智慧公路车路协同系统数据加密与隐私保护技术

秦昊

江西慧通科技发展有限责任公司，中国 · 江西 南昌 331000

摘要：在现代科学技术发展之下，智慧公路建设逐步进行，车路协同（V2X）技术广泛应用到实践中，能有效提升交通效率和安全性。目前 V2X 系统中高频次车 - 路 - 云数据交互，能有效防止发生隐私侵犯或数据泄露风险。本文从目前智慧公路场景下数据安全方面展开研究，研究基于国密算法的混合加密机制、基于区块链的去中心化身份认证体系以及差分隐私数据发布策略，进而保证智慧公路系统稳定运行。

关键词：智慧公路；车路协同；数据加密；隐私保护；国密算法

Data Encryption and Privacy Protection Technology for Smart Highway Vehicle Road Collaboration System

Qin Hao

Jiangxi Huitong Technology Development Co., Ltd., China Jiangxi Nanchang 331000

Abstract: With the development of modern science and technology, the construction of smart highways is gradually underway, and vehicle to road collaboration (V2X) technology is widely applied in practice, which can effectively improve traffic efficiency and safety. At present, high-frequency vehicle road cloud data interaction in V2X systems can effectively prevent privacy infringement or data leakage risks. This article conducts research on data security in the current smart highway scenario, studying hybrid encryption mechanisms based on national encryption algorithms, decentralized identity authentication systems based on blockchain, and differential privacy data publishing strategies to ensure the stable operation of the smart highway system.

Keywords: Smart highway; Vehicle road collaboration; Data encryption; Privacy protection; National cryptographic algorithm

0 引言

智慧公路是促进公路交通领域发展的关键，也是新型基础设施的核心部分。智慧公路通过在公路系统内安装毫米波雷达、激光雷达、摄像头等感知设备，能实现公路交通系统内人、车、路、云的全面互联。车路协同系统是智慧公路体系内的神经中枢，其作用是获取车辆状态、路况信息、信号灯相位等数据，并且能实现自动驾驶决策和交通流优化。近年来网络事业发展加速，网络攻击事件屡见不鲜，尤其是很多外部势力随意截取车辆大规模数据信息，对智慧公路系统以及社会稳定发展造成不利影响。因此，深入研究智慧公路车路协同系统数据加密与隐私保护技术，确保数据不会发生泄露问题[1]。

1 智慧公路 V2X 数据安全风险分析

1.1 通信链路窃听与数据篡改

V2X 通信主要采用 C-V2X 或 DSRC 技术，其广播特性是任何覆盖范围内接收设备均可截获信号。如果未能采取有效数据加密措施，网络攻击者能及时掌握车辆基本安全信息，包含车辆坐标、速度、加速度、航向角等。这些数据在分析后，能了解车主出行习惯、居住地址以及工作地等。

1.2 身份伪造与重放攻击

如果网络系统中未能落实强身份认证机制，恶意节点可伪装成合法车辆或路侧设备接入系统。例如，攻击者模拟多辆虚拟车辆，制造虚假拥堵，进而对交通信号产生一定干扰影响。重放攻击是攻击者录制合法通信报文，在规定时间或地点重新发送，从而欺骗系统，造成某路段存在异常，进而对正常交通秩序产生破坏。

1.3 隐私追踪与关联分析

虽然智慧交通系统内进行部分交通数据字段的加密，但如果车辆使用固定标识符，则网络攻击者通过长期监测标识符位置、时间等，建设精确的运动轨迹模型。这种去匿名化攻击侵害交通参与者的隐私，还会造成人身安全问题[2]。

2 数据加密与隐私保护总体架构设计

2.1 基于国密算法的混合加密机制

智慧公路车路协同系统在建设时，为保证数据信息

达到安全性要求，基于国密算法的混合加密机制极为重要。该机制符合国家法律法规要求，其利用中国国家密码管理局发布的 SM 系列算法，进而在智慧公路系统内构建多层次数据防护体系。在数据传输中，针对基本安全消息等高频率、低时延业务，其利用运算高效的 SM4 对称加密算法，以确保数据安全性。这一算法具备 128 位密钥长度，能够适配车载 OBU 与路侧 RSU 等资源受限环境。同时，该系统构建会话密钥动态协商机制，每次会话都能保证数据安全性，防止网络攻击者存在批量破解的风险。

2.2 基于区块链的去中心化身份管理

以往 PKI 体系主要依赖中心化证书颁发机构，其容易造成单点故障风险以及证书撤销列表更新滞后，进而引发数据的丢失或篡改。在本次的改造方案中，其利用联盟链技术，将交通管理部门、通信运营商构建形成数据体系，确保各方积极参与到数据信息安全管理中。在该体系引领下，通过分布式账本机制，使车辆公钥证书及状态实时上链存储，再利用区块链不可篡改的特性，从根本上保证证书的真实性与可信度。同时，该系统中部署智能合约实现自动化响应。若系统监测发现车辆私钥泄露或车辆报废等异常情况，则立即将相关信息传输到后台控制中心，从而使其数据传输的延迟从分钟级压缩到秒级[3]。

2.3 基于差分隐私的轨迹数据保护

智慧公路车路协同系统在运行时，其利用云控平台实现数据分析和共享，并利用差分隐私技术，避免发生个体轨迹被还原的情况。根据智慧公路体系建设要求，其在车端或路侧单元节点，需向原始位置数据中添加符合拉普拉斯分布或高斯分布的噪声，然后再将车路协同数据传输到控制系统。隐私预算分配：合理设置隐私预算参数∈，在保护隐私∈越小保护越强）和数据可用性（∈越大精度越高）之间寻找最佳平衡点。

3 关键技术实现与性能评估

3.1 混合加密通信流程

车路协同系统数据加密中，其利用数字信封技术，实现加密效率的提升。在该系统运行中，数据发送形成随机的 SM4 会话密钥加密业务数据，然后利用接收方的 SM2 公钥解密，该会话密钥实现两者打包发送。数据接收方使用 SM2 私钥解密会话密钥，然后利用 SM4 解密密文。该过程实现加密效果提升，能有效解决对称密钥安全分发问题。

3.2 仿真测试环境搭建

为验证该方案是否具备可行性，本次研究中搭载包含 50 个 RSU 节点和 2000 辆 OBU 节点的仿真测试窗，主要模拟公路交通的真实通行环境。而该次试验阶段，需模拟多种外在威胁，如数据篡改、窃听、重放、Sybil 攻击等，以验证数据模型是否具备安全性，见表 1。

从表 1 结果进行分析，在国密算法方案应用后，公路交通数据时延以及吞吐量均优于 RSA 方案，并保证车路协同系统时延在 100ms 以内。同时，引入区块链技术后，其具备数据不可篡改性，并且缩短数据证书撤销延迟，从而提高系统响应效率，见表 2。

通过对表 2 数据进行分析，传统的 K- 匿名法在面对拥有辅助信息攻击者时，隐私效果明显下降。而差分隐私技术在∈ =0.5 时，则可以将轨迹重识别成功率设定为 5% 以内，还会把交通流统计误差设定为 2% 以内，确保数据隐私保护达到目标。

表1 不同安全方案下的系统性能对比

性能指标	传统RSA-2048+AES方案	国密SM2+SM4方案	无加密明文传输	本方案(SM2+SM4+区块链)
端到端平均时延(ms)	52.4	41.8	12.5	46.3
签名验证耗时(ms)	18.5	12.2	0	14.8
吞吐量(Mbps)	78.5	89.2	100.0	85.6
CPU占用率(%)	32.5	24.1	5.2	27.8
抗量子计算能力	弱	较强	无	强
证书撤销延迟(s)	>60	>60	N/A	<2

表2 不同隐私保护策略下的轨迹重识别风险与数据效用

保护策略	隐私预算(ϵ)	轨迹重识别成功率(%)	平均位置误差(m)	交通流统计误差率(%)	抗背景知识攻击能力
无保护	–	98.7	0.5	0.0	无
K-匿名(k=10)	–	42.5	15.8	8.5	弱
差分隐私	0.1	2.1	45.2	6.2	强
差分隐私	0.5	4.8	18.5	2.5	强
差分隐私	1.0	12.3	8.2	1.1	中

4 实施挑战与应对策略

4.1 密钥全生命周期管理

智慧公路系统建设下，车路协同系统运行时，其在车联网环境下，密钥生成、分发、更新、销毁具备复杂性，需构建完善的密钥全生命周期管理体系。在该体系内，根密钥采取离线冷存储方式，二级密钥利用专用安全信道下发到各节点，会话密钥进行动态协商机制建设。

4.2 异构设备兼容与性能优化

对于路侧设备算力差异明显的问题，通过国密算法进行软硬件协同优化。该环节中针对资源受限的低算力设备，其利用查表法预计算和汇编指令级加速技术，从而缩短运算时间。而高算力云控中心则布置硬件安全模块，能满足数据加密运算需求。

4.3 合规性与标准化

严格遵循《汽车数据安全管理若干规定（试行）》及 GB/T 37374 等国家强制标准，将智慧公路车路协同系统数据进行分类管理，构建完善管理机制，并对原始数据进行清洗和匿名化处理，从而避免非敏感性数据丢失。

5 结语

智慧公路车路协同系统数据加密与隐私保护尤为重要，这是保证我国道路交通事业高速发展的关键。在该体系运行下，通过仿真模拟验证方案效果，并发挥国密算法、区块链身份认证、差分隐私技术的优势，以确保智慧公路数据具备安全性。

参考文献：

[1] 范晨歌，黄辉，马岁等. 高速公路通信系统中量子加密技术应用研究[J]. 公路交通科技 (应用技术版)，2020, 16(11): 307-310.

[2] 李天俊，任荣，张钰尧. 基于矩阵张量积的高速公路智慧屏显信息加密方法[J]. 中国交通信息化，2024(S2): 139-141.

[3] 陈旺松，高明应，丁晓冬. 高速公路情报板加密技术探究[J]. 中国交通信息化，2024(08): 94-98.