高速公路网络安全运营管理技术研究及探索

刘贵宣

云南云岭高速公路交通科技有限公司 云南 昆明 650051

【摘　要】：随着高速公路网络化、智能化发展，网络安全运营面临基础设施脆弱、数据泄露、攻击防护不足及管理机制漏洞等多重挑战，严重威胁路网稳定运行。本文以高速公路网络安全运营管理为核心，先分析现存安全风险，再构建边界防护、数据加密、入侵检测及态势感知相关技术，最后从技术效能、管理流程、人员能力、长效机制四个维度提出效能提升路径，形成“风险分析—技术构建—效能提升”的完整研究体系，为高速公路网络安全运营管理提供技术支撑与实践参考，助力实现网络安全主动防控与长效管控。

【关键词】：高速公路；网络安全；运营管理；技术构建

DOI:10.12417/2811-0722.26.05.098

当前，数字化转型加速推动高速公路路网实现全面智能化升级，收费、监控、调度等核心业务均依托网络系统开展，网络已成为高速公路运营的核心支撑。与此同时，网络技术的广泛应用也使高速公路网络边界不断扩大，设备互联、数据交互日益频繁，各类网络安全隐患随之凸显，对路网运营的安全性、稳定性提出更高要求。网络安全运营管理水平直接关系公共交通出行安全与路网运营效率，构建科学完善的网络安全运营管理体系、破解现存安全难题，已成为高速公路行业高质量发展亟待解决的重要课题，也是推动交通网络安全现代化建设的关键抓手。

1 高速公路网络安全运营管理风险分析

1.1 网络基础设施安全风险

高速公路网络基础设施是网络安全运营的核心载体，涵盖收费终端、监控设备、核心服务器、通信链路及路由交换设备等关键组件，其安全状态直接关联路网运营稳定性。部分老旧路段仍沿用早期硬件设备，未随网络技术迭代更新，运行稳定性不足，既易因故障导致网络中断，又因缺乏新型防护模块，无法抵御新型网络威胁。通信链路中，有线链路存在接口老化、传输损耗问题，无线链路在偏远路段覆盖不足，易受电磁干扰出现数据卡顿、丢包，为非法入侵提供突破点。基础设施运维管控缺乏标准化流程，巡检内容不全、频次不合理，设备运行参数监测不到位，隐患难以及时排查，安全漏洞长期存在，持续威胁网络运营基础安全。

1.2 运营数据安全泄露风险

高速公路网络运营产生的核心数据涵盖车辆通行信息、收费明细、路网监控录像、设备运行参数等，此类数据涉及公共交通运行与用户隐私，敏感性极高。数据存储环节缺乏分级管控体系，核心敏感数据与普通运营数据未实行分类存储，访问权限划分模糊，未落实最小权限原则，各类人员均可接触不同等级数据，易引发数据非法获取与篡改问题。数据传输过程中未全面部署加密防护措施，跨路段、跨管理部门的数据交互多以明文形式进行，易被非法拦截、窃取[1]。数据生命周期管理存在明显短板，过期数据未按规范完成清理与销毁，废弃存储介质未进行安全脱密处理，存在数据残留风险，同时备份机制不完善，备份数据更新不及时，无法形成有效数据冗余，进一步放大数据泄露隐患。

1.3 网络攻击防护能力不足风险

高速公路网络面临的网络攻击呈现多样化、智能化趋势，恶意代码、分布式拒绝服务、SQL 注入、端口扫描等攻击手段频发，而网络攻击防护能力尚未实现同步提升。防护设备配置存在明显短板，部分路段部署的防火墙、入侵检测设备性能落后，无法精准识别新型变异攻击行为，防护规则更新滞后于攻击手段升级，对未知攻击的拦截能力薄弱。网络攻击监测缺乏全面性，未构建全覆盖的态势感知体系，无法实时捕捉网络流量异常、端口异常访问、数据传输异常等攻击前兆，导致攻击发生后无法及时察觉，延误处置时效。攻击处置环节缺乏标准化流程，防护系统与应急处置机制衔接不畅，无法快速遏制攻击蔓延，难以在短时间内恢复网络正常运营，持续影响路网运营秩序。

1.4 安全管理机制漏洞风险

高速公路网络安全运营管理机制存在诸多短板，导致安全管控缺乏系统性与规范性，无法形成闭环管理。安全管理制度过于笼统，未结合高速公路网络运营的特殊性制定针对性细则，条款缺乏可操作性，无法有效指导一线安全管理工作。安全责任划分不清晰，各运营部门、岗位之间的安全职责存在交叉或空白，出现安全问题后难以明确责任主体，易出现推诿扯皮现象，延误问题处置。安全培训工作未常态化开展，未针对不同岗位制定差异化培训内容，导致相关人员安全意识薄弱，对安全隐患的识别、处置能力不足，易因操作不规范引发安全问题。安全考核机制不完善，未将网络安全运营管理成效纳入常态化考核，缺乏有效的激励与约束，导致安全管理工作落实不到位，进一步加剧管理漏洞。

2 高速公路网络安全运营管理技术构建

2.1 网络边界防护技术构建

网络边界防护技术构建聚焦高速公路网络出入口、内外网衔接处及路段间接口的安全管控，通过分层部署防护架构实现边界闭环防护。采用下一代防火墙技术，基于深度包检测机制，对进出网络的数据包进行多层次解析，精准识别恶意数据包、异常连接及违规访问行为，结合动态端口管控策略，对非必要端口进行封闭，仅开放路网运营必需端口，减少非法入侵入口[2]。部署网络隔离设备，实现内网核心区域与外网、收费系统与监控系统的物理隔离与逻辑隔离，阻止跨区域非法数据交互。引入边界入侵防御系统，实时监测边界数据传输动态，对异常访问行为进行即时阻断，同时构建边界访问控制体系，落实身份认证与权限校验机制，对所有接入边界的设备进行安全准入审核，未通过审核的设备严禁接入网络，通过技术手段构建坚固的网络边界防线，为高速公路网络安全运营筑牢第一道屏障，其技术实施可为同类交通网络边界防护提供技术参考。见图 1。

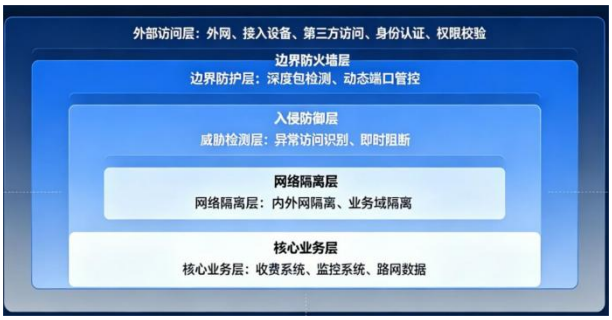

图 1 智慧高速背景下网络边界闭环防护架构图

2.2 数据加密与脱敏技术构建

数据加密与脱敏技术构建围绕高速公路敏感数据全生命周期防护展开，结合数据分级管控要求，实现数据安全与可用性的平衡。采用对称加密与非对称加密相结合的方式，对核心敏感数据实施双重加密保护，对称加密用于内网数据传输与存储加密，保障加密效率与数据传输速度，非对称加密用于跨部门、跨区域数据交互加密，通过公钥与私钥的对应验证，确保数据传输的完整性与保密性[3]。针对用户隐私数据、收费敏感数据，部署数据脱敏技术，通过字符替换、数据掩码、模糊化处理等方式，对敏感字段进行脱敏处理，在保留数据运营价值的前提下，避免敏感信息泄露。构建加密密钥管理体系，对加密密钥进行分级存储、定期更新与安全备份，建立密钥生命周期管理机制，防止密钥泄露或失效导致加密防护失效，该技术构建可有效解决数据安全防护与数据利用的矛盾，具有重要的学术研究价值与工程应用价值。

2.3 入侵检测与应急响应技术构建

入侵检测与应急响应技术构建以快速识别、有效遏制、及时处置网络攻击为核心，构建全流程攻击防护与应急处置体系。部署分布式入侵检测系统，结合异常检测与误用检测技术，对网络流量、设备运行状态、数据交互过程进行实时监测，通过特征提取、行为分析等技术，精准识别恶意攻击行为，包括 SQL 注入、恶意代码植入、分布式拒绝服务等常见攻击，实现攻击行为的早期预警。建立攻击应急处置技术架构，制定标准化处置流程，攻击发生后，系统自动触发应急响应机制，快速切断攻击源与受影响区域的连接，对受攻击设备进行隔离，同时启动数据恢复与系统重启程序，最大限度降低攻击造成的损失。引入攻击溯源技术，通过日志分析、流量回溯等手段，定位攻击源头与攻击路径，为后续防护优化提供数据支撑，其技术方案可为高速公路网络攻击处置提供标准化技术参考。

2.4 安全态势感知技术构建

安全态势感知技术构建聚焦高速公路网络整体安全状态的实时监测、分析与预判，实现网络安全的主动防护。构建全路网安全态势感知平台，整合各路段监控设备、防护设备、服务器的运行数据与网络流量数据，通过数据融合技术，对分散的数据进行汇总、分析与挖掘，提取网络安全关键指标，实时呈现网络安全态势。采用大数据分析与人工智能算法，对网络异常行为、潜在安全隐患进行精准预判，识别安全风险发展趋势，提前发出预警信号，为安全管控提供决策依据。搭建态势感知可视化系统，将网络安全状态、攻击预警信息、隐患排查情况等以可视化形式呈现，实现安全态势的直观展示与动态更新。同时，构建态势感知与防护设备、应急处置系统的联动机制，实现预警、处置、优化的闭环管理，提升网络安全主动防护能力，其技术构建思路与实施细节可为交通行业网络安全态势感知建设提供借鉴。

3 高速公路网络安全运营管理效能提升

3.1 优化安全技术应用效能

优化安全技术应用效能需立足已构建的网络安全技术体系，通过技术迭代与精准适配，提升各类安全技术的运行效率与防护效果。针对已部署的边界防护、数据加密、入侵检测及态势感知技术，建立技术适配性评估机制，定期检测技术应用与高速公路网络运营场景的匹配度，根据路网规模扩张、业务升级需求调整技术参数，避免技术资源浪费。搭建技术优化迭代平台，实时跟踪网络安全技术发展趋势，对老旧防护技术进行升级改造，推动安全技术与路网运营业务深度融合，提升技术响应速度与处置精度[4]。建立技术应用监测体系，实时采集各类安全技术的运行数据，分析技术应用短板与瓶颈，通过参数优化、算法升级等方式，提升技术防护的针对性与有效性，其优化思路可为同类交通网络安全技术效能提升提供技术参考，具备明确的工程应用价值与学术研究意义。

3.2 完善安全运营管理流程

完善安全运营管理流程需围绕技术应用、隐患排查、应急处置等核心环节，构建标准化、闭环化的管理体系，弥补前期管理流程碎片化短板。梳理网络安全运营全流程，明确各环节的操作标准、责任节点与时间要求，将技术防护操作、隐患排查、数据管控等内容纳入流程管控，实现流程全覆盖、无死角。优化隐患排查流程，制定精细化排查清单，明确排查内容、频次与标准，结合安全态势感知数据，精准定位隐患位置，实现隐患排查、登记、处置、销号的闭环管理。规范应急处置流程，明确不同类型安全事件的处置步骤、技术操作与时间节点，推动应急处置与技术防护系统高效联动，缩短处置周期，降低安全事件造成的损失，其流程优化方案可为高速公路网络安全运营管理提供标准化参考。

3.3 强化安全人员专业能力

强化安全人员专业能力需依托系统化培训与实战化演练，提升人员对安全技术的操作水平与隐患处置能力，破解人员能力不足导致技术无法充分落地的难题。构建分层分类培训体系，结合不同岗位的安全职责，针对性设置技术培训内容，重点涵盖边界防护设备操作、数据加密技术应用、入侵检测系统运维、态势感知平台操作等核心内容，兼顾理论深度与实操能力。开展实战化演练，模拟各类网络安全场景，让人员在实战环境中熟悉技术操作流程，提升隐患识别、攻击处置与应急响应的实操能力。建立培训考核与复盘机制，定期对培训效果进行评估，针对考核不合格人员开展专项补训，同时通过演练复盘总结操作短板，持续提升人员专业素养，为网络安全运营提供人力支撑，其培训模式具备较强的借鉴意义。

3.4 建立安全运营长效机制

建立安全运营长效机制需立足高速公路网络安全运营的长期性与复杂性，实现安全管控从被动处置向主动防控转变，保障网络安全持续稳定[5]。整合技术防护、流程管理、人员培训等各类资源，构建“技术防护-流程管控-人员能力”三位一体的长效管控架构，明确各环节的管控要求与实施标准。建立安全风险动态评估机制，定期开展全路网安全风险排查与评估，根据评估结果优化技术防护方案与管理流程，实现风险精准防控。完善技术与管理更新机制，同步跟进网络技术与运营业务的升级需求，及时优化安全技术、更新管理制度，确保长效机制的适应性与可行性，其构建模式可为交通行业网络安全长效管理提供理论参考与实践借鉴，具备较高的学术价值与应用价值。

4 结语

高速公路网络安全运营管理是保障路网智能化、规范化运行的核心支撑，面对数字化转型带来的安全挑战，需立足风险防控实际，完善技术构建与管理体系。通过系统剖析网络安全风险，构建针对性的边界防护、数据加密、入侵检测及态势感知技术，优化技术应用效能、完善管理流程、强化人员能力并建立长效机制，可有效破解现存安全难题。结合高速公路运营特性形成的技术构建与效能提升路径，能够实现网络安全从被动防御向主动防控转变，填补行业安全运营管理短板，为交通行业网络安全建设提供可行借鉴，助力推动高速公路行业高质量、安全化发展。

参考文献：

[1] 钱进,周杰.高速公路网络安全管理研究[J].云南水力发电,2024,40(S1):92-94.

[2] 于志青.高速公路交通安全态势感知技术研究[J].中国安全防范技术与应用,2025,(02):66-70.

[3] 蓝瑞福.福州高速公路网络安全体系建设探析[J].中国交通信息化,2025,(11):120-125+129.

[4] W X P Z ,梁琨昊 .智慧高速公路系统本质安全化评价指标体系[J].中国安全科学学报,2025,35(09):28-35.

[5] 苏文琦,傅文路.高速公路收费网络安全建设实践与研究[J].西部交通科技,2024,(10):175-176+196.