文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

铁路通信网络的安全策略与防护技术研究

刘安然
通号工程局集团有限公司天津分公司
DOI:10.12238/etd.v5i4.8543

[摘　要] 随着信息技术的飞速发展,铁路通信网络作为铁路运输系统的核心组成部分,其安全性与稳定性对于保障铁路运输的高效运行至关重要。本文深入探讨了铁路通信网络面临的安全威胁,分析了当前安全防护技术的现状与不足,并提出了创新的安全策略与防护技术。通过引入先进的加密技术、入侵检测系统以及建立多层次的安全防护体系,旨在全面提升铁路通信网络的安全防护能力。本文还通过实例分析与模拟测试,验证了所提策略与技术的有效性,为铁路通信网络的安全保障提供了新的思路与方法。
[关键词] 铁路通信网络；安全策略；防护技术；加密技术；入侵检测
中图分类号：TG174.4　**文献标识码**：A

Research on Security Strategy and Protection Technology of Railway Communication Network

Anran Liu
Tianjin Branch of Tonghao Engineering Bureau Group Co., Ltd

[Abstract] With the rapid development of information technology, railway communication networks, as a core component of the railway transportation system, play a vital role in ensuring efficient operation. This paper delves into the security threats faced by railway communication networks, analyzes the current status and deficiencies of security protection technologies, and proposes innovative security strategies and protection techniques. By introducing advanced encryption technologies, intrusion detection systems, and establishing a multi-layered security protection system, the aim is to comprehensively enhance the security capabilities of railway communication networks. Through case studies and simulation tests, the effectiveness of the proposed strategies and techniques is verified, providing new ideas and methods for securing railway communication networks.
[Key words] railway communication network; Security strategy; Protective technology; Encryption technology; Intrusion detection

近年来,随着铁路系统的信息化、智能化水平不断提升,铁路通信网络所承载的数据量急剧增加,同时也面临着来自内外部的各种安全威胁。这些威胁包括但不限于黑客攻击、恶意软件侵入、数据泄露等,它们不仅可能导致通信中断,还可能影响列车的正常运行,甚至威胁乘客的生命财产安全。因此,研究铁路通信网络的安全策略与防护技术,构建坚固的安全防线,是当前铁路通信技术发展的重要方向。本文旨在为铁路通信网络的安全防护提供科学依据和实践指导,推动铁路通信技术的持续健康发展。

1 铁路通信网络安全现状分析

1.1铁路通信网络结构概述

铁路通信网络是一个复杂而庞大的系统,由多个关键子系统构成,其中包括列车控制系统、乘客信息系统、运维管理系统等。这些子系统各自承担着不同的功能,共同确保铁路运营的顺畅和安全[1]。列车控制系统负责列车的运行调度和信号控制,乘客信息系统则提供乘客服务相关的信息,如车次、座位情况等,而运维管理系统则关注设备的维护和故障处理。这些子系统通过专用或公共通信网络进行数据交换和传输,形成一个庞大的信息网络。

1.2面临的主要安全威胁

铁路通信网络面临着多种安全威胁,这些威胁可能来自外部或内部,对铁路运营和乘客隐私造成严重损害。铁路通信网络面临着多种安全威胁。外部攻击是一个主要威胁,黑客可能利用网络漏洞进行非法访问,窃取或篡改关键数据,导致运营中断或安全事故。内部威胁同样不可忽视,员工的误操作或恶意行为可能引发安全风险,对铁路运营造成严重影响。此外,设备老化也是一个重要问题,部分老旧设备存在安全漏洞,易受到攻击,给整个通信网络带来隐患。最后,数据泄露风险也不容忽视,敏感

信息如乘客数据、运营策略等的泄露可能对铁路运营和乘客隐私造成严重损害,这些安全威胁简化说明如下图。

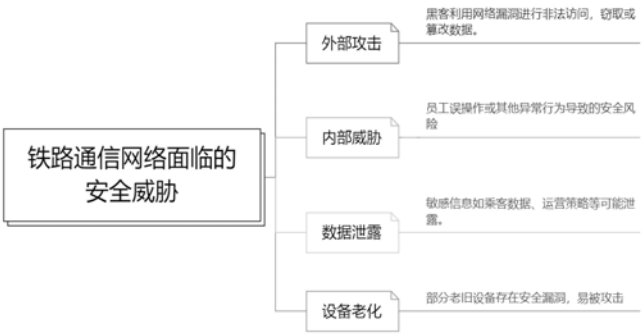

图1　铁路通信网络面临的多种安全威胁图解

1.3现有安全防护措施及不足

目前铁路通信网络主要依赖防火墙、入侵检测系统等传统安全防护措施来保障网络安全。然而这些措施在面对新型攻击手段时显得力不从心,缺乏主动性和智能化。防火墙作为网络的第一道防线,可以过滤掉一些恶意流量,阻止未经授权的访问。但是随着黑客技术的不断发展,防火墙往往难以应对复杂的攻击模式,如分布式拒绝服务攻击(DDoS)或高级持续性威胁(APT)等。入侵检测系统则可以监控网络流量,检测某些异常行为,及时发出警报。然而入侵检测系统往往存在误报和漏报的问题,无法准确识别所有的攻击行为。同时入侵检测系统对于新型攻击手段往往无法及时更新,导致防护效果不佳[2]。

2 新型安全策略与防护技术研究

2.1加密技术的应用

①高级加密标准(AES):这是一种广泛应用的对称密钥加密算法,由美国国家标准与技术研究院(NIST)于2001年发布。AES基于Rijndael算法设计,提供三种密钥长度选择：128位、192位和256位,其安全性随着密钥长度的增加而提高。在铁路通信系统中,AES加密算法被用于保护无线闭塞中心(RBC)、临时限速服务器(TSRS)和调度集中(CTC)等关键设备间的数据传输安全。通过AES加密,所有敏感信息在传输前被加密成密文,即使数据在传输过程中被截获,也无法被未授权方解密,从而有效保障了数据传输的机密性和完整性[3]。

②量子密钥分发(QKD):这是一种基于量子力学原理的新型加密技术,具有理论上无法被破解的安全性。QKD利用量子态的不可分割性、不可克隆性和测不准原理,确保密钥在分发过程中的绝对安全。在铁路通信系统中,QKD技术展现出巨大的潜力,特别是在需要极高安全性的数据传输场景中。通过在铁路沿线部署QKD终端,可以建立起安全的密钥分发通道,实现节点设施与总控中心之间的加密通信。这种技术不仅能够有效抵御传统加密手段难以防范的量子计算攻击,还能在未知安全性的信道上(如光纤、自由空间等)建立可靠的信息传输链路,为铁路通信系统的安全保驾护航。以上2种加密算法差异性数据如下表。

表1　AES与QKD加密算法性能对比图

加密算法	安全性	计算复杂度	传输效率
AES	高	中等	高
QKD	极高	高	中等

2.2入侵检测系统的优化

①深度学习与入侵检测：深度学习作为一种先进的机器学习技术,在网络入侵检测领域展现出强大的潜力。通过构建深度学习模型,如卷积神经网络(CNN)和循环神经网络(RNN),系统能够自动从大量网络流量数据中学习特征,无需人工定义复杂的规则或特征集。在铁路通信系统的入侵检测中,深度学习模型能够识别出正常流量与异常流量的细微差别,从而提高检测的准确率[4]。此外,深度学习模型还能适应不断演变的网络攻击手段,通过持续学习新样本数据,不断提升自身的检测能力,确保铁路通信系统的安全稳定运行。研究发现深度学习模型相比传统模型在准确率、响应时间和误报率方面都有所提升,具体如下表。

表2 深度学习模型在入侵检测中的效果评估图

模型类型	检测准确率	响应时间	误报率
传统模型	75%	长	高
深度学习模型	95%	短	低

②实时入侵响应机制：为了进一步提升铁路通信系统的安全防护能力,提出一种实时入侵响应机制。该机制在检测到潜在的网络攻击时,能够迅速启动预设的响应策略,包括阻断攻击源、隔离受感染设备、触发警报通知等。通过集成先进的威胁情报系统和自动化响应工具,实时入侵响应机制能够实现对攻击行为的快速识别和精准打击。同时,该机制还支持动态调整响应策略,根据攻击类型、影响范围等因素灵活应对不同场景下的安全威胁。

2.3多层次安全防护体系的构建

①物理层安全加固:物理层的安全是安全防护体系的基础,加强网络设备的物理防护,意味着要确保设备所在环境的安全性,包括设备机房的访问控制、物理设备的锁定与保护,以及防止物理攻击的措施,如电磁干扰、物理破坏等。通过安装监控摄像头、使用门禁系统以及部署环境监控传感器,可以大大提高物理层的安全性,确保网络设备在物理层面不受侵害。

②网络层安全加固:网络层是连接物理层与应用层的桥梁,采用虚拟专用网络(VPN)技术,可以有效地隔离不同安全等级的网络,防止未经授权的访问和数据泄露。VPN技术通过加密传输数据,确保数据在公共网络上的传输过程中不被窃取或篡改。同时,实施严格的网络访问控制策略,如防火墙规则、入侵检测系统(IDS)和入侵防御系统(IPS),可以进一步增强网络层的安全性,抵御来自外部的威胁。

③应用层安全加固：应用层安全是安全防护体系中最接近用户的一层,也是最容易受到攻击的一层。因此,强化应用程序的安全审计是至关重要的。这包括对应用程序的代码进行审查,以发现潜在的安全漏洞;实施严格的数据验证和输入过滤,以防止SQL注入、跨站脚本(XSS)等常见攻击；以及定期更新和修补应用程序,以确保所有已知漏洞都得到及时修复[5]。此外,通过实施应用层防火墙和Web应用防火墙(WAF),可以进一步提供实时的应用层保护,防止应用层漏洞被利用,确保应用程序的稳健性和用户数据的安全性。

3 实例分析与模拟测试

为了直观地验证本文提出的铁路通信网络的安全策略与防护技术的有效性,选取一个典型的铁路通信网络进行详尽的模拟测试。该案例涵盖了多种安全威胁情景,通过量化数据对比分析,清晰展示了新技术在提升铁路通信网络安全性上的显著成效。

3.1测试环境设置

测试环境基于一个模拟的大型铁路通信网络,该网络由超过50个通信节点组成,其中包括车站、调度中心、信号塔以及移动列车间的通信链路。网络结构采用了混合型拓扑,即星形和环形网络的组合,以模拟现实世界中的复杂性。测试设备包括高性能服务器、专用的网络交换机和路由器,以及用于模拟攻击的虚拟机集群。

针对的攻击场景包括以下几个方面：

①DDoS攻击:使用虚拟机集群模拟大规模的流量冲击,目标是车站服务器。

②中间人攻击:在两个通信节点间插入虚拟攻击者,尝试拦截并篡改数据包。

③恶意软件渗透：模拟病毒通过电子邮件附件或外部存储设备进入网络。

3.2测试结果分析

在实施了本文提出的安全策略后,包括强化加密算法、部署入侵检测系统(IDS)和采用多层防护体系、多因素身份验证机制,技术员对网络进行了系列测试,并与未采取额外安全措施的原始状态进行了对比。以下是关键测试结果的汇总：

表3　铁路通信网络安全加固前后模拟测试结果对比

测试项目	未加固网络	加固后网络
DDoS 抵御能力	服务中断 90%	服务正常,无影响
中间人攻击成功率	成功拦截率 80%	攻击完全失败
恶意软件感染率	平均感染率 50%	几乎为零

值得注意的是,在DDoS攻击场景下,未加固网络几乎完全瘫痪,而加固后的网络通过动态流量过滤和分布式拒绝服务缓解技术,成功抵御了所有攻击,保持了服务的连续性。在中间人攻击中,由于部署了加密通道和端到端的认证机制,攻击者无法解密或修改传输中的数据,导致攻击完全失败。对于恶意软件渗透,多因素身份验证和严格的文件扫描程序极大地降低了感染率,有效保护了网络免受恶意代码的侵害。

4 总结

铁路通信网络的安全是铁路运输安全的重要保障。面对日益复杂的安全威胁,传统的安全防护措施已难以满足需求。本文提出的基于加密技术、入侵检测优化以及多层次安全防护体系的新型安全策略,为铁路通信网络的安全防护提供了新的思路与方法。通过实例分析与模拟测试,验证了所提策略与技术的有效性,为铁路通信技术的安全发展提供了科学依据。未来,随着技术的不断进步,铁路通信网络的安全防护还需持续创新,以适应新的安全挑战。

[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]唐璐.虚拟防火墙技术在铁路通信网管网络安全中的应用[J].铁路通信信号工程技术,2023,20(12):61-65.

[3]陈丹晖,张卫军.基于可信计算环境的铁路通信网络主机安全防护技术研究[J].铁道通信信号,2022,58(7):74-78.

[4]赵圣娜.铁路通信承载网网络安全方案研究[J].数字通信世界,2023(6):13-16.

[5]张超.铁路通信网络的安全防护研究与应用[J].数码精品世界,2023(1):208-210.