铁路5G专用移动通信网络安全探讨

曹宁哲
广东粤东城际铁路有限公司　广东　汕头　515000

摘　要：本文聚焦铁路5G专用移动通信网络安全。先介绍5G技术基础、铁路5G专用网络架构与功能，接着分析其面临的外部、内部及特殊场景下的安全威胁。随后阐述网络架构安全设计、数据传输安全等安全策略与技术。最后展望未来，指出技术发展趋势、政策法规与标准建设方向，以及安全管理体系完善方向，为铁路5G网络安全发展提供参考。

关键词：铁路5G；移动通信网络；网络安全；安全防护

1 铁路 5G 专用移动通信网络概述

1.1 5G技术基础

5G作为第五代移动通信技术，具有高速率、低时延、大容量等显著特性。5G高速率特性体现在峰值速率可达数十Gbps，相比4G有了质的飞跃，使高清视频、虚拟现实（VR）、增强现实（AR）等大流量业务能够在移动网络中流畅运行。5G低时延特性体现在端到端时延可低至1毫秒，对自动驾驶、远程医疗手术等实时性要求极高的应用场景至关重要。5G大容量特性体现在能够支持海量设备的连接，每平方公里可连接数百万台设备，满足物联网时代大量设备接入网络的需求。5G采用了多种关键技术来实现上述特性，其中，毫米波技术利用高频段频谱资源提供更宽的带宽以实现数据的高速传输，但毫米波传播损耗大、穿透能力弱，需通过大规模天线阵列（MassiveMIMO）技术来增强信号覆盖和方向性[1]。MassiveMIMO通过在基站端配置大量天线，能够同时服务多个用户，提高频谱利用率和系统容量。网络切片技术将物理网络划分为多个虚拟的逻辑网络，每个切片可根据不同的业务需求进行定制化配置，为铁路等特定行业提供专属网络服务。

1.2 铁路5G专用移动通信网络架构

铁路5G专用移动通信网络架构在5G公网架构的基础上，结合铁路行业特殊需求进行定制化设计。核心网是网络的控制中心，负责处理用户认证、移动性管理、会话管理等功能。铁路专用移动通信网络核心网采用分布式部署，以提高网络的可靠性和容灾能力。在铁路沿线重要节点设置核心网设备，实现本地化业务处理，减少对公网核心网的依赖，降低数据传输时延。接入网由基站、天线等设备构成，负责将终端设备连接到核心网。考虑到铁路沿线山区、隧道、桥梁等复杂地形，接入网部署采用分布式基站架构，基带处理单元（BBU）和射频拉远单元（RRU）分离，RRU在铁路沿线灵活部署并通过光纤与BBU连接，实现信号覆盖。针对隧道等特殊场景，利用泄漏同轴电缆等特殊天线技术，确保信号的连续覆盖。列车车载终端、车站调度终端、工作人员手持终端等终端设备是用户与网络交互的接口，需具备可靠性高、抗干扰能力强等特点，以适应铁路恶劣的工作环境。

1.3 铁路5G专用移动通信网络功能

铁路5G专用移动通信网络具有多种重要功能，以满足铁路运输生产和管理需求。列车运行控制方面，5G网络可实现列车与地面控制中心间的高速、可靠通信，将列车位置、速度、运行状态等信息实时传输至地面控制中心，为精确控制列车运行提供信息支撑，实现列车自动驾驶和精确停车，提高列车运行安全和效率。调度指挥方面，铁路调度人员可通过5G网络提供的高清视频、语音等通信手段实时了解车站、线路的实际情况，及时做出准确的调度决策，并利用5G网络的低时延特性实现调度指令的快速下达和执行，提高调度指挥的及时性和准确性。旅客服务方面，5G网络可为旅客提供高速稳定的互联网接入服务，让旅客能够在旅途中畅享高清视频、在线游戏等娱乐内容，车站和列车车载智能终端设备可为旅客提供实时的列车信息、车站导航、餐饮预订等服务，提升旅客的出行体验。设备维护方面，5G网络支持大量设备物联网接入，可实现铁路设备的实时监测和远程维护，主要通过传感器实时采集铁路设备运行状态、温度、振动等数据并传输至维护中心，维护人员根据数据分析结果可提前发现设备故障隐患，及时维修、保养以减少设备故障对铁路运输的影响。

2 铁路 5G 专用移动通信网络安全威胁分析

2.1 外部威胁

铁路5G专用移动通信网络面临黑客攻击、恶意软件

传播、电磁干扰等多种外部威胁，其中，黑客攻击主要是利用系统漏洞、软件漏洞等入侵铁路5G专用移动通信网络并窃取或篡改铁路运营数据，干扰列车正常运行。恶意软件传播主要是通过网络传播并感染车载终端、调度终端等铁路终端设备，进而窃取设备中的敏感信息或破坏设备的正常运行，导致通信中断或数据丢失[2]。电磁干扰主要是铁路沿线的高压输电线路、牵引变电所等电气设备运行过程中产生的电磁噪声对5G网络信号产生干扰，影响5G网络信号的质量，导致通信中断或数据传输错误。暴雨、洪水、地震等自然灾害也可能对铁路5G网络的基础设施造成破坏，影响网络的正常运行。

2.2 内部威胁

内部威胁主要分为铁路工作人员不当操作和恶意行为两种。不当操作主要表现为铁路工作人员工作疏忽或安全意识缺乏，操作网络设备时错误配置导致网络出现安全漏洞，如错误设置防火墙规则使外部网络能非法访问内部网络，增加了网络被攻击的风险。恶意行为主要表现为部分内部人员出于个人利益或其他目的，故意泄露网络拓扑结构、用户身份信息等铁路5G网络敏感信息，并被外部攻击者利用对网络进行更有针对性的攻击。内部人员还可能利用自身权限实施删除重要数据、篡改系统配置等恶意破坏网络行为，严重影响铁路5G网络的正常运行。

2.3 特殊场景下的安全威胁

特殊场景下，铁路5G专用移动通信网络会面临独特的安全威胁。隧道场景下，信号传播环境复杂，多径效应和信号衰落等问题易导致通信中断或信号质量下降；隧道封闭环境会增强电磁干扰，进一步影响网络的稳定性；隧道内火灾、坍塌等事故会造成网络设备严重破坏，导致网络瘫痪。山区场景下，地形起伏大大增加信号覆盖难度，山体遮挡会导致信号衰减严重，出现信号盲区。山区易受暴雨、大风等恶劣天气影响，可能损坏网络设备，影响网络正常运行。高速移动场景下，列车高速行驶会导致信号频繁切换和多普勒频移，若信号切换不及时或不准确，可能导致通信中断，影响信号的稳定性和可靠性，进而影响列车运行控制和调度指挥等关键业务的正常运行。

3 铁路 5G 专用移动通信网络安全策略与技术

3.1 网络架构安全设计

网络架构采用分层防御的安全策略。在接入网层面，部署防火墙、入侵检测系统（IDS）等安全设备对进入网络的流量进行过滤和监测，防止外部非法访问；采用身份认证技术对接入网络的终端设备进行身份验证，确保只有合法的设备能够接入网络[3]。在核心网层面，采用冗余设计和容灾备份机制，在不同地理位置部署多个核心网节点，实现数据异地备份和容灾切换，一个节点故障能快速切换到其他节点，保证网络的正常运行。同时，对核心网设备进行访问控制，仅限授权人员可进行设备配置和管理操作，防止内部人员非法操作。在网络切片层面，为不同的业务切片设置独立的安全策略。对于旅客服务切片，在保证基本安全的前提下，注重用户体验，提供便捷的访问方式。

3.2 数据传输安全

数据传输安全是铁路5G专用移动通信网络安全的重点，采用加密技术对传输数据进行加密处理，防止数据在传输过程中被窃取或篡改。对于列车运行控制等关键业务数据，采用高级加密标准（AES）等高强度加密算法确保数据的安全性。同时，采用完整性保护技术对传输数据进行完整性校验，发送端计算数据校验和并与数据一起发送，接收端重新计算校验和并与发送端发送的校验和进行比对，校验和不一致则说明数据在传输过程中被篡改，接收端丢弃该数据并要求发送端重新发送。采用虚拟专用网络（VPN）技术，基于公网构建一个虚拟的专用网络，建立安全的数据传输通道，实现铁路内部网络之间的安全通信。VPN技术通过加密和隧道技术，对传输的数据进行保护，防止数据被窃取或篡改。

3.3 身份认证与访问管理

身份认证是确保网络安全的重要环节，采用多因素身份认证技术，结合用户名、密码、数字证书、生物特征等多种认证方式，提高身份认证的准确性和安全性。访问管理方面，建立细粒度的访问控制策略，根据用户角色和权限，对用户能够访问的网络资源和操作进行严格限制，如调度人员只能访问与调度指挥相关的网络资源和数据，不能访问列车运行控制等敏感数据。同时，对用户的访问行为进行实时监测和审计，及时发现异常访问行为，并采取相应的措施进行处理。

3.4 安全监测与应急响应

建立完善的安全监测系统，对铁路5G专用移动通信网络的运行状态进行实时监测。通过部署入侵检测系统（IDS）、入侵防御系统（IPS）、安全信息和事件管理系统（SIEM）等安全监测设备，对网络流量、设备状态、用户行为等进行实时监测和分析，及时发现网络中的安全威胁和异常事件，并发出警报。制定完善的应急响应预案，明确在发生安全事件时的应急处理流程和责任分工。当发生安全事件时，能够迅速启动应急响应预案，采取隔离受攻击设备、恢复受损数据、追踪攻击源

等有效措施进行处置，同时，对应急响应过程进行记录和总结，分析安全事件发生的原因和教训，不断完善安全策略和技术措施，提高网络的安全防护能力。

4 铁路 5G 专用移动通信网络安全未来展望

4.1 技术发展趋势

随着技术的不断发展，铁路5G专用移动通信网络的安全技术将不断创新和完善，人工智能和机器学习技术将在网络安全领域得到广泛应用。利用人工智能和机器学习算法对网络流量和用户行为进行深度分析，能够更准确地检测和识别安全威胁，实现智能化的安全防护。如利用机器学习算法对正常的网络流量模式进行学习，当出现异常流量时能够及时发出警报。量子通信技术也将为铁路5G网络安全提供新的保障，量子通信具有绝对的安全性，能够实现无条件安全的密钥分发。将量子通信技术与5G网络相结合，可以为铁路关键业务数据提供更高级别的安全保护，防止数据被窃取或篡改。软件定义网络（SDN）和网络功能虚拟化（NFV）技术将进一步推动铁路5G网络架构的灵活性和可扩展性。通过SDN和NFV技术，可以实现网络资源的动态分配和灵活调度，提高网络的安全性和可靠性。同时，也能降低网络建设和运维成本，促进铁路5G网络的快速发展。

4.2 政策法规与标准建设

政策法规和标准建设是保障铁路5G专用移动通信网络安全的重要依据。政府和相关部门将加强对铁路5G网络安全的监管，出台更加完善的政策法规，明确铁路5G网络建设和运营的安全要求和责任。例如，制定铁路5G网络安全准入制度，要求网络设备和服务提供商必须符合一定的安全标准才能进入铁路市场。加快铁路5G网络安全标准的制定和完善，统一的安全标准能够规范铁路5G网络的建设和运营，提高网络的安全性和互操作性[4]。例如，制定铁路5G网络设备的安全标准、数据传输安全标准、身份认证标准等，为铁路5G网络的安全发展提供有力的支撑。

4.3 安全管理体系的完善

未来，铁路部门将进一步完善安全管理体系，加强安全管理和人才培养。建立健全安全管理制度，明确各部门和人员的安全职责，加强对网络安全工作的考核和监督。同时，加强对铁路工作人员的网络安全培训，提高工作人员的安全意识和安全技能，确保网络安全策略和技术措施能够得到有效落实。另外，加强与行业内外相关机构的合作与交流。与其他铁路企业、通信运营商、安全厂商等建立合作关系，共享安全信息和技术经验，共同应对网络安全挑战。同时，积极参与国际网络安全合作，借鉴国际先进的安全理念和技术，提升我国铁路5G专用移动通信网络的安全水平。

结束语

铁路5G专用移动通信网络对铁路运输意义重大，其安全保障至关重要。本文全面探讨了该网络面临的安全威胁，并提出针对性策略与技术。未来，随着技术发展、政策法规完善以及安全管理体系健全，铁路5G网络安全水平将不断提升。各方需持续努力，共同推动铁路5G网络安全、稳定发展，为铁路事业进步筑牢安全根基。

参考文献

[1]韩利祥.铁路5G专用移动通信网络安全探讨[J].铁路通信信号工程技术,2025,22(4):51-57.

[2]戴蕊,钟章队,孙宵芳,等.移动通信网中加密算法演进及其在铁路5G-R应用展望[J].中国铁路,2024(8):69-76.

[3]李欢欢,顾建国.人工神经网络下5G通信网络信息安全防护探索[J].中国新通信,2023,25(21):6-8+15.

[4]沈毅波,林志维.人工神经网络下5G通信网络信息安全防护研究[J].宁德师范学院学报(自然科学版),2023,35(01):31-37.