轨道交通视频监控系统的网络安全防护策略研究

巴金哲
通号通信信息集团有限公司北京轨道交通分公司　北京　100070

摘　要：随着轨道交通智能化的深入发展，视频监控系统在保障运营安全、维护秩序等方面发挥着关键作用。然而，该系统面临着日益复杂的网络安全威胁，如黑客攻击、数据泄露等。本文深入剖析轨道交通视频监控系统的网络架构与安全现状，从身份认证、加密通信、入侵检测、安全管理等多个维度提出针对性的防护策略，并探讨策略实施的保障措施与应用效果评估方法，旨在提升轨道交通视频监控系统的网络安全性，为轨道交通的稳定运行提供有力支撑。

关键词：轨道交通；视频监控系统；网络安全；防护策略

1 引言

轨道交通作为城市公共交通的重要组成部分，其安全性和可靠性备受关注。视频监控系统作为轨道交通运营管理的“眼睛”，实时采集和传输大量关键信息，包括车站、车厢、轨道沿线等区域的视频图像，为安全防范、应急处置、运营调度等提供了重要依据。但与此同时，随着信息技术的飞速发展，网络安全威胁不断升级，轨道交通视频监控系统也面临着前所未有的挑战。一旦系统遭受攻击，可能导致视频数据泄露、监控画面中断、系统瘫痪等严重后果，不仅危及乘客生命财产安全，还会对轨道交通的正常运营秩序造成巨大冲击。因此，研究有效的网络安全防护策略，保障轨道交通视频监控系统的安全稳定运行，具有极其重要的现实意义。

2 轨道交通视频监控系统概述

2.1 系统架构

轨道交通视频监控系统通常由前端设备、传输网络、存储设备和监控中心四大部分构成。前端设备包括各类摄像机，分布在车站出入口、站台、车厢、轨道区间等关键位置，负责采集视频图像信息。传输网络承担着将前端设备采集的视频数据传输至存储设备和监控中心的重任，常见的传输方式有有线、无线通信等，不同线路和区域根据实际情况选择合适的传输方案。存储设备用于存储海量的视频数据，以便后续查询和分析，存储时长一般根据相关规定存储90天。监控中心则是整个系统的核心，配备专业的人员和监控软件，实现对视频图像的实时浏览、控制和管理。

2.2 系统功能

实时监控：能够实时呈现轨道交通各区域的画面，使监控人员及时掌握现场情况，如人员流动、设备运行状态等，以便及时发现异常并采取措施。

录像存储与回放：对视频数据进行长时间存储，当发生安全事件或需要回溯时，可方便地进行录像回放，为调查提供证据。

智能分析：借助先进的图像识别技术，系统可实现对人员行为、物体运动轨迹、异常事件（如闯入、火灾等）的智能分析和预警，提高监控效率和准确性。

联动控制：与其他系统，如门禁系统、消防系统等实现联动，当视频监控系统检测到异常情况时，可自动触发相关系统的响应，实现协同工作，提升应急处置能力。

2.3 在轨道交通中的重要性

安全防范：有效威慑潜在的违法犯罪行为，及时发现和制止盗窃、破坏、袭击等安全事件，保障乘客和工作人员的人身安全以及轨道交通设施设备的安全。

运营管理：帮助运营人员实时了解车站客流情况、列车运行状态等，为合理安排运营计划、调整客流疏导策略提供依据，提升运营效率和服务质量。

应急处置：在突发事件发生时，为应急指挥提供直观、准确的现场信息，辅助决策制定，提高应急响应速度和处置效果。

3 轨道交通视频监控系统面临的网络安全威胁

3.1 外部攻击

黑客入侵：黑客通过各种手段，如漏洞扫描、密码破解等，试图获取系统权限，进而控制视频监控设备、篡改视频数据或干扰系统正常运行。例如，利用系统软件存在的安全漏洞，植入恶意程序，实现对监控画面的截取或替换，误导监控人员。

恶意软件传播：如病毒、木马、蠕虫等恶意软件，可通过网络传播至视频监控系统。一旦感染，恶意软件可能窃取视频数据、消耗系统资源，甚至导致系统崩溃。

DDoS攻击：分布式拒绝服务攻击通过控制大量的僵尸网络，向视频监控系统的服务器发送海量请求，使服务器瘫痪，无法正常响应合法用户的请求，导致监控服

务中断。在高峰时段发动DDoS攻击，将严重影响轨道交通的正常运营秩序。

3.2 内部威胁

权限滥用：内部人员如果对自身权限进行滥用，如越权访问、篡改数据、泄露视频信息等，可能对系统安全造成严重损害。例如，某些员工可能因个人私利，将敏感区域的监控视频泄露给外部人员。

安全意识薄弱：部分内部工作人员缺乏足够的网络安全意识，在操作过程中容易出现安全漏洞，如设置简单易猜的密码、随意点击不明来源的链接、使用未经授权的移动存储设备等，给外部攻击者可乘之机。

3.3 数据安全风险

数据泄露：无论是外部攻击还是内部失误，都可能导致视频数据泄露。一旦涉及乘客隐私、关键设施设备运行状态等敏感数据被泄露，将引发严重的社会问题和法律风险。

数据篡改：攻击者篡改视频数据，可能会掩盖安全事故、违法犯罪行为的真相，或者干扰运营决策，影响轨道交通的安全管理。

4 轨道交通视频监控系统网络安全防护策略

4.1 身份认证与访问控制

多因素身份认证：采用用户名/密码、动态令牌等多种因素相结合的认证方式，提高身份认证的准确性和安全性。例如，在监控中心工作人员登录系统时，不仅需要输入正确的用户名和密码，还需正确输入动态令牌，确保只有授权人员能够访问系统。

基于角色的访问控制（RBAC）：根据不同人员在轨道交通运营中的职责和任务，为其分配相应的角色，每个角色被赋予特定的操作权限。如监控人员只能查看视频画面，而系统管理员拥有对系统进行配置和维护的权限，避免权限混乱和滥用。

定期更新与管理：定期更新用户账号和密码，并强制用户设置复杂密码，同时对用户账号进行严格管理，及时删除或冻结离职人员、临时人员的账号，防止账号被盗用。

4.2 加密通信

数据传输加密：在视频数据传输过程中，采用SSL/TLS等加密协议，对传输的数据进行加密处理，确保数据在传输过程中不被窃取或篡改。例如，前端摄像机与监控中心之间的视频数据传输通过SSL加密通道进行，保证数据的安全性。

存储加密：对存储在设备中的视频数据进行加密存储，防止数据在存储介质丢失或被盗时泄露。可以采用AES等加密算法对数据进行加密，只有通过授权的密钥才能解密读取数据。

4.3 入侵检测与防御

部署入侵检测系统（IDS）和入侵防御系统（IPS）：IDS实时监测网络流量，对异常流量和攻击行为进行检测和报警；IPS则不仅能够检测攻击，还能在发现攻击时自动采取措施进行阻断，如屏蔽攻击源IP地址。在视频监控系统的网络入口处部署IDS和IPS，可有效防范外部攻击。

建立安全态势感知平台：通过整合各类安全设备的数据，实时感知系统的安全态势，及时发现潜在的安全威胁，并进行分析和预警。例如，安全态势感知平台可对IDS、IPS以及防火墙等设备的数据进行关联分析，发现隐藏的攻击链，提前采取防范措施。

4.4 安全漏洞管理

定期漏洞扫描：使用专业的漏洞扫描工具，定期对视频监控系统的软件、硬件进行漏洞扫描，及时发现系统存在的安全漏洞。扫描范围包括操作系统、应用程序、网络设备等。

及时补丁更新：针对扫描发现的漏洞，及时获取软件供应商提供的补丁，并进行更新安装，修复系统漏洞。同时，在补丁更新前，要进行充分的测试，确保补丁不会影响系统的正常运行。

漏洞评估与修复优先级确定：对漏洞进行评估，根据漏洞的严重程度、影响范围等因素，确定修复的优先级。对于高风险漏洞，要优先进行修复，确保系统安全。

4.5 安全管理

制定安全管理制度：建立完善的网络安全管理制度，明确各部门和人员在网络安全管理中的职责，规范系统操作流程，如设备维护、数据备份、用户权限管理等。

人员安全培训：定期对轨道交通运营相关人员进行网络安全知识培训，提高其安全意识和操作技能，使其了解常见的网络安全威胁和防范措施，避免因人为失误导致安全事故。

应急响应预案制定：制定详细的应急响应预案，明确在系统遭受攻击或出现故障时的应急处置流程、责任分工和联络方式。定期进行应急演练，确保在实际发生安全事件时，能够迅速、有效地进行应对，降低损失。

5 防护策略实施的保障措施

5.1 技术保障

持续技术更新：随着网络安全技术的不断进步和发展，我们必须紧跟时代步伐，及时引入最新的安全技术和先进设备，对现有的网络安全防护策略进行全面优化和升级。通过这种方式，我们能够确保整个系统能够有

效抵御不断变化和日益复杂的网络安全威胁，保障轨道交通视频监控系统的稳定运行。

建立技术研发团队：轨道交通运营单位应当高度重视技术研发工作，积极建立自己的专业技术研发团队，或者与具备丰富经验和实力的网络安全企业展开深度合作。通过这种方式，开展针对轨道交通视频监控系统的专项安全技术研究和开发工作，不断提升系统的自主可控能力，增强系统的安全防护水平，确保在面对各种网络安全挑战时能够从容应对。

5.2 资金保障

预算投入：为了确保网络安全防护工作的顺利进行，必须将网络安全防护所需的各项资金纳入轨道交通建设和运营的整体预算中。这样，我们才能确保有充足的资金用于安全设备的采购、软件系统的升级、人员的专业培训以及技术研发等多个方面，为网络安全防护提供坚实的资金支持。

成本效益分析：在进行网络安全防护措施的投入决策时，必须进行科学的成本效益分析，合理配置有限的资源。通过选择性价比高的安全产品和服务，确保每一笔资金都能得到有效利用，避免资源的浪费，从而在保障网络安全的同时，实现经济效益的最大化。

5.3 组织保障

成立安全管理小组：由轨道交通运营单位的高层领导亲自牵头，成立一个专门的网络安全管理小组。该小组将负责统筹协调各项网络安全防护工作，制定科学合理的安全策略和详细的工作计划，并严格监督各项措施的落实情况，确保网络安全防护工作有序推进。

明确部门职责：为了确保网络安全防护工作能够落到实处，必须明确各部门在网络安全防护中的具体职责。例如，信息技术部门负责系统的技术维护和日常安全管理，运营部门负责配合实施各项安全管理制度和操作规范，人力资源部门则负责组织人员的安全培训工作。通过明确各部门的职责分工，形成合力，共同筑牢轨道交通视频监控系统的网络安全防线。

6 防护策略应用效果评估

6.1 评估指标

安全事件发生率：统计在一定时间内，轨道交通视频监控系统遭受外部攻击、数据泄露、内部违规操作等安全事件的次数，评估防护策略对降低安全事件发生概率的效果。

系统可用性：通过监测系统正常运行时间与总时间的比例，衡量防护策略在保障系统稳定运行、减少服务中断方面的成效。例如，系统可用性达到99%以上，表明系统运行较为稳定。

数据完整性：检查视频数据在传输、存储和使用过程中是否保持完整，有无被篡改的情况，评估加密通信和数据存储加密等措施对保障数据完整性的效果。

人员安全意识提升程度：通过定期组织安全知识考核、问卷调查等方式，评估人员在接受安全培训后，安全意识和操作技能的提升程度。

6.2 评估方法

实时监测：利用安全设备和监控软件，实时监测系统的网络流量、设备运行状态、用户操作行为等，及时发现安全问题，并对防护策略的实施效果进行实时评估。

模拟攻击测试：定期聘请专业的网络安全测试团队，对轨道交通视频监控系统进行模拟攻击测试，如漏洞扫描、渗透测试等，检验系统在面对真实攻击时的防护能力，评估防护策略的有效性。

数据分析：收集和分析系统运行过程中产生的各类数据，如安全设备的报警数据、系统日志数据等，通过数据分析评估防护策略的应用效果，发现潜在的安全问题和改进空间。

7 结论

轨道交通视频监控系统的网络安全防护是一个系统工程，涉及多个方面的技术和管理措施。通过实施身份认证与访问控制、加密通信、入侵检测与防御、安全漏洞管理、安全管理等一系列防护策略，并建立完善的保障措施和应用效果评估机制，可以有效提升轨道交通视频监控系统的网络安全性，降低安全风险，保障轨道交通的安全稳定运行。在未来，随着轨道交通智能化的不断发展和网络安全威胁的日益复杂，还需持续关注网络安全技术的发展动态，不断优化和完善防护策略，以适应新的安全挑战。

参考文献

[1]王海燕.城市轨道交通既有综合监控系统网络安全改造研究[J].铁路通信信号工程技术,2025,22(02):78-83.

[2]张万康.基于软件定义网络技术与网络功能虚拟化技术的城市轨道交通视频监控系统新型网络架构[J].城市轨道交通研究,2024,27(11):141-145.DOI:10.16037/j.1007-869x.2024.11.032.

[3]周品荣,戴海燕.轨道交通网络安全管理中心与综合监控系统融合的网络安全监控与协同联动研究[J].城市轨道交通研究,2023,26(10):206-210.

[4]金晶,刘健帅.城市轨道交通综合监控系统网络安全方案设计[J].自动化博览,2021,38(01):104-107.

[5]赵晓朴.上海城市轨道交通网络级视频监控系统的研制[J].城市轨道交通研究,2020,23(S2):132-137.DOI:10.16037/j.1007-869x.2020.S2.032.