

智慧交通网络实时安全监测技术的应用探讨

夏锦宇

合肥大学, 安徽 合肥 230601

DOI: 10.61369/SSSD.2026050008

摘 要 : 智慧交通作为现代交通体系发展的核心方向,已成为推动交通强国战略实施的关键支撑力量。其通过深度融合车辆感知终端、道路基础设施、云端数据中心等多维度资源,构建起高效协同、智能互联的现代化交通生态系统。近年来,随着5G通信、边缘计算、物联网等前沿技术的大规模应用与深度赋能,智慧交通系统的设备连接规模持续扩大,数据交互总量呈指数级增长,系统复杂性与开放性显著提升。与此同时,智慧交通网络也面临着日益严峻的安全挑战,包括设备层面面临的非法入侵与恶意控制、数据传输过程中的泄露与篡改、系统通信中断与服务瘫痪等多维度安全威胁。传统的以事后响应和周期性排查为主的安全防护机制,因其滞后性和静态性,已难以适应智慧交通高实时、高动态、高连续的业务特性。在此背景下,实时安全监测技术逐步兴起并得到广泛应用。该技术通过对交通系统内各类节点、链路及数据流的持续嗅探、动态分析与异常预警,实现对安全威胁的即时识别与快速响应,已成为保障智慧交通网络可靠运行的第一道防线。系统化研究实时安全监测技术的落地路径、优化方法及推广策略,对提升智慧交通系统整体韧性、促进行业可持续健康发展具有重大的现实意义和战略价值。

关 键 词 : 智慧交通; 安全监测; 智能化

Discussion on the Application of Real-Time Security Monitoring Technology in Intelligent Transportation Networks

Xia Jinyu

Hefei University, Hefei, Anhui 230601

Abstract : As the core development direction of the modern transportation system, intelligent transportation has become a key supporting force for advancing the implementation of the Transportation Power strategy. By deeply integrating multi-dimensional resources such as vehicle sensing terminals, road infrastructure, and cloud data centers, it constructs a modern transportation ecosystem characterized by efficient collaboration and intelligent interconnection. In recent years, with the large-scale application and in-depth empowerment of cutting-edge technologies including 5G communication, edge computing, and the Internet of Things (IoT), the scale of device connections in intelligent transportation systems has continued to expand, the total volume of data interaction has grown exponentially, and the system complexity and openness have been significantly enhanced. At the same time, intelligent transportation networks are also facing increasingly severe security challenges, including multi-dimensional security threats such as unauthorized intrusion and malicious control at the device layer, data leakage and tampering during transmission, as well as system communication interruptions and service paralysis. The traditional security protection mechanisms, which mainly rely on post-event response and periodic inspections, have become increasingly unable to adapt to the operational characteristics of intelligent transportation—high real-time performance, high dynamics, and high continuity—due to their lag and static nature. Against this backdrop, real-time security monitoring technology has gradually emerged and been widely applied. Through continuous sniffing, dynamic analysis, and anomaly early warning of various nodes, links, and data flows within the transportation system, this technology enables the real-time identification and rapid response to security threats, and has thus become the first line of defense for ensuring the reliable operation of intelligent transportation networks. Systematically studying the implementation paths, optimization methods, and promotion strategies of real-time security monitoring technology holds great practical significance and strategic value for improving the overall resilience of intelligent transportation systems and promoting the sustainable and healthy development of the industry.

Keywords : intelligent transportation; security monitoring; intellectualization

一、智慧交通网络面临的安全威胁

（一）设备层安全风险

智慧交通网络包含大量路侧传感器、车载终端、信号控制机等智能设备，部分设备部署于户外开放环境，易遭受物理破坏或恶意入侵。同时，部分低端设备存在固件漏洞，缺乏完善的身份认证机制，极易被黑客控制，进而篡改设备采集的数据，影响交通决策的准确性。

（二）通信层安全风险

车路协同、车车通信是智慧交通的核心应用场景，其依赖无线通信技术实现数据传输。在无线传输过程中，数据易被窃听、伪造或篡改，攻击者可通过发送虚假的交通信息，如伪造拥堵预警、信号灯指令等，引发交通混乱，甚至造成交通事故。

（三）数据层安全风险

智慧交通网络产生的海量数据包含车辆轨迹、人员出行信息、交通流量等敏感内容，这些数据在存储、共享、分析环节均存在泄露风险。若数据管理不当，不仅会侵犯用户隐私，还可能被不法分子利用，威胁城市交通安全与公共利益。

具体而言，数据存储环节可能因数据库权限管理松散、加密机制缺失导致数据被非法访问。例如，部分交通管理平台未对敏感数据进行分级保护，普通运维人员可随意调取车辆轨迹数据，增加了数据泄露的隐患。在数据共享过程中，不同部门、企业间的数据交互缺乏统一的安全协议，数据传输通道易被劫持，导致数据在传输途中被窃取或篡改。而在数据分析环节，若采用的算法模型存在安全漏洞，攻击者可通过投毒攻击污染训练数据，使分析结果偏离实际，影响交通管理策略的制定。此外，智慧交通数据还面临着跨境流动的安全风险，若未严格遵守数据出境管理规定，可能导致国家关键信息泄露，危害国家安全。

二、智慧交通网络实时安全监测技术的核心架构

智慧交通网络实时安全监测体系采用“感知—传输—分析—预警”四层递进式架构，实现对交通系统全链路安全状态的动态、实时与精准监测。该架构通过层层衔接、功能互补的方式，有效支撑从数据采集到风险响应的闭环管理，全面提升交通安全运行的保障能力。

1. 感知层：作为整个监测体系的数据基础，该层依托部署于道路沿线的各类传感器、车辆内置智能终端以及网络探针等物联网设备，实时采集包括设备运行状态参数、网络流量特征、数据交互行为日志在内的多维度、海量监测数据。这些数据不仅覆盖交通基础设施和车载单元，还涉及通信网络关键节点，为后续的安全威胁识别与深度分析提供了充分、多样且高质量的数据来源。

2. 传输层：承担监测数据高效、稳定上传的关键任务。该层主要基于5G通信、边缘计算等先进技术，构建具备低时延、高带宽、高可靠特性的数据传输通道。在实现监测数据实时、完整传递至上层分析平台的同时，传输层还集成了数据加密与完整性校

验机制，有效防范数据在传输过程中被窃取或篡改，确保敏感信息安全抵达处理单元。

3. 分析层：作为智慧安全监测的核心决策支撑层，融合了人工智能算法、大数据挖掘与机器学习等先进技术，构建了多类安全风险分析模型。该层对实时汇入的监测数据进行解析与聚合，通过行为模式识别、异常检测、关联分析等手段，精准识别诸如设备异常登录、数据异常流量、协议非合规篡改等潜在威胁，并依据预定义规则与自适应学习机制，对识别出的安全事件进行风险等级评估与分类。

4. 预警层：基于分析层输出的风险判定结果，该层实现及时、有效的安全风险响应。通过集成短信通知、监测平台实时告警、现场声光设备提示等多种方式，向交通管理相关部门及人员发送分级预警信息，并提供包括风险定位、处置建议和应急预案在内的决策支持，从而达成“早发现、早预警、早处置”的主动安全防护目标，最大限度降低安全事故发生概率及影响范围。

三、智慧交通网络实时安全监测关键技术

（一）物联网感知技术

物联网感知技术是实时安全监测的基础，通过部署RFID射频识别、视频监控、毫米波雷达等设备，实现对交通基础设施状态、车辆运行参数、网络节点连接情况的全面感知。例如，利用毫米波雷达监测路侧设备的物理位移，判断是否存在人为破坏；通过RFID技术对车载终端进行身份认证，防止非法设备接入网络。

（二）边缘计算技术

智慧交通网络对监测实时性要求极高，边缘计算技术将数据处理能力下沉至网络边缘节点，减少数据传输延迟。在车路协同场景中，边缘节点可实时分析车辆与路侧设备的通信数据，识别虚假信息攻击，无需将数据上传至云端，大幅提升风险处置效率。

（三）人工智能异常检测技术

传统的安全监测依赖预设的规则库，难以应对新型网络攻击。人工智能异常检测技术通过机器学习算法，对智慧交通网络的正常运行数据进行训练，构建正常行为模型。当监测数据偏离模型阈值时，系统自动判定为异常行为，可有效识别未知的、变异的安全威胁，提升监测的智能化水平。

（四）区块链数据安全技术

区块链技术具有去中心化、不可篡改的特性，可应用于智慧交通数据安全监测。将关键数据，如车辆轨迹、信号灯控制指令等，存储于区块链节点中，实时监测数据的修改记录，防止数据被恶意篡改。同时，通过智能合约实现数据访问权限的动态管控，降低数据泄露风险。

区块链技术的分布式账本结构，为智慧交通网络构建了一个透明且可信的数据共享环境。例如，在交通数据交互场景中，参与数据传输的各方节点需通过共识机制验证数据的合法性，确保每一条数据的来源可追溯、操作可审计。当某一节点试图上传伪

造的车辆位置信息时，区块链的共识算法会快速识别并拒绝该数据的写入，避免虚假信息对整个交通调度系统造成干扰。此外，区块链的时间戳功能能够精准记录数据生成的时间顺序，为安全事件的事后溯源提供可靠依据。在车路协同通信中，通过将路侧设备的状态数据与车辆的行驶数据同步上链，可实现对通信过程的全程监测，一旦发现数据传输过程中存在异常篡改痕迹，系统会立即触发警报并锁定相关节点，有效保障车路协同指令的真实性与有效性。这种基于区块链的数据安全监测方式，不仅解决了传统中心化数据存储模式下的单点故障风险，还通过加密算法与分布式架构的结合，进一步强化了智慧交通网络数据的完整性与保密性。

四、智慧交通网络实时安全监测技术的应用场景

（一）交通基础设施安全监测

针对桥梁、隧道、信号灯等交通基础设施，部署实时监测设备，采集结构应力、设备运行电压、信号传输状态等数据。通过安全监测平台实时分析数据，当桥梁结构应力超过安全阈值，或信号灯控制机出现通信中断时，系统立即发出预警，提醒运维人员及时检修，避免因设施故障引发交通拥堵或事故。

（二）车路协同安全监测

在车路协同系统中，实时监测技术可对车与路、车与车之间的通信数据进行解析，识别虚假信息攻击。例如，当攻击者伪造路侧设备发送的“前方畅通”指令时，监测系统可通过对比周边车辆的实际行驶数据，判定该指令为异常信息，并向相关车辆发送告警，同时调整交通诱导策略，保障行车安全。

（三）交通数据安全监测

构建数据全生命周期安全监测体系，实时跟踪数据的采集、传输、存储、使用等环节。通过监测数据访问日志，识别非法访问行为；利用数据脱敏技术，对敏感信息进行实时处理，防止隐私泄露。同时，监测数据的流向，确保数据在共享过程中不被篡改或滥用，保障数据的完整性与安全性。

（四）城市交通网络应急监测

在突发交通事件，如交通事故、恶劣天气等场景下，实时安

全监测技术可快速采集事件区域的交通流量、车辆拥堵状态、设备受损情况等数据，为交通管理部门提供应急决策支持。例如，在暴雨天气中，监测路面积水深度与交通信号灯运行状态，自动调整信号灯配时，并向公众发布绕行建议，提升应急处置效率。

五、智慧交通网络实时安全监测技术的发展趋势

（一）多技术融合化发展

未来，实时安全监测技术将朝着多技术深度融合的方向发展，物联网、人工智能、区块链、量子通信等技术的结合，将构建起更加全面、可靠的安全监测体系。例如，量子通信技术可实现监测数据的绝对安全传输，结合人工智能异常检测技术，进一步提升对高级持续性威胁的识别能力。

（二）监测体系智能化升级

随着大模型技术的发展，智慧交通安全监测平台将具备更强的自主分析与决策能力。通过构建交通安全大模型，整合多源监测数据，实现对安全风险的预判与主动防御，从“被动监测”向“主动预警”转变。

（三）标准化与规范化建设

目前，智慧交通网络实时安全监测技术缺乏统一的标准规范，不同厂商的设备与平台兼容性较差。未来，行业将加快制定监测指标、数据格式、接口协议等标准，推动监测体系的规范化建设，实现跨区域、跨平台的安全数据共享与协同预警。

六、结语

智慧交通网络实时安全监测技术是保障智慧交通系统稳定运行的核心支撑，其通过多维度感知、智能化分析、实时化预警，有效应对设备、通信、数据等层面的安全威胁。随着技术的不断创新与融合，实时安全监测体系将更加完善，为智慧交通行业的高质量发展筑牢安全屏障。在未来的发展中，需进一步加强技术研发与标准建设，推动实时安全监测技术在更多场景的落地应用，助力交通强国战略的实施。

参考文献

- [1] 交通运输部. 数字交通“十四五”发展规划 [Z]. 2021.
- [2] 张明, 李强. 基于边缘计算的车路协同安全监测技术研究 [J]. 交通信息与安全, 2023, 41(02): 112-118.
- [3] 王芳. 人工智能在智慧交通网络安全防护中的应用 [J]. 智能城市, 2022, 8(15): 67-69.
- [4] 安邦 (Asim Farooq). 适用于未来北京均衡可持续发展的城市交通规划方法 [D]. 北京科技大学, 2019.
- [5] 陈悦鹏. 义乌市城市道路交通优化策略研究 [D]. 西安电子科技大学, 2019.
- [6] 高胜庆, 刘花, 顾宇忻, 等. 交通与国土空间协同评价方法及应用——以广州市为例 [J]. 城市规划, 2021(9).
- [7] 顾宇忻. 现代中小城市道路规划与设计研究 [J]. 中国房地产业, 2018(12).
- [8] 林晓生, 顾宇忻, 张薇, 等. MaaS 场景下考虑用户异质性的交通分配模型 [J]. 交通与运输, 2024(1).
- [9] 江苏省交通运输厅. 智慧交通关键技术攻关试点: 342省道无锡段打造智慧公路示范 [R]. 2022.
- [10] 魏传佳, 何世伟. 基于大数据分析的实时交通安全监测与预警研究 [J]. 信息化理论与实践, 2019, 1(01): 47-53.