智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

跨链技术支持下的车联网可信认证系统

李子欣, 施水玲, 刘文奇

引用本文:
李子欣, 施水玲, 刘文奇. 跨链技术支持下的车联网可信认证系统[J]. 智能系统学报, 2025, 20(5): 1188-1197.
LI Zixin, SHI Shuiling, LIU Wenqi. A trusted authentication system for telematics with cross-chain technical support[J]. *CAAI Transactions on Intelligent Systems*, 2025, 20(5): 1188-1197.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202411010

DOI: 10.11992/tis.202411010
网络出版地址: https://link.cnki.net/urlid/23.1538.tp.20250825.1716.002

跨链技术支持下的车联网可信认证系统

李子欣[1,2], 施水玲[1,2], 刘文奇[1,2]
(1. 昆明理工大学 理学院, 云南 昆明 650500; 2. 昆明理工大学 数据科学研究中心, 云南 昆明 650500)

摘　要: 在智能交通系统快速发展的背景下, 车联网已成为实现智能化交通管理的关键技术。然而, 确保车辆间通信的安全性和隐私保护仍是重要挑战。为此, 提出了一种基于跨链技术的车联网可信认证系统。系统集成多种密码学和盲签名技术, 设计了基于侧链技术的双链车联网架构, 优化车辆与路侧单元间的身份认证和数据交换过程。侧链采用拜占庭共识协议, 主链存证与哈希锁定, 协同保障跨区域数据一致性与安全性。此外, 系统利用智能合约模拟双链结构并实现系统参数的自动更新。基于 Fabric 的仿真实验表明, 该系统相比于传统单链的公钥基础设施 (public key infrastructure, PKI) 方案, 将每笔交易计算开销降低了 12% ~ 33%, 显著提高认证效率, 有效解决了传统车联网中心化认证的不足, 同时验证了系统的实用性和可扩展性。

关键词: 区块链; 车联网; 跨链; 认证协议; 密码学; 盲签名; 数据共享; 隐私
中图分类号: TP393; TN92　　**文献标志码**: A　　**文章编号**: 1673−4785(2025)05−1188−10

中文引用格式: 李子欣, 施水玲, 刘文奇. 跨链技术支持下的车联网可信认证系统 [J]. 智能系统学报, 2025, 20(5): 1188–1197.
英文引用格式: LI Zixin, SHI Shuiling, LIU Wenqi. A trusted authentication system for telematics with cross-chain technical support[J]. CAAI transactions on intelligent systems, 2025, 20(5): 1188–1197.

A trusted authentication system for telematics with cross-chain technical support

LI Zixin[1,2], SHI Shuiling[1,2], LIU Wenqi[1,2]
(1. Data Science Research Center, Kunming University of Science and Technology, Kunming 650500, China; 2. Faculty of Science, Kunming University of Science and Technology, Kunming 650500, China)

Abstract: As intelligent transportation systems rapidly evolve, telematics plays a vital role in enabling efficient traffic management. However, maintaining security and privacy in inter-vehicle communication remains a challenge. To address this issue, we propose a trusted authentication system built on cross-chain technology. The system introduces a dual-chain vehicular networking architecture using side-chain technology, cryptographic methods, and blind signature schemes to enhance authentication and facilitate secure data exchange between vehicles and roadside units. The side chain adopts a Byzantine consensus protocol, while the main chain employs deposit-based validation and hash locks to maintain data consistency and ensure cross-regional security. Smart contracts are used to emulate the dual-chain structure and support the dynamic updating of system parameters. Fabric-based simulation experiments demonstrate a 12%–33% reduction in computational overhead per transaction compared with traditional single-chain PKI-based schemes. The results confirm significant improvements in authentication efficiency, address the limitations of centralized authentication in vehicular networks, and validate the system's scalability and practical applicability.

Keywords: blockchain; telematics; cross-chain; authentication protocols; cryptography; blind signatures; data sharing; privacy

智能交通系统 (intelligent transportation systems, ITS)[1] 与人类社会的关系是多方面的, 包括社会形态、交通系统设计和社会行为, 这些因素相互依存, 相互影响[2]。车联网 (internet of vehicles, IoV)[3] 作为智慧交通的核心领域, 是一个包含人、车和路侧设施等多个元素的复杂网络。车联网系统具有多种通信方式, 包括车辆与车辆 (vehicle-to-vehicle, V2V)、车辆与基础设施[4](vehicle-to-infrastructure, V2I) 和车与路侧单元 (vehicle-to-

收稿日期: 2024−11−11.　**网络出版日期**: 2025−08−26.
基金项目: 国家自然科学基金项目 (12371460).
通信作者: 施水玲. E-mail: shishuiling0409@sina.com.

roadside unit, V2RSU) 等。这些通信方式使得车辆能够获取交通指挥、出行向导和交通环境等信息和服务, 提升智能交通系统运行的安全性和可靠性。

随着车联网技术的快速发展, 安全和隐私成为了先进交通管理系统设计中最关键的挑战之一。特别是在智能交通系统中, 车辆之间以及车辆与路侧单元之间的通信必须得到充分的保护以抵御各种恶意攻击和隐私泄露风险。为了确保通信的可靠性和安全性, 有效的可信认证机制成为了必不可少的要求。基于密码学的公钥基础设施 (public key infrastructure, PKI)[5] 是一种目前广泛使用的身份认证技术, 该技术通过为参与的车辆和设备提供数字证书来验证其身份。但传统的采用 PKI 认证的车联网数据交换系统依赖于中心化的管理, 不仅增加了系统的复杂性, 还可能成为安全漏洞的来源。区块链技术具有去中心化、不可篡改性和透明性等特点[6], 这些特点使得证书数据能在区块链上的所有节点之间进行可信共享。基于此方向, 张勖等[7] 提出了一种利用区块链技术的去中心化公钥基础设施认证系统, 旨在提供密钥查询与身份绑定服务, 然而由于用户的公钥和身份信息直接记录在区块链上, 存在隐私泄露的风险。Jiang 等[8] 提出了一个基于区块链的公钥基础设施中的隐私保护轻客户端认证方案, 用于协助终端设备进行身份认证, 但未考虑区块链负荷问题。Ma 等[9] 提出了基于公钥基础设施认证的原理设计, 用以提升事件验证的可靠性与安全性, 但此方案可能不足以支持高效的密钥更新和撤销。

跨链技术为解决以上问题提供了新的可能性, 通过在不同的区块链网络之间进行车辆间和车辆与基础设施之间的通信和交互, 解决城市车联网中的数据孤岛问题, 从而促进更加安全、可靠和高效的车载网络通信和数据传输[10], 大大减轻了单个节点或网络的压力。在此方向上, Steger 等[11] 通过跨链技术实现了一种安全的无线汽车软件更新机制, 提供了一个概念验证。Dubois 等[12] 和齐林海等[13] 通过跨链技术加强车联网资源共享和数据交换, 优化能源管理并提升系统的可持续性。Singh 等[14] 提出了一种利用智能合约和跨链技术在车联网中实现动态信任评估和数据共享的系统, 从而增强网络安全性和可信度。Tan 等[15] 提出了一种基于原子跨链交换的管理系统, 利用哈希时间锁定确保车载自组网中的数据和资源交换的安全协同管理效率。He 等[16] 通过跨链技术实现各个区块链网络间的信誉数据互联互通。Kang 等[17] 引入中继链技术开发了一种高效通信的联邦学习框架, 优化不同区块链网络间的通信和数据处理, 为车辆提供安全的跨链交互。Lu 等[18] 提出了一种基于 Oracle 的联盟区块链跨链互操作方法, 将预言机作为信任中介来实现不同区块链网络之间的数据资产交换。因此, 将跨链技术引入车联网的 PKI 认证系统具有优化认证流程的广泛可操作性。在跨链交互中, 交易数据需要在不同的链上进行广播, 以保持链间的数据一致性。这种操作的透明性虽然增加了系统的可信度, 但同时也可能导致敏感信息被泄露等问题, 因此需要进一步引入加密技术对数据进行隐私保护。

基于以上问题, 本文创新性地提出一个基于跨链技术的车联网可信认证系统。该系统不仅通过分层架构优化了车辆与路侧单元间的身份认证和数据交换过程; 且通过多方认证减少了网络中对证书颁发机构 (certificate authority, CA) 的通信拥堵, 以确保车辆节点迅速获得认证与授权, 实现跨域认证。主要工作如下:

1) 本文设计了一个基于侧链技术的双链结构的车联网系统, 该系统通过侧链处理本地车辆身份认证, 主链进行哈希锁定和存证, 使用拜占庭容错 (practical Byzantine fault tolerance, PBFT) 算法保证跨区域数据一致性。

2) 所提系统集成多种密码学技术, 包括使用双线性映射、SM2 椭圆曲线公钥密码算法和盲签名, 以增强交易数据的安全性和隐私保护。系统利用盲签名和哈希时间锁定技术避免中间人攻击和重放攻击的风险, 确保数据的不可篡改。同时支持身份的匿名化处理, 保护用户隐私。

3) 本文通过 Fabric 仿真实验对相关指标进行性能测试, 通过智能合约自动更新系统密钥和参数。仿真结果表明, 所提系统能够有效降低计算开销并提高了认证效率。

1　预备知识

1.1　区块链

区块链是金融行业的颠覆性技术之一[19], 由中本聪 (Satoshi Nakamoto) 于 2008 年首次提出作为比特币的底层技术[20]。目前, 区块链已成为工业物联网或工业 4.0 的驱动力之一, 它吸引了工业界、学术界和研究机构的广泛关注。其高安全性 (默克尔树、哈希函数)、去中心化、共识、一致性和可靠性等显著特点使其成为在车联网中建立和管理信任模型的潜在候选者之一[21]。区块链改变了传统的中心化支付交易方式, 不需要可信第

三方机构系统的介入，通过分布式存储、数据信息加密和共识机制，使得分布式账本允许互不信任的双方进行交易。根据不同的访问权限和管理方式，区块链分为公有链、私有链和联盟链 3 种类型[22]。联盟链中仅有获取许可的用户能够加入或退出网络，CA 中心一般负责为用户提供使用授权，无论是联盟链还是公有链，交易数据都需要按照链式结构存储[23]。近几年，区块链研究从原有的账本应用拓展到隐私保护[24-25]、数据存证[26]等领域的研究。

区块链由相互链接并通过加密保护的区块组成，在区块之间建立了牢固的连接，如图 1 所示，并提供了隐式的强时间戳机制保证了区块的顺序。因此，在不更改其所有后续区块的情况下，任何区块都无法被修改。这种区块链数据结构可以共享，从而构建一个称为共享账本的分布式数据结构。区块链凭借其卓越的互操作特性，使得车联网中的数据得以有效记录于区块链平台[27]。

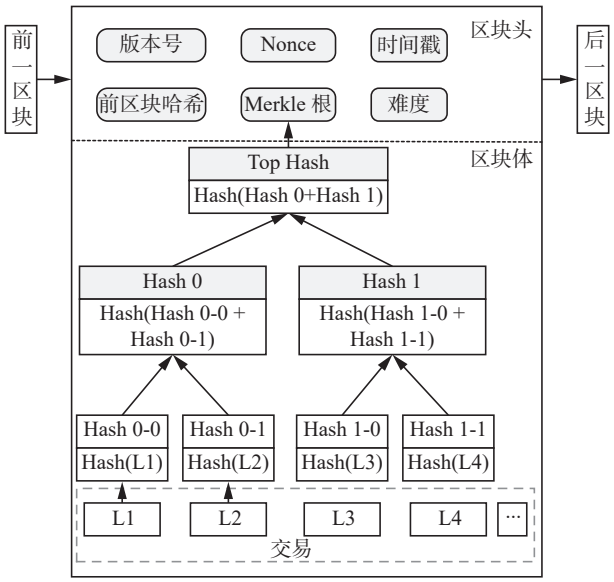

图 1　区块链结构

Fig. 1　Blockchain structure

1.2　加密算法

加密算法是支持消息发送方的公钥对明文消息加密以防止消息在传输过程中泄露的密码学技术，其中公钥可以对任何人公开，但用于解密的私钥只能由消息接收方持有。且加密算法可以保护敏感消息的隐私安全，有效地规避交互过程中的明文消息可能受到的盗取、伪造和篡改攻击。首先，发送方利用公钥对明文数据进行加密操作从而生成无法直接表达明确信息的密文数据。然后，将密文消息通过传输通道发送给消息接收方，接收方使用私人持有的私钥对密文数据进行解密[28]操作来获取明文消息。

加密算法用一个四元组来表示：{PtxData, KeyGen, Enc, Dec}，其中 PtxData 表示元数据，KeyGen 是加密密钥生成算法，Enc 是加密算法，Dec 是解密算法，具体描述为：

1) KeyGen(λ,s) 算法。输入安全参数 λ 和随机数 s，得到公钥 p_k 和私钥 s_k，其中公钥用于加密操作，私钥用于解密操作。

2) Enc(d_p,p_k) 算法。输入明文数据 d_p 和公钥 p_k，其中 $d_p \in$ PtxData，输出密文 cpd。

3) Dec(cpd, s_k) 算法。输入密文数据 cpd、私钥 s_k，输出明文数据 d_p，若输出非法字符“Γ”，表示 cpd 为错误密文。

1.3　盲签名

盲签名是一种独特的数字签名技术，允许接收者在隐藏消息具体内容的前提下完成签名操作，确保签名者无法获知签署的具体信息[29]。

盲签名的实现步骤为：

1) 用户把明文消息 M 通过盲因子变换为 M'，即得到盲化后的消息；

2) 把 M'给签名者，使用密钥生成中心 (key generation center, KGC) 分配的签名私钥对其进行签名；

3) 得到盲签名结果 Sig(M') 后，用户取回 Sig(M')，通过去盲变换，最终得到的 Sig(M) 就是原始消息的签名[30]。

盲签名的数字签名方无法获得待签消息的具体内容，这就使得盲签名具有一般数字签名不具备的 2 个特点[31]：

1) 盲性。签名者无法知晓消息的具体内容，消息内容对其保持隐藏。

2) 不可链接性。即使签名被接收方泄露，签名者也无法对签名进行追踪或关联。

2　系统架构与实体功能

本文构建了一个基于中继链和哈希锁定的两阶段跨链机制，CA 层主链存证，路侧单元 (road-side unit, RSU) 层侧链认证。该分层架构通过双向挂钩机制使车辆数据和交易在主链与侧链之间自由流动，进行身份认证后将盲签名共识于侧链层，哈希值上传锁定至主链层，以在城市车联网环境中安全传递车辆数据。RSU 在生成盲签名或其他认证信息后，会对这些信息进行哈希处理，RSU 将生成的哈希值通过轻节点上传至主链层，连同一个时间戳 (表示证书的有效期限) 一起发布至区块链上，意味着该哈希值被永久记录在主链的区块链中，确保其不可篡改性。

在侧链中, 节点利用简化支付验证 (simplified payment verification, SPV) 模式确认主链的锁定交易, 并释放相应资产。RSU 侧链之间使用哈希时间锁定来安全地进行数据交换, 传送方创建哈希时间锁并通过其智能合约调用 check 函数自动验证接收方提供的信息是否与最初设定的哈希值相匹配, 来确认数据的真实性和完整性, 并确认当前时间是否在设置的时间窗口内$|T_{SV}-T|<\Delta T$, 防止重放攻击的安全威胁。一旦哈希锁被正确解开, 数据交换即为成功。双方的侧链都会记录这次交易的细节, 确保所有操作的透明性和可追溯性。

图 2 为该方案的车联网系统架构, 包括主链层、侧链层和终端层。

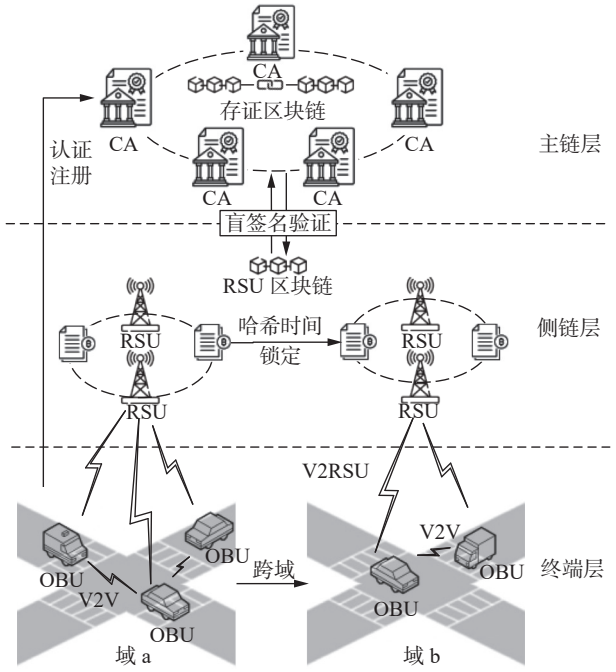

图 2　车联网跨域可信认证系统架构

Fig. 2　Cross-domain trusted authentication system architecture for telematics

主链层-CA 层　由多个 CA 中心共同构成的网络层。CA 中心通过主链层生成并管理车辆和 RSU 的证书。每个证书生成后, 会被写入主链中, 并通过 PBFT 共识算法共识于主链。主链层由多个全节点构成, 这些节点分布在不同的 CA 中心。每个节点都能够完全复制和验证区块链的内容, 确保链上数据的完整性和一致性。不同区域的 CA 中心通过加入主链层形成一个信任联盟, 当车辆在不同区域移动时, 主链层确保车辆的身份认证在各区域内都被信任。

侧链层-RSU 层　RSU 组成的分布式网络。每个 RSU 既可以作为主链的轻节点参与全网共识, 又可以作为侧链的全节点处理域内车辆的身份认证。作为全节点的 RSU 在侧链层内管理和验证车辆的身份认证请求, 包括生成、存储和共识本地的认证信息, 如身份凭证或盲签名。侧链层的全节点通过 PBFT 快速共识算法达成本地共识, 以实现高效的验证。

终端层-OBU 层　由安装在车辆内部的车载单元 (on board unit, OBU) 设备构成。OBU 通过 RSU 与 CA 中心和其他车辆进行交互, 实现车与车、车与路侧单元、车与 CA 中心的可靠通信。OBU 层的设备通常具有较小的存储和计算能力, 但足以处理本地的身份验证和通信任务, 车辆密钥安全存储在 OBU 的防篡改设备 (tamper-proof device, TPD)[32] 中。

3　认证方案实现流程

该方案的流程包括 5 个主要步骤: 系统初始化、实体注册、通信验证、消息盲签名和哈希时间锁定。在本章中, 各符号及其对应的含义如表 1 所示。

表 1　符号及其含义

Table 1　Symbols and their meanings

符号	含义
G	q阶乘法循环群, 双线性对e的值域
G_T	q阶循环子群, 加法循环群
g, g_T	G, G_T的生成元
e	双线性映射
$H(\cdot)$	哈希加密函数
Z_q^*	模q的整数群
s	系统主密钥
P_{sub}	系统公钥
T_S	时间戳
Cert_{CA}	CA自签证书
RID_V	车辆真实身份
VID_V	车辆假名
RID_R	RSU真实身份
s_{kV}	车辆私钥
p_{kV}	车辆公钥
s_{kR}	RSU私钥
p_{kR}	RSU公钥
M,M'	车辆请求消息,盲化消息
r	盲因子
σ,σ'	原始签名, 盲签名
$\mathrm{Sign}(\cdot)$	签名算法

3.1　系统初始化

CA 根据安全参数 1^k 生成参数 $(q, G, G_T, g, g_T, e, H(\cdot))$, G 和 G_T 是素数 q 阶双线性群, g 是 G 的生成元, g_T 是 G_T 的生成元, e 是双线性映射 $e: G\times G\to G_T$ 并且满足 $g_T=e(g,g)$。映射 e 有以下特性:

1) 双线性。$\forall P \in G_1$, $\forall Q \in G_2, a, b \in Z_q$, 有 $e([a]P,[b]Q) = e(P,Q)^{ab}$。

2) 非退化性。$\exists P \in G_1$, $\exists Q \in G_2$, 有 $e(P,Q) \neq 1_{Gr}$其中 1_{Gr} 是 G_T 的单位元。

3) 可计算性。$\forall P \in G_1$, $\forall Q \in G_2$, 可有效计算 $e(P,Q)$。

其中, $H(\cdot)$ 是单项哈希函数 $H:\{0,1\}^* \to G$, CA 随机数选择系统主密钥 $s \in Z_q^*$, 计算系统公钥 $p_{\text{sub}} = s \cdot g$。CA 保存系统主密钥 $m_{\text{sk}} = s$, 随后将公共参数、m_{sk} 和 P_{sub} 传播给其他车辆并广播至区块链网络, 将区块链交易池初始化为空, 系统参数由各可信域的 CA 共同维护。CA 中心根据系统公钥 P_{sub}、域 ID 和时间戳 T_{S} 生成自身的自签证书 Cert_{CA} 存于 OBU 存储设备, 并计算证书的哈希值 $H_{\text{CA}} = H(\text{Cert}_{\text{CA}})$锁定至主链, 并定期由 CA 区块链上的智能合约更新系统主密钥和系统公钥。车联网跨域可信认证流程如图 3 所示。

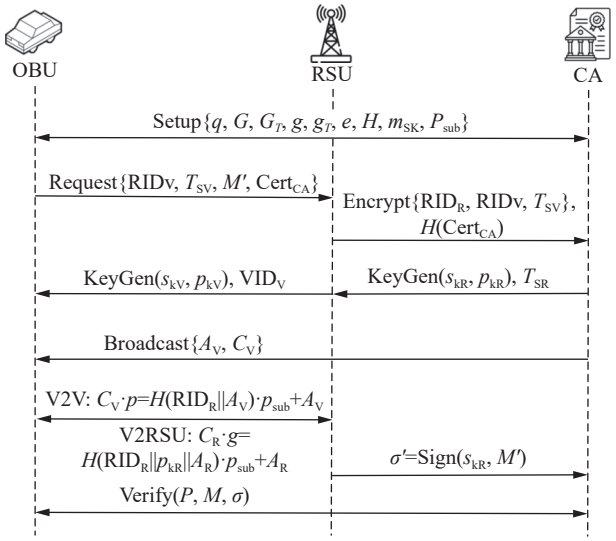

图 3　车联网跨域可信认证流程

Fig. 3　Telematics cross-domain trusted authentication process

3.2　实体注册

所有参与车联网的 RSU 及车辆都需要向 CA 进行身份注册, 车辆绑定其身份信息 (例如车辆 VIN 或驾驶执照) 来保证身份的合法性。车辆向 CA 发送注册请求 $\{\text{RID}_{\text{V}}, T_{\text{SV}}\}$, 其中 RID_{V} 为车辆的真实身份, T_{SV} 为车辆申请时的时间戳, 对于真实身份为 RID_{V} 的车辆用户, CA 接收到车辆 V_i 的身份信息后通过查询存储的身份数据库对车辆 V_i 的真实身份 $\text{RID}_{\text{V}i}$ 进行验证[33], 在确保其身份已经注册并合法后计算:

$$C = \text{RID}_{\text{V}} \oplus H(p_{\text{sub}} \,\|\, s) \tag{1}$$

式 (1) 为车辆边缘节点的唯一标识符, $\oplus$代表异或运算, $\|$表示连接操作。为保护其身份隐私, CA 为其生成匿名身份:

$$\text{VID}_{\text{V}} = C \oplus H(s \cdot p_{\text{sub}})$$

该假名与车辆的真实 ID 具有唯一的映射关系, 并存储在 CA 的数据库中。CA秘密保存注册信息表registry = $\{\text{RID}_{\text{V}}, \text{VID}_{\text{V}}, T_{\text{SV}}\}$, CA 验证身份信息中的假名是否在假名列表中, 若假名不存在, 则拒绝该私钥的生成请求; 若假名存在, 则继续以下步骤。

通过利用基于椭圆曲线密码学 (elliptic curve cryptography, ECC) 的 SM2 加密算法, CA 产生一个椭圆曲线:

$$\text{Ep}(a,b): y^2 = x^3 + ax + b (\text{mod } p) \tag{2}$$

式 (2) 必须满足 $4a^3 + 27b^2 \neq 0$, p表示一个质数, 用于定义椭圆曲线加密中的有限域, 表示该运算的模数。选取一个基点 $E(x_E, y_E)$, 产生随机数生成车辆私钥 s_{kV}, 生成公钥 $p_{\text{kV}} = s_{\text{kV}} \cdot E$, 表示为 $(x_s^{\text{kV}}, y_p^{\text{kV}})$ 即该椭圆曲线上的点。

同样, RSU 生成系统参数 RID_{R} 并交由 CA 验证身份的合法性与唯一性[34], CA 利用 SM2 算法随机生成公私钥对 $(s_{\text{kR}}, p_{\text{kR}})$, 随后将 RSU 注册完成的时间戳 T_{SR} 及 p_{kR} 向全网广播。CA 确定 RSU 合法性后选择随机整数 a_{R} 并计算函数:

$$A_{\text{R}} = a_{\text{R}} \cdot g$$

$$C_{\text{R}} = H(\text{RID}_{\text{R}} \,\|\, p_{\text{kR}} \,\|\, A_{\text{R}}) \cdot s + a_{\text{R}}$$

将计算结果应用于后续认证。当移动车辆进入某个 RSU 的通讯覆盖区域内时, 便会收到来自该 RSU 的广播消息。此时, 车辆会将其信息发送至认证中心 CA, 在接收到车辆真实身份 RID_{V} 后 CA 选择随机整数 a_{V} 以计算函数:

$$A_{\text{V}} = a_{\text{V}} \cdot g$$

$$C_{\text{V}} = H(\text{RID}_{\text{V}} \,\|\, A_{\text{V}}) \cdot s + a_{\text{V}}$$

CA 存储并发送 $\{A_{\text{V}}, C_{\text{V}}\}$给车辆。

3.3　通信验证

车辆在通信验证阶段将相关信息发送至 RSU, RSU 在接收到信息后进行消息对比并发送到 CA, 分别对 RSU 或车辆节点计算函数:

$$C_{\text{R}} \cdot g = H(\text{RID}_{\text{R}} \,\|\, p_{\text{kR}} \,\|\, A_{\text{R}}) \cdot p_{\text{sub}} + A_{\text{R}} \tag{3}$$

$$C_{\text{V}} \cdot g = H(\text{RID}_{\text{V}} \,\|\, A_{\text{V}}) \cdot p_{\text{sub}} + A_{\text{V}} \tag{4}$$

根据式 (3)、(4) 是否成立进行 V2RSU 与 V2V 的验证, 在吻合后完成对车辆节点的数字签名认证流程。

3.4　车辆消息盲签名

车辆 (请求方) 需要向 CA 进行盲签名以获得数字证书。当车辆需要向 RSU 验证身份或提交某项请求时, 车辆首先将该请求消息进行盲化。车辆选择盲因子 r 对消息 M 进行盲化处理, 生成盲

化消息 $M'=M+r\cdot E$, 盲化后的消息被发送给 RSU。

由于消息已经被盲化, RSU 无法知晓其原始内容, 随后 RSU 使用其私钥 s_{kR} 对 M'进行签名 $\sigma'=\mathrm{Sign}\left(s_{kR},M'\right)$, 签名生成过程使用 SM2 的标准签名算法, 具体步骤包括生成随机数 k 并计算签名点 $R=k\cdot G$。

CA 将签名后的数字证书颁发给相应实体 (如接收该消息的车辆或基础设施, 这里以车辆为例), 车辆使用盲因子 r 以及签名方的公钥 P 将盲签名 σ' 去盲化, 进行逆运算得到原始消息 M 的签名 σ。车辆对消息 M 和签名 σ 分别计算其哈希值 $H(M)$ 和 $H(\sigma)$, 并将两者上传到主链, 同时设置哈希时间锁 (hashed timelock contract, HTLC)。主链的智能合约验证哈希值 $H(\sigma)$ 的合法性, 确保签名未被篡改, 并将 $H(M)$ 广播到相关的侧链, RSU 接收到来自主链的哈希值 $H(M)$ 后, 通过智能合约查询本地存储的签名哈希值 $H(\sigma)$, 验证其与主链中存储的值是否匹配。如果验证通过, 说明消息 M 和签名均合法, 侧链释放与消息相关的数据或权限, 确保主侧链之间的数据一致性。

若车辆进入新的 RSU 区域管辖范围且时间戳没有过期的情况下, 车辆无需重新进行新的认证流程生成签名, 只需将之前的 $H(M)$ 和数字签名提交到新 RSU 的侧链。新的 RSU 使用主链广播的 $H(M)$ 和侧链的签名验证逻辑, 相应实体使用 RSU 或 CA 中心公钥 P 验证签名 σ 是否有效:

$$\mathrm{Verify}\left(P,M,\sigma\right)$$

如果验证成功, 则说明消息 M 的签名合法且未被篡改。通过这种方式, 减少了重复认证的开销, 优化了跨域认证的效率, 从而减少车联网中通讯资源的浪费。

算法 1　SM2 盲签名算法

输入　消息 M

输出　是否有效 isValid

1) 初始化椭圆曲线

2) 生成密钥对公钥 p_k 和私钥 s_k

3) 根据椭圆曲线随机生成盲因子 r

4) 使用盲因子 r 盲化消息 M 生成 M'

5) 生成随机数 k

6) 计算签名点 R

7) 使用公钥 p_k 和盲消息 M'生成盲签名 σ'

8) 拆分盲签名将 r_{Sig} 作为 σ'的第一个分量, s_{Sig} 作为 σ'的第二个分量

9) 计算盲因子逆点 invertedRP

10) 生成最终签名 σ (r_{Sig} • invertedRP, s_{Sig} • invertedRP)

11) IF 使用公钥 p_k 验证最终签名 σ 是原始消息 M 的有效签名 THEN

12) PRINT(“签名有效:”, True)

13) ELSE

14) PRINT(“签名有效:”, False)

15) END IF

4　安全性分析

匿名性　CA 生成每辆车的匿名身份, 并确保了车辆的匿名身份与其真实身份之间存在唯一的映射关系, 但无法直接从匿名身份推导出真实身份; 车辆在请求盲签名时, 由于消息在盲化后被加上了随机盲因子, RSU 在签名过程中无法识别消息的原始内容, 从而保护了消息的隐私; CA 的公钥和私钥用于生成和管理系统中的密钥, 而这些密钥对车辆的匿名性提供了支持。

安全性　该方案通过 CA 主链的管理, 实现系统初始化和实体注册, 从中避免了中间人攻击, 并采用数字签名来防止消息内容被篡改, 确保只有具备合法假名和完整私钥的车辆才能生成有效签名, 从而有效抵御模仿攻击。为保证消息的时效性, 系统引入签名时间戳机制, 以抵抗重放攻击并防止了单点故障问题。

轻负载性　侧链技术可以很好地分担主链的存储和认证压力, 扩展主链的性能, 本方法将车辆的盲签名分散存储于侧链, 其哈希值同步至主链层, 从而减缓主链的存储和验证压力, 解决主链在认证过程中的拥堵和时延问题。交易信息可以通过不同的双向挂钩机制在侧链和主链之间转移。当主链承受高负载时, 侧链能暂存数字资产或交易, 减轻主链负担并提升其处理能力。

可追溯性　CA 可以通过区块链追踪和验证相关设备的信息, 使每个车辆和路侧单元的身份信息及其交互数据都被记录在区块链上, 实现数据的一致性。智能合约用于自动执行交易验证和数据同步, 链式结构使得任何交易或数据变动都有确切的执行逻辑和时间戳, 每一条消息都可以被追踪和验证, 增加了系统的透明度和可追溯性。本文方案与其他方案安全性对比见表 2。

表 2　方案安全性对比

Table 2　Comparison of programme security

方案	匿名性	可追溯性	轻负载性	抵抗常见攻击	跨域批量认证	支持跨链
关振宇等[35]	√	√	×	√	×	×
Chen等[36]	×	√	√	√	√	×
刘雪娇等[33]	√	√	√	√	√	×
本文方案	√	√	√	√	√	√

5　实验与评估

本实验在一台操作系统为 Windows 10 的笔记本电脑上进行，为搭建实验环境，使用 VMware Workstation 17 版本运行虚拟机。区块链平台采用 Hyperledger Fabric，部署在 Linux 操作系统中搭建联盟链模型，使用 Docker 24.0.7 进行容器化管理，基于 Golang 编写智能合约。为支持相关依赖，安装了版本为 12.22.9 的 Node.js。实验模拟了主侧链认证的同步过程，在主链部署若干个 CA 节点，使用简化拜占庭容错共识算法将车辆的盲签名同步至 Fabric。每个 CA 认证节点连接一条侧链，每条侧链中部署 4 个 RSU 节点，RSU 节点调用智能合约验证车辆发送证书的合法性，以此实现认证。

5.1　可行性分析

为对该实验可行性进行分析，表 3 给出测试某侧链的全部 RSU 节点在 1 h 内的运行情况，结果表明共识节点均保持合理的更新状态。

表 3　节点可行性测试

Table 3　Node feasibility testing

节点	在线状态/min	是否更新
r_1	49	是
r_2	52	是
r_3	54	是
r_4	59	是

该实验使用外部服务调用 Miracl 密码库与链码通信，忽略开销极小的运算，计算出认证过程中所涉及的相关密码操作的执行开销，如表 4 所示。系统通过轻节点架构和高效的密码算法，能够在低计算能力环境下正常运行，特别是对于 OBU 设备，既能满足实时认证需求，又能保持较低的功耗和资源消耗。

表 4　方案基础密码执行开销

Table 4　Program base password execution overhead

符号	含义	执行时间/ms
T_{bp}	双线性配对	4.248 5
T_h	哈希运算	0.000 7
T_{pm}	G上的标量乘运算	0.364 1
$\oplus$	异或运算	0.000 1
T_{add}^{ecc}	椭圆曲线的点加运算	0.019 3
T_{mul}^{ecc}	椭圆曲线的点乘运算	0.293 4

5.2　性能分析

仿真实验主要对系统吞吐量和相关时延进行相关指标测试。该实验模拟车辆终端向系统发送 1 500 笔交易，通过改变交易发送速率观察性能的变化。在该系统中，吞吐量与跨链系统的处理能力直接相关，通过利用 Caliper 性能测试工具来测试车辆不同交易发送速率的吞吐量，交易速率系统吞吐量使用每秒处理事务数量 (transactions per second, TPS)，并在单链模式下进行测试作为比较。实验结果如图 4 所示，随着交易发送速率的增长，系统吞吐量呈上升趋势并逐渐趋于平稳，并且基于跨链模式的性能超过了单链模式，表现出显著优势。且图 4 表明，当交易速率达到 1 000 TPS 时，系统吞吐量稳定在近 242 TPS，而单链模式仅能达到近 225 TPS，即约有 8% 的性能提升。这一结果表明该系统通过侧链分担了主链的存储和认证压力，验证了系统在高并发交易场景中的扩展能力。但吞吐量在交易发送速率达到 1 200 TPS 后趋于饱和，说明侧链与主链之间的通信仍存在性能瓶颈。

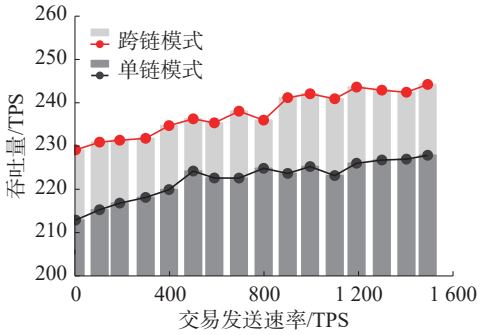

图 4　单双链交易吞吐量对比

Fig. 4　Single and dual chain transaction throughput comparison

为验证 PBFT 共识算法在本文方案的可行性，测试交易发送速率分别为 300、900、1 500 TPS 时的各自共识时延情况。如图 5 所示，Hyperledger Fabric 在此条件下的共识速度表现显著性良好，平均共识时延符合车联网环境对实时认证通信毫秒级的实时要求。其高效性得益于系统通过侧链完成本地快速认证，仅将哈希值同步至主链，从而避免了主链全网共识的高时延。

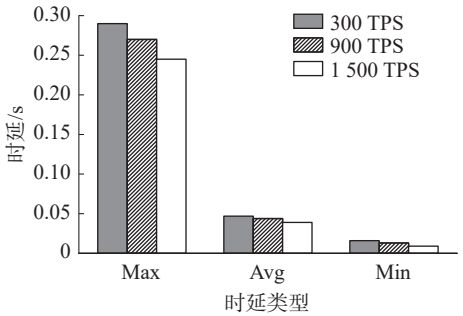

图 5　PBFT 共识时延

Fig. 5　PBFT consensus latency

该方案通过智能合约模拟双向身份认证过程, 方案设置每秒车辆发出的请求数量, 验证请求数量每秒增加 500 时车辆认证的时延情况, 并分别对 PKI 和本方案的工作效率进行时延对比, 结果如图 6 所示。由于减少了 CA 中心间的频繁交互过程, 解决了传统 PKI 方案中心化 CA 的性能瓶颈问题, 基于侧链的车联网跨域认证方案更为高效, 并在车辆身份认证及共识方面满足车联网双向认证需求, 且不存在单点故障问题, 具备更高的可靠性。

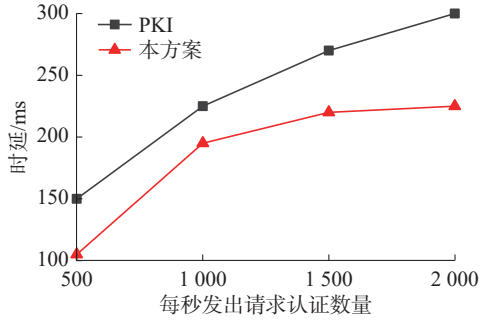

图 6　认证时延对比

Fig. 6　Authentication latency comparison

6　结束语

本文针对目前中心化车联网系统中存在的数据安全和身份认证问题, 提出了一个基于跨链技术的车联网可信认证系统。该系统采用了主侧链双链结构的认证模型, 不仅减轻了车联网传统 PKI 中 CA 的认证负荷, 而且降低了交互认证时延以及复杂度, 使其负载均衡化; 借助密码学相应算法, 提升了跨域认证信息上链的效率和响应速度, 增强了车与车、车与 RSU 间通信消息的保密性, 实现了设备间的无缝通信, 并确保数据交换过程的安全与一致性。最后, 通过仿真实验从计算开销等方面验证了该系统的可行性。在实际车联网场景中, 大量低计算能力的 OBU 设备需要频繁与 RSU 交互, 而实验结果表明, 该系统可以支持这些设备的低功耗运行需求。然而, 实验场景未能覆盖网络拥堵、节点失效等现实条件, 未来的性能表现可能需要在更复杂的环境中进一步评估。在未来工作中, 将继续在车联网应用场景结合现有实际案例研究认证中的隐私安全问题。

参考文献:

[1] LIN Jie, YU Wei, YANG Xinyu, et al. An edge computing based public vehicle system for smart transportation [J]. IEEE transactions on vehicular technology, 2020, 69(11): 12635−12651.

[2] WANG Feiyue, LIN Yilun, IOANNOU P A, et al. Transportation 5.0: the DAO to safe, secure, and sustainable intelligent transportation systems[J]. IEEE transactions on intelligent transportation systems, 24(10): 10262−10278.

[3] YANG Zhe, YANG Kan, LEI Lei, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things journal, 2019, 6(2): 1495−1505.

[4] 李子健, 章国安, 陈葳葳. 基于区块链的车联网安全通信策略[J]. 计算机工程, 2021, 47(10): 43−51.
LI Zijian, ZHANG Guoan, CHEN Weiwei. Blockchain-based secure communication strategy for Internet of vehicles[J]. Computer engineering, 2021, 47(10): 43−51.

[5] QI Jiayu, GAO Tianhan. A privacy-preserving authentication and pseudonym revocation scheme for VANETs[J]. IEEE access, 2020, 8: 177693−177707.

[6] KANG Jiawen, YU Rong, HUANG Xumin, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things journal, 2019, 6(3): 4660−4670.

[7] 张勖, 马欣. 基于区块链的轻量化移动自组网认证方案[J]. 网络与信息安全学报, 2020, 6(4): 14−22.
ZHANG Xu, MA Xin. Lightweight mobile Ad Hoc network authentication scheme based on blockchain[J]. Chinese journal of network and information security, 2020, 6(4): 14−22.

[8] JIANG Wenbo, LI Hongwei, XU Guowen, et al. PTAS: privacy-preserving thin-client authentication scheme in blockchain-based PKI[J]. Future generation computer systems, 2019, 96: 185−195.

[9] MA Zhuo, ZHANG Junwei, GUO Yongzhen, et al. An efficient decentralized key management mechanism for VANET with blockchain[J]. IEEE transactions on vehicular technology, 2020, 69(6): 5836−5849.

[10] CHEN Mao, JIANG Yuan, HUANG Ju, et al. An attribute-encryption-based cross-chain model in urban Internet of vehicles[J]. Computers and electrical engineering, 2024, 115: 109136.

[11] STEGER M, DORRI A, KANHERE S S, et al. Secure wireless automotive software updates using blockchains: a proof of concept[C]//Advanced Microsystems for Automotive Applications 2017. Cham: Springer International Publishing, 2017: 137−149.

[12] DUBOIS A, WEHENKEL A, FONTENEAU R, et al. An app-based algorithmic approach for harvesting local and renewable energy using electric vehicles[C]//Proceedings of the 9th International Conference on Agents and Artificial Intelligence. Porto: SCITEPRESS - Science and Techno-

logy Publications, 2017: 1−6.

[13] 齐林海, 李雪, 祁兵, 等. 基于区块链生态系统的充电桩共享经济模式[J]. 电力建设, 2017, 38(9): 1−7.
QI Linhai, LI Xue, QI Bing, et al. Shared economy model of charging pile based on block chain ecosystem[J]. Electric power construction, 2017, 38(9): 1−7.

[14] SINGH P K, SINGH R, NANDI S K, et al. Blockchain-based adaptive trust management in Internet of vehicles using smart contract[J]. IEEE transactions on intelligent transportation systems, 22(6): 3616−3630.

[15] TAN Chenkai, BEI Shaoyi, JING Zhengjun, et al. An atomic cross-chain swap-based management system in vehicular ad hoc networks[J]. Wireless communications and mobile computing, 2021, 2021(1): 6679654.

[16] HE Yunhua, ZHANG Cui, WU Bin, et al. A cross-chain trusted reputation scheme for a shared charging platform based on blockchain[J]. IEEE internet of things journal, 9(11): 7989−8000.

[17] KANG Jiawen, LI Xuandi, NIE Jiangtian, et al. Communication-efficient and cross-chain empowered federated learning for artificial intelligence of things[J]. IEEE transactions on network science and engineering, 9(5): 2966−2977.

[18] LU Shaofei, PEI Jingru, ZHAO Renke, et al. CCIO: a cross-chain interoperability approach for consortium blockchains based on oracle[J]. Sensors, 2023, 23(4): 1864.

[19] 商琦, 陈洪梅. 区块链技术创新态势专利情报实证[J]. 情报杂志, 2019, 38(4): 23−28, 59.
SHANG Qi, CHEN Hongmei. Empirical analysis of the patent intelligence on the innovation status of blockchain technology[J]. Journal of intelligence, 2019, 38(4): 23−28, 59.

[20] JABBAR R, DHIB E, SAID A B, et al. Blockchain technology for intelligent transportation systems: a systematic literature review[J]. IEEE Access, 2022, 10: 20995−21031.

[21] SINGH P K, SINGH R, NANDI S K, et al. Blockchain-based adaptive trust management in Internet of vehicles using smart contract[J]. IEEE transactions on intelligent transportation systems, 2021, 22(6): 3616−3630.

[22] 代闯闯, 栾海晶, 杨雪莹, 等. 区块链技术研究综述[J]. 计算机科学, 2021, 48(S2): 500−508.
DAI Chuangchuang, LUAN Haijing, YANG Xueying, et al. Overview of blockchain technology[J]. Computer science, 2021, 48(S2): 500−508.

[23] ALFANDI O, KHANJI S, AHMAD L, et al. A survey on boosting IoT security and privacy through blockchain[J]. Cluster computing, 2021, 24(1): 37−55.

[24] GUAN Zhitao, SI Guanlin, ZHANG Xiaosong, et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities[J]. IEEE communications magazine, 56(7): 82−88.

[25] AN Dou, YANG Qingyu, YU Wei, et al. LoPrO: location privacy-preserving online auction scheme for electric vehicles joint bidding and charging[J]. Future generation computer systems, 2020, 107: 394−407.

[26] LIU C H, LIN Qiuxia, WEN Shilin. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning[J]. IEEE transactions on industrial informatics, 2019, 15(6): 3516−3526.

[27] LIU Jun, ZHANG Lei, LI Chunlin, et al. Blockchain-based secure communication of intelligent transportation digital twins system[J]. IEEE transactions on intelligent transportation systems, 23(11): 22630−22640.

[28] 刘佳. 基于 ECC 与嵌入式的智能家居安全协议研究与设计[D]. 成都: 电子科技大学, 2017.
LIU Jia. Research and design of smart home security protocol based on ECC and embedded technology[D]. Chengdu: University of Electronic Science and Technology, 2017.

[29] 史有辉, 李伟生. 盲签名研究综述[J]. 计算机工程与科学, 2005, 27(7): 83−85, 94.
SHI Youhui, LI Weisheng. A survey of blind signature studies[J]. Computer engineering & science, 2005, 27(7): 83−85, 94.

[30] 万丽, 李方伟, 闫少军. 基于改进椭圆曲线数字签名的盲签名[J]. 计算机应用研究, 2011, 28(3): 1152−1154.
WAN Li, LI Fangwei, YAN Shaojun. Blind signature scheme based on improved elliptic curve digital signature algorithm[J]. Application research of computers, 2011, 28(3): 1152−1154.

[31] 陈倩倩, 秦宝东. 基于 SM9 的两方协同盲签名方案[J]. 计算机工程, 2023, 49(6): 144−153, 161.
CHEN Qianqian, QIN Baodong. Two-party cooperative blind signature scheme based on SM9[J]. Computer engineering, 2023, 49(6): 144−153, 161.

[32] 汪锐, 曹素珍, 王斐, 等. 车载自组网中基于无证书的密钥隔离批量消息认证方案[J]. 计算机工程与科学, 2019, 41(9): 1588−1596.
WANG Rui, CAO Suzhen, WANG Fei, et al. A batch message authentication scheme based on certificateless key insulation in vehicular ad hoc networks[J]. Computer engineering & science, 2019, 41(9): 1588−1596.

[33] 刘雪娇, 钟强, 夏莹杰. 基于双层分片区块链的车联网跨信任域高效认证方案[J]. 通信学报, 2023, 44(5): 213−223.

LIU Xuejiao, ZHONG Qiang, XIA Yingjie. Efficient authentication scheme for cross-trust domain of IoV based on double-layer shard blockchain[J]. Journal on communications, 2023, 44(5): 213−223.

[34] 高春祺, 李雷孝, 史建平. 结合区块链的车联网可信认证与激励机制综述[J]. 计算机科学与探索, 2024, 18(11): 2798−2822.
GAO Chunqi, LI Leixiao, SHI Jianping. Overview of trusted authentication and incentive mechanisms in BlockchainBased Internet of vehicles[J]. Journal of frontiers of computer science and technology, 2024, 18(11): 2798−2822.

[35] 关振宇, 陈永江, 李大伟, 等. 一种基于区块链的车联网跨域认证方案[J]. 网络空间安全, 2020, 11(9): 62−69.
GUAN Zhenyu, CHEN Yongjiang, LI Dawei, et al. A cross-domain authentication scheme for Internet of vehicles based on blockchain[J]. Cyberspace security, 2020, 11(9): 62−69.

[36] CHEN Qingnan, WU Ting, HU Chengnan, et al. An identity-based cross-domain authenticated asymmetric group key agreement[J]. Information, 2021, 12(3): 112.

作者简介:

李子欣, 硕士研究生, 主要研究方向为区块链、车联网和密码学。E-mail: lizixin125@163.com。

施水玲, 博士研究生, 主要研究方向为机器学习、宽度学习系统、计算智能、情感计算和复杂网络。E-mail: shishuiling0409@sina.com。

刘文奇, 教授, 博士生导师, 主要研究方向为数据博弈、数据质量控制、复杂系统建模、认知学习和机器学习。发表学术论文 20 余篇。E-mail: liuwenq2215@sina.com。