

交叉口场景下基于区块链技术的匿名车辆身份认证方案

王昊, 吴天昊, 朱孔林, 张琳

(北京邮电大学信息与通信工程学院, 北京 100876)

摘要: 随着智能交通系统的不断发展, 未来车辆在进出交叉口时, 将不再受传统信号灯控制, 而是通过与交叉口附近的区域服务器进行信息交互, 接受区域服务器的统一调度。保证车辆在交叉口通信安全的基础是网络节点的身份认证。基于此, 提出一种基于区块链技术的匿名车辆认证方案, 在认证中采用基于身份和哈希消息认证码的混合密码认证机制, 并将认证结果记录在区块链中。通过仿真测试和结果分析表明, 该方案具有匿名性、保护隐私等特性。与其他方案相比, 该方案有效降低了通信开销。

关键词: 智能交通系统; 身份认证; 隐私保护; 区块链

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020057

Anonymous vehicle authentication scheme based on blockchain technology in the intersection scenario

WANG Hao, WU Tianhao, ZHU Konglin, ZHANG Lin

School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: With the development of intelligent transportation system, the vehicles will no longer be controlled by the traditional traffic light when they enter or leave the intersection. Instead, they will interact with the local server (LS) near the intersection and accept the regulation of LS. The basic of the security vehicle communication at intersections is authentication of network node. Based on this, an anonymous vehicle authentication scheme based on blockchain technology was proposed. The scheme employed a hybrid cryptography based on identity and hash message authentication code, and recorded the authentication results in blockchains. According to simulation testing and result analysis, the scheme ensures the anonymity and privacy-preserving, with less communication overhead compared to other methods.

Key words: intelligent transportation system, identity authentication, privacy preserving, blockchain

收稿日期: 2019-05-27; 修回日期: 2019-07-12

通信作者: 王昊, wanghao123@bupt.edu.cn

基金项目: 国家重点研发计划 (2016YFB0100902)

Foundation Item: The National Key R&D Program of China (2016YFB0100902)

论文引用格式: 王昊, 吴天昊, 朱孔林, 等. 交叉口场景下基于区块链技术的匿名车辆身份认证方案[J]. 网络与信息安全学报, 2020, 6(5): 27-35.

WANG H, WU T H, ZHU K L, et al. Anonymous vehicle authentication scheme based on blockchain technology in the intersection scenario [J]. Chinese Journal of Network and Information Security, 2020, 6(5): 27-35.

高了数据的交互效率和系统的防篡改能力。

2 相关工作

2.1 车联网中匿名认证机制

身份认证是一种保护 V2X 中各节点免受恶意实体攻击的机制,被认为是防御各种攻击的第一道防线。Biswas 等^[5]提出了一种车辆消息认证和针对道路周期性安全信息的高效验证策略。将椭圆曲线数字签名算法的一种变体与基于身份的签名相结合,利用车辆上的当前位置信息作为相应车辆的 ID,这就不需要第三方公钥证书来验证 V2X 中的消息。Shen 等^[6]提出一种协作消息认证协议 (CMAP, cooperative message authentication protocol),以发现恶意车辆在交通系统中传播的恶意信息。协作消息认证是一种很有前景的技术,它可以减少车辆在消息验证方面的计算开销。然而,随着车辆密度的增加,通信开销随之增加。该方法的主要限制是如果没有验证者来验证消息,那么恶意信息可能会被其他车辆用户错误使用。

隐私保护是 V2X 通信过程中的另一个关键问题。车辆以明文形式将其身份发送到 RSU 或其他车辆。通过捕捉车辆的信息,敌手可以追踪车辆的行驶路线。交通线路的泄露侵犯了驾驶员的隐私,并可能造成严重的后果,因为这些路线可能被用于某些违法行为。为解决隐私问题,必须在 V2X 通信中提供匿名消息,但可信的权威机构仍然可以从消息中提取真实的身份。例如,当恶意车辆发送虚假信息并导致犯罪或事故时,其真实身份可以被有效追溯,使恶意车辆因其行为而受到处罚。因此,应该在车联网认证中实现有条件的隐私,即保护车辆隐私的同时,实现车辆身份的可追溯性。文献[7]提出了一种基于群签名的认证方案,可以再车辆自组网中实现安全且隐私的车辆认证。文献[8]提出了一种车联网中基于密码和有条件隐私的身份认证和群密钥生成协议,该协议在设计时没有使用双线性对和椭圆曲线,因此在计算和通信方面是轻量级的。Azees 等^[9]提出了一种有效的匿名认证机制,该机制认证过程中提供了有条件的隐私保护,减少了车辆和道路匿名证书的存储开销。文献[10]介绍了一种基于身份的双线性对签名加密 (IBSC, identity-based

signcryption) 方案,适用于低带宽通信,但由于其计算量大,不适用于交通场景中 RSU 在短时间内验证大量车辆的情况。

2.2 区块链在身份认证中的应用

区块链是一种按照时间顺序将数据区块以链条的方式组合而成的特定数据结构,其本质上是一种分布式的数据库。目前的区块链系统大致可分为 3 类 (公有链、联盟链和私有链)^[11],本文主要使用联盟链。联盟链只选择部分节点来确定协商一致意见,其具有以下特性:首先,对于联盟链的一致性确定,由一组选定的节点负责对区块进行验证;其次,记录的读取权限可以是公开的,也可以是受限的;最后,半分布式并不是网络中所有节点都能加入联盟链的共识过程,共识效率高。

区块链的关键优势之一是促进所有分散的节点在数据有效性上达成一致,这是节点间相互信任的基础。常见的共识算法有基于工作量证明 (PoW, proof of work) 算法、权益证明 (PoS, proof of stake) 算法、实用拜占庭容错 (PBFT, practical Byzantine fault tolerance) 算法等^[12]。由于交叉口场景中对实时性要求高,不需要令牌,为提高认证效率,参与协商一致过程的节点数目相对固定的 PBFT 算法更适合在交叉口认证场景下使用。

传统认证机制需要用户和数据中心之间的多次交互,这是车辆有效访问路边节点的一个障碍。区块链作为一个分布式系统,多个网络节点可在不需要中央授权的情况下维护相同的信息,可以有效降低数据中心、区域、域管理器之间的通信开销。文献[13]提出了一种基于区块链的分布式 PKI (public key infrastructure) 认证系统,以提供密钥查询和身份绑定服务,但由于用户的身份和公钥直接存储在区块链中,可能会造成隐私泄露。文献[14]提出了一种适用于异构智能交通系统的基于区块链的动态密钥管理方法,通过仿真结果表明了使用区块链结构在密钥传输时间方面比中央管理器结构效果更好。Wang 等^[15]提出了一种基于区块链的跨域认证模型 BlockCAM,以保证在不同区域访问资源的安全性和效率。与传统的车联网认证机制相比,基于区块链的车联网身份认证机制既可以提高认证效率,又可以抵抗分布式拒绝服务 (DDoS, distributed denial of service) 攻击^[16],

因为区块链的节点是分散的,且每个节点具备完整的区块链信息,并能对其他节点的数据有效性进行验证,即使攻击者攻破某个节点,剩余节点也可以正常维持整个区块链系统,因此,针对区块链的 DDoS 攻击将会难上加难。

3 基于区块链的匿名认证方案

汽车正在向智能化、无人化的方向发展,对车辆进行管理,实现汽车安全行驶是车联网的重要课题。车联网属于物联网的一部分,同样具有分布式、去中心化等特点,因此,区块链技术可以解决车联网去中心化管理、隐私保护等问题。本节首先介绍系统模型,然后提出安全目标和系统的设计细节。

3.1 系统模型

本文研究了基于区块链技术的车辆匿名认证方案,系统模型如图 2 所示,主要包括 4 类参与者,分别为信任机构(TA, trust authority)、区域服务器、共识节点(WP, witness peer)和车辆(vehicle)。

(1) 信任机构

为了保证系统的有序运行,需要一个充分可信的机构 TA,负责生成系统参数,以及追踪非法车辆。

(2) 区域服务器

LS 是在交叉口中为汽车通行提供路径规划的服务提供方。车辆不需要信号灯的指示,而是根据 LS 为其规划的通过交叉口的先后顺序依次通过,在此之前需要对进入交叉口的车辆进行身份认证。可将 LS 理解为具有较高的计算与数据交互功能的 RSU。LS 可以通过无线与车辆通信,接收车辆发过来的请求信息,也可以通过有线与 TA 和 WP 通信。在建立系统之前 LS 需要先在 TA 上注册。每个 LS 维护一个包含所有车辆访问记录的公共账本。公共账本只能由 TA、LS 和 WP 访问。

(3) 共识节点

WP 是通过协商一致算法将身份认证结果写入公共分类账的对等方。每个交叉口设有一个 WP。所有的 WP 和 LS 组成联盟链。

(4) 车辆

本文中指无人驾驶汽车。每辆靠近交叉口的车辆会向 LS 申请路径规划服务,在此之前会进行车辆与 TA 的注册和车辆与 LS 的身份认证,以

确认其合法身份,并享受后续数据共享与控制管理等服务。每辆车内部均配有嵌入式计算机、无线网络接口、GPS 接收机、车载导航系统、数字地图等计算和通信单元。

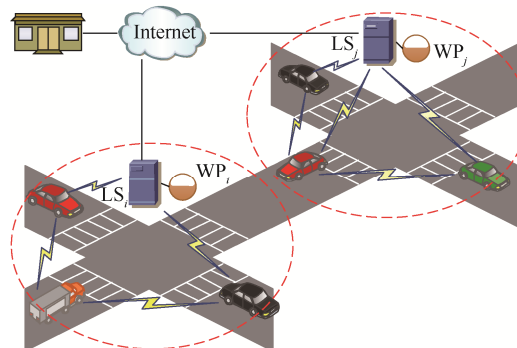


图 2 系统模型
Figure 2 System model

3.2 安全目标

在交叉口场景中,安全和隐私对于安全通信至关重要。在确定安全需求之前,应该首先讨论安全威胁,车辆与道路其他实体通信过程中几类常见的安全威胁有:伪装攻击、重放攻击、假消息攻击、拒绝服务(DoS)攻击等^[17-18]。

考虑到上述交叉路口可能存在的安全威胁,本文设计基于区块链技术的车辆匿名认证方案,并实现以下有关安全性的目标。

保密性:确保敌手不能解密传输的消息。

完整性:保证敌手不能篡改发送的消息。

匿名性:允许每辆车使用临时的假名。在访问 LS 期间,若更换假名,车辆可以选择重新验证自己的身份,使敌手很难对车辆进行追踪或统计。

可追溯性:保证 TA 能够追踪非法车辆并拒绝他们访问 LS。

不可否认性:保证当非法车辆被举报时,其不当行为是不可否认的。

轻量化:保证较低的计算和通信开销。

3.3 系统描述

本文提出的认证系统包含 5 个阶段,即初始化、注册、身份认证、协商一致和服务交付阶段。表 1 给出了相关符号含义。

(1) 初始化阶段

TA 进行初始化,生成自己的公私钥对和密

钥，并将公钥广播。初始化阶段仅由 TA 在系统建立期间执行一次。

TA 生成自己的公私钥对 $\{ \text{PuK}_{\text{TA}}, \text{PrK}_{\text{TA}} \}$ ，其中， PuK_{TA} 用 TA 来为 LS 和车辆生成公钥， PrK_{TA} 用 TA 来为 LS 和车辆生成私钥。

TA 利用式(1)生成密钥 Srk_{TA} ，用作车辆认证中 HMAC 运算的密钥。其中， Srk_{TA} 每 24 h 改变一次。

$$\text{Srk}_{\text{TA}} := \text{KeyGen}(\text{RID}_{\text{TA}}, \text{PrK}_{\text{TA}}, \text{TS}) \quad (1)$$

TA 对 PrK_{TA} 进行保密，公开参数 Srk_{TA} 、 PuK_{TA} 。

TA 初始化后获得的参数为

$$\text{TA_Parameters}: [\text{PuK}_{\text{TA}}, \text{PrK}_{\text{TA}} \& \text{Srk}_{\text{TA}}]$$

表 1 符号含义
Table 1 Definition of symbols

符号	含义
RID_{TA}	TA 真实 ID
PrK_{TA}	TA 的私钥
PuK_{TA}	TA 的公钥
Srk_{TA}	TA 生成的密钥
RID_{LS}	LS 真实 ID
PrK_{LS}	LS 的私钥
PuK_{LS}	LS 的公钥
RID_{V}	车辆真实 ID
PrK_{V}	车辆的私钥
PuK_{V}	车辆的公钥
PsID_{V}	车辆的假名
VTP_{PsID}	车辆假名的有效时间
TS	时间戳
HC_{V}	车辆计算的 HMAC
BS_{V}	车辆信标信号
HC'	LS 计算的 HMAC
$\text{SafeMsg}_{\text{V}}$	车辆生成的安全消息

(2) 注册阶段

本阶段主要执行 LS 和车辆的注册，LS 和车辆分别向 TA 进行注册，与 TA 共同生成公钥和私钥，使 LS 和车辆均注册为合法节点。其中，LS 注册时执行以下步骤。

TA 利用 RID_{LS} 、 PrK_{TA} 和 PuK_{TA} 按照式(2)和式(3)为 LS 生成公私钥对 $\{ \text{PuK}_{\text{LS}}, \text{PrK}_{\text{LS}} \}$ 。

$$\text{PrK}_{\text{LS}} := \text{KeyGen1}(\text{RID}_{\text{LS}}, \text{PrK}_{\text{TA}}) \quad (2)$$

$$\text{PuK}_{\text{LS}} := \text{KeyGen2}(\text{PrK}_{\text{LS}}, \text{PuK}_{\text{TA}}) \quad (3)$$

LS 对私钥 PrK_{LS} 进行保密，公开其公钥 PuK_{LS} 。

LS 完成注册后获得的参数为

$$\text{LS_Parameters}: [\text{RID}_{\text{LS}}, \text{PuK}_{\text{LS}}, \text{PrK}_{\text{LS}}, \text{PuK}_{\text{TA}} \& \text{Srk}_{\text{TA}}]$$

车辆在注册时主要执行以下步骤。

TA 利用 RID_{V} 和假名截止时间 VTP_{PsID} 为车辆计算假名，具体见式(4)。

$$\text{PsID}_{\text{V}} := \text{Hash}(\text{RID}_{\text{V}} \parallel \text{VTP}_{\text{PsID}}) \quad (4)$$

TA 利用 PsID_{V} 、 PrK_{TA} 和 PuK_{TA} 等参数按照式(5)和式(6)为车辆计算其公私钥对 $\{ \text{PuK}_{\text{V}}, \text{PrK}_{\text{V}} \}$ 。

$$\text{PrK}_{\text{V}} := \text{KeyGen3}(\text{PsID}_{\text{V}}, \text{PrK}_{\text{TA}}) \quad (5)$$

$$\text{PuK}_{\text{V}} := \text{KeyGen4}(\text{PrK}_{\text{V}}, \text{PuK}_{\text{TA}}) \quad (6)$$

与此同时，TA 将生成的参数 $\{ \text{PrK}_{\text{V}}, \text{PuK}_{\text{V}}, \text{Srk}_{\text{TA}}, \text{PuK}_{\text{TA}} \}$ 记录在车辆的防篡改设备中。

车辆完成注册后获得的参数为

$$\text{V_Parameters}: [\text{RID}_{\text{V}}, \text{PuK}_{\text{V}}, \text{PrK}_{\text{V}}, \text{PsID}_{\text{V}}, \text{VTP}_{\text{PsID}} \& \text{Srk}_{\text{TA}}]$$

(3) 身份认证阶段

此阶段目的是位于交叉口的 LS 对其覆盖范围内的车辆进行身份认证，随后 LS 将认证结果对 WP 进行广播，WP 在协商一致阶段将认证结果写入区块链中。图 3 展示了身份认证与共识过程的基本数据交互。

当一辆驶向交叉口的车辆访问 LS 时，它需要执行如下操作。

车辆利用 PsID_{V} 、 VTP_{PsID} 和 PuK_{V} 等参数按照式(7)计算 HC_{V} 。

$$\text{HC}_{\text{V}} = \text{HMAC}(\text{Srk}_{\text{TA}}, \text{PsID}_{\text{V}} \parallel \text{VTP}_{\text{PsID}} \parallel \text{PuK}_{\text{V}}) \quad (7)$$

车辆利用 PsID_{V} 、 VTP_{PsID} 、 HC_{V} 和 PuK_{V} 等参数按照式(8)计算 BS_{V} 。

$$\text{BS}_{\text{V}} = \text{PsID}_{\text{V}} \parallel \text{VTP}_{\text{PsID}} \parallel \text{HC}_{\text{V}} \parallel \text{PuK}_{\text{V}} \parallel \text{SIG}_{\text{PrK}_{\text{V}}}(\text{HC}_{\text{V}}) \quad (8)$$

车辆向其所处交叉口的 LS 发送 BS_{V} ，LS 接收 BS_{V} 后，执行如下操作。

LS 利用接收到的 BS_{V} 中包含的 PsID_{V} 、 VTP_{PsID} 和 PuK_{V} 等参数按照式(9)计算 HC' ，来验证 BS_{V} 的正确性。

$$\text{HC}' = \text{HMAC}(\text{Srk}_{\text{TA}}, \text{PsID}_{\text{V}} \parallel \text{VTP}_{\text{PsID}} \parallel \text{PuK}_{\text{V}}) \quad (9)$$

LS 验证式(10)是否成立。

$$HC_v = HC' \quad (10)$$

若成立, LS 将搜索其本地数据库认证信息是否存在。如果存在身份验证信息, LS 将更新其数据库中的身份验证结果。同时, 它将向所有 WP 广播认证结果, 并为车辆提供数据共享和路径规划服务。

至此, 车辆可根据其合法身份与 LS 进行数据交互, 车辆发送安全消息如下。

$$\begin{aligned} \text{SafeMsg}_v &= \text{MSG} \parallel \text{HMAC}_{\text{srk}_{TA}}(\text{MSG}) \parallel \\ &\parallel \text{PsID} \parallel \text{SIG}_{\text{PrK}_v}(\text{MSG}) \parallel \text{TS} \end{aligned} \quad (11)$$

LS 收到车辆的安全消息后, 即可通过 HMAC 检查来验证消息的合法性和完整性, 其中, 安全消息类型如表 2 所示。有效字节数 (payload) 统一为 67 B, 方便在性能分析中与其他认证机制进行比较; HMAC 采用常见的 HMAC-SHA1 算法, 其摘要长度取 20 B; 为减少签名所占字节, 本文采用 Shim 在文献[19]中的方法, 使签名降低到 64 B。考虑交叉口车辆数, 本文设置假名长度为 6 B; 参考文献[20]等研究, 时间戳默认为 4 B。

表 2 车辆发送的安全消息类型
Table 2 Safety message type sent by vehicles

有效字节数	HMAC	签名	假名长度	时间戳
67 B	20 B	64 B	6 B	4 B

(4) 协商一致阶段

WP 在收到认证结果之后, 通过实用拜占庭容错算法将认证结果写入区块链中, 具体操作如下。

假设共有 k 个 WP, 分别是 $\{\text{WP}_1, \text{WP}_2, \dots, \text{WP}_k\}$, 认证结果的每一轮写入, 都会有一个 WP 作为记录者, 其他 WP 作为共识者。

通过 $x = (\text{height} \bmod k) + 1$ 决定出一个记录者 $\text{WP}_x (1 \leq x \leq k)$, 其中, height 是当前的区块长度。

SM 向所有的 WP 广播附带 SM 签名的认证结果, 所有的 WP 独立监听广播的认证结果数据, 并保存在自己的内存中。

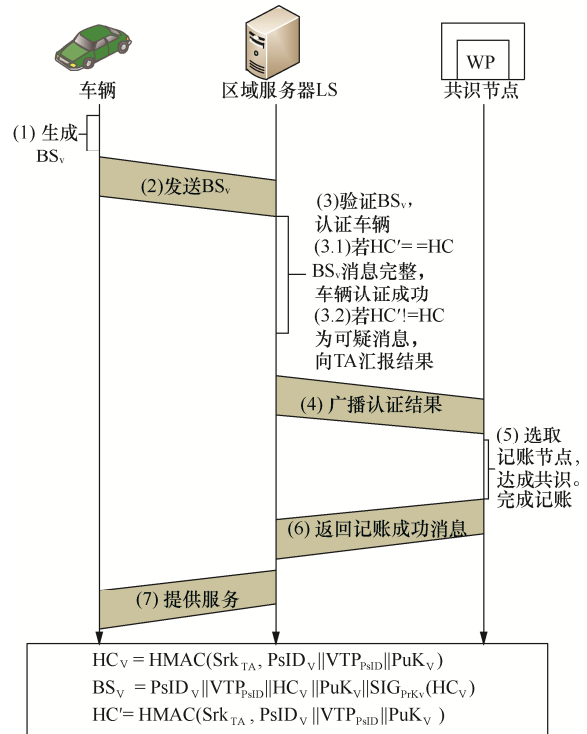
设置区块产生的时间间隔为 t , 经过时间 t 后, 记录者给所有共识者发送提议 $\langle \text{p_request}, \text{height}, \text{WP}_x, \text{block}, \text{SIG}_{\text{WP}_x}(\text{block}) \rangle$, 其中, p_request 表示记录者请求共识者投票。

共识者 WP_i 收到所述提议后, 发送 $\langle \text{p_response}, \text{height}, \text{WP}_i, \text{block}, \text{SIG}_{\text{WP}_i}(\text{block}) \rangle$, 其中, p_response 表示共识者回应记录者的请求。

每个 WP 至少收到 $k - f$ 个签名 $\text{SIG}_{\text{WP}_i}(\text{block})$ 时, 达成共识并且发布该区块; 如果签名数量没有达到 $k - f$, 将执行下一轮共识。其中, $f = \left\lfloor \frac{k-1}{3} \right\rfloor$,

表示系统中允许存在的最大数量的有问题的 WP。

任何 WP 收到完整区块后, 会从自己的内存中删除包含在区块中的认证结果信息, 然后开始下一轮共识。



(5) 服务交付阶段

在此阶段, 当车辆移动到新交叉口时, 意味着车辆移向了新的 LS 覆盖范围, 执行以下操作。

车辆提交访问请求 $\text{ac}_v = \{\text{SIG}_{\text{PrK}_v}(\text{PsID}_v, \text{TS}), \text{PsID}_v, \text{TS}\}$ 给 LS。

LS 首先搜索本地数据库查找车辆的公钥 PuK_v , 如果不存在, 则搜索公共账本, 找到 PuK_v 后, 如果它不在撤销列表中, 则验证签名 $\text{SIG}_{\text{PrK}_v}$, 如果验证成功并且时间戳 TS 是有效的, LS 方可响应车辆的服务请求, 否则拒绝服务。

其中, 如果一辆违法车辆被上报给 TA, TA 将会检查区块链找到违法车辆的 ID, 并通知 LS 该违法车辆的公钥是无效的, LS 将该恶意车辆 ID 标记

并存储到本地撤销列表中,同时广播给所有 WP。WP 将恶意车辆信息写入区块链中,写入过程同协商一致阶段中的操作,用于后续认证过程参考。

4 系统评估与分析

4.1 安全性分析

本节证明所提方案满足以下安全要求:① 保密性;② 匿名性;③ 可追溯性。另外,所提方案可以有效抵抗重放攻击和 DDoS 攻击等。

(1) 保密性

本文将基于身份的非对称密码和 HMAC 结合起来,实现道路交叉口场景下匿名车辆身份认证。公钥分发阶段,利用 LS 和车辆自身的 ID 生成公私钥对,保证了密钥的可靠性。认证阶段,安全消息 BS_V 中包含由 SrK_{TA} 生成的哈希消息认证码。只有合法注册的 LS 才有 SrK_{TA} 。另外,发送车辆的签名和假名 $PsID_V$ 附加在安全消息中。HMAC、签名和临时假名 $PsID_V$ 确保了车辆与 LS 通信认证过程中的保密性和消息完整性。此外,只有合法授权的 TA、LS、WP 等节点才可以访问区块链。在服务交付阶段,当发送的消息 $ac_V = \{SIG_{PrK_V}(PsID_V, TS), PsID_V, TS\}$ 被敌手篡改时,敌手只能获得毫无价值的假名 $PsID_V$ 和时间戳 TS。因此,所提方案保证了关键信息在整个工作流程中的保密性。

(2) 匿名性

为了实现匿名,必须确保在部署 BS_V 时,没有任何敌手能够提取真实身份。在认证阶段,车辆在交叉口附近向 LS 发送 BS_V 消息。此 BS_V 包含基于 ID 的数字签名和假名 $PsID_V$,而不是车辆的真实 ID。数字签名和 $PsID_V$ 实现 V2I 通信过程中节点认证的同时,保证了匿名性。如果一辆汽车更改了假名,它只需要重新认证。另外,认证结果被写入区块链中,但只有合法授权的实体才能访问区块链。敌手很难获得车辆的真实身份,车辆的假名也会随时间有规律地变化,从而保证该机制的匿名性。

(3) 可追溯性

TA 旨在实现可追溯性的功能。当发现和报告车辆的违规行为时,TA 将搜索区块链,以查明非法匿名车辆的相应真实身份,并撤销其公钥,从

而保证非法车辆的可追溯性。同时,揭露非法车辆的真实身份,使其无法对非法行为进行否认,实现了认证过程中的可追溯性和不可否认性。

另外,如 3.3 节服务交付阶段内容所述,在身份认证过程使用查询-响应握手机制,在传递消息时添加时间戳 TS。若时间戳 TS 是有效的,LS 方可响应车辆的服务请求,否则拒绝服务。通过验证时间戳是否有效,可以防止重放攻击。本文设计的方案建立在区块链的基础上,具有无中心化和冗余的特性。即使一个节点被破坏,其他节点也不会受到影响,因此可抵抗 DDoS 攻击。

结合车联网场景下身份认证需求,本文方案与其他认证方案的主要特性对比如表 3 所示。

表 3 本文方案与其他认证方案的主要特征对比
Table 3 Comparison of the main features between the scheme in this paper and other authentication scheme

认证方案	匿名性	可追溯性	抗 DDoS 攻击	区块链	
				共识算法	最大恶意节点数占比
PKI-Certi ^[21]	√	—	—	—	—
文献[2]	√	—	—	—	—
文献[3]	√	—	√	PoS	51%
文献[14]	√	√	√	PoW	51%
本文方案	√	√	√	PBFT	33%

注:“√”和“—”分别指“有”和“无”。

4.2 性能分析

本文采用车联网专用仿真软件 Veins 对方案进行了仿真,本次仿真使用的计算机系统配置为 Intel Core i3-3217, 1.8 GHz, 8 GB RAM。主要仿真参数如表 4 所示。

表 4 仿真参数
Table 4 Simulation parameters

参数	数值
车辆数	100
车辆速度	20~60 km/h
交叉口数	12
网络协议	LTE-V2X
仿真步长	1 s
仿真时间	14 400 s

将本文方案与现有 4 种车辆认证方法^[21-24]的

性能表现进行比较分析。对比方案解释如下：文献[21]采用基于证书的签名，简称为 PKI-Certi；文献[22]采用基于 ID 的签名认证机制，实现一种有条件隐私保护的认证方案，简称为 ECPP；文献[23]是一种使用代理车辆的基于身份的消息认证方案，简称为 ID-MAP；文献[24]采用批认证方式，简称为 bSPECS。将本文提出的方案与基于 PKI、基于 ID、基于批认证的方案进行对比，表明本文所提方案具备轻量化的特征，以及在安全性要求、开销和延迟方面有更好的性能。

通信开销定义为除去有效信息的字节数与传输总字节数（即有效信息字节加开销字节）的比值，表示为

$$\text{CommunOverhead} := \frac{\text{Overhead}}{\text{Payload} + \text{Overhead}} \quad (12)$$

表 2 以及表 5~表 8 分别列出了本文方案和 PKI-Certi、ECPP、ID-MAP 和 bSPECS 中使用的安全消息类型。对比的 5 种认证方案的传输字节分别为 161 B、248 B、172 B、191 B 和 451 B。

表 5 PKI-Certi 认证机制中安全消息类型
Table 5 Safety message type in PKI-Certi

包含信息	有效信息	证书	签名
字节大小	67 B	125 B	56 B

表 6 ECPP 认证机制中安全消息类型
Table 6 Safety message type in ECPP

包含信息	有效信息	签名	假名	时间戳
字节大小	67 B	60 B	41 B	4 B

图 4 显示了固定有效信息（payload=67 B）下通信开销与车辆密度之间的关系（车辆密度为 1 时对应实际密度为 1 080 veh/h）。本文方案的通信开销比 ECPP、ID-MAP、PKI-certi 和 bSPECS 分别低 2.66%、6.53%、14.59%和 26.75%。

表 7 ID-MAP 认证机制中安全消息类型
Table 7 Safety message type in ID-MAP

包含信息	有效信息	签名	时间戳
字节大小	67 B	120 B	4 B

表 8 bSPECS 认证机制中安全消息类型
Table 8 Safety message type in bSPECS

包含信息	有效信息	签名	假名
字节大小	67 B	128 B	256 B

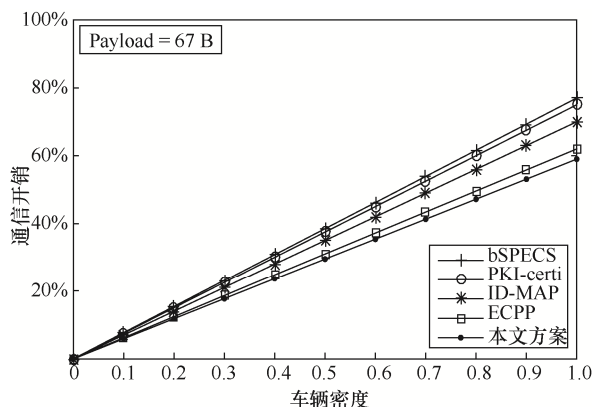


图 4 通信开销与车辆密度之间的关系

Figure 4 Relationship between communication overhead and vehicle density

协商一致阶段独立于身份认证过程。因此，本文对其进行单独评估，设置 $t = 1$ s 为区块生成时间，通过设置不同的共识节点数，得出协商一致过程时间开销，结果如表 9 所示。

表 9 协商一致过程时间开销
Table 9 Time overhead in consensus phase

WP 数量	时间开销/ms
5	2.1
8	2.8
12	4.9
15	7.9

5 结束语

随着 V2X 技术和智能网联汽车的发展，智能交通系统中的通信安全愈发重要，本文围绕道路交叉口这一具体场景，通过深入研究交通环境下认证机制的内在机理，提出一种基于区块链技术的匿名车辆认证方案。本文方案在认证中采用基于身份和哈希消息认证码的混合密码认证机制，并将认证结果记录在区块链中，提高了数据的交互效率和系统的防篡改能力。仿真与分析结果表明，本方案具有较好的安全性、匿名性等特性，同时在保证用户隐私的前提下具有一定的可追溯性。在交叉口车辆身份认证过程中具有较高的实用价值。

参考文献:

- [1] 李志强, 戴一凡, 李升波, 等. 智能网联汽车 (ICV) 技术的发展现状及趋势[J]. 汽车安全与节能学报, 2017, 8 (1): 1-14.
LI K Q, DAI Y F, LI S B, et al. State-of-the-art and technical trends of intelligent and connected vehicles[J]. Journal of Automotive

- Safety and Energy, 2017, 8(1): 1-14.
- [2] 孟震. 智能网联汽车信息共享安全机制的研究与实现. 北京: 北京邮电大学, 2016.
MENG Z. Research and implementation of security communication mechanism in intelligent-cyber vehicles[D]. Beijing: Beijing University of Posts and Telecommunications, 2016.
- [3] 戴婕. 基于密钥管理和无中心化加密的网联汽车信息安全的设计与实现[D]. 北京: 北京邮电大学, 2018.
DAI J. Design and implementation of vehicular information security based on key management and decentralized encryption[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
- [4] JIANG T G, FANG H, WANG H G. Blockchain-based internet of vehicles: distributed network architecture and performance analysis[J]. IEEE Internet of Things Journal, 2018 (Early Access).
- [5] BISWAS S, MIŠIĆ J. A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs[J]. IEEE Transactions on Vehicular Technology, 2013, 62(5): 2182-2192.
- [6] SHEN W, LIU L, CAO X. Cooperative message authentication in vehicular cyber-physical systems[J]. IEEE Trans Emerging Topics Comput. 2013, 1(1): 2182-2192.
- [7] GUO J H, BAUGH J P, WANG S Q. A group signature based secure and privacy-preserving vehicular communication framework[C]//Mobile Networking for Vehicular Environments. 2007.
- [8] ISLAM S H, OBAIDAT M S, VIJAYAKUMAR P, et al. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs[J]. Future Generation Computer Systems, 2018, 84(1): 216-227.
- [9] AZEES M, VIJAYAKUMAR P, DEBOARH L J. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, (18): 2467-2476.
- [10] KARATI A, ISLAM S H, BISWAS G P, et al. Provably secure identitybased signcryption scheme for crowdsourced industrial internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.
- [11] YUAN Y, WANG F Y. Towards blockchain-based intelligent transportation systems[C]//2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). 2016: 2663-2668.
- [12] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: beyond bitcoin[J]. Applied Innovation, 2016(2): 6-10.
- [13] 张勘, 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 X, MA X. Light weight mobile Ad Hoc network authentication scheme based on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 14-22.
- [14] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems[J]. IEEE Internet of Things Journal, 2017, 4(16): 1832-1843.
- [15] WANG W T, HU N, LIU X. BlockCAM: a blockchain-based cross-domain authentication model[C]//2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). 2018: 896-901.
- [16] 黄泽源, 孔勇平, 张会炎. 基于区块链的物联网安全技术研究[J]. 移动通信, 2018, 42(12): 8-13.
HUANG Z Y, KONG Y P, ZHANG H Y. Research on security technology of internet of things based on blockchain[J]. Mobile Communications, 2018, 42(12): 8-13.
- [17] VIJAYAKUMAR P, AZEES M, KANNAN A, et al. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks[J]. IEEE Trans Intell Transp Syst, 2016, 17(4): 1015-1028.
- [18] AZEES M, VIJAYAKUMAR P, DEBORAH L J. Comprehensive survey on security services in vehicular Ad-Hoc networks[J]. IET Intell Transp Syst, 2016, 10(6): 379-388.
- [19] SHIM K. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.
- [20] ZHU X, JIANG S, WANG L, et al. Efficient privacy-preserving authentication for vehicular Ad Hoc networks[J]. IEEE Transactions on Vehicular Technology, 2014, 63(2): 907-919.
- [21] IEEE trial-use standard for wireless access in vehicular environments (WAVE)-security services for applications and management messages[S]. 2006.
- [22] LO N, TSAI J. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. IEEE Trans Intell Transp Syst, 2016, 17(5): 1319-1328.
- [23] BAYAT M, BARMASHOORY M, RAHIMI M, et al. A secure authentication scheme for VANETs with batch verification[J]. Wireless Netw, 2015, 21(5): 1733-1743.
- [24] HORNG S, TZENG S, PAN Y, et al. b-SPECS+: batch verification for secure pseudonymous authentication in VANET[J]. IEEE Trans Inf Forensics Security, 2013, 8(11): 1860-1875.

[作者简介]



王昊 (1995—), 男, 山东潍坊人, 北京邮电大学硕士生, 主要研究方向为智能网联汽车、区块链。



吴天昊 (1992—), 男, 山东济南人, 北京邮电大学博士生, 主要研究方向为C-V2X 通信技术的应用。



朱孔林 (1985—), 男, 山东临沂人, 博士, 北京邮电大学副教授, 主要研究方向为智能网联汽车。



张琳 (1974—), 男, 上海人, 博士, 北京邮电大学教授、博士生导师, 主要研究方向为超宽带生物雷达成像及生命信号检测、网络信息处理、车联网。