轨道交通信号系统网络安全防护策略研究

朱耀辉
浙江杭海城际铁路有限公司　浙江　嘉兴　314000

摘　要：本文针对轨道交通信号系统网络安全防护策略展开研究。随着轨道交通系统的智能化和网络化发展，信号系统面临的网络安全威胁日益严峻。文章首先分析了轨道交通信号系统的网络架构，包括其组成、特点及与传统IT系统的差异。随后，深入探讨了信号系统面临的主要网络安全威胁。基于此，本文提出了一系列安全防护措施，包括网络隔离、访问控制、数据加密和安全监测等。最后，通过实际应用案例分析，验证了所提出防护策略的有效性。研究结果表明，采取多层次、全方位的安全防护策略可显著提升轨道交通信号系统的网络安全水平，为城市轨道交通的安全运营提供有力保障。

关键词：轨道交通；信号系统；网络安全；防护策略；网络架构

引言：随着城市化进程的加快和智能技术的快速发展，轨道交通系统已成为现代城市交通的重要组成部分。作为轨道交通的核心子系统，信号系统负责列车运行控制、调度指挥和安全保障，其可靠性和安全性直接关系到整个轨道交通系统的运营效率和乘客安全。然而，随着信号系统日益网络化和智能化，其面临的网络安全威胁也日益严峻。近年来，全球范围内发生了多起针对轨道交通系统的网络攻击事件，严重威胁了城市交通的安全运行。在此背景下，研究轨道交通信号系统的网络安全防护策略具有重要的现实意义。本文旨在深入分析轨道交通信号系统的网络架构，识别其面临的主要网络安全威胁，并提出相应的防护措施。

1 轨道交通信号系统网络架构分析

轨道交通信号系统是一个复杂的网络化系统，主要由列车自动监控系统（ATS）、计算机联锁系统（CBI）、列车自动保护系统（ATP）和列车自动运行系统（ATO）等子系统组成。ATS 负责监控列车运行状态、调整列车运行计划；ATP 通过轨道电路等设备获取列车位置信息，对列车运行速度进行实时监控和控制，防止列车超速、冒进信号等危险情况发生；ATO 则根据 ATP 提供的速度命令和 ATS 的运行计划，实现列车的自动驾驶。这些子系统通过网络相互连接，实现信息的实时传输和共享，从而确保列车的安全、高效运行。信号系统的网络架构通常采用分层设计，包括现场设备层、车站控制层和中央控制层，各层之间通过专用通信网络进行数据传输。

2 轨道交通信号系统面临的网络安全威胁

2.1 外部攻击威胁

恶意软件攻击：黑客可能通过网络传播病毒、木马、蠕虫等恶意软件，入侵轨道交通信号系统。恶意软件一旦感染信号系统设备，可能会窃取敏感信息、篡改系统配置、破坏数据，导致信号系统故障。

网络渗透攻击：攻击者利用信号系统网络中的漏洞，通过端口扫描、漏洞利用等技术手段，试图获取系统的控制权。他们可能会绕过防火墙、入侵检测系统等安全设备，对信号系统的核心设备进行攻击，如篡改列车运行控制指令，引发严重的安全事故。

2.2 内部威胁

员工误操作：轨道交通信号系统的维护人员、操作人员等内部人员，由于对网络安全知识了解不足或操作失误，可能会导致安全漏洞的出现。

内部人员恶意行为：极少数内部人员可能出于个人利益或其他原因，故意对信号系统进行破坏。他们可能会篡改系统数据、删除日志文件、关闭安全防护设备等，给信号系统的安全运行带来极大危害。

2.3 通信网络安全威胁

无线通信干扰：轨道交通信号系统中，部分设备采用无线通信方式进行数据传输，如列车与地面设备之间的通信。无线通信容易受到来自其他无线设备的信号干扰、电磁干扰等。干扰可能导致通信中断、数据丢失或错误，影响信号系统的正常运行。

通信数据被窃听和篡改：在无线通信过程中，通信数据可能被攻击者窃听和篡改。攻击者可以通过监听无线信号，获取列车运行状态、控制指令等敏感信息，甚至篡改这些信息，误导列车运行[1]。

3 轨道交通信号系统网络安全防护措施

3.1 访问控制策略

用户身份认证与授权：采用多因素身份认证方式，

如用户名/密码、指纹识别、智能卡等，确保只有合法用户能够访问信号系统。根据用户的角色和职责，为其分配最小权限，限制用户对系统资源的访问范围。例如，信号维护人员只能访问与维护工作相关的设备和数据，而列车调度员只能进行列车运行调度相关的操作。

网络访问控制：在信号系统网络边界部署防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等安全设备，对进出网络的流量进行严格控制。设置访问控制列表（ACL），限制外部网络对信号系统内部网络的访问，只允许特定的 IP 地址和端口进行通信。同时，对内部网络不同区域之间的访问也进行限制，防止内部攻击扩散。

3.2 入侵检测与防御策略

入侵检测系统（IDS）：部署 IDS 实时监测信号系统网络流量，通过分析网络数据包的特征、行为模式等，检测是否存在入侵行为。IDS 可以采用基于特征的检测方法，即根据已知的攻击特征库进行匹配检测；也可以采用基于异常的检测方法，通过建立正常网络行为模型，当检测到网络行为偏离正常模型时，发出警报。

入侵防御系统（IPS）：IPS 不仅能够检测入侵行为，还能在检测到入侵时自动采取防御措施，如阻断攻击流量、关闭受攻击的端口等。IPS 可以与防火墙、IDS 等安全设备进行联动，形成多层次的安全防护体系[2]。

3.3 数据加密策略

通信数据加密：在信号系统设备之间进行数据传输时，采用加密算法对通信数据进行加密，确保数据在传输过程中的保密性和完整性。例如，采用 SSL/TLS 协议对列车与地面设备之间的通信数据进行加密，防止数据被窃听和篡改。

数据存储加密：对信号系统中存储的敏感数据，如列车运行计划、设备配置信息等，进行加密存储。可以采用对称加密算法或非对称加密算法，确保数据在存储介质上的安全性。

3.4 安全漏洞管理策略

漏洞扫描与评估：定期对信号系统设备和网络进行漏洞扫描，及时发现系统中存在的安全漏洞。采用专业的漏洞扫描工具，对操作系统、应用程序、网络设备等进行全面扫描，并对扫描结果进行评估，确定漏洞的严重程度和影响范围。

漏洞修复与更新：根据漏洞扫描结果，及时采取措施修复安全漏洞。对于操作系统和应用程序的漏洞，及时安装官方发布的补丁程序；对于网络设备的漏洞，联系设备供应商获取解决方案。同时，建立漏洞修复跟踪机制，确保漏洞得到有效修复。

3.5 安全审计与应急响应策略

安全审计：建立完善的安全审计系统，对信号系统的操作行为、网络流量等进行审计记录。审计日志应包括用户登录信息、操作时间、操作内容、网络访问记录等。通过对审计日志的分析，可以发现潜在的安全问题，追溯攻击源，为安全事件的调查和处理提供依据。

应急响应预案：制定详细的应急响应预案，明确在发生网络安全事件时的应急处理流程。定期组织应急演练，提高信号系统运维人员的应急响应能力，确保在安全事件发生时能够迅速、有效地进行处理，降低损失。

4 防护策略实施的难点与应对措施

4.1 实施难点

兼容性问题：轨道交通信号系统通常由多个厂商的设备组成，不同设备之间的兼容性可能存在问题。在实施网络安全防护策略时，新的安全设备和技术可能与现有信号系统设备不兼容，导致系统故障或性能下降。

成本问题：实施全面的网络安全防护策略需要投入大量的资金，包括安全设备采购、系统升级、人员培训等方面的费用。对于一些轨道交通运营企业来说，可能面临资金压力，难以承担高昂的安全防护成本。

技术复杂性：网络安全技术不断发展，防护策略的实施需要具备专业的技术知识和技能。轨道交通信号系统运维人员可能对最新的网络安全技术了解不足，在实施防护策略时遇到技术难题，影响防护效果。

4.2 应对方案

兼容性测试与优化：在引入新的安全设备和技术之前，进行充分的兼容性测试。与信号系统设备供应商密切合作，对安全设备与现有设备进行联调测试，确保其兼容性。对于存在兼容性问题的设备，及时进行优化和调整，必要时寻求供应商的技术支持。

成本效益分析与合理规划：在实施网络安全防护策略时，进行全面的成本效益分析。根据信号系统的实际安全需求，合理规划安全防护方案，选择性价比高的安全设备和技术。同时，可以通过与其他轨道交通运营企业合作，共同采购安全设备，降低采购成本。

技术培训与人才培养：加强对轨道交通信号系统运维人员的网络安全技术培训，定期组织培训课程和技术交流活动，提高其技术水平和安全意识。鼓励运维人员参加网络安全相关的认证考试，培养专业的网络安全人才队伍。

5 轨道交通信号系统网络安全防护应用案例分析

5.1 案例背景

某城市轨道交通线路在运营过程中，面临着日益严

峻的网络安全威胁。随着线路周边商业区域的发展，网络环境变得更加复杂，信号系统曾遭受过多次外部网络攻击的尝试。为了保障信号系统的安全运行，该城市轨道交通运营企业决定实施全面的网络安全防护策略。

5.2 实施过程

访问控制策略实施：对信号系统的所有用户进行身份认证和授权管理，采用指纹识别和智能卡相结合的多因素身份认证方式。在网络边界部署防火墙和入侵检测系统，设置严格的访问控制列表，限制外部网络对信号系统内部网络的访问。

入侵检测与防御策略实施：部署入侵检测系统和入侵防御系统，实时监测网络流量，对异常流量进行及时报警和阻断。定期对入侵检测系统的规则库进行更新，以应对不断变化的网络攻击手段。

数据加密策略实施：在列车与地面设备之间的通信链路中，采用 SSL/TLS 协议进行数据加密，确保通信数据的安全性。对信号系统中存储的关键数据进行加密存储，防止数据泄露。

安全漏洞管理策略实施：定期对信号系统设备和网络进行漏洞扫描，及时发现并修复安全漏洞。建立漏洞管理台账，对漏洞的发现、修复和验证过程进行记录和跟踪。

安全审计与应急响应策略实施：建立安全审计系统，对信号系统的所有操作行为进行审计记录。制定详细的应急响应预案，并定期组织应急演练，提高运维人员的应急响应能力。

5.3 应用效果

通过实施上述网络安全防护策略，该城市轨道交通线路的信号系统网络安全性得到了显著提升。在实施后的一段时间内，成功抵御了多次外部网络攻击，未发生因网络安全问题导致的信号系统故障。安全审计系统为运维人员提供了详细的操作记录和安全事件分析报告，有助于及时发现和解决潜在的安全问题。应急响应能力的提高，确保了在发生安全事件时能够迅速采取措施，将损失降到最低。

6 轨道交通信号系统网络安全防护未来发展趋势

6.1 人工智能与机器学习技术的应用

随着人工智能和机器学习技术的不断发展，未来将在轨道交通信号系统网络安全防护中得到更广泛的应用。利用人工智能和机器学习算法，可以对海量的网络安全数据进行分析和挖掘，自动识别网络攻击行为和安全漏洞，实现智能化的安全防护。

6.2 零信任安全架构的推广

传统的网络安全防护基于边界防护的理念，认为内部网络是可信的。然而，随着网络攻击手段的不断变化，内部威胁也日益严重。零信任安全架构打破了这种传统观念，认为网络中的任何用户、设备和数据都不可信，需要进行持续的身份验证和授权。零信任安全架构已经在轨道交通信号系统网络安全防护中得到推广应用，重点从新技术融合、标准化与规范化建设以及云平台应用几个方面。

与新技术融合：随着 5G、物联网、大数据、人工智能等新技术在轨道交通领域的广泛应用，零信任安全架构将与这些新技术深度融合，形成更加智能化、高效化的网络安全防护体系。

标准化与规范化：为了推动零信任安全架构在轨道交通信号系统网络安全防护中的应用，相关部门和行业组织将制定一系列的标准和规范，明确零信任安全架构的技术要求、实施流程、评估方法等，为企业的应用提供指导和依据。

云平台应用拓展：轨道交通云平台的建设将不断推进，零信任安全架构将在云平台上得到更广泛的应用，为云环境下的信号系统网络安全提供保障。通过在云平台上实施零信任安全架构，实现对云资源的安全访问控制、数据保护和安全监测等功能，确保轨道交通云平台的安全运行[3]。

结束语

本研究深入分析了轨道交通信号系统的网络架构和面临的网络安全威胁，提出了一系列针对性的安全防护措施，并通过实际案例验证了其有效性。研究表明，采取网络隔离与分段、严格的访问控制与身份认证、数据加密与完整性保护，以及全面的安全监测与应急响应等措施，可以显著提升轨道交通信号系统的网络安全水平。

然而，随着网络攻击技术的不断演进，轨道交通信号系统的网络安全防护仍面临诸多挑战。未来研究应重点关注新型攻击手段的防御策略。同时，应提高系统运维人员的安全意识和技能。此外，还需要进一步完善相关法规和标准，为轨道交通信号系统的网络安全建设提供指导和保障。

参考文献

[1]张明远,李华东.城市轨道交通信号系统网络安全防护策略研究[J].铁道通信信号, 2022,58(4):1-8.

[2]王立新,陈思远.基于深度学习的轨道交通信号系统入侵检测方法[J].中国铁路, 2021,12(6):78-85.

[3]李强,周晓峰.城市轨道交通信号系统网络安全架构设计[J].铁道科学与工程学报, 2022,19(5):1320-1328.