

上海轨道交通 3、4 号线升级改造后的列车视频监控系统

施家裕

(上海地铁维护保障有限公司车辆分公司,200237,上海//工程师)

摘 要 城市轨道交通列车视频监控数据庞大而又复杂,对视频监控数据的有效传输、存储和检索,能够大大提高视频监控数据的管理水平和利用效率,进而能够有效监控列车运营、保证列车运营安全。介绍了上海轨道交通 3、4 号线升级改造后的列车视频监控系统的架构、功能和安全性设计。增加车地无线传输功能的新系统更加稳定、安全。

关键词 上海轨道交通; 视频监控系统; 无线传输; 升级改造

中图分类号 U270.38⁺9

DOI:10.16037/j.1007-869x.2023.S1.030

Upgraded and Reconstructed Train Video Surveillance System of Shanghai Rail Transit Line 3/4

SHI Jiayu

Abstract The video surveillance data of urban rail transit trains is enormous and complex. Effective transmission, storage and retrieval of video surveillance data can greatly improve the management level and utilization efficiency of video surveillance data. Then train operation can be effectively supervised, ensuring train operation safety. The architecture, function and safety design of upgraded train video surveillance system of Shanghai Rail Transit Line 3/4 are introduced. The new system with vehicle-wayside wireless transmission function is more stable and safer.

Key words Shanghai rail transit; video surveillance system; wireless transmission; upgrading and reconstruction

Author's address Vehicle Branch of Shanghai Metro Maintenance Support Co., Ltd., 200237, Shanghai, China

近年来,城市轨道交通因其具有快速、安全、便捷、环保及大运量等特点,在我国得到广泛应用与发展。与之相关的大数据研究也日趋成为热门学科,利用大数据的信息采集、分析和挖掘技术,研究客流现状分布特征及变化规律,可实现城市轨道交通运营、施工的智能化管理。将城市轨道交通庞大而又复杂的数据更高效、更准确地转化为可视、可

读且可用的信息,是大数据应用扩展的领域,也是当前城市轨道交通行业发展的重要课题。车载视频监控系统是城市轨道交通安全生产的重要组成部分,已成为监控列车运营、保证列车运营安全,以及处理紧急突发事件的必要技术手段。通过无线传输和智能资源管理平台可以有效地传输、管理海量的视频监控数据,对服务器资源和视频资源的实时状态进行监控,实时掌握资源利用情况,并可以对视频资源进行分类存储、预览和检索,大大提高视频资源的管理水平和利用效率。本文介绍了上海轨道交通 3、4 号线升级改造后的列车视频监控系统的架构、功能和安全性设计。

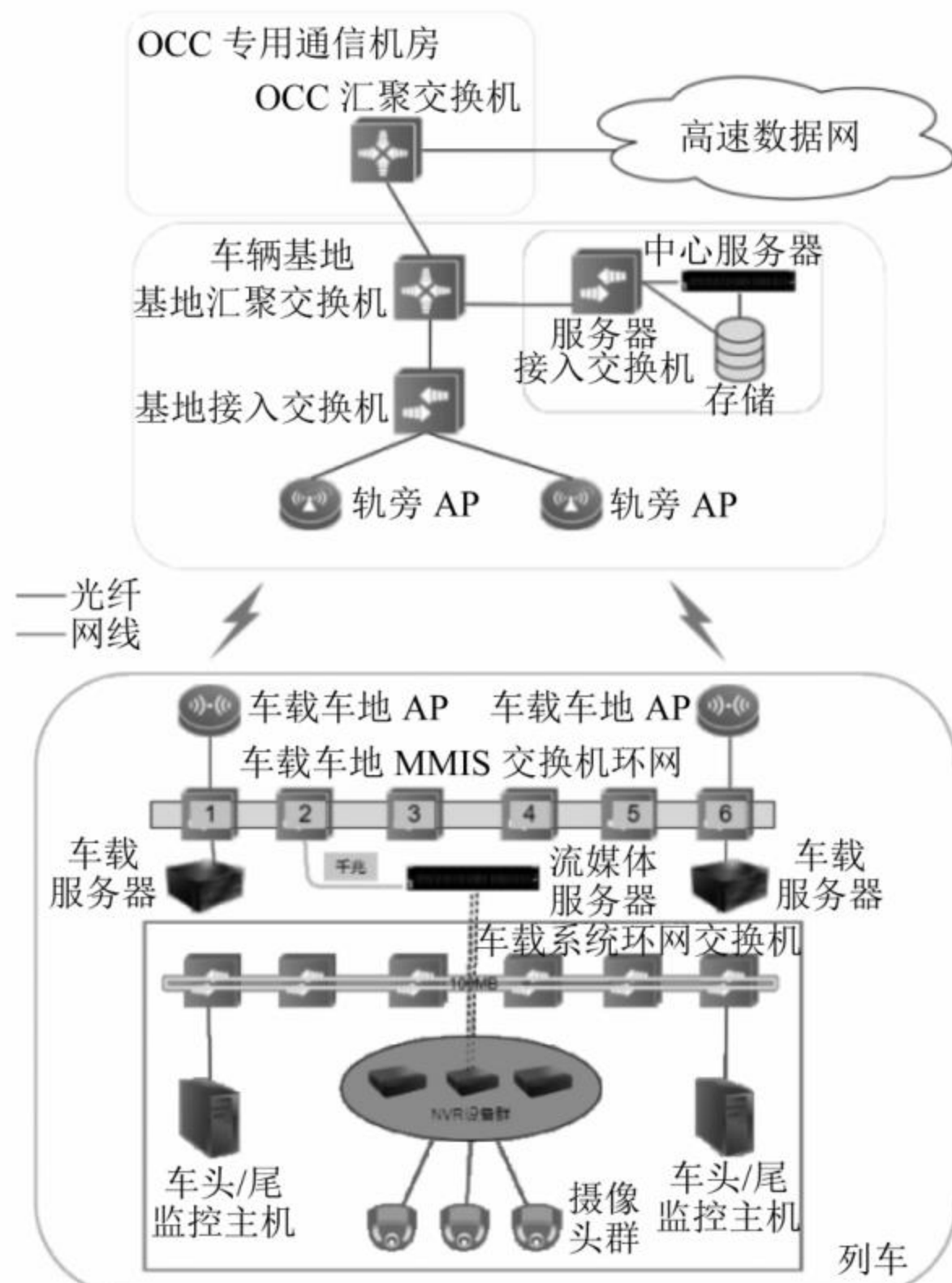
1 视频监控系统需求分析

上海轨道交通 3、4 号线列车现有的视频监控系统,提取视频资源时,需等列车回库后,安排人员将列车上的视频监控数据下载到电脑上进行备份。采用人工提取视频资源的方式,对于需下载的海量列车监控视频数据而言,既浪费人力物力,也不便视频资源的管理和使用。同时,由于车载视频监控设备存储容量有限,3、4 号线列车现有的视频监控系统只能存储 15 d 的视频,且当存储设备发生故障时,视频数据会有丢失的风险。因此,落地存储可以有效解决列车视频监控数据统一管理的问题。

2 改造后视频监控系统结构

2.1 03A01/04A01 车型视频监控系统结构

要实现视频监控文件的上传,需要在列车原视频监控系统端加装一台流媒体服务器。流媒体服务器配双千兆网卡,网口 1 与车载 PIS(乘客信息系统)环网交换机相连;网口 2 与车载 MMIS(管理信息系统)交换机环网相连。车载服务器与车载 MMIS 交换机环网相连。在基地新增万兆交换机及存储服务器。03A01/04A01 车型视频监控系统网络拓扑图如图 1 所示。



注: OCC—运营调度中心; AP—无线接入点; NVR—网络视频录像机。

图 1 03A01/04A01 车型视频监控系统网络拓扑图

Fig. 1 Network topology diagram of video surveillance system on 03A01/04A01 model train

在车载服务器上安装视频同步客户端,通过流媒体服务器接口获取视频监控文件,流媒体服务器会主动调取车载监控视频系统各车 DVR(硬盘录像机)上的监控视频文件,并按照时间顺序将监控视频文件转码生成数据包;同时,在车载服务器上安装视频上传客户端,通过车地 Wi-Fi 将监控视频文件上传到总控中心的存储服务器,并按照一定规则存储;通过 Wi-Fi 与地面中心服务器建立连接,并主动上传视频监控文件。当遇到网络故障或拥堵时,需合理调整网络效率。系统支持校验功能,能够确保视频监控文件的完整性。

2.2 03A02/04A02 车型视频监控系统结构

要实现视频监控文件的上传,需要在列车司机室各安装一台车载服务器,车载服务器具备两个千兆以太网接口(自适应百兆),一个接口与车载 PIS 环网交换机互联,另一接口与车载 MMIS 交换机接口互联。03A02/04A02 车型视频监控系统网络拓扑图如图 2 所示。

在车载服务器上安装视频同步客户端,车载服务器可获取 NVR(网络视频录像机)上的视频监控文件;在车载服务器上安装视频上传客户端,视频监

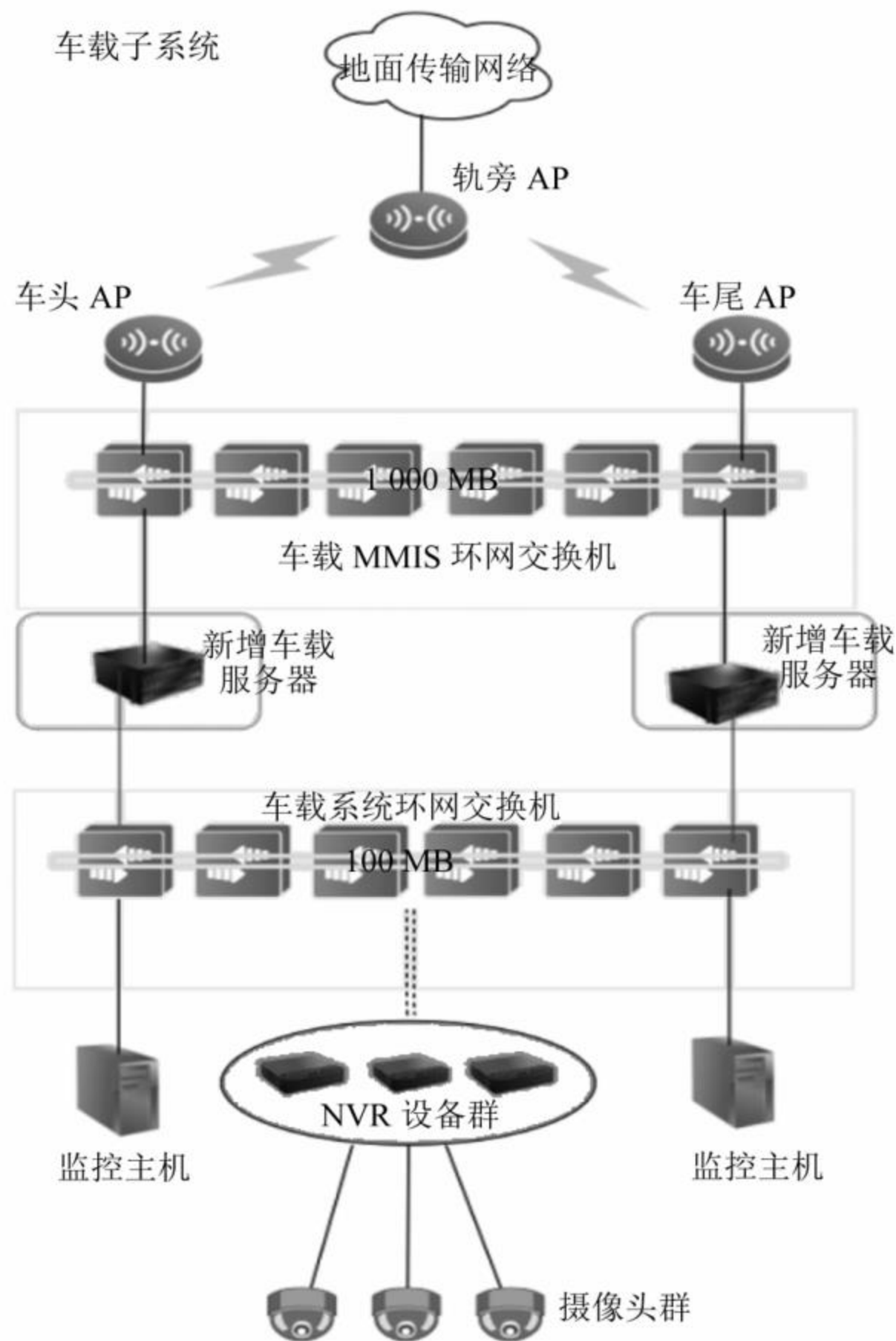


图 2 03A02/04A02 车型视频监控系统网络拓扑图

Fig. 2 Network topology diagram of video surveillance system on 03A02/04A02 model train

控文件通过 MMIS 网络上传到地面存储服务器,并按照一定规则存储在服务器上;通过 Wi-Fi 与地面中心服务器建立连接,并主动上传视频监控文件。当遇到网络故障或拥堵时,需合理调整网络效率。系统支持校验功能,能够确保视频监控文件的完整性。

3 改造后视频监控系统软件功能

1) 流媒体服务器配套软件功能模块:包含视频监控文件下载列表刷新功能模块、视频监控文件下载模块、上传传输协议交互模块、上传会话管理模块、本地视频监控文件上传列表刷新模块、本地视频监控文件上传模块和流量控制模块等 7 个功能模块。

2) 列车数据同步软件功能:可以将列车摄像头采集的视频监控文件暂存在车载服务器上,同时拥有对中心存储服务器的上传、断点续传等功能,其他功能还包括系统自动升级和日志上传等。

3) 车载视频实时查看软件功能:部署于车载服务器,用于总控中心视频监控客户端轮训查看各列

车车载 CCTV(视频监控)视频信息。

4) 云存储中心管理软件功能:布署于中心端服务器,用于同步列车视频监控数据,管理存储视频数据,并提供视频监控数据回放、查询等功能。

4 改造后视频监控系统安全性设计

4.1 系统整体安全性

为确保网络系统的整体安全可靠,并以网络安全等级保护安全通用要求第二级的要求为指导,通过如下方案搭建完整的安全体系:

1) 确保网络结构安全:将网络划分为不同的区域,并按照方便管理和控制的原则为各网络区域分配地址;避免将重要网络区域布署在网络边界处,并通过布署边界防护措施(堡垒机、防火墙、入侵检测设备等),为相关系统配置相关安全策略,对相关主机、数据库等设备设施进行初步安全配置,形成初步安全防护能力;针对主机服务器采用必要的安全运行维护措施,如周期性安全基线检测、漏洞检测、安全设备上线前后有效性检测及防护策略优化;对源地址、目的地址、源端口、目的端口和协议等进行检查,以允许/拒绝数据包进出;在关键网络节点处布署审计和入侵检测设备,监视网络攻击行为;在网络边界、重要网络节点进行安全审计,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;保证跨越边界的访问和数据流通过防火墙等边界设备提供的受控接口进行通信;根据可比拟的高可用性和高可靠性。

系统会对每份数据进行分片,每一个分片的不同副本被分散保存到不同的存储节点上。恶意用户无法利用单个存储节点或物理磁盘获取用户数据,单个节点的损坏或故障也不会影响副本数据的完整性。系统保证应用成功写入一份数据到存储系统后,无论从哪个副本上读取时都是之前写入的数据。对象存储和元数据存储可以平衡它们的负载,以适应不断变化的情况和使用方式。支持使用 SSD(固态硬盘)替代 HDD(机械硬盘)作为高速存储设备。SSD 可以降低随机访问时间和读延时,同时增加吞吐量,能够为高性能要求的大数据量实时访问提供更好的支持。

5 结语

上海轨道交通 3、4 号线列车视频监控系统升级

(下转第 146 页)

3) 对登录用户进行身份标识和鉴别。身份标识具有唯一性,鉴别信息具有复杂度要求并定期更换;用户身份鉴别信息丢失或失效时,采用技术措施保证鉴别信息重置过程的安全;根据网安监管需求,布署审计设备,对无线接入用户的接入行为进行记录;采取策略,禁止未授权访问和非法使用用户个人信息,仅采集和保存业务必需的用户个人信息。

4.2 视频监控数据安全性

CCTV 视频存储采用分布式云存储系统,系统采用弹性、稳定、高效、融合,支持纵向和横向全方位扩展的全对称分布式架构。

系统集群扩展无理论上限,可以从 2 个初始节点架构扩展到 EB 级存储容量;数据全局动态均衡,支持不同特性的节点共存于同一集群;具有极佳的在线扩展能力,添加通用架构 x86 机器即可扩展集群,系统可自动复制数据到新增节点,且能保持业务不中断。

系统基于全冗余部件节点、全冗余高速网络、去中心化的全冗余整体架构,保障数据可靠性和业务可用性。节点或硬盘故障后将被自动从集群中隔离,数据恢复期间,可以保持正常的访问,不会影响业务系统的正常使用。系统采用多数据副本机制来保证系统数据的可靠性和多重纠错,可跨硬盘、跨节点、跨机柜、跨地域存储,通过智能完善的系统自命和数据自修复功能,实现传统存储不可新安全形势增加和补充的其它安全规则和策略等。

2) 布署堡垒机和认证审计系统对登录的用户进行身份标识和鉴别。身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换;具有登录失败处理功能,配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;当进行远程管理时,采取加密措施,防止鉴别信息在网络传输过程中被窃听;授予管理用户所需的最小权限,实现管理用户的权限分离;启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;对审计记录进行保护,定期备份;遵循最小安装的原则,仅安装需要的组件和应用程序;通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;对入侵检测设备,启用防恶意代码软件,并定期进行升级和更新防恶意代码库;限制单个用户或进程对系统资源的最大使用限度。

