基于人工智能的广播电视网络安全预警与应急处置机制研究

魏鹏举
内蒙古自治区广播电视传输发射中心额尔古纳712台　内蒙古　呼伦贝尔　022250

摘　要：随着智慧广电建设推进，广播电视网络面临的网络攻击、信号干扰等安全风险日益突出，传统预警与应急处置机制存在响应滞后、误报率高的短板。本文结合人工智能核心技术，构建适配广播电视网络公益性、实时性特点的预警与应急处置机制，设计科学的预警指标体系和深度学习模型，优化应急处置流程与资源调度模式，通过测试验证机制有效性，可有效提升网络安全防护智能化水平，保障广播电视公共服务稳定供给，为行业网络安全保障提供理论与实践支撑。

关键词：人工智能；广播电视网络；安全预警；应急处置机制

引言：广播电视作为国家关键信息基础设施，承载着意识形态传播与公共服务重要职能，其网络安全直接关系社会稳定与国家安全。当前，媒体融合深入推进，网络架构日趋复杂，DDoS攻击、内容篡改等安全威胁频发，传统依赖人工的防护模式已难以适配需求。人工智能技术的实时性、智能化优势为破解这一难题提供了可能，因此，开展基于人工智能的广播电视网络安全预警与应急处置机制研究，具有重要的现实意义与应用价值。

1 相关理论与技术基础

1.1 广播电视网络安全相关理论

（1）广播电视网络的结构与特点：由发射端、传输介质、接收端构成，涵盖有线、无线、卫星等传输方式，核心是实现音视频信号远距离、大范围稳定传播，具有公益性、实时性和广覆盖性，结构上呈现多节点、多链路交织特征，对传输稳定性和信号完整性要求极高。（2）广播电视网络安全的核心需求：首要保障信号传输安全与内容安全，防止信号中断、篡改或非法插播；其次保护用户隐私与网络设备安全，同时满足业务连续性要求，确保广播电视服务不中断，契合公共服务的核心定位。（3）广播电视网络安全的主要风险类型：包括网络攻击风险（如DDoS攻击）、信号干扰风险、设备故障风险，以及人为操作失误和恶意篡改风险，此外还有外部威胁情报带来的未知安全隐患。

1.2 人工智能核心技术概述

（1）机器学习与深度学习技术：机器学习是AI核心子集，通过算法从数据中学习并预测，应用于威胁识别；深度学习作为其分支，依托多层神经网络处理复杂数据，在网络安全中更适用于复杂威胁分析。（2）自然语言处理与异常检测技术：自然语言处理实现人与系统的自然交互，可处理安全日志等文本信息；异常检测通过算法识别偏离正常模式的行为，常用统计、深度学习等方法，是网络安全防护的关键技术。（3）人工智能在网络安全领域的应用特性：具备实时性、智能化和自适应性，能自动分析海量数据、关联安全事件，减少误报，提升威胁检测与响应效率，可替代部分繁琐人工操作[1]。

1.3 网络安全预警与应急处置基础理论

（1）安全预警的核心内涵与流程：核心是提前识别安全隐患、预测威胁趋势，流程包括安全信息采集、分析研判、风险分级和预警发布，依托多源数据整合实现主动防御。（2）应急处置的原则与关键环节：遵循快速响应、损失最小化、预防为先原则，关键环节包括事件发现、遏制、清除、系统恢复和事后分析，需明确职责分工与协同机制。（3）预警与应急处置的协同关系：预警是应急处置的前提，为处置提供方向和依据；应急处置反馈结果可优化预警模型，二者形成闭环，提升整体网络安全防护能力。

2 基于人工智能的广播电视网络安全预警机制构建

2.1 预警机制构建的目标与原则

（1）构建目标：依托人工智能技术，实现广播电视网络安全威胁的精准识别、提前预警与快速响应，降低网络攻击、信号干扰等风险造成的损失，保障广播电视信号传输稳定、内容安全，提升网络安全防护的智能化水平，确保广播电视公共服务持续稳定供给，弥补传统预警机制响应滞后、误报率高的短板。（2）构建原则：坚持实用性原则，贴合广播电视网络的结构特点和安全

需求，确保机制可落地、可操作；遵循智能化原则，充分发挥AI技术在海量数据处理、异常识别中的优势；秉持安全性原则，预警机制自身需具备抗攻击能力，避免成为新的安全隐患；恪守动态性原则，可根据网络威胁变化和业务升级实时优化调整。

2.2 人工智能驱动的预警指标体系设计

（1）指标选取依据与筛选方法：依据广播电视网络安全核心需求、风险类型及AI技术适配性选取指标，结合行业规范和实际运维经验，剔除冗余、低效指标；采用相关性分析、主成分分析等方法，筛选出具有代表性、可量化的核心指标，确保指标体系科学合理、简洁高效。（2）核心预警指标分类与说明：分为设备安全指标、传输安全指标、内容安全指标和网络环境指标四类。设备安全指标包括设备运行状态、漏洞数量等；传输安全指标涵盖信号传输速率、误码率等；内容安全指标涉及内容篡改、非法插播等；网络环境指标包含网络流量、连接异常等，全面覆盖网络安全各关键环节。（3）指标权重确定与预警等级划分：采用层次分析法结合AI算法，根据指标重要程度确定各指标权重，突出传输安全、内容安全等核心指标的权重；将预警等级划分为一般、较重、严重、特别严重四级，依据指标量化结果及权重叠加，自动判定预警等级，为后续处置提供依据[2]。

2.3 基于人工智能的预警模型构建与实现

（1）预警模型的整体架构设计：采用“数据采集-预处理-分析研判-预警生成”四层架构，数据采集层获取网络设备、传输链路等多源数据；预处理层对数据进行清洗、归一化；分析研判层依托AI算法进行异常识别；预警生成层根据研判结果输出预警信息，实现端到端的智能化预警。（2）基于深度学习的异常识别模型训练：选取广播电视网络历史安全数据、模拟攻击数据作为训练样本，构建CNN-LSTM混合深度学习模型，训练模型识别网络流量异常、信号篡改等行为，通过反复迭代优化，降低误报率、提升识别精度，确保模型适配广播电视网络的实时性需求。（3）预警信息的生成与推送机制：根据预警等级自动生成标准化预警信息，明确威胁类型、影响范围、处置建议；建立多渠道推送机制，通过运维平台、短信、邮件等方式，将预警信息推送至相关负责人，确保预警信息快速传达、及时处置。

2.4 预警机制的有效性测试与优化

（1）测试环境与数据准备：搭建模拟广播电视网络测试环境，还原真实网络结构、业务场景和各类安全威胁场景；准备涵盖正常运行数据、各类异常数据、模拟攻击数据的测试数据集，确保测试数据的全面性、真实性和代表性，为测试工作提供可靠支撑，全面检验预警机制的适配性和有效性。（2）测试结果分析与问题排查：重点统计测试过程中的预警准确率、响应速度、误报率、漏报率等核心指标，对比预期构建目标开展分析，排查预警机制存在的漏洞和不足，重点解决误报漏报、响应滞后、指标适配性不足等问题，明确优化方向和整改措施，确保预警机制达到预期效果。（3）预警机制的优化策略：根据测试结果，优化预警指标体系，调整指标权重和预警阈值；迭代升级异常识别模型，优化算法参数，提升模型识别精度；完善预警推送机制，缩短响应时间；建立常态化优化机制，结合网络威胁新趋势和业务发展需求，持续更新指标、迭代模型，保障预警机制的长效性和有效性。

3 基于人工智能的广播电视网络安全应急处置机制构建

3.1 应急处置机制的整体框架设计

（1）应急处置的组织架构与职责划分：构建“决策层-执行层-支撑层”三级组织架构，明确各层级职责分工。决策层由广播电视网络安全领导小组组成，负责重大应急事件的决策、指挥和统筹协调；执行层包含技术运维组、内容审核组、设备保障组，分别承担应急处置的具体实施、内容管控和设备抢修工作；支撑层依托人工智能技术平台，提供数据支持、算法支撑和技术保障，确保各层级高效协同、权责清晰，避免推诿扯皮。（2）应急处置的流程梳理与优化：结合广播电视网络安全事件特点，梳理出“事件发现-风险研判-应急响应-处置实施-系统恢复-复盘改进”全流程，依托人工智能技术优化各环节衔接。简化冗余流程，压缩决策响应时间，实现事件发现与研判的同步推进，处置实施与系统恢复的高效衔接，打破传统应急处置流程繁琐、响应滞后的瓶颈，提升应急处置的整体效率。

3.2 人工智能在应急处置各环节的应用

（1）风险研判与应急分级：利用人工智能算法对安全事件的类型、影响范围、危害程度进行快速研判，整合网络流量、设备状态、威胁情报等多源数据，自动识别事件等级，对应匹配一般、较重、严重、特别严重四级应急响应，为决策层提供精准的研判结果和处置建议，替代传统人工研判的主观性和滞后性，提升决策科学性。（2）应急响应与处置方案智能生成：基于人工智能技术构建应急处置方案库，结合当前安全事件的具体特征，通过案例匹配、算法推演，自动生成针对性的处置方案，明确处置步骤、责任主体、技术手段和时间节

点。针对信号中断、内容篡改、网络攻击等不同类型事件，生成差异化处置方案，确保处置工作有序、高效推进[3]。（3）处置过程的实时监控与动态调整：利用人工智能监控工具，实时跟踪应急处置全过程，采集处置过程中的设备状态、网络参数、处置进度等数据，动态分析处置效果。若发现处置措施不合理或事件出现新的变化，自动发出调整建议，指导执行层优化处置策略，确保处置工作贴合实际需求，最大限度降低事件造成的损失。

3.3 应急处置资源的智能调度与配置

（1）资源分类与库存管理：将应急处置资源分为技术资源、设备资源、人力资源三大类，技术资源包括安全防护软件、漏洞修复工具等，设备资源包括备用传输设备、抢修工具等，人力资源包括技术骨干、抢修人员等。依托人工智能系统建立资源库存台账，实时更新资源数量、状态和存放位置，实现资源库存的智能化管理，确保资源可查、可用。（2）基于人工智能的资源调度算法设计：设计基于遗传算法的智能调度算法，结合应急事件的等级、影响范围、资源需求和存放位置，自动计算最优调度方案，实现资源的快速调配。优先调度距离事件发生地近、适配性强的资源，缩短资源调配时间，确保应急处置工作及时开展，提升资源利用效率。（3）应急资源的动态补充与优化配置：通过人工智能算法分析历史应急事件的资源消耗规律，预测不同类型事件的资源需求，提前做好资源储备规划。针对资源消耗较快、缺口较大的类型，自动发出补充提醒；同时，优化资源配置结构，合理分配各类资源的储备数量，避免资源闲置或短缺，确保应急资源能够高效支撑应急处置工作[4]。

3.4 应急处置后的复盘与改进机制

（1）处置效果的智能评估：利用人工智能技术构建处置效果评估体系，从处置速度、损失控制、系统恢复效率、用户满意度等多个维度，对本次应急处置工作进行量化评估，自动生成评估报告，明确处置工作中的优势与不足，为后续复盘和改进提供数据支撑。（2）基于案例库的人工智能复盘分析：建立应急处置案例库，将每次处置的事件详情、处置过程、处置结果等信息录入库中，利用人工智能算法对案例进行分类、分析，挖掘不同类型事件的处置规律和共性问题，总结经验教训，为后续类似事件的处置提供参考，提升应急处置的规范化水平[5]。（3）处置机制的迭代改进策略：根据复盘分析结果，结合网络威胁新趋势和广播电视业务发展需求，利用人工智能技术优化应急处置流程、完善组织架构、调整资源配置和算法参数。建立常态化迭代改进机制，定期更新案例库、优化处置方案，持续提升应急处置机制的适配性和有效性，构建闭环式应急处置体系。

结束语

本文围绕人工智能在广播电视网络安全预警与应急处置中的应用展开研究，构建了完整的机制体系，优化了预警模型与处置流程，有效弥补了传统防护模式的不足。研究虽取得一定成果，但仍存在模型适配性可进一步提升、多场景兼容不足等问题。未来将结合广电5G、超高清等新技术发展，迭代优化模型算法，完善案例库建设，推动机制持续升级，为智慧广电网络安全筑牢防护屏障。

参考文献

[1]雷刘敏,刘有坤.广播电视信息系统网络安全风险与策略探究[J].中国有线电视.2022,12(4):78-81.

[2]常祖国.智慧广电视域下广播电视网络安全防护体系构建[J].电视技术.2024,48(3):143-147.

[3]段亮.咸阳市广播电视台网络安全系统建设及运行管理机制[J].电视技术.2024,48(4):211-215.

[4]魏君对.基于大数据分析的智慧广电用户行为研究[J].电视技术.2024,48(12):149-152.

[5]吴量.贵州广播电视台网络安全云枢纽中心设计与实践[J].电视技术.2025,49(2):346-349.