

基于物联网的智能汽车远程监控系统设计

张鹤, 盛庆祝, 程刚

长春大正博凯汽车设备有限公司, 吉林 长春 130000

DOI:10.61369/ERA.2026070035

摘 要 : 针对传统车辆监控存在的数据孤岛、实时性差、运维成本高等问题, 本文从一线工程实践出发, 从车载终端数据采集、低功耗广域传输、云端智能分析三个方面入手, 提出了一套基于物联网的智能汽车远程监控系统架构。从安全角度来讲, 系统创建起包含车载网络入侵检测、传输层双向认证以及云端 API 纵深防御的三级安全体系, 从经济角度出发, 创建起包含硬件摊销、通信资费以及云服务订阅的透明化成本模型, 从而证明了不同规模车队的经济可行性, 从方法论角度来讲, 利用开源工具链和标准化数据集来提高研究成果的可复现性。实际部署结果表明, 该系统可以把故障预警响应时间缩短到秒级, 在860辆纯电动公交车规模化应用的情况下, 单车年综合运维成本降低约18%, 有效预警率91.3%, 为车队智能化管理提供了一条可落地的技术路径。

关 键 词 : 物联网; 远程监控; CAN 总线; MQTT; 边缘计算; 预测性维护; 车载网络安全; 成本效益分析

Design of an IoT-Based Intelligent Vehicle Remote Monitoring System

Zhang He, Sheng Qingzhu, Cheng Gang

Changchun Dazheng Bokai Automotive Equipment Co., Ltd., Changchun, Jilin 130000

Abstract : Addressing the issues of data silos, poor real-time performance, and high operational and maintenance costs in traditional vehicle monitoring, this paper proposes an IoT-based intelligent vehicle remote monitoring system architecture from the perspective of frontline engineering practice. The architecture focuses on three key aspects: onboard terminal data acquisition, low-power wide-area transmission, and cloud-based intelligent analysis. From a security standpoint, the system establishes a three-tier security framework encompassing onboard network intrusion detection, transport layer mutual authentication, and cloud API defense-in-depth. Economically, it introduces a transparent cost model that accounts for hardware amortization, communication expenses, and cloud service subscriptions, demonstrating economic feasibility for fleets of varying sizes. Methodologically, the use of open-source toolchains and standardized datasets enhances the reproducibility of research findings. Practical deployment results show that the system reduces fault warning response times to the second level, lowers annual comprehensive operational and maintenance costs by approximately 18% per vehicle in a large-scale application involving 860 pure electric buses, and achieves an effective warning rate of 91.3%. This provides a viable technological pathway for intelligent fleet management.

Keywords : Internet of Things (IoT); remote monitoring; CAN Bus; MQTT; edge computing; predictive maintenance; onboard network security; cost-benefit analysis

一、问题提出与技术切入点

在商用车队管理的一线场景中, 传统的 GPS 定位终端只能给出位置轨迹, 不能得到发动机工况、制动系统状态等重要的运行数据。维修人员一般依靠驾驶员的主观描述或者定期进站检测来发现潜在的故障, 从而造成小故障变成大故障。这一痛点就决定了系统要同时满足数据多维、传输可靠、云端高并发、安全可量

化这四个硬性约束。因此, 以车载多源异构数据采集、轻量级可靠传输、云端实时流处理、全栈安全防护为完整的工程化实现, 而不是泛泛地讨论物联网的概念^[1]。

二、系统总体架构设计

系统采用端、边、云三层架构。车载终端层完成原始信号采

作者简介: 张鹤 (1985.03-), 男, 汉族, 吉林省长春市人, 大学本科学历, 高级工程师, 机器人部经理, 从事工业机器人应用、虚拟仿真、数字孪生、工业机器人离线及实施, 工业物联网与数字孪生。主要从事汽车焊装生产线工业机器人模拟仿真、数字孪生、虚拟调试、在线编程、多种金属连接工艺等相关工作。

集、本地预处理和入侵检测，边缘网关层完成协议转换、数据压缩、断点续传和访问控制，云平台层完成海量数据存储、业务规则引擎、纵深防御和可视化展示^[2]。

车载终端硬件不再使用单一 GPS 模块，而采用集成 OBD-II 解码、CAN 总线收发、4G 通信、MEMS 加速度的多功能 T-Box。OBD-II 端口用标准 PID 指令读取发动机转速、冷却液温度、燃油系统状态等通用参数；对于新能源车型，直接挂载 CAN 总线，以 250kbps 或者 500kbps 速率捕获电池管理系统 BMS、电机控制器 MCU 的私有帧。实践证明，OBD-II 可以覆盖乘用车 90% 以上的动力相关故障码，CAN 直连可以获取电池单体电压、母线电流等 OBD 无法提供的深度数据，两者互补就可以达到车型兼容最大化的目的。T-Box 采用工业级处理器，宽电压供电可以适应 12V、24V 车型。

边缘网关层的关键设计就是采用 MQTT 协议作为通信的主干。相比 HTTP 轮询，MQTT 的发布 / 订阅模型大大减少了空口流量，车辆只在数据变化或者心跳周期到达的时候才发送消息，实测 4G 流量消耗降低了约 60%。主题命名采用 "fleet/{vehicleId}/{subsystem}/{metric}" 四级结构，例如 "fleet/V001/engine/coolantTemp"，便于云平台按车、按系统灵活订阅。QoS 按照业务进行分级，网关内置 1GB 循环缓存支持断点续传，断线重连使用指数退避策略^[3]。

云平台使用时序数据库 InfluxDB，告警引擎采用规则链和轻量级机器学习双轨并行的方式；用 WebSocket 推送实现监控大屏秒级刷新；微服务架构支持十万级接入；数据冷热分层降低存储成本。

三、车载网络安全架构与纵深防御

（一）车载网络攻击面分析与防御机制

目前文献对于传输层安全（TLS 1.3 和 X.509 双向认证）已经进行了详细的论述，但是对于车载网络内部的攻击面却有所忽略。OBD-II 端口属于物理接口，存在恶意设备注入伪造 CAN 报文的明显危险。攻击者可以使用市售的 OBD-II 适配器向 CAN 总线发送非授权帧，篡改发动机转速或者制动系统状态，干扰车辆正常运行。为抵御该威胁，本系统在 T-Box 固件里创建了基于规则的入侵检测模块，先创建正常工况下的 CAN ID 白名单和信号变化率基线，对于超出物理合理范围的报文（冷却液温度在 1 秒内上升 50℃）自动丢弃并发出安全告警，然后在总线层开启消息认证码（MAC）功能，对关键控制帧加上 HMAC-SHA256 校验，未通过校验的指令会被网关拦截^[4]。

（二）云端 API 纵深防御体系

云平台 API 受到 SQL 注入、越权访问、分布式拒绝服务（DDoS）等各方面的威胁。本系统使用四层防御策略，WAF+ 速率限制、OAuth 2.0+JWT 短令牌、RBAC 和 ABAC 混合授权、ELK 日志审计四层防御，具体的阈值和角色分级在这里从略。

（三）数据隐私与合规性保障

系统严格按照汽车数据安全法规若干规定（试行）和个人信

息保护法的要求执行。车辆采集的地理位置、驾驶行为等敏感数据在 T-Box 端就进行了 AES-256 加密，密钥由硬件安全模块（HSM）保管，云平台不能解密原始数据。数据留存期限按照用途分层，运维诊断数据保留 90 天，事故追溯数据保留 3 年，到期自动不可逆删除。跨车队数据共享使用联邦学习框架，模型参数加密传输，原始数据不出域，协同优化和隐私保护并重^[5]。

四、成本结构模型与经济可行性分析

（一）全生命周期成本分解

为了评价系统的经济可行性，本文建立了一个包含硬件、通信和云服务的全生命周期成本模型。以 100 辆车队规模为基准，成本结构如下：

硬件年均摊销 76 到 90 元，通信费 180 到 300 元（实际流量小于套餐阈值），云服务 12 到 18 元，单车年均总成本 268 到 408 元。

综合计算得出单车年均总成本为 268-408 元。相比传统的方案（单个 GPS 终端硬件年费约为 150 元，人工巡检年均工时成本约为 800 至 1200 元），本系统用预测性维护代替固定周期保养，在 860 辆公交车的实测中使单车年运维成本降低约 18%。成本节约与车队规模呈正相关，大规模车队回收期可以缩短到 6-9 个月。

（二）与商用方案的横向对比

为了确定本文方案的技术经济定位，选取国内主流的商用方案做横向比较。第一类为整车厂原厂系统，如吉利商用车远程监控平台、宇通车联网系统，其优势是与车辆 ECU 深度集成、协议兼容性好，但是存在品牌锁定效应，跨品牌车辆无法接入，年费订阅模式（单车年均 600-1200 元）对混合车队成本较高。第二类是第三方 SaaS 平台（G7 物联、中交兴路等），其优点是即开即用、功能成熟，支持多品牌接入，但是数据存储在服务商云端，存在数据主权和定制化受限的问题，并且按功能模块阶梯计价，深度诊断功能需要另外付费。第三类为开源方案（OpenXC+ThingsBoard），硬件成本可控但是缺少企业级的安全认证和技术支持，运维门槛高。

开放性上可以支持跨品牌的接入，避免品牌锁定，数据主权上支持私有化部署，敏感数据不出域，成本上单车年均总成本比原厂系统低约 35% 到 55%，比第三方 SaaS 低约 20% 到 40%，但是需要承担初期 CAN 适配和系统集成的工程投入。核心差异化优势有三个，一是 CAN 总线深度解析能力，可以获取 BMS 单体电压等原厂系统不开放的底层数据；二是边缘-云协同计算架构，使 4G 流量消耗比传统 HTTP 方案降低约 60%；三是三级安全防护体系，填补了商用 SaaS 在车载网络入侵检测方面的空白。

五、关键技术实现与可复现性保障

（一）CAN 总线数据解析与信号还原

商用车 CAN 矩阵是由整车厂自行定义的，DBC 文件一般不对外公开。项目组在一线实践当中总结出“逆向+标定”双轨策

略，即先用 CANoe 或者开源工具 CANalyzatOr（基于 Python 的 can-utils 库）抓取总线原始帧，再结合维修手册中已知的信号（如车速、油门踏板开度）进行位域匹配，初步还原信号起始位、长度和偏移量；然后将还原结果与 OBD-II 同维度数据比对，修正比例因子和偏移误差。对于多路复用帧，根据消息 ID 后面的 2 字节节点地址来区分不同的发送控制器，防止信号混淆^[6]。

平台 A 为某国产柴油轻卡（CAN 2.0B 标准帧，250kbps），平台 B 为某纯电动公交（CAN 2.0B 扩展帧，500kbps，BMS 多包传输），平台 C 为某混动物流车（双通道 CAN，动力 CAN 与车身 CAN 分离）。验证方法以平台 A 为例，选取车速、发动机转速、冷却液温度等 12 个可以和 OBD-II 交叉验证的信号，用 CANalyzatOr 连续采集 2 小时行驶数据（约 180 万帧），经过位域匹配和标定修正后，将还原值与 OBD-II 读取值逐秒进行比对。结果表明，在三种平台上信号还原的平均绝对百分比误差（MAPE）分别为 2.1%、3.4% 和 4.7%，综合准确率大于 97%。需要说明的是，97% 的准确率是针对已经标定的信号，对于未经验证的私有信号（proprietary 的尿素喷射脉宽）准确率会降低到 80% 左右，需要结合台架试验进行标定。

为了提高研究的可复现性，项目组公开了部分脱敏数据集和工具链，在 GitHub 仓库中提供平台 A 的 10 分钟原始 CAN 日志样本（约 15 万帧，已经脱敏车辆识别信息）、对应的 OBD-II 基准数据 CSV 文件、基于 Python 的自动标定脚本。研究者可以通过脚本复现信号还原过程，但是完整的 DBC 文件由于整车厂的知识产权原因没有公开。项目组用 Car Hacking Dataset 公开的数据（Roel Vlugt 发布的 Jeep Cherokee CAN 日志）做跨车型验证的补充基准，该数据集包含已标注的逆向结果，可以供学术界独立验证方法的有效性^[7]。

（二）MQTT Broker 高并发优化

车队规模扩大之后，单个 Broker 节点在 5000 辆车同时在线的时候就会出现消息堆积。优化措施有，第一，使用 EMQX 集群部署，用节点间的路由表分担连接和订阅关系；第二，启用共享订阅（Shared Subscription），把同一个主题的消费负载均衡到多个后端服务实例上；第三，设置消息过期时间（Message Expiry Interval），防止离线车辆堆积历史消息造成内存溢出。经过压力测试，优化后的集群可以稳定地承载 2 万并发连接，消息端到端延迟中位数小于 80 毫秒，P99 延迟小于 300 毫秒。同时使用 TLS 1.3 加密传输，证书采用 X.509 双向认证，防止中间人攻击和设备伪造接入。鉴权层面采用 RBAC 模型，车辆设备只拥有发布自身主题和订阅 OTA 下行主题的权限，杜绝横向越权访问其他车辆数据^[8]。

（三）边缘计算与 OTA 升级

为了减小云端计算压力、提高实时性，T-Box 内部使用 ARM Cortex-M7 微控制器运行轻量级推理框架。以驾驶行为识别为例，加速度计原始数据在本地做滑动窗口特征提取（均值、方差、过零率），用预训练好的决策树模型实时判断急加速、急减速事件，只把事件标签和置信度上传到云端，原始波形数据本地保存 7 天后自动覆盖。该设计使得云端数据吞吐量下降了大约

75%，并且可以满足监管部门对于驾驶行为监控的实时性要求。边缘端运行 CAN 信号滤波算法，对总线负载率大于 70% 的高频场景，用变化率阈值触发机制，只有信号变化超过设定容差的时候才会上报，避免无效数据淹没信道。冷却液温度在稳态工况下波动幅度一般小于 2℃，设定容差为 3℃即可过滤掉 90% 以上的冗余上报。

固件升级使用差分 OTA。云端根据当前版本号和目标版本号生成差分包，T-Box 通过 MQTT 主题 fleet/{vehicleId}/ota/diff 接收后本地重组完整固件，校验 SHA-256 哈希值无误再切换启动分区。实测差分包体积为完整包的 15% 到 30%，在 4G 网络下可以将升级时长从 20 分钟缩短到 6 分钟，大大减少升级过程中对车辆正常运营的影响。升级过程分为 A/B 两部分，升级失败会自动回退到旧版本，保证系统的可用性。升级时段策略使车队排班自动选择低运营时段推送，避开早晚高峰^[9]。

六、典型应用场景与实测效果

系统在某省会城市公交集团部署，覆盖纯电动公交车 860 辆。运行 18 个月的关键指标如下：

系统共捕获电池单体电压偏差、电机绝缘下降等三级预警 4217 次，经检修确认有效预警率 91.3%，平均提前发现时间 72 小时，避免途中抛锚事件 127 起。电池热失控早期预警 3 次，均在温度异常上升阶段就被识别并处理，没有发生安全事故。

能耗优化依靠远程采集的能耗数据同线路坡度、载客量联系分析，改善调度和驾驶培训方案，单车百公里电耗下降 6.8%。识别出高能耗驾驶行为并加以针对性的培训之后，急加速次数减少了 43%，制动能量回收效率提高了 11%。

运维成本上，用预测性维护代替固定周期保养，年维保工时减少约 14%，配件库存周转率提高 22%。传统的按里程强制更换制动片的方法改为根据实际磨损数据动态调整，单车年制动片消耗量降低 31%。综合测算得出单车年运维成本降低 18% 左右，和成本模型预测基本一致^[10]。

运营效率上，实时监控使调度中心可以掌握车辆实时位置和剩余电量，线路排班匹配度提高 19%，车辆日均运营里程增加 8.2%。

七、结论与展望

本文从一线车队管理真实需求出发，从数据采集、可靠传输、智能分析、安全防护四个方面构建起一套可以落地的物联网远程监控系统。核心经验就是协议层面用 MQTT 代替传统的 HTTP 可以大大降低移动场景下的带宽和功耗开销，数据层面打通 OBD-II 和 CAN 总线通道是实现车型兼容和深度监控的关键，计算层面将规则引擎和边缘推理结合起来，兼顾了实时性和成本可控性，安全层面构建的三级防御体系填补了车载网络入侵检测的能力空白，经济层面的透明化成本模型给不同规模车队的投资决策提供量化依据。

后续研究会从四个方面展开，一是5G-V2X 以及车路协同场景下的毫秒级低时延监控，探究 MQTT over 5G NR 的 QoS 改善，二是联邦学习框架下跨车队数据隐私保护，在不共享原始数据的情况下达成模型协同训练，三是数字孪生技术在车辆全生命周期健康管理中的应用，创建虚实映射的预测性维护体系，四是车载网络入侵检测的智能化升级，探寻图神经网络（GNN）的 CAN 总线异常检测办法，应对愈发繁杂的网络攻击形式。

参考文献

[1] 劳俊元. 5G 物联网技术在汽车智能诊断与维修中的应用研究 [J]. 通讯世界, 2026, 33 (04): 160–162.

[2] 卢志敏, 潘勇. 基于物联网技术的智能充电桩远程监控与管理系统分析 [J]. 电子技术, 2026, 55 (01): 175–177.

[3] 张川. 物联网技术在智能车载系统中的应用 [J]. 电子元器件与信息技术, 2025, 9 (12): 237–240.

[4] 王海洪, 李倍倍, 胡伟. 物联网安全的隐秘战场：远程攻击引发的非传统威胁概述 [J]. 工业信息安全, 2025, (06): 6–13.

[5] 杨朝. 基于物联网的汽车电气自动化远程监控系统开发研究 [J]. 汽车测试报告, 2025, (22): 1–3.

[6] 金贵阳, 陈罡, 竺银军, 等. 基于物联网的冲压设备远程管理系统 [J]. 锻压装备与制造技术, 2025, 60 (04): 77–81.

[7] 汪莉, 权爱平, 梁雪峰. 物联网驱动的智能汽车远程预测性维护系统设计与应用 [J]. 汽车维修技师, 2025, (16): 61–62.

[8] 杨凯, 肖卫东. 基于物联网的汽车电气自动化远程监控系统开发研究 [J]. 汽车测试报告, 2025, (08): 22–24.

[9] 欧书琴. 物联网技术在智能汽车电子系统中的应用 [J]. 汽车测试报告, 2025, (01): 43–45.

[10] 蒋丽娜. 基于物联网的智能汽车信息管理系统设计 [J]. 专用汽车, 2024, (12): 106–108.