轨道交通系统通信网络安全防护研究

赵方捷，张仕针*，金斌斌

（中兴（温州）轨道通讯技术有限公司，浙江 温州 325000）

摘 要 通过对城市轨道交通通信网络系统的安全研究，可有效提高城市轨道交通运行效率、提升安全保障水平，对保障城市轨道交通的平稳运行具有重要意义。针对轨道交通通信网络系统安全防护工作，本文分析了轨道交通通信网络系统的安全威胁和攻击方法，从通信网络系统架构、设备配置、安全防护策略三个方面提出了防护建议，同时对通信网络系统的安全防护体系进行了研究。

关键词 轨道交通系统；通信网络；安全防护

中图分类号：U12 **文献标识码**：A **文章编号**：1007-0745(2023)05-0016-03

随着国家安全战略的不断深入，城市轨道交通行业正在开展一系列的安全标准研究工作，从安全理论到应用实践都取得了一定成果。目前，我国城市轨道交通行业正在开展多项标准的编制工作，例如：《城市轨道交通工程通信设备通用技术条件》（GB/T 39513-2020）、《城市轨道交通运营管理规范》（GB/T 35687-2017）等。这些标准为城市轨道交通通信网络系统安全提供了理论依据，同时也为其提供了安全保障。但是目前这些标准中关于轨道交通通信网络系统的相关内容比较少，而且在各个标准中也未对通信网络系统的安全问题进行深入的阐述。因此，有必要对城市轨道交通通信网络系统的安全进行深入分析，提出相关对策建议。

1 信息系统面临的威胁和攻击方式

在实际运行过程中，轨道交通通信系统面临着多种安全威胁，主要包括物理安全威胁、环境安全威胁和管理安全威胁。其中物理安全威胁是指由于人为因素导致的城市轨道交通通信网络设备、传输线路等受到破坏；环境安全威胁主要指由于自然灾害等意外事故造成通信网络的中断，导致乘客无法及时疏散，同时影响行车效率；管理安全威胁主要指由于轨道交通通信网络系统的不安全性造成信息泄密、业务中断等情况。以物理安全威胁为例，一般是通过物理入侵、物理污染等方式进行攻击。其中物理入侵方式是指通过采用暴力破解、越权访问、后门程序等手段对城市轨道交通通信网络设备进行破坏，进而达到窃取信息数据，造成城市轨道交通通信网络瘫痪；而物理破坏方式是指通过物理入侵手段对城市轨道交通系统造成损坏。

2 网络系统架构

城市轨道交通通信网络系统架构主要包括城域网、车站、区间和设备间（区间控制中心）4个部分。

2.1 城域网

城域网是轨道交通车站和区间之间的通信传输媒介，其作用是向控制中心、车站及区间提供业务数据通信、视频会议、监控图像传输等服务，为列车运行控制中心提供各种信息。在设计上应满足以下要求：

（1）通信容量大。城域网传输的数据量较大，主要包括视频会议、监控图像及语音传输等，要求城域网具有足够的带宽；（2）网络拓扑灵活。在线路布置上可以将光纤、电缆等各种物理介质结合起来，采用分层结构，构建一个灵活、可靠的网络拓扑；（3）设备功能完善。城域网主要是为各设备间提供通信支持，要考虑到在线路使用过程中的设备维护，保证各设备间正常运转；（4）可靠性高。在线路架设时要考虑到线路上信号电缆等介质的分布情况，确保网络的可靠性；（5）业务实现方便。城域网应能向不同业务需求的用户提供统一的协议标准。

2.2 车站

车站应设计成三层结构：车站层、微机联锁设备层、通信设备层。其中：车站层采用双核心结构，分为两个核心点；微机联锁设备层采用2个核心点，均采用双核心架构；通信设备层采用3种交换结构。

1.车站设备核心网络：包括主交换节点、备交换

*本文通讯作者，E-mail：422080759@qq.com。

节点，用于实现与列车自动监控系统、调度中心、中央空调等设备之间的数据传输；主交换节点还负责将各微机联锁设备、中央空调等设备进行统一管理；备交换节点负责对各微机联锁设备进行统一管理。

2. 通信网络核心：采用三层交换机，将车站、列车运行调度与通信中心和主交换节点及列车控制中心相连，主要用于实现各设备间数据传输和信号传输。

3. 通信网络：主要用于实现对车站与设备间之间的通信需求。包括与各微机联锁设备间、站内各配电室的通信连接，与车站站台以及站内信息系统进行连接，实现通信网络信号的互通。

2.3 区间

区间由 2 个核心网络组成，分别为控制中心和各设备间。

控制中心是整个网络的中枢，负责整个系统的调度指挥，向车站和车辆段下达调度命令。控制中心与设备间之间采用 3 层交换结构进行互联互通，以光纤作为传输媒介。其中，各设备间均为单路双向通信方式，分别向控制中心、车站、车辆段传输各自信息。

各设备间之间采用 3 层交换结构进行互联互通，3 层交换结构包括交换机 1 台、路由器 1 台和防火墙 2 台。交换机 1 用于各设备间之间的通信联络和信息交换；路由器 2 用于各设备间之间的通信联络和信息交换；防火墙 2 用于各设备间、隧道之间以及隧道内和隧道外的通信联络和信息交换。各个设备间采用 VLAN 方式进行划分，对每个 VLAN 分配相应 IP 地址及子网掩码。由于 VLAN 的划分比较灵活，因此对实际应用中网络服务质量保障提出了较高的要求。

各设备间内除使用交换机 1 台外，还需配置防火墙 1 台以及其他防护措施；当发生通信网络中断时，将采取应急措施对通信线路进行隔离和恢复 [1]。

2.4 设备间

设备间位于车站与区间之间，在车站设置一套信号设备，主要为乘客提供上下车及引导服务。设备间主要由轨道控制中心和通信机房组成。轨道控制中心和通信机房分别设置在车站和区间，保证控制中心与站内各设备之间能够安全稳定地进行数据通信。

为保障控制中心对区间的远程监控和管理，区间设备间需配置一套远程监控系统，用于实时监控车站与区间的生产状态、车站与区间的设备运行状态及其他重要信息，同时也能实时对设备运行状况进行检测。远程监控系统包括一台服务器和多台触摸屏，由服务器提供显示、控制等功能；触摸屏用于实现相关操作功能。为了实现网络通信的安全性和可靠性，还需配备一套安全防护系统，该系统可通过对通信网络各节点的安全防护设计，实现对通信网络的安全监控及对通信设备进行保护，从而保证城市轨道交通控制中心网络的安全性和可靠性。

3 设备配置

对轨道交通系统内的网络设备进行配置时，应遵循“统一规划、合理布局、集中管理、资源共享”的原则。采用“网元唯一化”的原则，网络设备配置应尽可能采用成熟技术，并在网络规划时与其他业务系统进行有效隔离，避免接入控制中心和其他业务系统的网络设备成为互联网的传播通道，从而降低恶意攻击、病毒传播及不可控因素对系统安全的影响。

对骨干网设备进行配置。骨干网设备应采用安全隔离技术，如：防火墙、入侵检测系统等。防火墙采用多冗余的方式，保证某一个节点发生故障时，其他节点正常工作；入侵检测系统采用“入侵检测 + 深度包检测”的方式，对网络中存在的攻击、病毒进行拦截，提高网络安全防范能力。

城域网设备应尽可能采用成熟技术，如：IPSEC VPN、IPSec VPN 等技术。根据安全需求和实际情况，城域网设备应在一定程度上实现物理隔离或逻辑隔离，保证内部网络不与其他网络直接互联。为防止网络攻击和病毒传播等给整个网络带来严重影响，在进行业务系统数据传输时必须对数据进行加密处理，且所有传输数据都是从目的 IP 地址开始发送。

核心交换机应采用安全稳定、性能优越的工业交换机，以保证其与业务系统间的安全防护隔离和性能要求。当采用工业交换机时，应配置流量控制模块以实现流量控制和负载均衡功能；当采用路由器时，应配置网络管理模块以实现网络管理功能 [2]。

城域汇聚交换机应采用工业级交换机或防火墙设备，保证其在发生攻击或故障时能够恢复正常运行。当城域汇聚交换机与业务系统之间有明显的物理隔离要求时，应采用工业级交换机或防火墙设备进行组网；当业务系统与城域汇聚交换机之间没有明显的物理隔离要求时，可采用工业级交换机或防火墙设备组网。

无线专网设备应采用安全稳定的工业级无线路由器和防火墙设备进行组网，如：MSP430、MSP430+VPN 等产品；对于有线无线融合组网方案中使用的 WLAN 系统的接入方式，在安全防护要求方面应参照 WLAN 技术相关标准和规范要求进行设计。无线专网设备应具有防雷、接地、电源管理功能；网络拓扑结构应符

合IPSec VPN方案相关要求；无线专网设备的频率范围应符合要求。

4 安全防护策略

4.1 控制网内人员进出权限

网络安全管理部门根据需要在控制网内设立相关的审核流程，以确定哪些用户可以进入，哪些用户不能进入。对进入网络的人员进行严格控制，需要对其权限进行严格审核。

4.2 安全区域隔离

通过使用安全产品、安全防护设备来实现对网络内部通信活动的控制，对于网络中不需要使用到的部分，可实现通信活动的隔离。对重要的通信服务器、路由器和交换机等设备采用双机热备或多机热备等方式实现网络隔离；对关键通信设备采用冗余配置，通过备份减少故障时产生的影响；对不需要使用到的部分进行拆除，避免攻击者在控制网内留下漏洞。

4.3 主机安全

要求操作人员通过身份验证后才能访问网络。为避免非授权访问，需配置相应的访问控制策略，防止非法用户越权访问和恶意程序破坏；设置相应的用户和主机安全管理措施，明确用户和主机安全职责权限。为防止恶意程序破坏及非法病毒入侵，可安装入侵检测系统等技术手段。

4.4 认证和访问控制

采用一种或多种认证方式（如IPSec、SSL等），对进入网络的通信设备进行身份认证。根据信息系统等级保护标准（GB/T 22239-2019）规定：“通信网络系统应当按照分级保护原则进行分级保护”，可采用密匙、数字证书或安全令牌等方法对通信设备进行认证。若通信网络系统需与其它系统进行交互，应使用协议加密方法进行通信。在安全策略中应明确通信双方身份验证、通信内容加密方式、通信数据传输格式等信息；根据需求设计通信协议，支持数据完整性检验及传输不可抵赖性控制[3]。

4.5 入侵检测与防御

通过利用各类入侵检测系统识别并定位各类攻击行为和异常事件，发现各类攻击行为和异常事件并进行报警处理；通过利用各种安全设备对可疑数据进行检测分析，在发现异常后通过相关警报及策略实现防御功能。入侵检测系统按照攻击类型可分为两类：被动式和主动式。主动式入侵检测系统是一种能够及时发现入侵行为并主动报警的入侵检测系统，它通过对来自互联网的信息进行分析识别和对已知的危险信号进行标记，并及时通知相关人员进行处理；被动式入侵检测系统是指基于被动形式的入侵检测系统。

4.6 安全审计

安全审计是指通过对网络中所有操作日志、通信数据包等的安全审计来确定是否发生了攻击或错误。安全审计通过对日志的收集、整理、分析来识别潜在的安全威胁并及时提供信息或采取相应措施。对于攻击事件或者数据进行分析、记录和提供必要的证明资料是审计过程中重要的一环。

5 安全防护体系规划建议

应采取信息资产梳理、分类分级管理、增强关键设备配置等手段形成有效的安全防护体系。为保障轨道交通通信网络系统安全建设，应从信息资产梳理出发，对涉及系统所采用的安全设备进行统一部署。如：服务器操作系统安全加固。通过在服务器上安装防护软件或定期对服务器进行杀毒软件扫描、配置策略等措施，对操作系统进行加固，提高操作系统的安全性；应用系统安全加固。通过加强对应用程序代码进行检测，避免程序漏洞和后门的存在，防止病毒和恶意代码等非法入侵；移动存储设备安全加固。通过在存储设备上安装防病毒软件等措施，防止内部病毒扩散并及时更新补丁程序，避免因病毒入侵造成严重后果[4]。

6 结语

轨道交通通信系统是保障城市轨道交通安全运营的重要手段之一，是城市轨道交通和运营管理不可或缺的组成部分。在我国，城市轨道交通系统目前主要由通信系统、牵引供电系统、综合监控系统四大系统构成，其中通信网络作为通信系统中的关键组成部分，对保障城市轨道交通安全运营发挥着至关重要的作用。因此，加强对轨道交通通信网络安全防护工作的研究，实现通信网络的安全可靠运行是城市轨道交通建设和发展过程中一项重要的工作任务。

参考文献：

[1] 熊栋宇，黄魏．城市轨道交通生产系统网络安全设计方案研究[J]．城市轨道交通研究，2021(03):81-86,91.
[2] 李源浩．基于大数据的信息网络安全研究综述[J]．中国安全防范认证，2021(03):74-77.
[3] 杨荣凯．城市轨道交通信号系统信息安全等级保护策略研究与实现[J]．大科技，2021(08):105-106.
[4] 王春军．城市轨道交通信号系统安全防护体系建设研究[J]．中国新通信，2022,24(10):101-109.