基于区块链的车辆信息管理和事故自动取证系统*

汤志宏[1]　彭雅丽[2]

（1.江西科技学院，南昌 330098；2.江西师范大学，南昌 330022）

【摘要】为提高交通事故取证和定责的智能化水平，提出了基于区块链和共识机制的车辆信息管理和事故取证系统。基于许可区块链进行车辆信息管理，利用车辆电子控制单元（ECU）与路侧单元（RSU）的通信确保车辆数据的合法性和完整性。其中，利用RSU自动管理相关车辆数据，并通过实用拜占庭容错（pBFT）协议达成数据可靠性共识。试验结果表明，所提出的区块链方案能够满足交通应用的实时性需求，试验场景下的区块创建延迟和质询-应答验证耗时分别不超过18.13 ms和1.55 ms。定性试验结果表明，所提出的框架能够抵御已知的安全攻击，并确保数据可靠性，可帮助执法部门完成交通事故定责。

主题词：车辆信息管理　交通事故数字取证　区块链　共识机制　信用管理系统　实用拜占庭容错

中图分类号：TP311　　**文献标识码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20220694

Vehicle Information Management and Accident Digital Forensics System Based on Blockchain

Tang Zhihong[1], Peng Yali[2]

（1. Jiangxi University of Technology, Nanchang 330098; 2. Jiangxi Normal University, Nanchang 330022）

【Abstract】In order to improve the intelligent level of evidence collection and responsibility determination of traffic accidents, this article proposed a vehicle information management and accident forensics system based on blockchain and consensus mechanism. Vehicle information was managed in a permissioned blockchain framework, and the communication between the Electronic Control Unit (ECU) of the vehicle and the Road Side Unit (RSU) was used to ensure the legitimacy and integrity of vehicle data. In the proposed traffic accident digital forensics scheme, the data from involved vehicles was automatically managed by the RSU, and a consensus on data reliability was achieved through the practical Byzantine Fault Tolerance (pBFT) protocol. The experimental results show that the proposed blockchain scheme is able to meet the real-time requirements of transportation applications, and the block generation delay and Q-A verification delay in the experimental scenario do not exceed 18.13 ms and 1.55 ms, respectively. The qualitative results show that the proposed framework is able to resist known security attacks, ensure data reliability, and can help law enforcement achieve fair traffic accident liability determination.

Key words: Vehicle information management, Traffic accident digital forensics, Blockchain, Consensus mechanism, Credit management system, Practical Byzantine fault tolerance

【引用格式】汤志宏，彭雅丽. 基于区块链的车辆信息管理和事故自动取证系统[J]. 汽车技术，2023(6): 17-23.

TANG Z H, PENG Y L. Vehicle Information Management and Accident Digital Forensics System Based on Blockchain[J]. Automobile Technology, 2023(6): 17-23.

1　前言

根据世界卫生组织（World Health Organization，WHO）的报告，全球每年约有135万人死于交通事故[1]。很多交通事故由于取证困难，影响了事故定责和保险赔付[2]。随着汽车产业的技术进步，当前汽车上配置了大量复杂的电子控制单元（Electronic Control Unit，ECU），为车联网[3]的自动化连接创造了基础。利用这些先进技术，可以有效缓解交通拥堵，减少交通事故。ECU提供的车辆数据可帮助执法人员有效地完成交通事故责任

*基金项目：国家自然科学基金项目（71661015）。

的划分[4]。

汽车智能化的发展，需要可信的低延迟数据平台对车辆生成的大量数据进行处理[5]：参与的相关实体（包括车辆、路侧单元、交管和执法部门等）必须能验证接收信息的真实性，确保数据来自合法实体且未被篡改；考虑到交通应用的实时性（利用路况更新和事故报告），必须确保较低的验证延迟[6]。

安装在车辆上的ECU会对车联网的安全性带来威胁。例如，通过入侵车辆的ECU，攻击者可在网络中广播虚假数据，影响其他车辆的驾驶决策[7]。区块链具有透明可信、去中心化和不可篡改性[8]，区块链的去中心化特性允许多个实体对相同数据进行管理和维护，不可篡改性确保了取证数据的完整性，因此有助于执法机关公平定责[9]。文献[10]分析了交通事故取证数据的自动采集技术，并利用周边车辆的数据确保数据一致性。文献[11]提出基于区块链的交通事故取证方案，在交通事故定责中考虑了数据可信度。文献[12]提出了基于区块链的车联网电子取证方案，利用智能合约机制完成证据检索和证据链追溯，通过令牌机制控制数据访问，但未考虑恶意路侧单元（Road Side Unit，RSU）的数据篡改问题。此外，常用的区块链方案（如比特币和以太坊）的计算和带宽资源的需求量过大，信息交换的延迟过高[13]，不适用于交通领域。

为提高交通信息管理的智能化程度和隐私性，并确保交通事故取证的公平性和效率，本文基于许可区块链建立去中心化交通信息管理系统，确保车辆数据完整性和可用性，并结合信用管理系统评估事故附近车辆的可信度，结合区块链技术和信用管理，基于传感器完整性校验、传输数据完整性校验和车辆信用分校验，仅使用高可信度车辆生成的数据开展自动取证，以确保取证数据的真实性。最后，通过互联网安全敏感协议和应用的自动化验证工具对所提出的系统进行形式化验证。

2 系统架构

本文提出的自动取证系统架构如图1所示。为监测车辆行为并跟踪ECU的状态变化，网络架构分为车辆信息管理系统（Vehicle Information Management System，VIMS）和交通事故取证系统（Traffic Accident Forensics System，TAFS）。新型多输入多输出的无线技术和正交频分复用技术可以保证车辆网络的通信性能[14]。

2.1 基于许可区块链的车辆信息管理系统

VIMS框架中包含车辆制造商、维修商、交管部门和执法部门。该框架中的实体主要负责车辆的注册和维护：使用车辆的初始注册数据创建记录（区块）；记录车辆状态和所有ECU的哈希值，保存车辆的维护数据；交管部门和执法部门为可信实体，负责验证车辆ECU的状态变化。

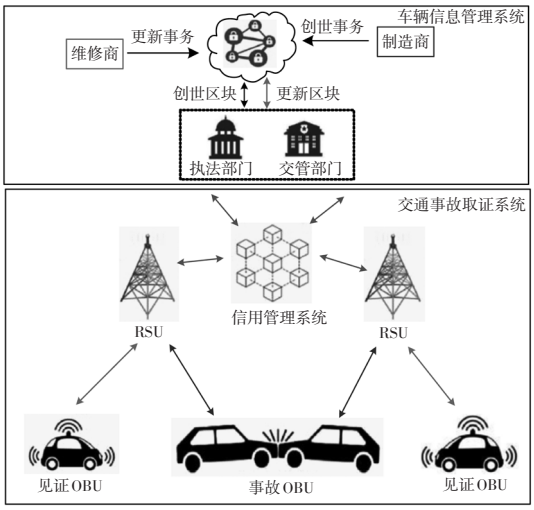

图1 基于区块链的交通安全和事故取证系统框架

该框架中的实体分为提议节点和验证节点：提议节点向区块链发送数据，包括车辆节点（On Board Unit，OBU）、制造商和维修商；验证节点负责核实和确认发送到区块链的数据，包括RSU、交管部门和执法部门。

在交通密度较高的城区，OBU会生成大量事务，传统区块链设计将事务分组，为每组事务分别建立一个区块，然后将新区块附加到区块链中，即顺序事务插入，此操作不能满足交通应用的效率要求。为克服该限制，本文使用可追加区块技术，支持多个OBU将事务同时添加到不同区块[15]，每个OBU以公钥区分，区块链数据结构如图2所示。在区块链数据结构中，为每个不同公钥创建1个区块，区块分为2个部分：区块头，包含OBU公钥、前一个区块头哈希和时间戳；区块载荷，保存所有事务。事务存储采用链表数据结构，第1个事务包含区块头哈希，后续事务包含前一个事务的哈希。利用该数据结构，可将新事务插入已有区块。利用OBU私钥对每个事务进行签名，在签名通过区块公钥验证后，OBU可将事务附加到其公钥识别出的区块。基于公钥验证，区块链可将特定OBU的事务映射到同一个区块。

2.2 VIMS的事务生成和更新

VIMS的主要活动包含创建和更新操作。车辆制造商建立OBU的创世事务后，VIMS中的可信节点（交管部门和执法部门）进行验证，验证通过后，在TAFS中对创世区块进行广播，各方实体通过区块链中的事务完成信息交流。同时，利用256位加密哈希函数（Secure Hash Algorithm-256，SHA-256）、数字签名和非对称加密确保事务安全性。

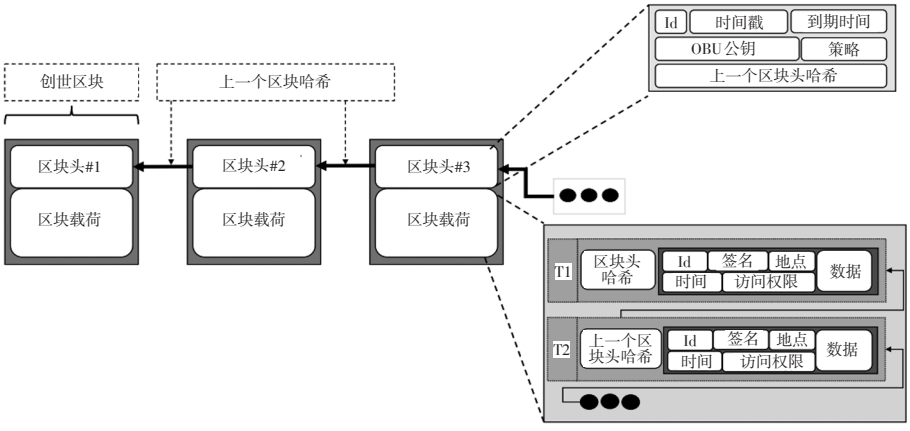

图2　区块链数据结构

交管部门和执法部门利用创世事务为OBU建立创世区块G。该区块为OBU的永久性记录，包含初始事务、OBU公钥、时间戳（区块建立时间）及外部地址（OBU数据的云端地址）。初始事务在制造商生产车辆后生成，表示为：

$$G=[S_{SID},T_S,(H(\mathrm{ECU})_1,T_1),(H(\mathrm{ECU})_2,T_2)\ ...(H(\mathrm{ECU})_n,T_n),K_P,S_M] \quad (1)$$

式中，S_{SID}为OBU出厂时，所有ECU哈希的默克尔（Merkle）树根值；T_S为出厂时间戳；$(H(\mathrm{ECU})_n,T_n)$为每个ECU的哈希值和在ECU上执行动作的相关时间戳；K_P为公钥；S_M为制造商签名。

基于区块链的Merkle树[16]，对配置了8个ECU的OBU的S_{SID}进行推导，如图3所示。

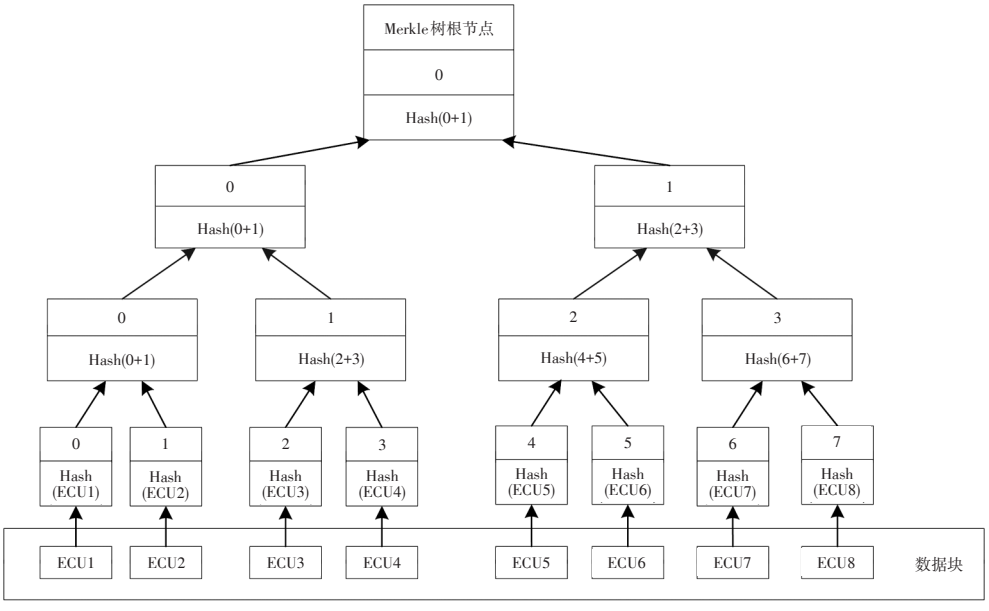

图3　Merkle树结构

若在车辆保养和维护中对ECU进行升级或更换，维修商可发起事务更新。VIMS接受更新后，对OBU的记录（区块）进行更新，RSU利用更新后的OBU区块进行车辆验证。具体流程如下：

a. 在车辆保养或维修后，维修商检索OBU中所有传感器的哈希值，并计算新的ECU Merkle树根节点值；

b. 创建更新事务，以反映在OBU上执行的动作，该事务中包括计算出的ECU的Merkle根值、动作时间戳、维修商签名，以及在车辆上实施动作类型的元数据描述字段；

c. 在VIMS框架中广播更新，由可信节点（交管部门和执法部门）验证更新发起方的签名；

d. 通过验证后，为该OBU创建更新区块，并在TAFS框架中广播。

3　交通事故自动取证系统框架

在发生交通事故时，通过TAFS完成交通事故自动取证。图1中的TAFS框架主要包括以下实体：

事故OBU：直接涉及交通事故的车辆。发生事故时，这些车辆首先向附近OBU和RSU发送安全性消息以通报事故，其后记录并保存其观察到的事故数据，供交通事故定责参考。

见证OBU：事故车辆通信范围内的其他车辆。接收事故OBU的通知消息，记录观察到的事故数据，并将数据发送至RSU，用于交通事故定责和信用评估。

RSU：接收来自事故OBU和见证OBU的事故相关数据，评估OBU传感器的完整性，基于评估结果更新车辆行为档案，并计算车辆的信用分。

交管部门：负责RSU的安装和维护。若在执行可靠性评估的过程中识别出恶意RSU，该信息将在区块链内广播，并由交管部门进行相应处理。

执法部门：处理交通事故时，执法人员接收来自区块链的辅助证据，基于信用分选择高可信度见证车辆，以保障交通事故定责的公正性。

信用管理系统：由RSU管理，保存RSU执行的完整性评估结果，提供车辆的可信度档案。

3.1 设计原理

TAFS采用RSU和OBU联合执行质询-响应机制，RSU执行完整性校验，确定车辆内部控制状态。发生交通事故时，当相关OBU进入RSU的无线通信范围时，RSU发送质询消息，要求OBU计算其ECU生成数据的哈希值。利用OBU应答，RSU检查区块链中的对应公钥，验证车辆合法性，并比较车辆应答数据和区块链内的数值，评估传感器的完整性。将数据保存到区块链前，为防止恶意RSU对OBU生成应答的更改，其他RSU执行数据可信分析，对OBU应答的完整性进行复评，将评估结果保存在区块链中，作为信用管理系统的基础。由此，RSU基于信用分对取证车辆进行排序，执法部门利用高信用分车辆的数据开展定责决策。

3.2 完整性评估

为确定车辆数据完整性，RSU向进入覆盖区域的OBU发送质询消息，要求车辆提供内部控制的部分或全部状态。车辆通过计算，选定ECU的哈希值及所有ECU的Merkle根值，并发送至RSU。RSU将该数值与保存在区块链中的数值进行比较，若数值一致，则认为车辆可信，否则将车辆视为恶意实体。

RSU和OBU之间的质询-应答（Questions-Answers，Q-A）数据交换为双签名事务：OBU进入RSU覆盖范围后，由RSU发起质询，OBU经计算完成应答。利用RSU和见证OBU验证事务完整性，基于哈希函数检测Q-A数据内容是否被篡改：

$$Q\text{-}A=[T_{ID}|Q|T_{S1}|K_{PR}|S_R|R|T_{ID}'|A_D|T_{S2}|K_{Pv}|S_v] \quad (2)$$

式中，Q为质询；A为应答；R为发起质询的RSU；T_{ID}为事务标识，即RSU生成的质询内容的哈希值；T_{S1}为质询生成时刻；K_{PR}为RSU公钥；S_R为RSU签名；T_{ID}'为OBU生成应答时的新事务标识，即车辆应答哈希值；A_D为OBU生成的事故数据；T_{S2}为应答生成时刻；K_{Pv}为OBU公钥；S_v为OBU签名。

假定被入侵的恶意RSU可更改车辆数据。在检查OBU数据可靠性后，由多个RSU对OBU生成的应答数据进行复评，确保数据一致性。

首先，RSU将事务保存在区块链之前，将多签名事务向其他RSU广播并请求验证。其他RSU通过签名和区块链公钥检查OBU合法性，并评估事务完整性，确保事务未被更改。利用事务哈希值重新计算T_{ID}'，并与事务中的T_{ID}'相比较。若数值一致，则复评通过；否则，意味着数据遭到篡改。其后，RSU对事务有效性进行投票。投票机制基于实用拜占庭容错（practical Byzantine Fault Tolerance，pBFT）协议[17]，若恶意RSU数量未达到投票RSU数量的1/3，即数值不一致的恶意RSU节点数量低于pBFT阈值，则事务成功通过验证并被保存到区块链中。由此，确保了多签名事务的数据完整性。

3.3 信用管理系统

为提高见证OBU的可信度，本文提出信用管理方案，跟踪车辆长期行为。基于完整性评估的结果判断OBU行为，通过历史评估结果评定OBU信用分。

首先，以保存在区块链上的Q-A完整性评估结果的历史记录为基础，在信用计算的输入中综合考虑车辆历史行为。

其次，引入时效权重α，提高车辆近期交互行为的影响，降低历史数据的影响。对于涉及到n个OBU的交通事故，基于事故现场不同车辆与RSU的完整性评估次数计算交互权重β。当前OBU的交互权重β为：

$$\beta=\frac{k_1}{k_1+k_2+k_3+\cdots+k_n} \quad (3)$$

式中，k_1为当前OBU与RSU的历史交互次数；k_2~k_n为该事故中涉及的其他OBU与RSU的历史交互次数。

每个OBU的整体信用分为：

$$R_o=(\sum_{i=1}^{k}\beta_i\cdot\alpha^{p-k}\cdot x)\log(k) \quad (4)$$

式中，β_i为加权因子；α^{p-k}为时效参数，用于降低历史交互的影响；k为OBU的交互次数；p为RSU的交互次数；x为当前Q-A完整性评估输出，若通过验证，则$x=x_{pos}>0$，否则$x=x_{neg}<0$，令$x_{pos}<|x_{neg}|$，以确保信用分更容易下降而非增加；x_{pos}、x_{neg}分别为评估成功参数、评估失败参数。

4 试验与分析

4.1 试验平台和仿真参数

为评估所提出的交通信息管理和自动取证系统架

构的性能，利用通用开放式研究模拟器（Common Open Research Emulator，CORE）[18]进行试验。硬件平台为Intel I5-9400 CPU，16 GB RAM，运行Linux系统。仿真参数为：x_{pos}=+1；x_{neg}=-2；哈希算法为SHA-256；时效因子α=0.97。每次与RSU成功交互并通过验证后，将OBU的信用分加1；验证不通过，则信用分减2。

4.2 系统可行性分析

首先分析该系统在实际交通运行中的可行性。评估场景包括多辆汽车（10~200辆），在基于区块链的网络中与5个RSU进行信息交换。先分析系统初始化的时间：基于制造商发送的创世事务信息为新出厂车辆创建区块的时间，其中包括接收连接请求、验证请求、创建区块和更新区块链的时间。表1所示为同时接收到不同数量的新出厂车辆时系统的处理速度，以及RSU对经过的不同数量的OBU进行质询-应答验证的耗时，结果取10轮验证的均值。对比方法分别为：文献[11]提出的基于区块链的交通事故取证方案，该方案采用车辆决策作为证据数据；文献[12]利用智能合约机制完成证据检索和证据链追溯的方案，通过令牌机制对数据进行访问控制。

表1 区块创建和质询验证耗时 ms

车辆数量/辆		10	25	50	100	200
区块创建时长	本文方法	16.25	16.61	16.82	17.01	18.13
	文献[11]方法	17.65	17.92	18.23	18.52	18.71
	文献[12]方法	105.17	112.83	145.01	162.91	191.38
Q-A验证耗时	本文方法	1.45	1.49	1.52	1.54	1.55
	文献[11]方法	1.57	1.62	1.68	1.73	1.78
	文献[12]方法	52.75	54.17	58.91	61.03	64.72

由表1可知：随车辆数量增加，区块创建时间呈线性增长，在最大汽车数量为200辆的场景下，本文方法的记录创建时间仅为18.13 ms，可满足实际交通应用需求；即使场景内车辆数量大幅增加，Q-A验证的实际耗时的增加依然非常小，在汽车数量为200辆的场景下仅为1.55 ms，这证明所提出的方法具有极好的可扩展性；文献[12]方法的耗时明显高于文献[11]和本文提出的方法的耗时。

综上，本文提出的方案通过基于许可区块链的去中心化交通信息管理系统确保车辆数据的完整性和可用性。在高密度事务区，传统区块链设计将事务分组，顺序插入事务，不能满足交通应用的效率要求。本文使用可追加区块概念，支持多个OBU同时将事务添加到不同区块，提高效率，在区块创建和质询-验证耗时方面得到了验证。

4.3 信用管理系统验证

首先分析RSU执行车辆信用计算的耗时。图4所示为随着出现在网络中的新车辆与RSU交互次数的增加，RSU计算车辆信用分的累积耗时。

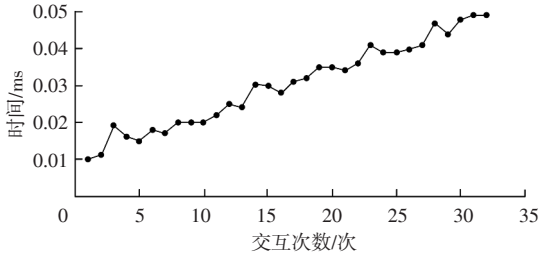

图4 信用分计算耗时

由图4可知：经过30次以上交互，RSU计算车辆信用分的累积耗时仍低于0.05 ms，证明了系统的实时性。

为观察车辆信用分随时间的变化情况，首先模拟车辆的恶意行为，并改变车辆与RSU的100次交互中验证失败次数的占比。图5所示为车辆信用分变化情况。

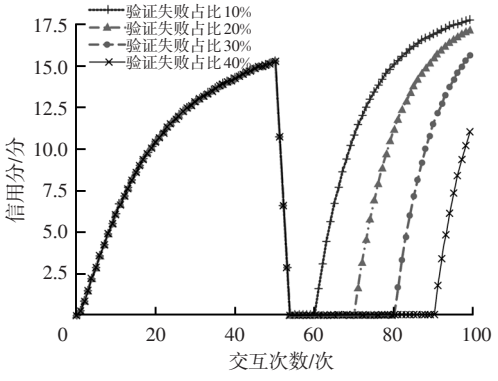

图5 车辆信用评估仿真结果

由图5可知：历史验证失败次数对车辆信用分造成了显著影响，证明了所提出的方案能确保取证数据的有效性。

4.4 安全性分析

4.4.1 攻击模型

为验证所提出方案的安全性，首先建立攻击模型，分析攻击者为篡改事故相关记录或车辆信用分记录发起的不同类型攻击。攻击方可能是恶意OBU或变节RSU，攻击手段列举如下：

a. 伪造数据攻击：恶意OBU通过篡改传感器数据向RSU发送假消息，达到混淆事实、逃避交通肇事责任的目的。该攻击中，恶意OBU包括事故OBU和与其串通的见证OBU。

b. 女巫攻击：OBU为车辆建立多个身份，生成来自多个实体的假消息并发送至RSU。通过多个伪造身份提供来自不同视角的事故虚假证据，增加执法部门定责难度，影响定责结果。

c. 信用分篡改攻击：恶意RSU提交错误的完整性评估结果，降低正常车辆的信用分，影响交通事故取证的公正性。

d. 数据操纵攻击：恶意RSU通过篡改或隐瞒正常车辆发送的数据，干扰执法部门对交通事故的公正定责。

4.4.2 安全验证

基于上述攻击模型，分析所提出方案中针对各种恶意行为的防御机制，验证方案的安全性：

a. 抵御伪造数据攻击：所提出的方案中，RSU执行可靠性评估，向进入覆盖范围的OBU发送质询消息，要求OBU计算其传感器的Merkle树（累积哈希值），以验证传感器的数据完整性。该数值保存在基于区块链的VIMS中，对RSU始终可用。车辆提供与区块链不一致的哈希值会造成验证失败，降低其信用分，证明该方案能够抵御伪造数据攻击。

b. 抵御女巫攻击：所提出的方案采用许可区块链技术，基于OBU公钥验证每个OBU身份，每个不同公钥对应区块链数据结构中的一个区块。只有可信节点（交管部门）有权限向车辆发放公钥，因此伪造的车辆身份无法记录在VIMS中，确保了系统内每个车辆的合法性，证明了该方案能够抵御女巫攻击。

c. 抵御信用分篡改攻击：所提出的方案中，将完整性评估结果保存在区块链之前，需要向其他RSU广播并请求验证。通过复评机制和基于pBFT的事务有效性投票，确保能够检测到恶意RSU节点对信用系统的任何篡改行为，证明了该方案能够抵御信用分篡改攻击。

d. 抵御数据操纵攻击：恶意RSU对数据的操纵行为，可能发生在存储前或存储后。所提出的方案通过完整性评估和复评机制确保了存储前数据的完整性。其后，将OBU生成的所有数据按时间顺序保存在区块链上，任何数据更改均会破坏区块链的一致性，确保存储后数据的不可篡改性，证明了该方案能够抵御恶意RSU的数据操纵攻击。

4.5 形式化验证

本文使用互联网安全敏感协议和应用的自动化验证（Automated Validation of Internet Security-sensitive Protocols and Applications，AVISPA）形式化分析攻击，证明所提出方案的安全性。AVISPA使用高级协议规范语言（High Level Protocol Specification Language，HLPSL）进行安全性验证。

所提出的方案中，当OBU进入RSU覆盖范围时，RSU向OBU发送质询消息Q，OBU给出应答A。其后，RSU验证OBU，并在区块链网络中广播，以供其他RSU进一步验证，确保保存在区块链上数据的端到端完整性。表2所示为形式化验证的符号。

表2 AVISPA建模符号

符号	描述	符号	描述
R	RSU节点	U	附近RSU节点
O	OBU节点	I	入侵者
B	区块链	K,K^{-1}	公钥和私钥对
Q	质询消息	K_I,K_I^{-1}	入侵者公钥和私钥对
A	应答消息	K_V,K_V^{-1}	车辆公钥和私钥对
B_{ID}	O在B中的保存地址	K_R,K_R^{-1}	RSU节点的公钥和私钥对

所提出的方案在AVISPA中的建模遵循以下步骤：

a. $R\rightarrow O:\left(\left(R.O.(Q).T_{ID}\right)_{K_V}\right)$

b. $O\rightarrow R:\left(\left(R.O.(A).T_{IDnew}\right)_{K_V^{-1}}\right)$

c. $R\rightarrow B:\left(\left(\left(R.B.(A).B_{IDnew}.K_V\right)_{K_R^{-1}}\right)_B\right)$

d. $B\rightarrow U:\left(\left(B.I.(A).B_{ID}\right)_U\right)$

e. $U\rightarrow B:\left(\left(U.B.(A).B_{IDnew}\right)_{K_I^{-1}}\right)$

步骤a，R利用公钥加密Q，并发送至O。本文方案中，R与V之间的交互为双签名事务，要求两方签名均有效。RSU发送的质询包括事务标识符T_{ID}，确保了R生成质询的完整性。步骤b，V提供包含ECU哈希值和事故数据的应答A，并计算代表Q和A的哈希值T_{IDnew}。步骤c，执行完整性评估后，R使用T_{IDnew}和B_{ID}为O计算B_{IDnew}。步骤d，R将多签名事务与B_{IDnew}在B中广播，以供U进行复评。步骤e，复评通过，U生成B_{IDnew}，实现端到端完整性，防止非法数据篡改。此外，R利用O生成的T_{IDnew}计算B_{IDnew}，由此可检测到恶意RSU所进行的数据篡改。以上结果证明所提出的方案能够抵御入侵者攻击。

5 结束语

本文提出了基于区块链和拜占庭容错机制的交通信息管理和事故取证平台方案，通过查询车辆内部传感器状态识别恶意节点，确保取证数据来自高度可信的车辆，以促进执法部门的公正定责。该方案不但对车辆数据完整性进行验证，而且确保数据不会被恶意RSU更改。试验结果表明，该方案能够抵御各种攻击，实现端到端的数据完整性校验，且处理速度能够满足交通应用的实时性需求。未来将考虑更多安全性方面的问题，如抵御执法部门的内部攻击，这可能需要为ECU增设更多的状态参数，并将更多实体行为信息存储在区块链中。

参 考 文 献

[1] MAAROUFI S, PIERRE S. BCOOL: A Novel Blockchain Congestion Control Architecture Using Dynamic Service Function Chaining and Machine Learning for Next Generation Vehicular Networks[J]. IEEE Access, 2021, 9(1): 53096-53122.

[2] 赵学刚. 交通事故现场警务取证区块化溯源分析方法[J]. 中国安全生产科学技术, 2020, 16(11): 172-177.
ZHAO X G. Analysis Method of Block Traceability for Police Evidence Collection at Traffic Accident Scene[J]. Journal of Safety Science and Technology, 2020, 16(11): 172-177.

[3] 李猛坤, 柯正轩, 于定荣, 等. 基于移动边缘计算的车联网车牌号码识别算法[J]. 计算机工程与设计, 2021, 42(11): 3151-3157.
LI M K, KE Z X, YU D R, et al. Vehicle License Plate Number Recognition Algorithm Based on Mobile Edge Calculation[J]. Computer Engineering and Design, 2021, 42(11): 3151-3157.

[4] LIU S, ZHANG Z J, YU Z H. Research on Liability Identification System of Road Traffic Accident[J]. Journal of Computers, 2022, 33(1): 215-224.

[5] SUMALEE A, HO H W. Smarter and More Connected: Future Intelligent Transportation System[J]. IATSS Research, 2018, 42(2): 67-71.

[6] 刘雪娇, 殷一丹, 陈蔚, 等. 基于区块链的车联网数据安全共享方案[J]. 浙江大学学报(工学版), 2021, 55(5): 957-965.
LIU X J, YIN Y D, CHEN W, et al. Secure Data Sharing Scheme in Internet of Vehicles Based on Blockchain[J]. Journal of Zhejiang University (Engineering Science), 2021, 55(5): 957-965.

[7] MATSUSHITA A, OKUBO T. Survey on Intrusion Detection System for Vehicle Security Techniques[J]. IEICE Technical Report, 2021, 120(1): 114-119.

[8] 任条娟, 郑佳莹, 陈友荣, 等. 基于区块链的车联网节点数据安全通信模型研究[J]. 汽车技术, 2021(5): 30-35.
REN T J, ZHENG J Y, CHEN Y R, et al. Research on Data Security Communication Model for IoVs Nodes Based on Blockchain[J]. Automobile Technology, 2021(5): 30-35.

[9] FRAGA-LAMAS P, FERNANDEZ-CARAMES T M. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry[J]. IEEE Access, 2019, 7(1): 17578-17598.

[10] OHAM C, JURDAK R, KANHERE S S, et al. B-FICA: Blockchain Based Framework for Auto-Insurance Claim and Adjudication[C]// 2018 IEEE International Conference on Internet of Things (iThings). Halifax, NS, Canada: IEEE, 2018: 1171-1180.

[11] CEBE M, ERDIN E, AKKAYA K, et al. Block4forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles[J]. IEEE Communications Magazine, 2018, 56(10): 50-57.

[12] 陈葳葳, 曹利, 顾翔. 基于区块链的车联网电子取证模型[J]. 计算机应用, 2021, 41(7): 1989-1995.
CHEN W W, CAO L, GU X. E-Forensics Model for Internet of Vehicles Based on Blockchain[J]. Journal of Computer Applications, 2021, 41(7): 1989-1995.

[13] PENG C R, WU C, GAO L M, et al. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues[J]. Sensors, 2020, 20(18): 5079-5115.

[14] 李烁, 马云飞, 谢谨. 基于Wi-Fi入射信号到达角超分辨率估计的无源车速测量[J]. 仪器仪表学报, 2020, 41(10): 268-276.
LI S, MA Y F, XIE J. Device-Free Vehicle Speed Estimation Based on Ultra-Resolution Estimation of Arrival Angle of Wi-Fi Incident Signal[J]. Chinese Journal of Scientific Instrument, 2020, 41(10): 268-276.

[15] MICHELIN R A, DORRI A, STEGER M, et al. SpeedyChain: A Framework for Decoupling Data from Blockchain for Smart Cities[C]// 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. New York City, NY, USA: IEEE, 2018: 145-154.

[16] 王杨, 黄少芬, 许闪闪, 等. 基于Merkle哈希树的机会社会网络节点协作转发机制[J]. 小型微型计算机系统, 2019, 40(7): 1462-1467.
WANG Y, HUANG S F, XU S S, et al. Opportunity Social Network Node Cooperation Forwarding Mechanism Based on Merkle Hash Tree[J]. Journal of Chinese Computer Systems, 2019, 40(7): 1462-1467.

[17] XU X, SUN G, YU H. An Efficient Blockchain PBFT Consensus Protocol in Energy Constrained IoT Applications [C]// 2021 International Conference on UK-China Emerging Technologies (UCET). Chengdu, China: IEEE, 2021: 152-157.

[18] OHAM C, MICHELIN R A, JURDAK R, et al. B-FERL: Blockchain Based Framework for Securing Smart Vehicles [J]. Information Processing & Management, 2021, 58(1): 1-11.

(责任编辑 斛 畔)

修改稿收到日期为2022年10月5日。