DOI:10.14188/j.1671-8844.2025.0214 文章编号:1671-8844(XXXX)XX-0001-15

基于双区块链的VANETs隐私保护认证方案

陈雷

(中国刑事警察学院公安信息技术与情报学院,辽宁 沈阳 110854)

摘要: 针对VANETs中认证开销大与隐私泄露风险等问题,提出一种融合联盟链与私有链的双区块链隐私保护认证方案,并引入短签名与部分同态加密技术,以兼顾系统的安全性、效率与隐私保护。安全性分析表明,该方案具备良好的隐私防护能力和抵御多种攻击的能力。仿真结果也进一步验证了本方案在计算和通信损耗方面的低负载特性,并在认证延迟、数据丢失率和系统吞吐量等指标上优于现有方案。

关键词: 车载自组网络;双区块链;隐私保护;身份验证

中图分类号: TN 929.53 **文献标志码:** A

A Privacy-preserving authentication scheme for VANETs based on dual blockchain architecture

CHEN Lei

(School of Public Security Information Technology and Intelligence, Criminal Investigation Police University of China, Shenyang 110854, China)

Abstract: To address issues like high authentication costs and risks of privacy leakage in VANETs, this paper proposes a dual-blockchain privacy-preserving authentication scheme that integrates consortium and private blockchains. The scheme also incorporates short signature and somewhat homomorphic encryption techniques to balance security, efficiency, and privacy protection. Security analysis demonstrates that the proposed scheme offers strong privacy preservation and resilience against various attacks. Simulation results further confirm that the scheme imposes low computational and communication overhead, and outperforms existing solutions in terms of authentication delay, packet loss rate, and system throughput.

Key words: vehicular ad hoc networks; dual blockchain; privacy-preserving; authentication

1 背景

众所周知,典型的VANETs是一个集成的开放异构网络,它通过商定的通信协议和数据交换标准在实体之间进行通信。如图1所示,典型的VANETs主要由三个实体组成:可信机构(Trusted Authority, TA)、路侧单元(Roadside Unit, RSU)和车载单元(Onboard Unit, OBU)。作为物联网(Internet of Things, IoT)的经典变体,VANETs旨在通过移动互联网收集和共享有关车辆的信息,实现

收稿日期: 2025-06-11

作者简介: 陈雷,男,副教授,硕士生导师,主要从事车联网安全、物理层安全传输、资源分配等方面的研究,E-mail:807175471@qq.com。

基金项目: 中国刑事警察学院重大培育项目(编号:D2023002);辽宁省教育厅科学研究项目(编号:ZGXJ2020005);中国刑事警察学院校级项目(编号:D2022045);2026年度辽宁省应用基础研究项目

本文引用格式: 陈雷.基于双区块链的VANETs隐私保护认证方案[J].武汉大学学报(工学版),XXXX,XX(XX):1-15.

Citation: CHEN Lei.A Privacy-preserving authentication scheme for VANETs based on dual blockchain architecture[J].Engineering Journal of Wuhan University,XXXX,XX(XX):1-15.

车辆与基础设施(Vehicle to Infrastructure, V2I)、车辆与车辆(Vehicle to Vehicle, V2V)、可信机构与路侧单元(Trusted Authority to RSU, T2R)、车辆与第三方服务提供商之间的通信,为人们带来更智能、更安全的汽车服务[1]。RSU分别部署在城市街道和高速公路上,由于RSU处在开放的地理环境中缺乏安全保护,因此其被攻击者入侵的成功率很高[2]。此外,如何在开放的信息传输环境中确保通信安全和用户隐私安全也需要仔细考虑。VANETs作为智能交通系统的关键支撑技术,其具备节点高速移动、社交互动频繁、网络连接动态变化以及通信实时性强等显著特征。然而,正是这些特性导致VANETs在开放环境中更易遭受安全威胁,如伪装攻击、重放攻击、身份盗用等,严重影响了网络的稳定性与数据的可信性。因此,如何在保障通信效率的同时增强系统的安全性与隐私保护,成为当前研究的重点方向。

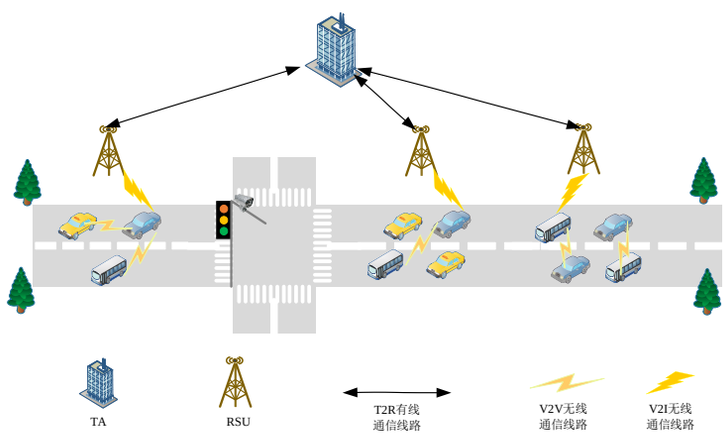


图1 典型的VANETs通信架构

Fig.1 A typical structure of VAENTs

身份验证和隐私保护被认为是解决VANETs安全问题的关键挑战,传统的处理方案大致分为:基于密码学、基于身份的数字签名和基于消息的身份批量验证方案[3-14]。基于密码学的认证方案由于采用的加密机制都依赖于TA,因此存在潜在的安全隐患;而混合加密机制虽试图在安全性与效率间取得平衡,但在实际应用中仍难以有效控制计算与通信的总体开销。基于身份的数字签名方案可以保障数据的完整性,但在进行数字签名时一般采用长签名的方式,因此增加了过多的计算和通信开销。相较之下,基于消息的身份批量验证方案在提升认证效率方面表现优越,但在隐私保护方面依然存在不足,难以满足VANETs对高隐私保障的需求。

近年来,随着区块链技术的飞速发展,将区块链技术引入VANETs中就成为研究的热点。新兴的区块链技术提供了一个由整个网络节点共同维护的去中心化、安全可靠的数据库,为解决与VANETs相关的问题提供了新的见解[15-18]。目前,大多数研究VANETs中基于区块链的身份验证与隐私保护方案,多是在单链架构下进行的分析,虽然在提升系统安全性方面表现突出,但在车辆与RSU之间的通信效率方面仍显不足,同时区块链数据的公开透明特性也增加了用户隐私泄露的风险。然而,在不断变化的环境中,不可能简单地采用过去的传统单链的车辆网络架构来适应新的复杂性。因此,需要新的方案来寻求突破。为提升区块链技术在VANETs中的适用性与安全性能,本文提出了一种基于双链架构的隐私保护认证方案,该方案中设计了七个关键流程模块。同时,本文又分别提出了短签名和部分同态加密机制,来减少签名开销和保护数据隐私。

2 相关研究

本文将综述当前在隐私保护认证方面的相关研究成果,重点涵盖基于密码学方法、基于身份的数字签名技术以及基于区块链机制的认证方案。

1) 基于密码学的隐私保护认证方案[3-6]

文献[3]提出了采用混合密码学即车辆对基础设施采用非对称密码学,车辆对车辆采用对称哈希消息认证码的隐私保护认证方案。然而,该方案对消息进行认证时需要消耗额外的开销和增加了时间复杂性。文献[4]提出了一种基于消息认证码的VANETs匿名条件隐私保护认证方案。该方案下

车辆可以在相互认证阶段后获得用于消息生成和认证的组密钥。然而,该方案由于采用对称加密的方式,因此容易受到多种安全攻击的威胁。为了解决这个问题,文献[5]提出了利用切比雪夫混沌映射来保护V2I之间的通信,该方案将对称密钥加密与公钥签名相结合,来满足方案的轻量级和数据传输时的完整性保护。然而,该方案中采用的双线性配对法增加了隐私保护方案的复杂性。文献[6]提出一种用于车载云的隐私保护和数据安全传播方案,该方案采用车辆的公钥作为其假名,从而消除了证书管理机构。在地理位置相近的车辆间通过采用非对称组密钥协商协议,来实现匿名安全的通信。然而,该方案没有考虑对恶意车辆身份披露的问题。

2)基于身份的数字签名的隐私保护认证方案[7-10]

文献[7]提出通过设置区域信任权限,来为车辆提供匿名身份验证服务,同时采用群签名机制来实现匿名和条件隐私。然而,该方案采用集中的机构,容易出现单点故障影响整个网络的问题。针对集中式的机构带来的弊端,文献[8]通过分散的组认证协议有效地应对集中认证的问题,该方案有效地利用了车辆的机动性、行驶道路的限制和RSU分布的特性,通过为每个RSU在其通信范围内维护和管理一个实时组来提供匿名身份验证服务。然而,RSU的安全问题没有被考虑。文献[9]提出利用基于身份的密码系统和环签名方法来实现条件隐私保护方案,其中消息发布者通过环签名方法来实现匿名信息的可靠发布。然而,该方案没有考虑如何披露恶意车辆的身份问题。文献[10]中的方案使用基于环签名的条件隐私保护认证方案来确保安全的消息认证和可追溯性。发送方在传输安全消息的同时附加其假名和环签名,接收方则通过假名识别并验证发送者身份,并利用环签名机制验证消息的合法性与完整性。

3)基于消息认证的隐私保护认证方案[11-14]

文献[11]提出了一种高效的匿名消息批量认证和密钥交换方案来减轻RSU的认证负担。然而,该方案中的公钥容易遭受攻击。文献[12]通过分析伪造位置信息的安全问题,提出使用位置验证技术来防止节点传播虚假位置信息,以减轻虚假攻击的影响。文献[13]提出了一种基于无证书签名的单消息协同认证方案,该方案会根据一定的概率直接选择车辆进行消息签名验证。文献[14]基于车辆身份的聚合签名技术,提出了一种分布式聚合隐私保护的消息认证方案,该方案可同时验证许多消息,并可以将它们的签名压缩到一个消息中,进而大大减少了车辆所需的存储空间。

4)基于区块链的隐私保护身份认证方案[15-18]

文献[15]提出基于区块链技术的一种可追溯和分散的车联网系统框架,以实现车辆与RSU之间的安全认证访问方案,该方案防止车辆广播伪造信息和保护车辆隐私免受追踪攻击,同时该方案实现了条件隐私,可以在匿名公告中追踪恶意车辆的真实身份。然而,该方案无法抵抗证书颁发机构受攻击的问题。文献[16]提出了一种基于区块链的VANETs去中心化的密钥管理机制来实现用户公钥的注册、更新和撤销。同时又提出了互认证模式下的轻量级密钥协商协议,该协议可以防止分布式拒绝服务(Distributed Denial of Service, DDoS)攻击、公钥篡改等多种攻击。然而,该方案中密钥管理和密钥的更新和撤销复杂度较高,实时性较差。文献[17]提出利用生物识别的区块链框架,来确保VANETs中车辆间的数据安全共享,在所提出的框架中,利用生物特征信息来记录发送者的真实身份,从而保护用户的隐私,同时该方案还可在需要时能够追踪用户的身份。然而,生物特征的采集和更新延迟较大因此很难应用于实际的VANETs场景中。文献[18]提出了一种基于区块链的VANETs隐私保护认证方案,其中采用Merkle Patricia树存储用户身份,同时提供了一种没有撤销列表的分布式身份验证方案,然而,该方案存储用户身份需要较多的计算消耗。

如前所述,现有方案普遍存在对第三方集中式机构的过度依赖,导致其在防御攻击方面效果有限。尤其是考虑到RSU由于地理位置固定,往往成为攻击的重点目标。现有文献对于隐私和安全问题尚未给出有效的解决方案,且随着车辆数量的增加,VANETs中的计算负载和通信开销等问题将更加严重。因此,本文提出了基于双区块链的VANETs隐私保护认证方案。该方案巧妙融合了联盟链与私有链的优势,实现去中心化管理的同时,减轻了节点间通信压力,有效防范了单一RSU被攻破的风险。此外,方案采用短签名和部分同态加密技术,既提升了实体间通信的效率,又保障了隐私数据的安全传输。

3 系统模型和安全要求

3.1 系统模型

本文所述框架的网络模型采用三层架构,如图2所示。顶层由TA与联盟链构成;中间层由所有RSU组成联盟链;底层则由携带OBU的车辆及私有链组成。接下来,本文将详细定义该网络模型中的三类参与主体。

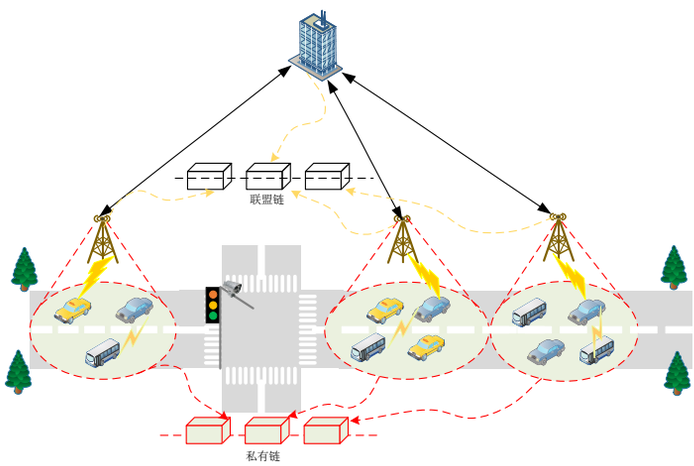


图2 联盟链结合私有链的VANETs架构

Fig.2 The proposed consortium blockchains combined with private blockchains structure of VANETs

1)TA:是智能交通服务提供商,同时也负责管理整个VANETs。该实体有足够的内存和计算能力,并受到VANETs中所有参与者的信任。TA负责为所有用户生成匿名身份、公钥和私钥,并通过智能合约上传相关数据。此外,它可以追踪用户的真实身份和拥有撤销恶意用户的权限。TA同时还负责整个VANETs的初始化、智能合约的部署、车辆的注册等工作。

2)RSU:该实体位于路边,作为TA与车辆之间的中介。RSU通过专用短程通信(Dedicated Short Range Communication, DSRC)协议可以实现与周围车辆的连接,同时RSU之间、RSU与TA之间采用有线连接的方式进行通信。同时RSU作为VANETs的中间实体,还能够调用智能合约来更新区块链中的车辆信息。

3)OBU:是每辆车辆必备的设备,其通过DSRC协议接收来自车辆或RSU的消息并进行验证,同时OBU是一个轻量级节点,只需要存储私有链中的区块头。作为模型的底层,相比之下具有最小的计算和存储资源,车辆作为私有链成员参与维护区块链。

3.2 安全要求

1)单次注册:为提升用户体验,VANETs认证方案应支持车辆只需注册一次,注册信息随后可在网络中被其他参与方共享和使用。

2)身份认证与消息验证:仅经过身份认证的车辆才能接入系统并进行安全通信。为保证消息的可信度,RSU和车辆需验证消息发送者的身份合法性、消息的时效性及完整性,确保接收信息的可靠性。同时,必须及时检测并撤销存在恶意行为的车辆。

3)隐私保护:网络中参与的车辆隐私信息必须得到严格保护,RSU及其他车辆不得获知车辆的真实身份,任何对手也无法通过截获和分析通信内容追踪车辆的真实身份。

4)可追溯性:一旦出现恶意行为,如伪造或篡改安全消息,TA应具备有效手段追踪并识别车辆的真实身份。

5)不可关联性:为避免攻击者获取车辆的轨迹信息,系统应确保无法将多条不同的信息关联到同一辆车上。

6)抗攻击能力:鉴于VANETs节点间通过开放共享的无线信道进行通信,因此需要系统需具备抗离线密码猜测攻击、重放攻击、女巫攻击及DDoS攻击的能力。

4 构建双区块链

4.1 区块链基础

区块链的去中心化、防篡改和可追溯性与VANETs的安全需求相吻合,在VANETs中应用的区块链主要分为公有链、联盟链和私有链[19]。公有链具有完全去中心化的特点,任何节点都可以参

与其中，但由于公有链可扩展性和隐私性较差，因此它无法满足VANETs的应用需求[20]。联盟链具有部分去中心化的特点，经过授权的节点才可以参与其中，并且对联盟链数据的操作也需要不同的授权才可进行。私有链是一种封闭式网络，其参与者受到严格控制，只有授权的节点才可以加入网络并进行交易。私有链的交易速度通常非常快、费用较低且隐私性更强。共识机制通常使用实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）机制，它与工作量证明或权益证明等机制相比，需要较少的计算能力来确保交易安全。本文采用PBFT共识机制，该机制与工作量证明共识机制或权益证明共识机制相比，在保证交易安全的同时，所需计算资源更少[21]。

4.2 构建双区块链

本文提出了上层采用联盟链和下层采用私有链的双区块链结构，同时通过智能合约进行管理。

1）双区块链结构：在本文的网络模型中，上层采用联盟链以强化访问控制与安全保障。TA作为矿工负责维护车辆间的一系列关联关系数据，TA拥有智能合约的部署、插入、更新及撤销权限，其他受信任的RSU作为联盟链上的共识节点可以访问链上数据。所有交易和智能合约的更新均由TA验证，当验证通过后，RSU利用PBFT共识机制将区块上传至联盟链。底层采用私有链提供快速服务与提高通信效率，RSU作为矿工负责维护车辆假名和车辆公钥的关联数据，而车辆作为共识节点参与网络共识。车辆间及车辆与基础设施间的交易均被记录在私有链上，所有授权节点均可查询私有链上的车辆假名和公钥信息。

2）智能合约：如图3所示，在私有链中，智能合约加载第i辆车辆V_i的假名PID_i与公钥V_{pk_i}对应关系表（Vehicle Pseudonym identity and Public key Table，VPPT），用于集中管理所有车辆当前的假名身份及其公钥，并能自动且及时响应车辆公钥查询请求。如图4所示，在联盟链中，智能合约则加载包含车辆真实身份VID_i、假名身份PID_i及其公钥V_{pk_i}和私钥sk_i信息的表（Vehicle Real identity and Pseudonym identity and Public key and Private key Table，VRPPPT），该表作为$\mathrm{VID}_i-\mathrm{PID}_i-V_{pk_i}-\mathrm{sk}_i-t_i$关联映射，整合所有车辆信息并为联盟链中的RSU节点提供服务。

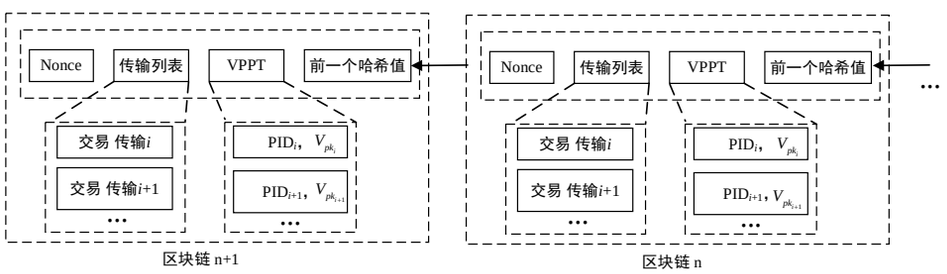


图3 私有链的区块结构

Fig.3 Block structure of the consortium blockchain

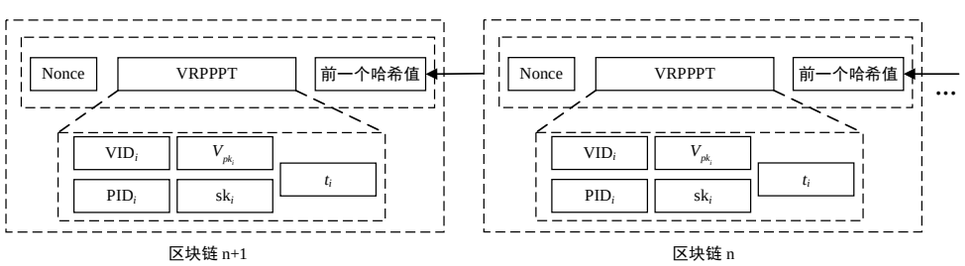


图4 联盟链的区块结构

Fig.4 Block structure of the consortium blockchain

3）双区块链之间的数据同步机制：私有链上，车辆产生的数据被打包进区块。系统会定期计算该时间段内私有链所有交易哈希的Merkle树的根哈希。私有链的一个授权节点将计算出的Merkle根哈希作为一条交易，调用联盟链上的一个特定的锚点智能合约。这条交易在联盟链上经过共识验证后，被永久地记录在联盟链的区块中。同理，联盟链也采用该机制将数据同步到私有链中。

4)智能合约的调用流程:在双链架构下,智能合约的调用是一个“私有链处理、事件触发、跨链验证、联盟链仲裁、状态同步”的协同过程。第一阶段:私有链内数据聚会参与计算。车辆采集数据并定期签名后作为作为交易,调用私有链上的智能合约。第二阶段:事件触发与中继捕获。当智能合约计算出某车的评分达到标准时,会触发一个链上事件,该事件包含车辆标识和必要的证明信息。一个负责双链通信的中继器一直监听私有链上的特定事件,一旦捕获到事件,它就把此事件中的信息作为参数,准备发起对联盟链的调用。第三阶段:跨链调用与联盟链验证。中继器在联盟链上发起一笔交易,调用联盟链上的智能合约。这笔交易中包含了从私有链事件中获取的参数。联盟链合约验证传来的Merkle证明是否与之前由私有链锚定在联盟链上的Merkle根相匹配,以确保数据的真实性和未被篡改。第四阶段:状态同步与回调。中继器同样监听联盟链上的事件。当捕获到某事件后,它可以在私有链上发起一笔回调交易。此调用会重置该车辆的行为评分,从而完成一个闭环的状态同步,确保双链状态最终一致。

5)车辆在双链间身份映射关系:在联盟链上建立全局、唯一的“真实身份”,在私有链上使用局部的、用于高频交易的“假名身份”。身份分层模型中,第一层:联盟链上的“真实身份”,通常是车辆的全球唯一标识符。第二层:私有链上的“假名身份”,通常是一个临时生成的假名或地址。身份映射的建立与验证机制:建立映射关系,通过数字签名与注册。首先车辆生成一对新的公私钥,车辆使用真实身份对应的私钥进行签名,创建一个“身份声明”。车辆将这份签名后的声明作为交易,提交到私有链上的身份管理合约。合约会验证该签名是否确实来自联盟链上已注册的车辆。验证通过后,私有链上就建立了车辆与假名身份的映射关系,并记录在合约状态中。

4.3 车辆撤销算法

在本文提出的隐私保护认证方案中,利用智能合约来管理联盟链上的VRPPPT。如算法1所示,该智能合约会根据VANETs中交通情况预先设定车辆撤销阈值,若车辆收到用户投诉,经过节点共识确认后,智能合约会将该车辆的投诉记录登记入链。随后,TA或RSU可通过智能合约查询该车辆的投诉次数是否已达到撤销阈值,若满足条件,智能合约自动执行车辆撤销操作,并将撤销结果同步通知联盟链中的所有节点。

算法1:车辆撤销算法

输入:用户车辆假名,车辆ID,用户地址,投诉计数器值,目标阈值
输出:阈值设置结果,投诉结果,车辆撤销结果
1:要求(车辆ID的状态为真);
2:if消息的发送者不是TA,这时
3:丢弃该消息;
4:end if;
5:映射响应[用户车辆假名]=车辆ID;
6:if实体阈值设置成功
7:返回 正确;
8:else
9:返回 错误;
10:end if;
11:if消息的发送者不是TA或RSU,这时
12:丢弃该消息;
13:end if;
14:当前计数器值=原有计数器值+投诉计数器值;
15:映射投诉者[用户地址]=当前计数器值;
16:返回投诉结果给消息发送者;
17:if当前计数器值≥映射响应[目标阈值]。then
18:删除VRPPPT中车辆的各种信息;
19:返回撤销结果给消息发送者
20:end if;

4.4 共识机制

在所提出的方案中,本文采用PBFT共识机制进行区块共识。如图5所示,联盟链中由TA担任矿工节点,可信RSU作为共识节点;而在私有链中,RSU充当矿工角色,车辆则作为共识节点参与共识。共识流程如下:首先,在广播数据块阶段,矿工节点(RSU或TA)签名需要共识的数据块并进行广播;其次,在数据块有效性验证阶段,共识节点(车辆或可信RSU)接收并验证这些数据块的签名和有效性,如果验证通过则将验证结果签名并发送给其他共识节点;再次,在一致性比较阶段,共识节点对收到的其他共识节点上反馈的结果和一致性进行比较,并将最终结果反馈给矿工。再次,在矿工节点处当至少三分之二的共识节点达成一致同意该数据块时,该数据块才能被写入区块链。最后,在存储数据块阶段,在联盟链和私有链中的TA和RSU保持完整区块链数据进行存储,而车辆作为轻节点仅保存用于数据查询与身份验证的区块头信息。

4.5 椭圆曲线密码体制(Elliptic Curve Cryptosystem, ECC)

基于有限域上椭圆曲线有理点群的密码系统称为椭圆曲线密码系统[22],它所采用的椭圆曲线技术具有存储需求低、安全性能强和计算负担轻的优

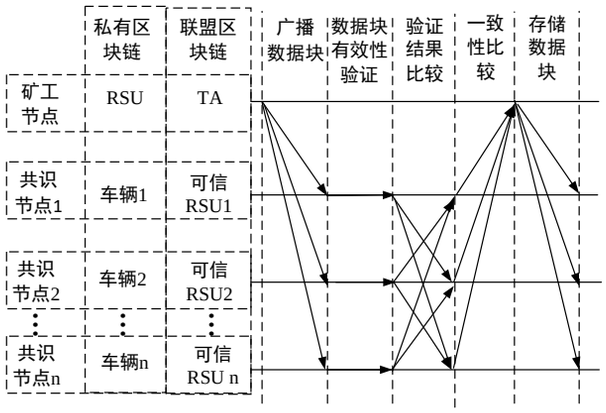


图5 区块链共识过程

Fig.5 Consensus process on blockchain

点,ECC相关定义如下。

素数有限域F_p上的椭圆曲线E是一个有限循环群,满足$y^2=x^3+ax+b \bmod p$,其中$a,b\in F_p$,$4a^3+27b^2\neq 0$,a和b是小于p的两个非负整数。在椭圆曲线E上,假设一个无穷远的点O和其他一些点,即P、R和Q,组成由P生成的一个q阶加性椭圆曲线群G,在ECC中,群G具有如下性质:

1)椭圆曲线上的点加法:给定椭圆曲线E上的两个点$P=(x_1,y_1)$和$Q=(x_2,y_2)$,它们的和$R=P+Q$是同一椭圆曲线上的另一个点,对于该点坐标(x_3,y_3)可以使用下列公式计算:$x_3=\lambda^2-x_1-x_2$,$y_3=\lambda(x_1-x_3)-y_1$,其中

$$\lambda=\begin{cases}(y_2-y_1)/(x_2-x_1), & \text{如果 } P\neq Q\\ (3x_1^2+a)/2y_1, & \text{如果 } P=Q\end{cases} \tag{1}$$

2)椭圆曲线上的乘法:乘法涉及多次执行点加法。在椭圆曲线上给定一个点P和另一个整数k,点乘运算决定结果kP。乘法公式为$kP=P+P+\ldots+P(k\text{次})$。

5 提出的方案

5.1 部分同态加密

本文需要对VANETs系统中的实体间传递的数据进行部分同态加密操作,部分同态加密由密钥生成、加密和解密三部分组成。与全同态加密支持任意次的加法和乘法运算不同,部分同态加密可同时支持有限次数的加法和乘法运算。全同态加密由于需要消耗更多的计算资源因此在实际VANETs系统中使用受限,而部分同态加密由于计算量相对较小,因此更适合于实际VANETs系统。

1)密钥生成:基于素数p和q,令$n=pq$,$\lambda'=lcm(p-1,q-1)=(p-1)(q-1)/2$。$lcm$表示最小公倍数,这时定义$\varphi=\left[L\left(g^{\lambda'} \bmod n^2\right)\right]^{-1} \bmod n$,其中$L(\chi)=(\chi-1)/n$和随机选取一个整数$g=(n+1)\in\mathbb{Z}_{n^2}^*$,公钥是$(n,g)$,私钥是$(\lambda',\varphi)$。

2)加密操作E:对于消息$0\leqslant m\leqslant n$,选择随机数$r\in\mathbb{Z}_n^*$且$0\leqslant r\leqslant n$,密文可以通过公式(2)计算。

$$c=E(m,r)=g^m r^n \bmod n^2 \tag{2}$$

3)解密操作D:给定密文$c\in\mathbb{Z}_{n^2}^*$,消息能通过公式(3)进行解密。

$$m=D(c)=L\left(c^{\lambda'} \bmod n^2\right)\varphi \bmod n \tag{3}$$

两种同态性质如下:

1)同态加法:$c=c_1\oplus c_2=c_1\cdot c_2 \bmod n^2$,其中$c_1$和$c_2$为密文。

2)同态标量乘法:$c=m\otimes c_1=c_1^m \bmod n^2$,其中$c_1$为密文,$m$为明文。

5.2 短签名机制

车辆V_i选择一个随机数$\mu_i\in\mathbb{Z}_q^*$,并设置它的私钥$sk_i=\{\mu_i,\lambda_i\}$,其中$\lambda_i=(k_i+\theta_i\beta) \bmod q$,随机数$k_i,\beta\in\mathbb{Z}_q^*$,$\theta_i=H_1(PID_i,U_i,P_{pub})$,$U_i=k_i\cdot P$,其中哈希函数$H_1:G\times\{0,1\}^{\pi}\times G\times G\rightarrow\mathbb{Z}_q^*$。令$X_i=\mu_i\cdot P_{pub}$,$Y_i=\lambda_i\cdot P_{pub}$,其中$P_{pub}$为系统公钥。这时车辆的公钥$V_{pk_i}=\{X_i+Y_i\}$。车辆$V_i$对消息$m_i$做如下短签名操作:

1) 选择随机数$r_i\in\mathbb{Z}_q^*$

2) 计算$R_i=r_i\cdot P_{pub}$

3)计算$\alpha_i=H_2(PID_i,R_i,m_i,t_i)$,其中哈希函数$H_2:\{0,1\}^*\times G\times\{0,1\}^{\pi}\times G\times G\times G\rightarrow\mathbb{Z}_q^*$为随机密钥的单向通用哈希函数。$\pi$表示固定比特数。

4)计算$\eta_i=\alpha_i(r_i+\mu_i+\lambda_i) \bmod q$。

5)在消息m_i上设置签名$Sig_i=\{\eta_i,R_i\}$,传递消息签名组$\{m_i,PID_i,V_{pk_i},Sig_i,t_i\}$给接收端。

车辆V_j对接收到来自车辆V_i的消息签名组$\{m_i,PID_i,V_{pk_i},Sig_i,t_i\}$,在时间戳$t_i$有效的情况下做如下签名验证操作:

1)首先计算$\alpha_i=H_2(PID_i,R_i,m_i,t_i)$

2)如果验证签名Sig_i有效。则车辆V_j接受消息m_i。否则车辆V_j拒绝该消息。验证签名Sig_i可通过公式(4)

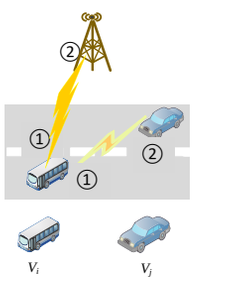
$$\eta_i\cdot P_{pub}=\alpha_i(R_i+V_{pk_i}) \tag{4}$$

签名验证正确性证明:公式(5)可以通过以下

证明。

$$\begin{aligned}\eta_i \cdot P_{pub} &= \alpha_i\left(r_i+\mu_i+\lambda_i\right)P_{pub}\\ &= \alpha_i\left(r_i \cdot P_{pub}+\mu_i \cdot P_{pub}+\lambda_i \cdot P_{pub}\right)\\ &= \alpha_i\left(R_i+X_i+Y_i\right)\\ &= \alpha_i\left(R_i+V_{pk_i}\right)\end{aligned} \tag{5}$$

本文提出的短签名机制的过程如图6所示。



① 发送端对消息进行短签名

② 接收端对消息签名进行验证

图6 短签名机制过程

Fig 6 The process for the short signature mechanism

下面将对本文提出的方案进行详细说明。该方案包括:系统初始化、区块链智能合约部署、车辆注册、车辆登录与身份验证、车辆假名身份更新、车辆撤销以及车辆密码修改共七个模块。需要特别强调的是,方案中的所有信息传输均采用部分同态加密技术进行保护。

5.3 系统初始化

TA首先生成系统参数$\text{para}_{ecc}=\left\{q,a,b,Z_q^*,n,P,P_{pub},H_0,H_1,H_2\right\}$,并在车辆注册阶段TA分享该参数给车辆。在对ECC的初始化中,定义方程$y^2=x^3+ax+b \bmod q$的非奇异椭圆曲线E,在有限域$\text{F}_p\left(q,a,b\right)\in\text{F}_{p'}$内满足$4a^3+27b^2\neq 0$。$P$是$n$阶加法群G的生成器,它由E上的所有点和无穷远$O$处的点组成,系统公钥$P_{pub}=s \cdot P$和系统私钥$s\in Z_q^*$,其中哈希函数$H_0:\text{G}\times\{0,1\}^{\pi}\times\text{G}\rightarrow Z_q^*$,$H_1:\text{G}\times\{0,1\}^{\pi}\times\text{G}\times\text{G}\rightarrow Z_q^*$,$H_2:\{0,1\}^{*}\times\text{G}\times\{0,1\}^{\pi}\times\text{G}\times\text{G}\times\text{G}\rightarrow Z_q^*$,$\pi$表示固定比特数。这三个函数为单向通用哈希函数。

5.4 区块链智能合约部署

网络模型的上层使用联盟链存储VRPPPT,并由TA作为矿工管理联盟链。区块通过联盟链节点的共识过程进行验证,然后TA调用智能合约将交易记录到联盟链中。本文假设TA和部分可信RSU作为联盟链节点协同工作,并赋予这一方可信RSU联盟链结点查询联盟链的权限。网络模型的底层支持以RSU为矿工的私有链存储VPPT,并记录VANETs间的车辆与车辆、车辆与RSU之间的交易,然后,RSU调用智能合约将交易记录到私有链中。

5.5 车辆注册

所有车辆用户在进行通信前需先在TA中进行登记以获取必要的身份认证信息,该过程在安全通道内完成,且TA在此阶段处于离线状态。

首先,在车辆收到系统参数para_{ecc}后,车辆用户V_i利用其真实身份VID_i、密码pw和随机数b_i计算$B_i=H_0\left(\text{pw},b_i\right)$。然后将$\text{VID}_i$与$B_i$一起返回给TA。

其次,TA在收到VID_i和B_i后,为该辆车计算假名身份集$\text{PID}_i=\text{VID}_i\oplus H_1\left(\text{sk}_i \cdot P_{pub}\right)$,其中车辆的私钥$\text{sk}_i=\left\{\mu_i,\lambda_i\right\}$,车辆公钥$V_{pk_i}=\left\{X_i+Y_i\right\}$。TA选择随机数$e_i\in Z_q^*$,并计算$A_i=H_0\left(x,e_i\right)$、$C_i=A_i\oplus B_i$和$D_i=H_0\left(\text{VID}_i,B_i,A_i\right)$。

最后,TA将参数集合$\left\{C_i,D_i,e_i,H_0,q,Z_q^*,\text{para}_{ecc},\text{VID}_i,\text{PID}_i,t_i\right\}$通过安全通道,加载到车辆的OBU中,$\text{PID}_1$作为该车辆的第一个假名。

此外,TA通过联盟链成员RSU的共识后,将$\left\{\text{VID}_i,\text{PID}_i,V_{pk_i},\text{sk}_i,t_i\right\}$上传到智能合约中,并将其添加到联盟链的VRPPPT中。同时,RSU上传车辆的$\left\{\text{PID}_i,V_{pk_i}\right\}$到私有链的VPPT中。

5.6 车辆登录和身份验证

当车辆想要向相邻的RSU和车辆广播交通信息时,需要对消息进行签名操作以确保完整性,执行过程如下:

1)车辆用户输入VID_i和pw到OBU,OBU计算$B_i^*=H_0\left(\text{pw},b_i\right)$、$A_i^*=C_i\oplus B_i^*$和$D_i^*=H_0\left(\text{VID}_i,B_i^*,A_i^*\right)$,并判断$D_i^*$是否等于$D_i$,如果相等则身份验证通过,否则身份验证失败OBU将拒绝该请求。

2)如果身份验证通过,则需要对消息进行签名操作,它需要计算$\text{Sig}_i=\left\{\eta_i,R_i\right\}$作为签名。同时车辆用户进一步生成一个随机数$r_i\in Z_q^*$,并计算$R_i=r_i \cdot P_{pub}$、$\alpha_i=H_2\left(\text{PID}_i,R_i,m_i,t_i\right)$和$\eta_i=\alpha_i\left(r_i+\mu_i+\lambda_i\right)\bmod q$,其中$m_i$表示在时间戳$t_i$发送的即时消息。最后,OBU广播以下消息$\left\{\text{PID}_i,m_i,\text{Sig}_i,t_i,V_{pk_i}\right\}$到邻近的RSU和车辆。

3)接收端通过t_i来验证消息的新鲜度。如果它

有效，接收端会向私有链的VPPT查询PID_i的记录，并通过私有链来请求发送方的公钥V_{pk_i}，并返回给查询端并比较是否等于$\{\mathrm{PID}_i, m_i, \mathrm{Sig}_i, t_i, V_{pk_i}\}$中的公钥，如果不等，则返回给发送端错误，否则接收该公钥。

4）在接收端获得V_{pk_i}后，接收端通过5.2节短签名机制进行验证签名。如果签名验证失败则接收端将删除该消息。

5.7 车辆假名身份更新

1）当车辆的假名身份即将到期时，可信节点RSU将定期从联盟链获取该车辆的新假名PID_i'和相应的新的公钥和新的私钥$\{V_{pk_i}', \mathrm{sk}_i'\}$。RSU在收到$\mathrm{PID}_i'$和$\{V_{pk_i}', \mathrm{sk}_i'\}$后形成消息$m_i$，这时RUS需要对消息$m_i$进行签名操作，即首先生成随机数$r_i \in Z_q^*$，并计算$R_i = r_i \cdot P_{pub}$、$\alpha_i = H_2(\mathrm{PID}_i', R_i, m_i, t_i)$和$\eta_i = \alpha_i(r_i + \mu_i + \lambda_i) \bmod q$。最后，将消息$\{\mathrm{PID}_i', m_i, R_i, t_i, \eta_i\}$在经过部分同态加密后，通过安全通道发送到相应的车辆。

2）接收车辆在收到签名后的消息$\{\mathrm{PID}_i', m_i, R_i, t_i, \eta_i\}$后检查$t_i$，$t_i$用于验证消息的新鲜度。如果无效则将其丢弃。反之，则将验证消息的正确性，即计算$\alpha_i' = H_2(\mathrm{PID}_i', R_i, m_i, t_i)$且仅当$\eta_i \cdot P_{pub} = \alpha_i(R_i + V_{pk_i})$时接受该消息并更新OBU中的车辆假名及其相应的公私钥。否则，拒绝该消息。

3）RSU会定期清理VRPPPT中的过期数据并进行更新，以便在未来能够有条件地追踪恶意车辆。同时，RSU还负责更新私有链上的VPPT信息。

5.8 车辆撤销

车辆撤销分为两种方式，第一种方式是车辆离开原RSU覆盖区域时，RSU上报车辆离开信息给TA，TA将通过RSU共识的方式撤销该车辆当前的状态信息并同步更新VRPPPT和VPPT。第二种方式为车辆处于等待撤销时，该方式则依托智能合约中设定的撤销阈值（该阈值会根据当前交通流量及其他相关因素动态调整），当达到设定的阈值时智能合约利用车辆撤销算法对车辆进行撤销。同时删除VRPPPT和VPPT中该车的数据并将该信息广播给VANETs中的每个节点。

5.9 车辆密码更改

车辆用户向OBU发送VID_i、原密码pw和新密码pw′，OBU计算$B_i^* = H_0(\mathrm{pw}, b_i)$、$A_i^* = C_i \oplus B_i^*$和$D_i^* = H_0(\mathrm{VID}_i, B_i^*, A_i^*)$，判断$D_i$是否等于$D_i^*$，如果此身份验证失败，则OBU将拒绝该请求。否则，接受车辆的新密码pw′，OBU选择b_i'，计算$B_i' = H_0(\mathrm{pw}', b_i')$、$C_i' = A_i \oplus B_i'$和$D_i' = H_0(\mathrm{VID}_i, B_i', A_i)$，OBU用新的$\{C_i', D_i', e_i, H_0, q_1, Z_q'\}$替换原$\{C_i, D_i, e_i, H_0, q_1, Z_q^*\}$。

6 安全分析

在这一部分中，讨论本文所提出的方案可以满足的安全要求。

1）单次注册：在本文所提的方案中可信机构为网络中的车辆颁发身份认证信息。随后，车辆可自主或通过私有链中的RSU查询所需的认证数据，实现无需依赖TA即可相互认证。因此，所提方案有效支持了单次注册的需求。

2）身份认证与消息验证：车辆或RSU可通过公式$\eta_i \cdot P_{pub} = \alpha_i(R_i + V_{pk_i})$对接收到的消息进行有效性验证，其中$\alpha_i = H_2(\mathrm{PID}_i, R_i, m_i, t_i)$。基于哈希函数的抗冲突特性，恶意用户无法在多项式时间内伪造合法用户的消息。因此，本文方案保障了消息传输的安全认证。

3）隐私保护：本文提出的方案使用定期更新的假名身份来保护车辆的真实身份VID_i。由于假名通过$\mathrm{PID}_i = \mathrm{VID}_i \oplus H_1(\mathrm{sk}_i \cdot s \cdot P)$产生，它的密钥是一个密钥交换算法中的一个元组，因此可以确保密钥在不安全的网络中进行安全的传递。因此，可以知道，没有恶意用户可以得到真实用户的身份信息。

4）可追溯性：当车辆离开当前RSU覆盖区域或被检测到该车辆存在恶意行为时，已经部署在区块链中的智能合约将启动，并通过车辆撤销算法处理以上这两种情况。针对违规车辆，TA会验证$\mathrm{PID}_i = \mathrm{VID}_i \oplus H_1(\mathrm{sk}_i \cdot s \cdot P)$，并在VRPPPT中定位该车辆的$\mathrm{VID}_i$，随后在多个RSU共识的支持下完成车辆的撤销操作。由此，该方案实现了车辆身份的可追溯性，确保车辆对其行为承担责任。

5）不可关联性：联盟链中的RSU节点会定期刷新车辆的匿名身份。这样一来，任何消息的接收方既无法识别发送者的真实身份，也无法将两条消息关联为同一实体，从而有效保障了不可关联性的要求。

6）抵抗离线密码猜测攻击：即使对手通过监听通信网络获取了消息$\{\mathrm{PID}_i, m_i, \mathrm{Sig}_i, t_i, V_{pk_i}\}$，但正如

前文所述,这些截获的信息中并不包含密码字符串的任何线索。换言之,攻击者无法判断其对密码的猜测是否正确,从而有效防止了离线密码猜测攻击。

7)抵抗重放攻击:车辆用于登录和身份验证阶段的消息中都包含签名,并且其发送的消息中均包含时间戳,以保证消息的时效性。通过验证消息$\{\mathrm{PID}_i, m_i, \mathrm{Sig}_i, t_i, V_{pk_i}\}$的时间戳确保了消息的实时性和唯一性。

8)抵抗女巫攻击:在登录阶段,OBU通过验证D_i来确认车主身份,而攻击者无法在有效时间内生成合法的身份进行登录。此外,由于预装在车辆OBU中的参数唯一,因此攻击者无法伪装成该合法车辆广播消息。

9)抵御DDoS攻击:本方案利用区块链技术中的去中心化特性和共识机制来抵御DDoS攻击。传统的网络是采用客户端-服务器模式有一个或多个中心化的服务器,攻击者只需攻击这些有限的、已知的IP地址,就能使服务器瘫痪。而区块链是一个点对点的分布式网络,由全球成千上万个节点共同维护。每个节点都存有完整或部分的数据副本。要成功攻击整个网络攻击者需要同时瘫痪掉网络中的大部分节点,这在成本和可行性上都极其困难。同时,区块链中的共识机制是区块链的灵魂,它要求节点付出某种"代价"来参与系统的维护,使得发起攻击的成本极高。另外,交易费用机制也使得攻击者无法承担。因为对于一个视图通过发送海量无效交易来堵塞网络的DDoS攻击者来说,它需要为每一笔无效交易支付真实的代币。这会使攻击成本迅速变得无法承受。攻击持续越久,攻击者的资金消耗就越快。最后,数据的不可篡改性与可追溯性也对追查封堵DDoS攻击者产生影响,因为虽然区块链的匿名性可能为攻击者提供一定掩护,但所有交易和数据都是公开透明、永久记录在链上。安全专家可以通过分析交易流,追溯攻击资金的来源和去向。虽然不能直接定位到现实世界的人,但可以对相关的恶意地址进行标记和封禁,增加攻击者的暴露风险。

7 仿真性能分析

在这一部分中,介绍了模拟实验和性能分析,并将本文提出的方案与BPPA方案[18]、BUA方案[23]和Anil的方案[24]进行了比较。在一个硬件平台上测试了该方案,该平台包含一个时钟频率为2.8GHz、8GB RAM的英特尔酷睿i7-8700处理器,并运行Windows 10操作系统。仿真实验在OMNET++、SUMO和Veins 5.2上构建了一个联合仿真平台,该平台具有集成的交通控制接口(TraCI),可在模拟器之间提供传输控制协议(TCP)连接。模拟区域为2Km×2Km的曼哈顿网格道路。在网络拓扑方面,车辆通过IEEE802.11p协议形成动态的VANETs。我们假设区块链全节点部署在所有路侧单元上,构成一个稳定的P2P覆盖网络。车辆作为轻节点,通过单挑V2I链路与最近的RSU或其他车辆交互,从而将动态的VANETs拓扑与相对稳定的区块链网络解耦。信道模型采用了贴合V2X场景的双斜率路径损耗模型和Nakagmi-m小尺度衰落模型,以准确捕获城市环境下信号的传播特性。同时,仿真中考虑了背景噪声和同信道干扰。节点分布上,车辆使用SUMO生成随机移动轨迹,密度在10至80辆之间变化以测试可扩展性。RSU以500米间隔均匀部署,共计4个。这种设置确保了区块链服务在整个仿真区域内的基本覆盖,并为分析计算损耗、通信损耗、认证延迟等提供了基础。仿真参数配置如表1所示。

表1 仿真配置参数

Table 1 Configuration parameters for simulation

参数	数值
面积	2000m×2000m
车辆数量	10~80
车辆速度	5m/s~20m/s
RSU覆盖范围	500m
RSU数量	4
无线协议	802.11p
信道带宽	4Mbps
缓存容量	2MByte
广播间隔	500ms
仿真时间	300s

7.1 计算损耗

首先,本文使用名为MIRACL的C/C++密码库,用于测量所提出和比较方案的所有相关密码操作所需的平均时间[25]。各种操作执行时间如表2所示,其中包括执行哈希运算的时间T_h、执行加密运算的时间T_e、执行标量乘法运算的时间T_{ecm}、执行点加法运算的时间T_{eca}、执行模乘法运算时间T_{mm}、执行模幂运算时间T_{me}、执行加密运算时间T_e和执行解密运算时间T_d,同时忽略其他不耗时的细节。然后,将本文提出的方案与BPPA方案、BUA方案和Anil的方案在假名生成、消息签名和消息验证方案,

这3个过程进行了比较和分析。在BPPA方案中,对身份的验证采用一种名为merkle patricia tree(MPT)的新型数据结构,它提供了一种没有撤销列表的分布式身份验证方案。为了实现有条件的隐私,证书和真实身份之间的可链接性被加密并存储在区块链中,只有在发生争议时才能披露。在BUA方案中,提出了一种基于区块链的不可链接身份验证协议,其中每个域的服务管理器充当联盟区块链的节点,以构建分布式系统。基于该系统,车辆使用同态加密来自生成任意数量的假名,以实现不可链接性。每个服务管理器都可以在本地验证匿名有效性和所有权。在Anil方案中,使用椭圆曲线密码学技术在车联网环境中设计了一种新的基于条件隐私保护批量验证的身份验证机制,其中车辆可以对其邻居车辆进行身份验证,路边单元也可以批量对其附近车辆进行身份认证。

表2 各种运算的执行时间

Table 2 Execution time of various operations

执行时间的符号	描述	平均执行时间(ms)
T_h	哈希运算	3.1421
T_{ecm}	与ECC相关的标量乘法运算	9.2916
T_{eca}	与ECC相关的点加法运算	7.1251
T_{me}	模幂运算	4.0125
T_{mm}	模乘法运算	3.3048
T_e	加密运算	30.0197
T_d	解密运算	20.7002

在BPPA方案中,车辆消耗1个标量乘法T_{ecm}和1个哈希运算T_h来进行一个签名,即$T_{ecm}+T_h$,接收端需要2个标量乘法和1个椭圆曲线点加法T_{eca}和1个哈希运算来验证一个签名,即$2T_{ecm}+T_{eca}+T_h$。证书验证需要执行24个哈希运算,因此总的计算损耗是$3T_{ecm}+T_{eca}+26T_h$。

在BUA方案中,车辆假名生成需要1个模幂运算T_{me}、1个椭圆曲线加法T_{eca}和1个标量乘法T_{ecm}即:$T_{me}+T_{eca}+T_{ecm}$。车辆对消息进行签名需要消耗8个模幂运算T_{me}、4个模乘法运算T_{mm}和1个哈希运算T_h,即:$8T_{me}+4T_{mm}+T_h$。接收端验证签名时需要消耗3个模幂运算、3个模乘法运算和1个哈希运算,即:$3T_{me}+3T_{mm}+T_h$,因此总的计算损耗是:$12T_{me}++7T_{mm}+2T_h+T_{eca}+T_{ecm}$。

在Anil的方案中,车辆假名生成需要4个标量乘法T_{ecm}和2个哈希运算T_h即:$4T_{ecm}+2T_h$。对消息进行签名需要2个标量乘法和1个哈希运算即:$2T_{ecm}+T_h$,接收端对消息签名进行验证需要1个椭圆曲线点加法T_{eca}和3个标量乘法和2个哈希运算即:$T_{eca}+3T_{ecm}+2T_h$,因此总的计算损耗为$9T_{ecm}+T_{eca}+5T_h$。

在本文方案中,假名由TA计算生成,并预先加载到车辆的OBU设备中,同时录入私有链中。车辆端无需进行计算,因此车辆端假名生成时没有计算损耗。对消息进行签名需要1个标量乘法、1个加密运算T_e和1个哈希运算即:$T_{ecm}+T_e+T_h$。车辆对于消息签名进行验证的计算损耗需要2个标量乘法、1个解密计算T_d、1个椭圆曲线加法和1个哈希运算即:$2T_{ecm}+T_d+T_{eca}+T_h$,因此总的计算损耗为$3T_{ecm}+T_{eca}+2T_h+T_e+T_d$。由图7可见,本文提出的方案的计算损耗最低,虽然随着车辆数量的增加,所有方案的计算损耗均呈线性增长趋势,但本文提出的方案依然由于其他三个方案。

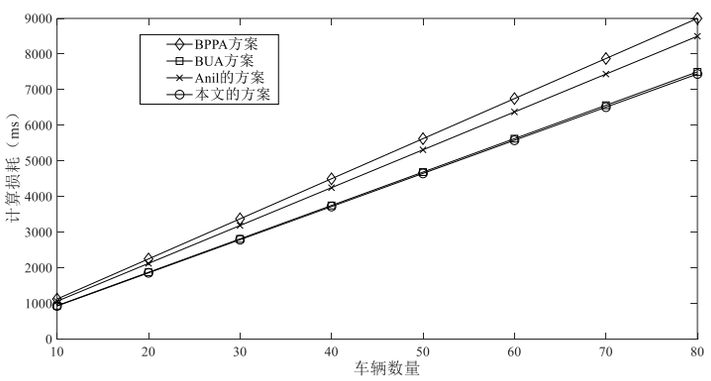


图7 计算损耗的比较

Fig.7 The comparison of the computation overhead

7.2 通信损耗

在BPPA方案中,车辆广播$\{C, \text{tuple}_M, \text{Sig}_{PR}\}$认证消息,其中$C=(\text{PU}, T, t, \text{Link})$,$C$为车辆的证书,同时也是MPT中的叶子节点,$\text{tuple}_M$为MPT相关节点信息,$\text{Sig}_{PR}$为签名,PU为公钥,$T$为公钥时限,Link表示车辆ID与车辆间的链路,$t$表示时间戳。总之,该方案的总通信损耗为270字节。

在BUA方案中,采用分布式认证方式,车辆广播$\{C^i_{\text{BID}_v}, \text{PS}^i_v, \text{AM}^i_v\}$认证消息,其中$C^i_{\text{BID}_v}$为加密后的地址,$\text{PS}^i_v$为车辆的假名,$\text{AM}^i_v$为车辆的辅助信息。因此,该方案的总通信损耗为250字节。

在Anil的方案中,车辆广播$\{M_i, \delta_i=\{f_i, g_i\}, B_i, R_i, K_i, \text{PID}_i, T_i\}$认证消息,其中$M_i$为消息,$\delta_i$表示车辆的签名,$B_i$表示随机选择加密值$b_i$时车辆的公钥,$(R_i, K_i)$表示车辆的公钥,$\text{PID}_i$表示车辆假名,$T_i$表示假名的时限。因此,该方案的总通信损耗为275字节。

在本文所提出的方案中,短签名机制最大限度地降低了签名生成和认证的计算损耗。车辆广播消息$\{\text{PID}_i, m_i, \text{Sig}_i, t_i, V_{pk_i}\}$的总通信损耗为202字节。结果如图8所示,本文提出的方案的通信损耗明显低于其他三种方案,即使是在车辆数量增加导致所有方案的通信损耗都在增加的时候,本文提出的方案的性能依然优于其他三个方案。

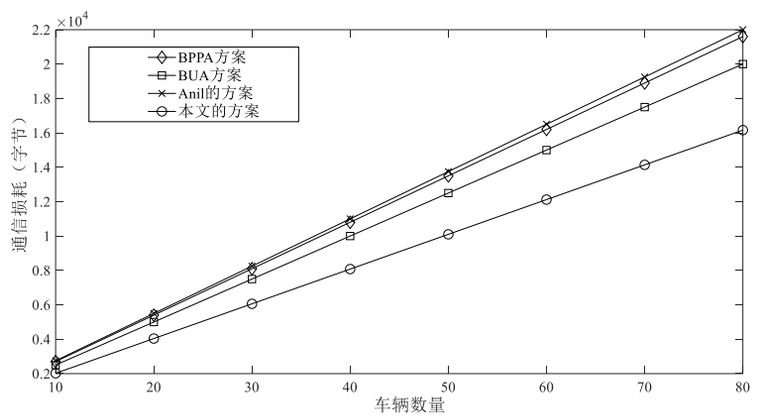


图8 通信损耗的比较

Fig.8 The comparison of the communication overhead

7.3 认证延迟

本节从签名认证延迟的角度进行了分析。签名认证延迟定义为从发送端生成消息签名到接收端验证该签名之间的时间间隔。平均签名认证延迟表示为:$\left(\sum_{i=1}^{N}\frac{T_i^{ver}-T_i^{gen}}{M_i}\right)\Big/N$,其中$N$为车辆数量,$M_i$表示车辆$V_i$接收到的消息数量,$T_i^{ver}$表示车辆$V_i$对消息签名验证完成的时间,$T_i^{gen}$表示车辆$V_i$生成消息签名的时间。仿真中车辆的平均速度为10m/s。结果如图9所示,本文提出的方案的认证延迟要远低于另外三种方案。在车辆数量增加时,虽然所有方案的认证延迟都有所增长,但本文提出的方案还是优于其他方案,并且本文提出的方案的增长率要低于其他三种方案,因此可以说本文提出的方案更适合车辆较多的情况。

7.4 丢包率

本节从丢包率的角度进行了分析。丢包率用于描述数据包长度与传输频率之间的关系。将本文提出的方案与BPPA方案、UBA方案和Anil的方案进行了比较。数据包丢失率可以表示为:$\left(\sum_{i=1}^{N}\left(\frac{N_i^{los}}{N_i^{rec}+N_i^{los}}\right)\right)\Big/N$,其中$N$表示车辆的数量,$N_i^{los}$表示车辆$V_i$丢失的数据包数量,$N_i^{rec}$表示车辆$V_i$正确接收数据包的数量。结果如图10所示。可以看出,随着车辆数量的增加,所有其他方案都在不同程度上增加。当车辆超过70时,特别是对于BPPA方案来说,其丢包率显著最为明显。然而,本文提出的方案低于其他方案,增长率基本保持不变。总体来看,所有方案的丢包率均随着车辆数量的增加而上升,但本文提出的方案始终保持低于其他方案的水平。

7.5 交易吞吐量

VANETs的繁忙程度与人们的生活习惯紧密相关,例如在每日高峰通勤时段和交通密集的十字路口,RSU需要处理大量的并发请求和交易,这对系统的稳定性和效率构成了挑战。因此,本节从交

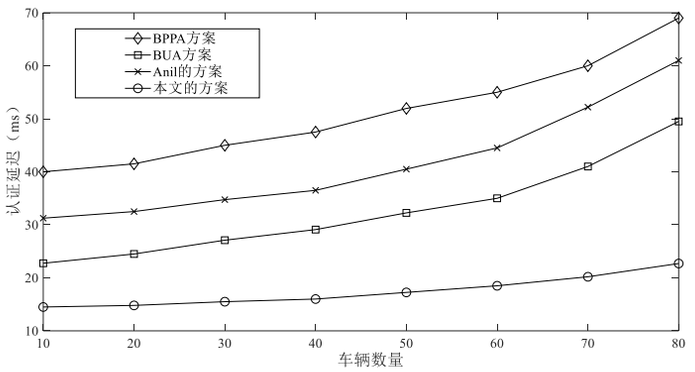


图9 认证延迟的比较

Fig.9 The comparison of the authentication delay

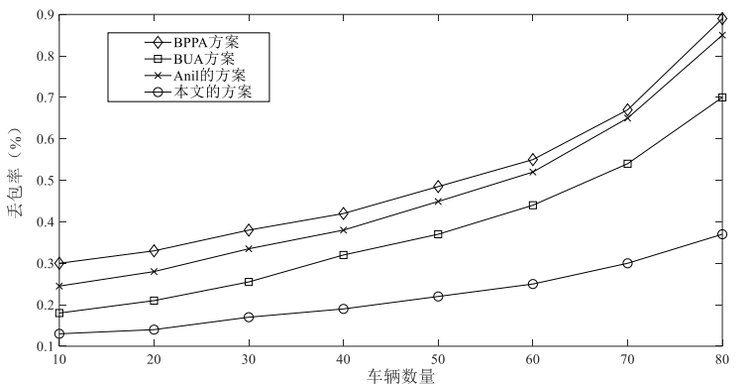


图10 丢包率比较

Fig.10 The comparison of the packet loss rate

易吞吐量的角度对本文提出的区块链架构进行了分析。在实验仿真中,模拟了公有链单链结构、本文提出的底层私有链+顶层联盟链双链结构,以及底层联盟链+顶层私有链双链结构下RSU处理的VANETs的交易吞吐量。仿真结果如图11所示。当VANETs的交易事务量达到每秒700时,公有链单链结构的吞吐量约为370,而双链结构则提升至580至600左右,表现明显优越。此外,本文采用的底层私有链加顶层联盟链结构性能优于另一种双链结构(底层联盟链加顶层私有链)。总体来看,双链架构在所有测试条件下均优于单链架构的处理能力。

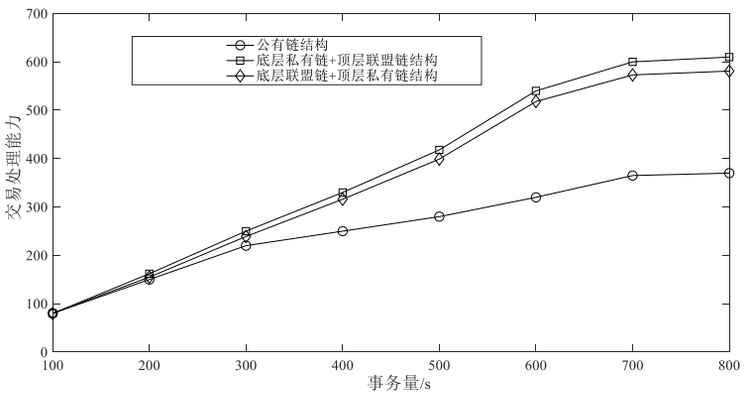


图11 交易吞吐量比较

Fig.11 The comparison of the transaction throughput

8 结论

本文提出了一种基于双区块链的隐私保护认证方案应用于VANETs,旨在提升现有VANETs的隐私保护能力和认证效率。该方案一方面利用联盟链的高安全性优势和私有链的交易速度快优势;另一方面,采用短签名技术降低了VANETs中各实体间签名与鉴权的通信负担,并结合部分同态加密技术保障VANETs中各实体间信息的安全加密传输。安全性分析表明,该方案具备良好的隐私防护能力和抵御多种攻击的能力。仿真结果也显示,本方案在计算与通信损耗上均优于其他三种方案,并在认证延迟、丢包率及交易吞吐量等关键性能指标上表现更为出色。

参考文献:

[1] ZIJIAN BAO, DEBIAO HE, HUAQUN WANG, et al. BAP: A Blockchain-Assisted Privacy-Preserving Authentication Protocol With User-Controlled Data Link ability for VANETs[J]. IEEE Transactions on Intelligent Vehicles, 2024, 9(2): 4206-4220. DOI: 10.1109/TIV.2023.3307699.

[2] QI TAO, HONGWEI DING, TIAN JIANG, et al. B-DSPA: A Blockchain-Based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad Hoc Networks[J]. IEEE Internet of Things Journal, 2024, 11(1): 1385 - 1397. DOI: 10.1109/JIOT.2023.3289057.

[3] SHRIKANT TANGADE, SUNILKUMAR S. MANVI, and PASCAL LORENZ. Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs [J]. IEEE Transactions on Vehicular Technology, 2018, 67(9): 8647-8655. DOI: 10.1109/TVT.2018.2839979.

[4] XINCHENG LI, YALI LIU, and XINCHUN YIN. An Anonymous Conditional Privacy-Preserving Authentication Scheme for VANETs [C]// 2019 IEEE 5th International Conference on Data Science and Systems (HPCC/Smart City/DSS). Zhang jia jie: IEEE Press, 2019: 1-10. DOI: 10.1109/HPCC/SmartCity/DSS.2019.00242.

[5] ROAYAT I. ABDELFATAH , NERMEEN M. ABDAL GHAFOUR, and MOHAMED E. NASR. Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions[J]. IEEE Access, 2022, 10(8): 1096 - 1115. DOI: 10.1109/ACCESS.2021.3137877.

[6] LEI ZHANG, XINYU MENG, KIM KWANG RANGMOND CHOO, et al. Privacy-Preserving Cloud Eloud Establishment and Data Dissemination Scheme for Vehicular Cloud[J]IEEE Transactions on Dependable and Secure Computing, 2020, 17(3): 634 - 647. DOI: 10.1109/TDSC.2018.2797190.

[7] YANJI JIANG, SHAOCHENG GE and XUELI SHEN. AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs[J]. IEEE Access, 2020, 8(2): 98986-98998. DOI: 10.1109/ACCESS.2020.2997840.

[8] LEI ZHANG, QIANHONG WU, AGUSTI SOLANAS, et al. A Scalable Robust Authentication Protocol for Secure Vehicular Communications [J]. IEEE Transactions on Vehicular Technology, 2010, 59(4): 1606 - 1617. DOI: 10.1109/TVT.2009.2038222.

[9] YING CAI, HAO ZHANG, and YUGUANG FANG. A Conditional Privacy Protection Scheme Based on Ring Signcryption for Vehicular Ad Hoc Networks[J]. IEEE Internet of Things Journal, 2021, 8(1): 647 - 656. DOI: 10.1109/JIOT.2020.3037252.

[10] MING LUO, YANZIBO ZHOU. An Efficient Conditional Privacy-Preserving Authentication Protocol Based on Generalized Ring Signcryption for VANETs [J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 10001 - 10015. DOI: 10.1109/TVT.2022.3179371.

[11] PANDI VIJAYAKUMAR, MARIA AZEES, SERGEI A. KOZLOV, et al. An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs [J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(2): 1630 - 1638. DOI: 10.1109/TITS.2021.3099488.

[12] A. ASLINE CELES , N. EDNA ELIZABETH . Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication[C]// 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai: IEEE Press, 2019: 1-10. DOI: 10.1109/ICCSP.2018.8524540.

[13] GREGORY NEVEN, GIANMARCO BALDINI, JAN CAMENISCH , et al. Privacy-preserving Attribute-based Credentials in Cooperative Intelligent Transport Systems [C]// 2017 IEEE Vehicular Networking Conference (VNC), Turin: IEEE Press, 2017: 1 - 8. DOI: 10.1109/VNC.2017.8275631.

[14] LEI ZHANG, QIANHONG WU, JOSEP DOMINGO FERRER, et al. Distributed Aggregate Privacy-Preserving Authentication in VANETs [J]. IEEE Transactions on Intelligent Transportation

Systems, 2017, 18(3): 516 - 526. DOI: 10.1109/TITS.2016.2579162.

[15] DONG ZHENG, CHUNMING JING, RUI GUO, et al. A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs [J]. IEEE Access, 2019, 7(2): 117716-117726. DOI: 10.1109/ACCESS.2019.2936575.

[16] ZHUO MA, JUNWEI ZHANG, YONGZHEN GUO, et al. An Efficient Decentralized Key Management Mechanism for VANETS With Blockchain [J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5836 - 5849. DOI: 10.1109/TVT.2020.2972923.

[17] ABDULLAH ALHARTHI, QIANG NI, and RICHARD JIANG. A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANETs[J]. IEEE Access, 2021, 9(2): 87299-87309. DOI: 10.1109/ACCESS.2021.3086225.

[18] ZHAOJUN LU, QIAN WANG, GANG QU, et al. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2792 - 2801. DOI: 10.1109/TVLSI.2019.2929420.

[19] HUIMIN SHEN, TAOCHUN WANG, JIAN CHEN, et al. Blockchain-Based Batch Authentication Scheme for Internet of Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 73(6): 7866 - 7879. DOI: 10.1109/TVT.2024.3355711.

[20] CHAO LIN, XINGYI HUANG, DEBIAO HE, et al. EBCPA: Efficient Blockchain-Based Conditional Privacy-Preserving Authentication for VANETs [J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(3): 1818 - 1832. DOI: 10.1109/TDSC.2022.3164740.

[21] XIAOTONG ZHOU, DEBIAO HE, MUHAMMAD KHURRAM KHAN, et al. An Efficient Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for VANETs [J]. IEEE Transactions on Vehicular Technology, 2023, 72(1): 81 - 92. DOI: 10.1109/TVT.2022.3204582.

[22] GUOHUAI SANG, JINGWEI CHEN, YILIANG LIU, et al. PACM: Privacy-Preserving Authentication Scheme with On-Chain Certificate Management for VANETs [J]. IEEE Transactions on Network and Service Management, 2023, 20(1): 216 - 228. DOI: 10.1109/TNSM.2022.3201551.

[23] JIAO LIU, XINGHUA LI, QI JIANG, et al. BUA: A Blockchain-based Unlinkable Authentication in VANETs [C]// International Conference on Communications(ICC), Dublin: IEEE Press, 2020: 1 - 6. DOI: 10.1109/ICC40277.2020.9148863.

[24] ANIL KUMAR SUTRALA, PALAK BAGGA, ASHOK KUMAR DAS, et al. On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment [J] IEEE Transactions on Vehicular Technology, 2020, 69(5): 5535-5548. DOI: 10.1109/TVT.2020.2981934.

[25] M. SCOTT . Miracl-a Multiprecision Integer and Rational Arithmetic C/C++ Library, 2003. http://www.shamus.ie.