铁路通信网络安全态势感知平台构建

林伸燃
通号通信信息集团有限公司北方分公司　北京　100070

摘　要：铁路通信网络作为铁路运输核心基础设施，面临多样安全威胁。本文聚焦铁路通信网络安全态势感知平台构建，分析其安全需求与典型威胁，阐述平台分层递进式架构及核心功能模块，包括数据采集、威胁检测、态势评估、预警响应层。研究多源异构数据融合、基于AI的威胁检测等关键技术，实现数据整合、精准检测、动态评估与直观交互，提升铁路通信网络安全防护能力，保障铁路运输安全稳定运行。

关键词：铁路通信网络；网络安全态势感知；威胁检测；数据融合

引言：随着铁路信息化、智能化发展，5G等技术融入使铁路通信网络架构更复杂开放，安全需求愈发多元严苛。当前网络面临恶意代码攻击、网络入侵等多样化威胁，传统安全防护手段难以满足需求。在此背景下，构建铁路通信网络安全态势感知平台十分必要。该平台可全面感知网络安全态势，实现精准预警与快速响应，为铁路通信网络提供全方位安全保障，对铁路运输的安全稳定运行具有重要意义。

1 铁路通信网络安全需求与威胁分析

1.1 铁路通信网络架构与安全需求

铁路通信网络是支撑铁路运输调度、行车控制、客运服务等核心业务的关键基础设施，其架构呈现分层分布式特点，主要涵盖骨干传输网、接入网、业务网及终端设备等层级，各层级通过标准化接口实现数据交互与协同工作。随着铁路信息化、智能化水平的提升，5G、物联网、云计算等技术的融入，网络架构的复杂性与开放性显著增加，衍生出多元且严苛的安全需求[1]。首要需求是业务连续性保障，需确保列车调度指令传输的实时性与准确性，避免网络中断或延迟引发行车安全事故；其次是数据完整性与机密性保护，列车运行数据、旅客个人信息、设备运维数据等敏感信息需防范被篡改、窃取或泄露；再者是网络可控性需求，要求对网络接入设备、数据传输路径进行精准管控，抵御非法接入与越权操作；最后是应急恢复需求，需具备快速检测故障、定位威胁源并完成系统恢复的能力，最大限度降低安全事件造成的损失。

1.2 典型安全威胁与攻击场景

当前铁路通信网络面临的安全威胁呈现多样化、精准化、规模化的发展趋势，典型威胁主要包括恶意代码攻击、网络入侵、拒绝服务攻击、数据篡改等。在具体攻击场景中，其一为工业控制系统靶向攻击，攻击者利用行车控制系统、信号系统等工业设备的漏洞，植入恶意代码或发送虚假控制指令，干扰列车正常运行，此类攻击直接威胁行车安全，后果极具破坏性；其二为网络钓鱼与社工攻击，攻击者伪装成铁路内部工作人员或正规服务机构，通过邮件、短信等方式诱导工作人员泄露账号密码，进而非法侵入核心业务系统；其三为DDoS攻击，攻击者控制僵尸网络对铁路通信骨干节点或服务平台发起流量冲击，导致网络带宽堵塞、服务瘫痪，影响调度指令传输与客运服务正常开展；其四为数据窃取场景，攻击者通过网络嗅探、漏洞利用等技术，窃取旅客身份信息、列车运行计划等敏感数据，用于非法牟利或制造不良社会影响。

2 铁路通信网络安全态势感知平台架构设计

2.1 平台总体架构

铁路通信网络安全态势感知平台采用分层递进式架构设计，以“数据驱动、智能感知、精准预警、快速响应”为核心目标，实现对铁路通信网络全生命周期的安全态势管控。平台总体架构自上而下分为数据采集层、威胁检测层、态势评估层、预警响应层，同时辅以支撑层与交互层保障平台稳定运行。支撑层提供硬件资源、操作系统、数据库及安全协议等基础支撑，为各核心层级的运行提供环境保障；交互层通过可视化界面实现态势展示、指令下发与人工干预等功能，助力运维人员实时掌握网络安全状态[2]。各层级之间通过标准化数据接口实现数据流转与协同联动，数据采集层完成多源数据的汇聚与预处理，为后续分析提供数据支撑；威胁检测层对采集的数据进行深度分析，识别潜在安全威胁；态势评估层结合网络拓扑、业务重要性等因素，对安全态势进行量化评估；预警响应层根据评估结果触发分级预警，并提供针对性的响应策略，形成“采集-检测-评估-响应”的闭环管控流程，全面提升铁路通信网络的安全

防护能力。

2.2 核心功能模块

2.2.1 数据采集层

数据采集层是安全态势感知平台基础，能全面、实时、精准采集与预处理铁路通信网络多源异构数据。它采用分布式架构，覆盖全网络节点，采集设备日志、流量、安全告警、配置信息及业务等多种数据。为保障效率与质量，多种采集技术协同，依设备与数据格式选适配方式，如SNMP、API接口等。内置预处理模块，完成数据清洗、标准化、融合与压缩存储，过滤无效数据，提升可用性。另外，该层级可动态调整采集策略，依业务需求与网络状态，灵活优化采集范围、频率和优先级，确保不影响核心业务，实现数据全面覆盖，为平台后续处理提供可靠数据支撑。

2.2.2 威胁检测层

威胁检测层是平台识别安全风险的核心，通过多维度分析精准识别铁路通信网络威胁与异常行为。它基于数据采集层预处理后的数据，构建多维度检测体系，融合特征匹配、异常检测、行为分析等技术。特征匹配用海量威胁特征库实时匹配，识别已知威胁；异常检测建立正常行为基线，定位未知威胁与零日攻击；行为分析追踪核心业务流程，识别潜在风险。融入AI算法，用机器学习模型训练历史数据，优化检测规则与特征库，实现自适应升级。同时具备威胁溯源功能，定位威胁源头，明确攻击路径、目标与手段，为态势评估与响应提供精准依据。

2.2.3 态势评估层

态势评估层基于威胁检测结果，结合铁路通信网络多维度信息，量化评估与动态研判网络安全态势。先构建评估指标体系，涵盖威胁严重程度、资产脆弱性、业务影响范围、网络可用性等关键维度，赋予差异化权重。再用动态风险评估模型，整合实时威胁、资产信息与历史安全事件数据，通过加权计算等方法生成量化评分与等级。具备态势趋势预测能力，分析历史与当前数据，预测未来安全态势变化，识别潜在风险聚集点。评估结果以标准化格式输出至预警响应层，为分级预警与精准响应提供科学依据，助力运维人员全面掌握网络安全整体状况。

2.2.4 预警响应层

预警响应层是衔接态势评估与安全处置的关键环节，核心目标是根据态势评估层的评估结果，实现安全风险的分级预警、快速响应与闭环管理。该层级首先建立分级预警机制，根据安全态势等级划分不同预警级别（如蓝色预警、黄色预警、橙色预警、红色预警），针对不同级别制定差异化的预警方式，包括平台弹窗提示、短信告警、邮件通知、语音播报等，确保运维人员第一时间获取预警信息。其次，构建智能化响应策略库，针对不同类型的安全威胁与预警级别，预设对应的响应措施，如针对非法接入可自动触发端口封禁、IP拉黑；针对恶意代码攻击可启动杀毒程序、隔离受感染设备；针对流量攻击可调整防火墙策略、疏导网络流量。同时支持人工干预响应，运维人员可根据预警信息与实际网络状态，手动下发响应指令，调整响应策略。另外，具备响应效果评估与闭环管理功能，对响应措施的实施效果进行实时监测，若威胁未消除则自动优化响应策略，直至威胁解除。

3 关键技术实现

3.1 多源异构数据融合技术

多源异构数据融合技术是保障安全态势感知平台精准分析的核心支撑技术，其核心目标是解决铁路通信网络中不同来源、不同格式、不同维度数据的碎片化问题，实现数据的有效整合与价值挖掘。该技术的实现主要分为三个关键环节：数据对齐、特征融合与知识融合。在数据对齐阶段，采用元数据管理技术，为不同类型的数据（如日志数据、流量数据、告警数据）定义统一的元数据规范，明确数据字段含义、格式标准与关联关系，通过数据映射实现多源数据的语义对齐；同时利用时间同步技术（如NTP协议），统一各数据源的时间戳，确保数据在时间维度上的一致性[3]。在特征融合阶段，采用特征提取算法（如PCA主成分分析、LDA线性判别分析）从不同数据源中提取关键特征，去除冗余特征与噪声数据，通过特征拼接、特征加权等方式，构建统一的特征向量空间，实现多源数据特征的深度融合。在知识融合阶段，结合铁路通信网络领域知识，构建知识库与规则库，通过本体建模技术建立数据与知识的关联映射，利用推理引擎实现多源数据的知识挖掘与关联分析，提升数据的可解释性与应用价值。通过多源异构数据融合技术，平台可将分散的碎片化数据转化为统一、连贯的结构化数据，为后续威胁检测、态势评估提供全面、精准的数据支撑，提升平台的整体分析能力。

3.2 基于AI的威胁检测技术

基于AI的威胁检测技术是提升铁路通信网络威胁识别能力的关键，通过引入机器学习、深度学习等AI算法，实现对已知威胁的精准识别与未知威胁的有效发现，克服传统特征匹配检测技术的局限性。该技术的实现主要包括模型构建、数据训练与实时推理三个核心环

节。在模型构建阶段，根据铁路通信网络的威胁特点与数据特性，设计多模型协同检测架构，整合决策树、随机森林、支持向量机等传统机器学习模型与循环神经网络（RNN）、卷积神经网络（CNN）、Transformer等深度学习模型，传统模型用于处理结构化数据，深度学习模型用于处理非结构化数据（如流量数据包、恶意代码样本）。在数据训练阶段，收集铁路通信网络的历史安全事件数据、正常运行数据与模拟攻击数据，构建大规模标注数据集，对检测模型进行监督训练与优化，通过交叉验证、网格搜索等方法调整模型参数，提升模型的检测准确率与泛化能力；同时采用增量学习技术，实时融入新增安全数据，实现模型的动态更新。在实时推理阶段，将预处理后的实时网络数据输入训练好的AI模型，通过模型并行计算实现威胁的快速检测与分类，输出威胁类型、置信度、攻击特征等关键信息；同时利用注意力机制聚焦核心业务相关数据，提升对关键业务威胁的检测优先级，确保检测结果的时效性与针对性，为后续安全处置争取时间。

3.3 动态风险评估模型

动态风险评估模型是实现铁路通信网络安全态势精准研判的核心技术，其核心优势在于能够实时感知网络状态变化，动态调整评估指标与权重，提升评估结果的时效性与准确性。该模型的实现主要包括指标体系构建、权重动态分配与风险量化计算三个关键环节。在指标体系构建阶段，基于铁路通信网络的资产特性、业务需求与威胁特点，构建多层次、多维度的评估指标体系，涵盖资产脆弱性指标（如漏洞等级、配置合规性）、威胁态势指标（如攻击频率、攻击强度）、业务影响指标与网络可用性指标（如设备故障率、带宽利用率），各指标均制定明确的量化标准与分级阈值。在权重动态分配阶段，摒弃传统固定权重分配方式，采用层次分析法（AHP）与熵权法相结合的组合权重法，层次分析法根据专家经验与业务重要性确定主观权重，熵权法根据实时数据的信息熵确定客观权重，通过动态融合两种权重，实现评估权重的自适应调整，确保权重分配符合网络实际安全状态。在风险量化计算阶段，采用模糊综合评价法将各指标的量化值转化为风险等级，通过加权求和计算出整体网络安全风险值，同时结合马尔可夫链模型预测风险发展趋势，为安全态势评估与分级预警提供精准的量化依据，助力运维人员科学制定安全防护策略。

3.4 可视化与交互技术

可视化与交互技术是提升安全态势感知平台易用性和运维效率的关键，能把复杂网络安全数据等转化为直观界面，实现高效人机交互。该技术实现分两部分：一是可视化展示模块，采用多层次、多维度设计。网络拓扑可视化以图形展示铁路通信网络层级、设备分布与连接，支持节点钻取查看，实时显示设备状态与告警；安全态势总览可视化用仪表盘等呈现风险等级、预警数量等核心指标，助运维人员快速掌握整体状况；威胁事件可视化通过时间轴等展示威胁事件关键信息，辅助溯源处置；业务影响可视化结合业务流程，呈现安全威胁对核心业务的影响程度，明确业务优先级[4]。二是交互控制模块，支持多样化交互操作，如数据筛选、指令下发等，运维人员可简单操作筛选安全数据；支持自定义预警规则与响应策略，通过界面配置参数并下发；还具备多终端适配能力，支持多设备访问，方便运维人员随时掌握状态并远程处置，提升运维灵活性与效率。

结束语

铁路通信网络安全态势感知平台的构建，是应对日益复杂网络安全威胁的有效举措。通过分层递进式架构与核心功能模块的设计，以及多源异构数据融合、基于AI的威胁检测等关键技术的实现，平台实现了对铁路通信网络全生命周期的安全态势管控。未来，随着技术的不断发展，平台将进一步优化完善，持续提升安全防护能力，为铁路运输的高效、安全运行提供坚实保障，推动铁路行业向更高水平发展。

参考文献

[1]李继元.铁路通信网络安全防护研究[J].中国铁路,2022(6):94-98.

[2]幸力.铁路通信网络安全加密自动控制系统研究[J].通信电源技术，2025，42(14):164-166.

[3]周志刚.铁路通信网络安全防护研究[J].工程建设与发展,2023,2(6):102-104.

[4]陈继仲,蒋明亮,摆晓军,等.基于云架构的集中式铁路通信网络安全防护方案研究[J].铁道通信信号,2025,61(12):41-49.