人工智能在电力行业网络安全检测中的应用探索

黄炳茜
大唐山西电力工程有限公司，中国·山西 太原 030032

摘　要：伴随电力行业对网络安全依赖程度不断攀升，电力行业网络安全监测里，人工智能技术的作用正变得越发关键，人工智能技术能显著增进检测效率，提升安全资源配置的合理性，同时增强对潜在隐患的检测水平，具体应用有像智能入侵检测系统（IDS）、智能威胁情报的细致分析、智能漏洞的有效扫描、智能安全事件的及时响应和智能安全态势的敏锐感知等，这些应用既提升了电力系统安全防护的层次，更为精准且高效的网络安全解决方案也被提供给电力行业。

关键词：人工智能；电力行业；网络安全；智能检测；安全态势感知

Exploration of the Application of Artificial Intelligence in Network Security Detection in the Power Industry

Bingqian Huang
Datang Shanxi Electric Power Engineering Co., Ltd., Taiyuan, Shanxi, 030032, China

Abstract: With the increasing dependence of the power industry on network security, the role of artificial intelligence technology in network security monitoring in the power industry is becoming increasingly critical. Artificial intelligence technology can significantly improve detection efficiency, enhance the rationality of security resource allocation, and enhance the detection level of potential hazards. Specific applications include intelligent intrusion detection systems (IDS), detailed analysis of intelligent threat intelligence, effective scanning of intelligent vulnerabilities, timely response to intelligent security events, and sharp perception of intelligent security situations. These applications not only enhance the level of power system security protection, but also provide more accurate and efficient network security solutions to the power industry.

Keywords: artificial intelligence; power industry; network security; intelligent detection; security situation awareness

0 前言

面对数字化时代的时代背景，电力行业作为国家关键基础设施的核心组成，其网络安全难题正不断凸显，以往的网络安全检测办法多依赖人工操作，应对不断复杂的网络威胁困难重重。

1 人工智能在电力行业网络安全检测中的优势

1.1 提高检测效率

在发电企业复杂、庞大的网络环境里面，传统网络安全监测手段在海量数据跟前往往力不从心，无法迅速精准地察觉潜在威胁，而强大的计算及处理能力让人工智能得以能对发电企业网络里产生的诸如设备运行日志、操作记录、流量数据等海量信息开展实时高速分析。以大唐发电企业为例，其囊括多个区域的发电场站与输电线路网络，每天制造的数据规模极为庞大，人工智能可凭借机器学习算法，自动探究正常网络行为模式，若有异常数据显现，可在极短时间马上触发预警，与人工检测相比，效率提升达数十倍之多，人工智能不受工作时间的约束以及疲劳因素的干扰，可实现全天 24 小时不停歇作业，实时对网络安全事件进行监测并迅速响应，大幅缩减安全威胁的发现时长，为发电企业赢得处理安全隐患的黄金时间，维持电力生产安全稳定地运转。

1.2 优化安全资源配置

发电企业针对网络安全领域的资源有限度，怎样合理配置人力、物力及财力资源，实现安全防护效益的最大程度提升是关键，人工智能有本事对发电企业的网络安全状况做全面评估分析，对网络拓扑结构、设备重要性、威胁风险等级等多维度数据做深度挖掘，精准判定网络里的关键节点与薄弱区域。大唐旗下诸如火电、水电、风电等不同类型发电站，各发电站网络安全风险点存在差别，人工智能可按照各电站当下的实际情况，制定贴合实际情况的安全资源配置方案，把有限的安全防护资源重点投放到高风险区域以及关键设备上，杜绝资源的无谓消耗，人工智能也能依据网络安全态势的动态改变，实时改变资源分配的策略，保障安全资源始终维持在最佳配置水平，增进发电企业网络安全防护的综合效能，用低成本实现更高效率的安全防护。

1.3 增强威胁监测

发电企业的网络系统跟电力生产、输送和分配的各环节紧密相连，若被网络攻击侵袭，造成的后果无法予以设想，传统威胁检测举措主要依靠预先设定的规则与模式，难以应对日渐复杂多变的新型网络攻击招式，人工智能借助引入深

度学习、自然语言处理等前沿技术，具有极强的威胁感知与分析本领。它不仅可快速辨认已知的网络攻击样式，还可凭借对网络行为数据的深入剖析，找出被正常流量掩盖的未知威胁，应对发电控制系统面临的高级持续性威胁，人工智能可从巨量网络流量里提取出细微的异常特性，迅速察觉攻击者的潜伏与渗透举动，人工智能还可利用对历史安全事件的学习分析，预估未来或许会出现的安全威胁，提早采取预防办法，为大唐等发电企业筑起一道更坚不可摧的网络安全防线，切实保障电力系统安稳运行。

2 人工智能在电力行业网络安全检测中的应用

2.1 智能入侵检测系统（IDS）

在大唐发电企业复杂网络架构的情境下，智能入侵检测系统（IDS）借由人工智能技术，形成一道紧凑的网络安全防线，其借助机器学习算法，对发电企业网络中的海量流量数据深度挖掘，不断探究网络正常行为模式，在大唐的某座水电厂，实时监控厂内设备间通信流量、用户登录行为等数据的工作由智能 IDS 承担。若网络流量出现异常的波动现象，如短时间里同一 IP 有大量访问请求集中出现，又或者某个设备的通信模式与所学得的正常模式不一致，智能 IDS 可迅速抓住这些异常端倪，依靠预先制定的规则及模型，精准判定是不是入侵行径，跟传统基于规则的 IDS 作比较，智能 IDS 不必人工频繁去更新规则库，可高效辨认新型以及变种的入侵手段，检测精确率大幅上扬。就实际运行数据的统计而言，引入智能 IDS 之后，该水电厂成功检测出的入侵行为数量比之前增加了 30 个百分点，极大优化了网络的安全环境，维系着水电生产的稳定运转，处于电力行业网络范畴中，网络攻击往往以异常流量作为前奏，人工智能技术能对电力系统传输的各类数据流量实施实时监测与智能分析。以大唐某个火电厂为例证，其安装部署的智能分析系统采用深度学习算法，有能力对电厂网络中各类业务场景的流量特征进行模型构建，诸如机组控制系统通信的流量、办公网络数据传输的流量等，当系统监测到某时段办公网络一下子出现大量流向不明地址的数据包，且流量特征与正常业务模式呈现显著差异之际，立即激活智能预警模式。

2.2 智能威胁情报分析

智能威胁情报分析为大唐发电企业赋予了具有前瞻性的网络安全防护视野，它依靠自然语言处理、机器学习这类人工智能技术，从遍布全球的各类数据源，诸如安全论坛、威胁情报共享的平台、官方安全公函等，采集、规整并分析与发电企业网络安全相关联的资讯。从大唐旗下分布广泛的火电、风电等发电站的角度，各个地区面临的网络威胁态势互有差别，智能威胁情报分析系统能依据各电站具体情形，对已收集的情报做筛选与深度解析，当分析显示某地区开始出现针对能源行业的新型恶意软件攻击趋势时，系统会把大唐在该地区发电站的网络架构、设备类型等内容进行结合，评估此威胁对电站预计造成的影响程度，即刻为电站给出有针对性的防护指引，像为特定设备更新安全补丁、对网络访问策略进行调整之类的。依靠智能威胁情报做分析，大唐发电企业可预先洞察潜在的威胁，在攻击未发生之时采取有效的防范举动，减少安全潜在风险，维护电力生产连续稳定地开展，智能威胁情报分析还能借助关联来剖析不同维度的威胁数据，探究潜在的攻击链及攻击团伙相关特征。系统会把某地区发电站经受的钓鱼邮件攻击特征，与全球空间里其他能源企业的类似攻击事件进行关联性操作，鉴别是不是同一攻击组织的持续性举动，进而为大唐发电企业给出跨区域的协同防御方案，采用时间序列分析技术，系统可预估特定类型威胁于不同季节及重大活动期间的爆发概率，助力企业预先调配资源，增强重点时段的安全巡查。面对新兴的 APT（高级持续性威胁）攻击现象，智能威胁情报分析借助机器学习模型持续捕捉攻击模式的细微变化，即刻找出伪装成正常业务流量的隐匿攻击，杜绝传统安全防护手段滞后性引发的防御漏洞，让大唐发电企业网络安全防护的智能化与精准化水平更上一层楼。

2.3 智能漏洞扫描

大唐发电企业网络系统内含大量设备以及复杂应用程序，保障系统安全，智能漏洞扫描发挥着不可替代的关键作用，运用人工智能算法，智能漏洞扫描工具，可对发电企业网络中诸多类型的资产，诸如服务器、网络装置、工业控制系统之类，实施精准、全面且高效的漏洞勘查。它不仅可迅速识别出已知的漏洞，还可借助对系统行为与代码逻辑的剖析，发掘潜藏的未知漏洞，在大唐某火电厂实施网络安全检测时，智能漏洞扫描工具对电站核心控制系统实施扫描时，采用模拟黑客攻击的方式并对系统运行数据进行实时监控，找出了一个基于软件设计缺陷所产生的潜在漏洞，然而传统扫描工具对该问题毫无察觉。智能漏洞扫描工具还可按照漏洞的严重程度、影响范畴以及修复的难易程度等因素，为大唐发电企业奉上细致的漏洞修复建议及优先级规划，帮扶企业恰当安排资源，迅速修补漏洞，切实减小网络安全隐患，实现火电厂网络系统的稳定运转，智能漏洞扫描工具还展现出动态适应的能力，可针对大唐发电企业网络环境的变化迅速调整扫描策略。当新设备接入、应用程序更新的情况出现，工具可自动辨识资产产生的变动，即刻启动靶向性扫描，杜绝由资产台账滞后引发的安全空白区域，好比在某风电场开始新监控系统部署的时候，工具迅速察觉该系统和老旧防火墙存在兼容性方面的漏洞，提前预警以阻断潜在的攻击渠道。此工具支持对多维度风险进行可视化分析，以热力图、趋势曲线等样式直观呈现企业整体的安全态势，大唐发电企业借此可迅速定位高风险地带，当某水电厂的远程运维模块漏洞集中出现时，借助可视化报表，安全团队于 1 小时内完成漏洞溯源以及应急响应方案规划，融合持续的漏洞修复效果跟踪体系，智能扫描正助力大唐构建起以“检测—分析—

修复—验证”为核心的闭环安全防护体系，为智慧能源系统的顺畅运行筑牢数字安全壁垒。

2.4 智能安全事件响应

若遭遇网络安全方面的事件，大唐发电企业凭借智能安全事件响应机制，可迅速且高效地应对网络安全事件，若智能入侵监测系统或其余安全监测手段发现了安全事件，智能安全事件响应系统马上开始启动，其借助人工智能技术，对安全事件展开快速剖析和归类，判定事件的属性、波及范围与严重等级。若发现针对继电控制系统的一场恶意攻击，系统将快速评估此次攻击给电力生产带来的潜在影响，诸如是否会引发设备故障、电力输出失常等情况，基于预先设定的应急预案以及机器学习得到的最佳实践经验，自动采取契合的响应手段，如隔离被攻击的设备、阻断不良流量、启动数据备份及恢复步骤等。系统可实时跟踪事件的处理情况，按照实际情形动态调整响应的策略，及时给相关人员发送事件进展的通告，采用智能安全事件响应方式，大唐发电企业可在极短时间内把控安全事件的影响，守护电力生产安全稳定地开展，大唐发电企业的智能安全事件响应机制具备强大的复盘及改进能力。事件处理操作结束后，系统将自动对整个响应流程开展全链路回顾分析，基于人工智能赋能的数据分析能力，探寻事件发生的根本缘由、响应流程的薄弱之处以及现有策略的改进要点，凭借对攻击路径分析，可精准探寻系统防护架构中的漏洞，以此对访问控制策略做优化，或对安全防护组件做升级。系统会把处理此次事件的经验自动融入机器学习模型里，不断刷新应急预案相关库，让响应策略跟着威胁环境的变化动态演进，此机制还可跟行业安全态势感知平台进行联动，实时分享新型攻击特征及应对方案，实现跨企业安全防护协同的效果，凭借“检测—响应—复盘—优化”的闭环管理机制，大唐发电企业网络安全防护体系实现持续迭代升级，持续维持对新兴威胁的高效抵御实力，为智慧能源体系的安全运营筑起牢固壁垒。

2.5 智能安全态势感知

智能安全态势感知给大唐发电企业带来了全面又实时的网络安全全景景象，它把发电企业网络中的各种安全数据整合在一起，涉及网络流量动态、设备实时状态、用户操作行为、威胁情报要点等，还借助人工智能算法开展多维度关联分析与可视化呈现。在大唐的地区集控中心，智能安全态势感知系统对下辖多个发电场站及输电网络的安全数据开展汇总分析，可实时展现该区域电力网络的整体安全态势，凭借直观呈现的可视化界面，管理人员能够清楚地看到网络当中哪些区域存在高安全风险，哪些设备大概会受到威胁，以及此刻正在进行的安全事件详细资讯。系统可依据历史数据与实时态势，预判未来一段时间网络安全态势走向，事先发出潜在预警，主要是察觉到某地区发电场站网络流量出现异常涨幅，且伴有疑似攻击举动时，系统会及时提示管理人员开展后续检测及防护事宜，为大唐发电企业网络安全决策提供可靠后盾，保证电力系统实现可靠运行，大唐发电企业现有的安全防护体系可跟智能安全态势感知实现深度联动。

3 结语

总之，伴着技术的不断演进，人工智能在电力行业网络安全检测的应用会不断拓展，其优势也会愈发显著，经由智能入侵检测系统（IDS）、智能威胁情报的挖掘分析、智能漏洞的全面扫描、智能安全事件的及时响应和智能安全态势的精准感知等应用，人工智能把检测效率提高了，提升了安全资源配置的合理性，还强化了对潜在威胁的识别能力，伴随人工智能技术的不断进步，电力行业网络安全检测会在智能与自动化方面更上一层楼，为国家关键基础设施的安全稳定运行给予有力技术支持。

参考文献：

[1] 向英,韩玄.电力行业人工智能技术应用的网络安全风险分析[J].信息安全与通信保密,2023(10):67-74.

[2] 佚名.电力行业网络安全建设路径与实践[J].网络安全和信息化,2023(7):37.

[3] 李越茂,姚枫,宋佩珂.人工智能技术在电力行业的应用现状和发展趋势初探[J].电力勘测设计,2022(2):59-64.

[4] 孙暄,冯勇,李响.基于大数据的电力安全监测系统设计与研究[J].通信技术,2019,52(9):2284-2290.

[5] 任峰,刘军青,牛东晓.基于改进BP神经网络模型的电力工业可持续发展综合评价研究[J].华北电力大学学报,2006(1):80-83.

作者简介：黄炳茜（1993-），女，中国山西太原人，本科，工程师，从事信息通信技术、网络安全研究。