性[3]。

2.3降低安全防护运维成本

大量的误告警会导致电力企业在安全运维方面投入过多的人力和物力资源。AI告警降噪技术减少了不必要的告警处理工作量,使得安全运维人员可以将更多的精力投入真正需要关注的安全问题上,减少了因误判告警而进行的不必要的设备检查和维护工作,降低了运维成本。例如,A告警降噪技术减少了因误告警而频繁派遣维修人员到现场检查设备的情况,节省了交通、人力等相关成本。

3 AI告警降噪技术在电力网络安全防护中的应用要点

廓清电力网络安全防护中,AI告警降噪技术应用要点,修正技术思维,完善技术路径,完整发挥技术优势,推动安全隐患识别、预警以及处置等工作有序开展。

3.1提升数据信息处理能力

AI告警降噪技术在应用过程中,要确保数据来源的可靠性：确保收集的电力网络告警数据来源准确可靠,建立电力设备传感器、网络监控设备、电力调度系统等多个数据源获取路径。工作团队要对数据源进行定期的检查和维护,防止数据采集过程中的错误或数据丢失。例如,对于电力变压器温度传感器的数据采集设备,要保证其正常运行,确保采集到的温度告警数据真实反映设备状态。在收集告警数据过程中,要保证数据的完整性,不遗漏关键信息。同时,要确保不同数据源的数据在格式和语义上具有一致性[4]。

3.2做好数据模型选择

工作团队在模型选择中,要依据电力网络特点,选择合适的AI模型,例如,对于规模较大、告警数据类型复杂的电力网络,深度学习模型如卷积神经网络(CNN)或长短期记忆网络(LSTM)可能更适合用于挖掘告警数据中的复杂模式。对于相对简单的小型电力网络,决策树、支持向量机等传统机器学习模型可能就能够满足需求。模型选择结束后,工作团队要训练AI告警降噪模型,提高模型的泛化能力,例如,训练数据要包含夏季高峰用电期电力设备过热告警数据、冬季冰雪天气对电力传输线路影响的告警数据,以及模拟黑客攻击电力调度系统的告警数据等。

3.3做好信息预警展现

工作团队要做好告警可视化界面设置,为安全人员提供直观、易于理解的告警可视化界面。具体来看,借鉴过往经验,高频使用图形、图表等方式展示告警信息,集中、准确传达告警的类型、严重程度、发生时间、相关设备等关键信息,以帮助安全人员快速了解电力网络的安全状况,及时作出决策。例如,使用

热力图展示不同区域电力设备的告警分布情况,使用柱状图对比不同类型告警的数量。

4 AI告警降噪技术在电力网络安全防护中的应用路径

创新AI告警降噪技术应用路径,搭建安全防护平台,助力安全防护的集成化、智能化与高效化,契合新形势下电力网络管理要求,实现电力资源精准调配,满足电力资源使用需求。

4.1构建智能安全防护平台

AI告警降噪技术应用环节,工作团队率先做好平台架构设计,形成集成化的电力网络安全防护平台,结合过往经验,集成化平台主体架构应包括数据采集层、数据处理层、AI分析层、决策执行层和用户界面层。数据采集层负责从各个电力网络数据源收集告警数据；数据处理层对数据进行清洗、预处理和特征提取；AI分析层运用告警降噪模型对告警进行分类和处理；决策执行层根据分析结果采取相应的安全防护措施；用户界面层为安全人员提供操作和监控的界面。

平台中融合多种先进的安全技术,保证平台服务能力,例如,区块链技术用于保障电力数据的安全性和不可篡改性,物联网技术用于更好地连接和管理电力设备。通过与AI告警降噪技术的协同工作,实现更全面、更智能的电力网络安全防护[5]。

4.2完善智能告警处理流程

利用AI告警降噪技术对电力网络中的告警进行实时监测,实现实时告警分析,降低告警信息共享成本。在告警产生的瞬间,模型对其进行处理,快速判断告警的性质。例如,当电力传输线路上的传感器检测到异常电流时,AI告警降噪技术可以立即分析该告警是由于临时的电网波动还是线路故障引起的,实现实时的安全隐患识别。根据告警的严重程度、影响范围、发展趋势等因素对经过降噪处理后的告警进行分级和排序。将重要的、可能导致严重后果的告警优先推送给安全人员,确保他们能够首先处理最关键的安全问题。例如,对于可能导致大面积停电的电力设备故障告警给予最高优先级,而对于一些不影响电力网络正常运行的轻微设备异常告警给予较低优先级。

4.3实现电力网络安全一体化

将电力网络安全防护与电力运营管理紧密结合起来,实现一体化管理。AI告警降噪技术不仅关注安全告警本身,还将其与电力生产、传输、分配等各个环节的运营数据相结合。例如,在制定电力调度计划时,考虑到当前的安全告警情况,避免将电力资源分配到存在安全隐患的区域或设备上,提高电力运营的安全性和效率。AI告警降噪技术可以为电力资源的调配提供决策支持。当检测到某个区域的电力网络存在安全隐患时,可以及时调整电力供应策略,避免因安全事故导致的电力供应中断。例如,如果某变电站附近出现网络攻击告警,经过降噪分析确定存在一定风险后,可以调整电力传输路径,减少该变电站的负载,保障电力供应的稳定性。

5 结语

AI告警降噪技术在电力网络安全防护中具有至关重要的作用。通过深入分析其在电力网络中的作用、应用要点和应用路径,我们能够更全面地认识到该技术对于提升电力网络安全防护水平的价值。在实际应用中,要注重数据质量保障、模型选择与训练优化、与现有安全系统的集成以及告警可视化与可解释性等应用要点,通过构建智能安全防护平台、实现智能告警处理流程以及助力电力资源精准调配与安全管理一体化等应用路径,充分发挥AI告警降噪技术的优势。

[参考文献]

[1]施南廷.基于AI告警降噪技术在政企网络安全防护中的实践应用[J].广播电视网络,2023(11):77-79.

[2]孟楠,周成胜,赵勋.生成式人工智能赋能网络安全运营降噪能力研究[J].信息通信技术与政策,2024(8):53-56.

[3]张蕴,刘志强,董卓东.基于AR技术的智能穿戴设备在新能源智能巡检中的应用[J].集成电路应用,2023(12):347-349.

[4]周劼英,张晓,邵立嵩.新型电力系统网络安全防护挑战与展望[J].电力系统自动化,2023(8):15-24.

[5]蒋涛,董贵山,杨乐怡.新形势下电力监控系统网络安全风险分析与防护对策[J].信息安全与通信保密,2022(4):79-85.

作者简介：

孙婧(1983--),女,蒙古族,吉林省松原市人,本科,高级工程师,从事的研究方向:电力信息化。