Journal of Computer Applications
计算机应用,2020,40(10):2992 - 2999
ISSN 1001-9081
CODEN JYIIDU
2020-10-10
http://www.joca.cn

文章编号:1001-9081(2020)10-2992-08
DOI:10.11772/j.issn.1001-9081.2020020211

基于区块链技术的车联网高效匿名认证方案

陈葳葳,曹　利*,邵长虹
(南通大学 信息科学技术学院,江苏 南通 226001)
(*通信作者电子邮箱cl@ntu.edu.cn)

摘　要:针对车联网(IOV)中心化认证效率低和隐私保护差的问题,提出一种基于区块链技术的高效匿名认证方案。该方案基于IOV开放、自组织、快速移动的特点,利用区块链技术防篡改和分布式的特性来完成车辆临时身份的生成和区块链存储。车辆相互通信时,通过触发智能合约实现高效匿名的双向身份认证。实验结果表明,在认证效率上,与传统公钥基础设施(PKI)认证、假名授权身份认证相比,随着验证量的增加,所提方案的匿名身份认证的时延增长较慢,效率较高;在安全性能上,所提方案中存入区块链的临时身份具有不可篡改、不可否认、可追溯等特点。所提方案中,恶意车辆身份可回溯并进行权限控制,并且,公钥密码体制和数字签名技术保证了通信数据的保密性和完整性。

关键词:车联网;区块链;匿名认证;智能合约;共识机制
中图分类号:TP393　　**文献标志码:**A

Blockchain based efficient anonymous authentication scheme for IOV

CHEN Weiwei, CAO Li*, SHAO Changhong
(*College of Information Science and Technology, Nantong University, Nantong Jiangsu* 226001, *China*)

Abstract: In order to solve the problems of low efficiency of centralized authentication and poor privacy protection in Internet of Vehicles (IOV), an efficient anonymous authentication scheme based on blockchain technology was proposed. According to the IOV's characteristics of openness, self-organization and fast movement, the tamper-proof and distributed features of blockchain technology were used to realize the generation and blockchain storing of temporary identities of the vehicles. Smart contract was implemented to make efficient anonymous two-way identity authentication while vehicles communicated with each other. Experimental results show that, in terms of authentication efficiency, the proposed scheme has the anonymous authentication with slower time delay growth and higher efficiency compared with traditional Public Key Infrastructure (PKI) authentication and identity authentication scheme with pseudonym authorization; in terms of safety performance, the temporary identity stored in the blockchain has characteristics of non-tampering, nondenying and traceability. In this scheme, the malicious vehicle identity and authority can be traced back and controlled respectively, and the public-key cryptography and digital signature technology ensure the confidentiality and integrity of communication data.

Key words: Internet of Vehicles (IOV); blockchain; anonymous authentication; smart contract; consensus mechanism

0　引言

车联网(Internet of Vehicles, IOV)是由车辆自组网(Vehicular Ad-Hoc Network, VANET)和移动互联网组成的开放异构网络,通过车、路、管理平台的实时关联与感知实现智能交通,并提供交通安全、信息娱乐等服务。在车联网中,车辆必须周期性地广播交通车辆的身份、当前位置、速度等相关信息给其周围的所有车辆,恶意车辆可以通过分析消息与发送者的关系,获取车辆驾驶者的隐私(身份、位置等)信息,对车辆用户的隐私造成潜在的威胁,可引发伪装攻击、消息篡改、窃听等一系列安全问题[1-3]。而身份的合法性认证是开放交通环境中车联网其他一切应用安全的基础,身份认证不仅包括对接入车辆身份合法性的校验,以保证通信双方身份的真实性,同时还需保护用户的隐私,以匿名方式进行。车联网身份认证需考虑的其他特性有:1)因车辆运动速度快、路侧单元(Road Side Unit, RSU)覆盖范围小,车辆需要频繁进行身份验证,高效的身份验证成为关键;2)认证节点RSU大多独立化,无人操作和管理,攻击者可以轻易访问认证设备,一旦认证节点遭到攻击或数据被篡改,将会严重影响交通安全。因此,研究如何适应车联网自身特点的身份认证方案,消除车联网推广应用的安全障碍,受到国内外学者的广泛关注。

车联网目前普遍采用公钥基础设施(Public Key Infrastructure, PKI)认证机制,通过为车辆分发唯一编号并提供证书颁发机构(Certification Authority, CA)证书进行身份认证,缺点是由于认证节点的中心化导致中心节点任务繁重、无法代理且易攻陷,此短板效应会引起用户敏感信息等数据泄露[4-6],且无法有效保护用户身份隐私。基于此,国内外学者提出车联网环境下基于假名的身份认证、基于环签名的认证和基于PKI系统的匿名认证等方法。文献[7]利用假名机制

收稿日期:2020-03-02;**修回日期:**2020-06-15;**录用日期:**2020-06-18。　**基金项目:**南通市科技计划项目(JC2018131)。
作者简介:陈葳葳(2000—),女,江苏南通人,主要研究方向:网络与信息安全;　曹利(1974—),男,江苏宜兴人,副教授,硕士,主要研究方向:网络与信息安全;　邵长虹(1997—),男,江苏徐州人,主要研究方向:网络通信。

研究公务用车通信协议,协议结合了同态密钥协商和数字签名等技术以管理和使用假名,确保公务用车的通信安全和隐私保护,但无法抵制身份的滥用和对中心节点的依赖。文献[8]在PKI系统的基础上设计了一种车联网安全通信与隐私保护机制。车辆使用可信中心机构(Trusted Authority, TA)中心为其计算的公钥进行通信,即使匿名密钥泄露也不会导致用户身份的泄露,但缺乏适合车联网环境的移动路由。文献[9]中提出了证书和假名机制结合的隐私保护方案。TA为认证机构颁发证书,认证机构再为每一个用户颁发假名授权证书,构建了智能传输系统的隐私框架,但网络性能无法满足车联网频繁认证的需求。文献[10]利用路边单元(Road Side Unit,RSU)批认证提出基于身份的高效匿名批认证方案。车辆根据TA参数产生假名进行通信,实现匿名性和高效认证,但是存在RSU认证工作频繁、负荷过大等问题。文献[11]利用离散对数难题(Discrete Logarithm Problem, DLP)提出一种高效条件隐私保护方案。结合TA提供参数计算所得假名存放于防篡改设备,有效实现匿名性,但是未阐明密钥分配和防篡改设备的使用问题。环签名方案是车辆签名信息时将自己的私钥与其他车辆的公钥混合,形成环签名,以混淆方式防止自己身份的泄露。文献[12]利用格困难问题设计环签名方案,实现了无条件匿名性,保障其在量子攻击下的安全性,但格签名的长度有待优化。文献[13]利用环签名和基于身份的加密技术对车辆间的通信进行认证,但缺乏对复杂网络环境的实验分析。文献[14]利用分布式车辆公钥基础设施提出隐私保护方案,采用票据为应用服务提供匿名访问和认证,但是随着车辆数目的增多,票据处理的时延成为问题。文献[15]利用多假名保护、消息分片、编码和缓存机制解决了车辆-基础设施(Vehicle-to-Infrastructure, V2I)通信过程中车辆隐私泄露问题,消除了多条转发路径上的消息关联性,但是没有考虑RSU的可靠性问题。

综合以上研究成果,车联网因对认证效率和隐私保护的特殊要求,传统的身份认证仍存在诸多问题有待解决。车联网数据是典型的时空数据,包括时间和空间两个维度,采用传统的集中式方式处理虽然具有一定的便捷性,但不能充分满足时空数据存储及查询等要求,而区块链(Block Chain)技术采用去中心化的分布式存储机制,并通过共识机制等技术来保证数据的安全性,适合作为车联网安全问题的新型解决方案。区块链技术于2008年被中本聪提出,其本质是一个对等网络的分布式账本数据库。一个完整的区块链系统包含数据加密、数字签名、时间戳等技术,以及作为支持的对等网络(Peer-to-Peer,P2P)和维护系统的共识算法、采矿和工作量证明、匿名交易机制和Merkle树快速检索等相关技术,为区块链上的交易、验证等功能提供了技术支撑和运行动力。目前,区块链以其特有的安全机制,在很多领域得到应用。很多学者将车联网安全问题与区块链技术相结合,进行了一些研究。文献[16]基于车联网通信(Wireless Access in Vehicular Environment, WAVE)协议设计了去中心化的车联网数据交换系统,利用区块链网络分布特征广播与存储数据,实现了车与车的数据交换,但位置隐私保护问题有待解决。文献[17]结合区块链技术设计出车联网身份认证系统框架,解决汽车与多服务器、路边单元之间的认证问题,但是由于车辆数量较多,通信频繁,缺乏高效、快速的共识机制。文献[18]中提出了以区块链为模型解决在车联网中传播重要信息的方案,区块链存储节点可信度达成车辆间信任机制,但事件传播延时有待改善。

针对车联网的特性与中心化认证系统的缺陷,本文提出一种基于区块链技术的车联网匿名身份认证方案。通过区块链技术和智能合约的结合,实现身份存储、认证的高效与可靠;利用公钥密码体制及数字签名技术实现信息传输的保密性和完整性;采用临时公钥进行匿名通信,实现身份隐私的保护。

1　区块链

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,并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账。

区块链结构如图1所示,每一个数据区块主要由区块头和区块体组成。区块头用来记录当前区块的元数据,主要封装了当前版本号、前一个区块的地址、当前区块的目标哈希值、Merkle根等。前一区块的地址,用于将当前区块与前一区块相连,形成链条。目标哈希值、随机数、时间戳等用于共识机制。区块体记录具体的数据,数据结构为Merkle树,数据记录在叶子节点,非叶子节点的值为所有叶子节点数据的哈希值而不是具体数据,降低了区块容量,便于同步与备份。区块体中数据经过哈希运算得到Merkle根,一个叶子节点数据的改动将会导致根节点数据的变化,达到快速查询和校验的目的。

车联网的安全需求与区块链技术特征(去中心化、防篡改及可追溯性)不谋而合。车联网中所有节点权利平等,并且有较好的容错能力。利用区块链技术在海量分布式节点间建立信任关系,能解决中心化低效率与数据不安全等问题。利用区块链的哈希函数的单向性、数字签名不可否认等性质将车

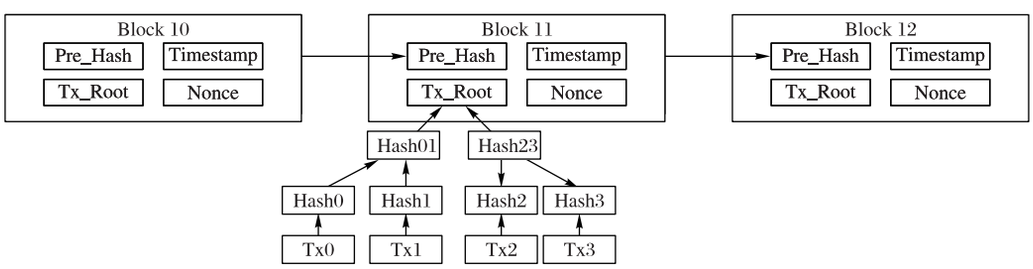

图1　区块链结构

Fig. 1　Structure of Blockchain

联网相关数据存储至区块链，若攻击者妄图篡改数据，不仅要修改当前区块的哈希值，还要修改所有区块的哈希值，极大增加了攻击难度和成本。区块链带有时间戳数据，将区块按照时间顺序关联，方便检索交易从发布源头到最新状态的整个变化流程，可以满足车联网快速认证的需求。

区块链技术为适应社会的需求，不断演进，目前发展到第三代：第一代以比特币网络为代表，以分布式账本模式存储交易，交易具有不可篡改、不可否认的特性，但其共识机制导致的时延无法满足车联网实时需求；第二代是以以太坊为代表的区块链技术，在比特币网络的基础上改进了区块结构，并设计了智能合约，可以实现交易的自动化处理，具有了可扩展的特性，将区块链底层技术推广至应用层，适合车联网的安全应用解决方案；第三代有向无环图（Directed Acyclic Graph，DAG）区块链结构正在起步阶段，采用全新的区块数据结构、大幅增加区块链网络吞吐量，但技术尚未成熟。本文方案的研究对象为车联网，具有开放性、自组织、变化快的特性，及身份认证时延小、可追溯、隐私保护的需求，所以采用第二代联盟链技术作为研究平台。方案选择 Hyperledger 作为验证平台，主要是基于其开源性，方便实现区块链共识机制的修改，并通过智能合约实现相关访问控制。

2 基于联盟链的高效匿名认证

本文以开源 Hyperledger 联盟链为原型设计了一种车联网匿名快速身份认证模型，该认证模型可实现：1）保证 RSU 认证系统的可靠性和健壮性；2）车辆在进行通信时，不使用真实身份关联的公私钥，实现匿名性；3）通信过程中消息全程加密，保障信息的完整性和保密性。

2.1 信任模型

车联网基本结构见图 2，主要由三个主体部分构成：

1）交通管理中心（Trust Center，TC）是 IOV 中最高权威机构，与路边单元（RSU）通过有线连接，主要负责交通参与者初始化，核心信息保存等；

2）路边单元（RSU）分布在十字路口及道路两旁，提供车辆接入、身份验证等相关服务；

3）车载单元（On Board Unit，OBU）安装在车辆嵌入式设备中，作为车辆的通信模块，与周围车辆交互信息。

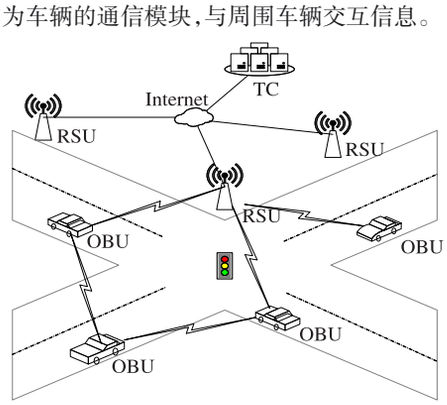

图 2 车联网系统结构

Fig. 2 Structure of IOV

车联网联盟链认证信任模型如图 3 所示：行驶车辆的 OBU 接入附近的路侧单元 RSU 并产生临时身份密钥对，RSU 作为记账节点，将车辆合法身份信息记录和临时身份密钥对进行映射处理，记入区块链，为车辆实现匿名通信提供凭证，各 RSU 组成联盟链网络。

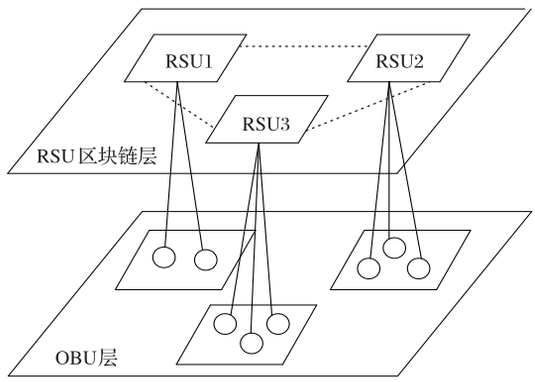

图 3 认证模型

Fig. 3 Model of authentication

2.2 协议流程

根据以上系统架构和信任模型，本文提出基于联盟链的高效匿名认证协议。协议在传统 PKI 认证的基础上，利用 RSU 构建认证的联盟区块链，实现本区域行驶车辆的快速认证。假定区域内 RSU 是可信设备，且已由 TA 注册证书。方案流程如图 4 所示：首先，车辆经过 TA 中心线下注册，生成公私钥，颁发证书。车辆上路时，OBU 自行生成用于隐私保护的临时公私钥对，然后申请入网并向 RSU 注册临时公私钥对。若 OBU 通过 PKI 机制完成初次身份验证，RSU 就生成临时公钥与证书公钥的映射关系，完成行驶中临时认证注册，并触发联盟区块链的智能合约，将该次映射关系记载入区块，各 RSU 达成共识后，发布至区块链。RSU 通过检索区块链中的信息快速验证通信车辆彼此的身份，车辆行驶中使用临时公私钥与其他车辆进行匿名双向通信。

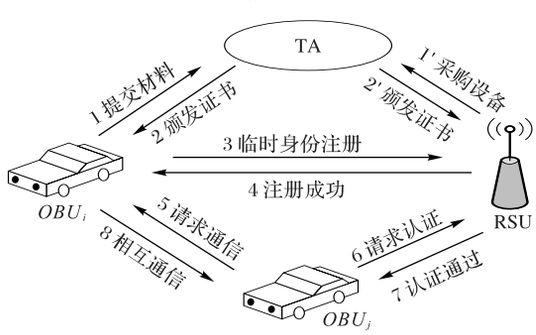

图 4 协议流程

Fig. 4 Process of protocol

2.2.1 Token 结构

匿名通信中，车辆采用临时公钥代替 TA 公钥进行通信。为便于区块链的检索和临时公钥 P_{Token} 的管理，方案生成 Token 进行身份信息的关联，并把 Token 记入区块链。Token 主要由区域号、时间戳与 P_{Token} 组成，其中 P_{Token} 为 Token 中标识符，结构如图 5 所示。

区域号	P_{Token}	时间戳

图 5 Token 结构

Fig. 5 Structure of Token

区域号:车辆注册TA所属区域行政区划代码,便于车辆身份的查询,区域号格式与国家行政区划代码类似,由6位构成,其中:1~2位表示省编码,3~4位表示市编码,5~6位表示区县编码。

标识符:利用EIGamal算法,结合TA公开参数和私钥计算得公钥,生成标识符M,私钥和离散对数难题的结合保证其唯一性、不可伪造性。

时间戳:规定其有效期,时间戳过期则无法使用。当检测到过期的Token,自动触发智能合约,删除Token与公钥的映射关系。时间戳还用于判断出块时间,在认证时,实现相应区块的快速定位。

2.2.2　区块结构

区块体记录车辆经过注册、更新、撤销后公钥和Token的映射关系,以MPT(Merkle Patricia Tree)的形式存储。区块头存储根节点的哈希值、生成时间等。

MPT结构中每一个节点的所有子孙都有相同的前缀,节点对应的key由根节点到该节点路径上的所有节点key值前后拼接而成,存储key-value数据结构。方案中key定义为Token, value定义为Token对应公钥。RSU以区域号归纳智能合约打包的映射关系,生成MPT。因在同一个地区注册车辆的Token区域号一致,故查询时可快速匹配到省市县组成的分支路径,提高查询效率,实现快速认证。区块结构如图6所示。

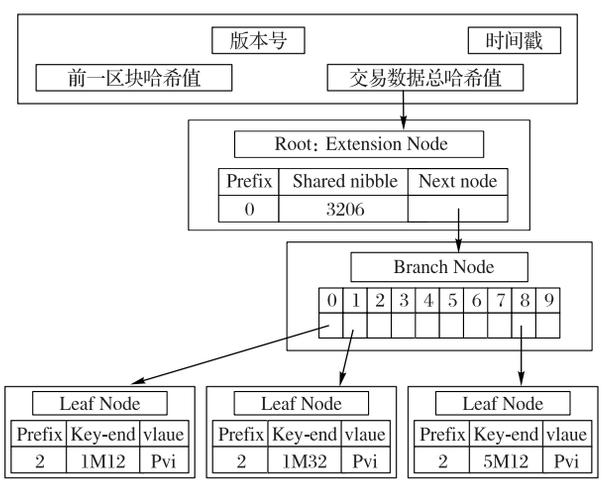

图6　区块结构

Fig. 6　Structure of block

2.2.3　PBFT共识机制和智能合约

区块链普遍采用工作量证明(Proof of Work, POW)共识机制达成共识,不适合车联网实时快速认证的需求。本文方案中,各区域RSU组成联盟链网络,改用实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)算法共识机制,缩短出块时间以满足车联网快速达成共识的需求,同时可容忍小于1/3个无效或者恶意节点。PBFT的算法流程如下:设共有$3n+1$个记账节点。首先,RSU_i节点接收车辆注册请求并认证其身份,其次RSU_i节点通过广播将请求发送至全网RSU节点。所有节点都执行认证并将结果发回RSU_i节点。RSU_i需要等待$n+1$个不同节点返回相同的结果,作为整个操作的最终结果。PBFT共识机制下的交易吞吐量可以达到200~2 000 TPS(Transactions Per Second),实现毫秒级的确认时间,无分叉可能,同时抵抗女巫攻击。

为了将OBU的临时公钥与证书公钥的映射关系即时计入联盟链,方案采用智能合约技术,智能合约可以看作是运行在分布式账本上的计算机程序,完成规则预设,无需第三方干涉处理,适应场景需求变换,监督合约的条款以检查合规性。本文方案采用智能合约实现:

1) 车辆生成Token后,触发智能合约实现Token与公钥的映射;

2) Token时间戳失效,将触发智能合约,将Token与公钥的映射删除;

3) 行驶中车辆身份验证的请求行为触发智能合约,对区块链上的Token快速检索;

4) 对恶意节点的判定将触发智能合约,将其加入撤销列表。

智能合约主要功能实现伪代码:

```
class Stack{…
    push();                                    //压栈操作…
    };                                         //存储数据的栈
class tree{ …
    preTraverser();                            //先序遍历MPT
    dleaf();                                   //删除MPT叶子节点…
}//存储MPT
constract identifcication{
    let stack = new Stack();      //存放Token-Public key映射关系
    let mnode = new Stack();                   //存放撤销信息的栈
    }
    //查询Token
    function Search(Token){…
        if(Token==preTraverser())
                                   //先根据时间戳找到对应区块,
                                    //再遍历区块MPT匹配Token
            return load;                       //数据所在MPT地址
        else return 0;}                        //不存在返回0
        //注册Token
        if(agreeun>=n)                         //全网认证通过
        {   registed(Token,Publickey); }
            function registed(Token,Publickey){
            if(Search(Token))                  //Token是否已被注册
                return false;                  //注册过返回false
            else{…
                stack.push(Token,Publickey);
                            //将Token和公钥的映射关系压入栈
                return true;} }
                //删除Token
                function Delete(Token){…
                deleaf(Search(Token));
                        //找到Token所在位置,删除其叶子节点
                return true;}
            //注销车辆公钥
            function revoke(Publickey,Token){…
                mnode.push(Publickey);
                            //找到公钥位置后将其压入撤销栈
                deleaf(Search(Token));
                            //删除公钥对应所有叶子节点
            …return true;} }
```

2.3 协议实现

方案中假设底层采用短程通信(Dedicated Short Range Communication, DSRC)技术和802.11P协议。802.11P标准对DSRC标准中的物理层(PHYsical, PHY)和介质访问控制层(Media Access Control, MAC)的内容进行了规范,能为车车和车路之间提供高速的无线广播通信服务,具有数据传输速率高、传输时延短的特点,且支持点对点或点对多点通信。所以在本文方案中,当OBU接入车联网时候,首先接收的是RSU的广播信息,属于一点对多点通信。而在认证过程中OBU和RSU的多次握手,采用的是点对点通信方式。

基于区块链的匿名快速认证可分为:预注册(线下注册、线上注册)和快速认证两部分。表1为本文方案中使用的符号说明。

表1 本文方案所使用符号

Tab. 1 Symbols of proposed scheme

符号	含义
V_x	车辆x
RSU_x	RSU设备x
$G1$、$G2$	满足双线性映射的群
q、α	群中素数
s	系统公钥
P_x	x的公钥
S_x	x的私钥
$Cert_x$	x的证书
r_i	随机数i
M	Token标识符
N_R	RSU的区域编码
$Sign_x()$	签名算法
$H()$	哈希函数

初始参数由TA权威中心(如车管所)产生。TA选择满足双线性映射特性的群$G1$和$G2$;选择随机数$s \in \mathbf{Z}_q^*$作为主密钥,其中$\mathbf{Z}_q^*$代表正整数集中素数;计算系统公钥$P_{pub} = sp$;提取群中素数α、q,$n = aq$。公开的参数有$\{G1, G2, n, \alpha, P_{pub}\}$。

2.3.1 预注册

预注册包含线下注册和线上注册两部分。

线下注册:部署RSU前,TA为每一个官方采购的RSU颁发证书$Cert_R$。车辆线下注册时,TA核实其材料真实性,为其颁发证书,并记录公钥与车主真实身份的映射关系。具体为:官方采购RSU设备后,TA用RSA算法生成RSU私钥S_R和公钥P_R,颁发证书$Cert_R$。证书中包含:RSU的公钥、证书有效期、TA私钥的签名、RSU所部署的区域编号N_R等信息。RSU存储TA公共参数、其证书和公、私钥。车主提交真实身份材料经核实后,TA利用RSA算法生成车辆私钥S_{vi}和公钥P_{vi},颁发证书$Cert_{vi}$。证书中包含:车辆的公钥、证书有效期、TA用私钥的签名和TA所在区域号等信息。OBU存储TA公共参数、车辆的证书和公、私钥。TA记录包含:车辆公钥与车主身份材料的映射关系,据此可以追溯违规车辆车主的真实身份;RSU证书与RSU编号N_R映射关系。若有RSU损坏,TA可以根据RSU证书中的区域编号查找损坏设备,实时维修。

线上注册:区域内RSU构成联盟链网络,RSU广播自己的证书信息。当车辆上路后进入初始RSU的广播范围,OBU自行生成公私钥对$\{P_{Token}, S_{Token}\}$,将P_{Token}、证书中的区域号附上时间戳组成Token,向RSU发送对该Token的注册请求。RSU进行初次身份PKI认证,验证通过后触发智能合约,生成车辆的Token与公钥的映射关系,同时返回Success消息,若认证不通过返回False消息。RSU根据新注册的Token更新本地区块中的MPT,使用PBFT共识机制,RSU间达成共识,完成记账。通过验证和注册请求的OBU在后继行驶过程中采用联盟链认证。线上注册算法的流程如图7所示。

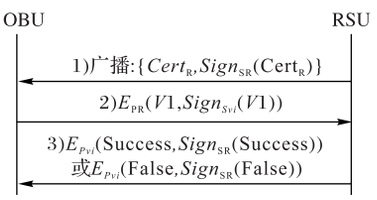

图7 线上注册流程

Fig. 7 Process of online registration

1)RSU→OBU:$\{Cert_R, Sign_{SR}(Cert_R)\}$。

RSU广播自己的证书和签名。

2)OBU→RSU:$E_{PR}(V1, Sign_{Svi}(V1))$。

① 车辆接收到RSU广播信息,验证RSU身份,并生成随机数,利用EIGamal算法生成私钥S_{Token},然后计算出公钥$P_{Token} = \alpha^{S_{Token}} \bmod q$,加上区域号和时间戳信息,生成本次的Token。

② OBU用S_{Token}签名车辆证书,与$Token$、证书形成注册请求内容:$V1 = Cert_{vi}, Token, Sign_{STken}(Cert_{vi})$,并对其签名$Sign_{Svi}(V1)$,用RSU公钥加密后发给RSU。

3) RSU→OBU:$E_{Pvi}(\text{Success}, Sign_{SR}(\text{Success}))\|E_{Pvi}(\text{False}, Sign_{SR}(\text{False}))$。

① RSU用私钥解密OBU注册请求,先利用PKI验证车辆的证书和签名,保证公钥不在撤销列表;接着验证$Token$里的区域号是否与车辆证书中的一致。验证通过,提取P_{Token},验证S_{Token}的签名,确保是P_{Token}拥有者发出的注册请求。

② 验证通过后,签名车辆注册的消息区块链网络同步,由本区域RSU分别验证,返回半数以上条成功结果后,智能合约触发Search()功能模块:区块链检索。检索算法为:Search()先由时间戳计算出块时间,定位到相应区块;然后根据Token区域号先找到其省级所在分支,再按照市县行政代号匹配分支路径。若P_{Token}是初次注册,执行registed()函数,生成车辆公钥与Token的映射关系。

③ RSU用私钥签名注册结果,注册成功返回:$E_{Pvi}(\text{Success}, Sign_{SR}(\text{Success}))$;若有一条验证未通过,返回失败消息:$E_{Pvi}(\text{False}, Sign_{SR}(\text{False}))$。

④ RSU根据新注册的Token更新区块中的MPT,并通过PBFT共识机制快速添加至区块链。

4) 车辆用私钥解密RSU响应消息,验证其签名,根据注册结果判断是否获得P_{Token}的使用权。

2.3.2 快速认证

车辆OBU_i、OBU_j在完成线上注册后,若需要彼此通信,就可发起快速身份认证。OBU_i向OBU_j发送身份信息:Token和时间戳,并对其签名。OBU_j根据接收的信息可向附近任何一个RSU请求认证OBU_i的身份。若认证成功,双方用对称密钥进行通信,否则中断连接。具体流程如图8所示。

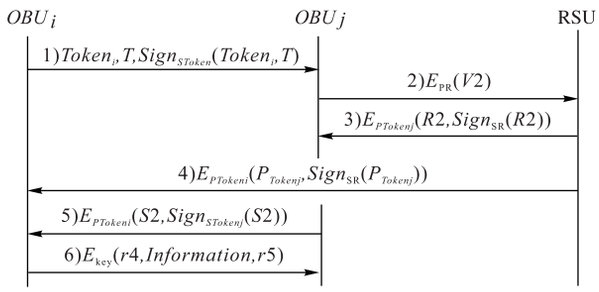

图8　快速认证过程

Fig. 8　Process of fast authentication

1)$OBU_i \rightarrow OBU_j$:$Token_i$, T, $Sign_{STokeni}(Token_i, T)$。

OBU_i将自己的$Token_i$、时间戳T签名后发给OBU_j。

2)$OBU_j \rightarrow$RSU:$E_{PR}(V2)$。

OBU_j将OBU_i身份信息附加自己的$Token_j$组成认证请求:$V2 = Token_i, T, Sign_{STokeni}(Token_i, T), Token_j$,用RSU公钥加密发送给RSU。

3)RSU$\rightarrow OBU_j$:$E_{PTokenj}(R2, Sign_{SR}(R2))$。

①RSU用私钥解密后触发智能合约,调用Search()函数检索区块链,查看区块链中是否记载$Token_i$、$Token_j$,若都存在并且Token时间戳都未过期,提取P_{Tokeni}验证S_{Tokeni}的签名,验证通过后检测消息中时间戳T是否有效。

②上述条件均满足返回认证成功:$R2$ = Success, T。否则返回认证失败:$R2$ = False, T。签名消息$Sign_{SR}(R2)$,提取P_{Tokenj}加密发送给OBU_j。

4)RSU$\rightarrow OBU_i$:$E_{PTokeni}(P_{Tokenj}, Sign_{SR}(P_{Tokenj}))$。

RSU将OBU_j的P_{Tokenj}签名,并用OBU_i公钥加密传给OBU_i。

5)$OBU_j \rightarrow OBU_i$:$E_{PTokeni}(S2, Sign_{STokenj}(S2))$。

①OBU_j验证RSU签名后,得到Success消息便提取$Token_i$中的P_{Tokeni},生成对称密钥key。key为临时会话密钥。

②封装对称密钥key、时间戳,和key加密的随机数$r4$:$S2 = key, T, E_{key}(r4)$,签名$Sign_{STokenj}(S2)$并用P_{Tokeni}加密发送给OBU。

6)$OBU_i \rightarrow OBU_j$:$E_{key}(r4, Information, r5)$。

①OBU_i收到消息4)后用私钥解密验证,并接收RSU发来的P_{Tokenj};

②用P_{Tokenj}解密获得OBU_j发来的key,并验证签名和时间戳,提取随机数$r4$;

③生成随机数$r5$,将通信消息与随机数$r4$、$r5$封装,使用临时会话密钥key加密发送给OBU_j;

7)OBU_j解密消息并验证签名,检测随机数$r4$(以保证通信对方身份并已拿到key),验证通过,接受信息。

3　实验与性能分析

为了测试方案的可行性,利用Hyperledger Fabric 1.4工具进行车联网身份部署,模拟快速认证过程。因实验环境限制,假设车联网节点预注册部分已经完成,安全性将在后面分析,实验主要完成区块链的共识建立和身份快速验证。在本地虚拟机中部署5个虚拟节点,用来实现不同的RSU构建区块链。实验开始时,调用智能合约,模拟预注册阶段OBU身份验证后生成的Token,身份信息被RSU打包,采用PBFT算法达成共识,经过节点间的共识认证后生成区块,存入区块链;各节点进行数据的更新操作。实验过程中涉及的测试工具及对应作用如表2所示。

表2　测试工具及其作用

Tab. 2　Testing tools and their functions

工具	作用
Ubuntu 16.04	实验底层系统
HyperledgerFabric 1.4	测试环境
Docker	运行Fabric
Go lang	编程语言

3.1　方案可行性分析

按照上述方式搭建仿真平台,本文仿真验证了5个RSU节点30 min内在区块链网络中的共识情况。通过分析节点的在线情况、打包次数、是否进行区块更新操作,检测RSU节点在区块链网络运行的可行性,结果如表3所示。实验结果表明,参与共识的节点均100%在线,打包次数分布平均,且各节点对网络中区块持续更新,在网络畅通情况下无掉线、停滞、阻塞等现象出现,实验结果说明了方案在区块链上的可用性及正确性。

表3　正确性实验结果

Tab. 3　Experimental results of correctness

节点号	是否在线	打包次数	是否更新
1	是	20	是
2	是	18	是
3	是	20	是
4	是	19	是
5	是	20	是

为验证PBFT共识算法在本文方案的可行性,实验设计查询请求发送速率为100、200 TPS(Transactions Per Second)的两种网络环境,检测各自共识时延情况,得到两组的最大、平均及最小共识时延。实验数据如图9所示,表明Hyperledger fabric中在发送请求速率不超过200 TPS时,平均时延均在40 ms左右,达到毫秒级的共识速度,满足车联网环境下实时认证的通信时延要求。

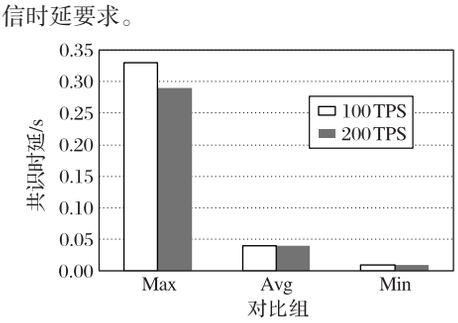

图9　PBFT算法时延

Fig. 9　Time delay of PBFT algorithm

方案采用联盟区块链分布式账本模式,可以抵御拒绝服务攻击,防止中心化单点故障对车联网认证系统带来的破坏。利用区块链智能合约的自动触发性,及MPT区块结构易于检索的特点,相较于传统公钥基础设施(PKI)模式,能有效缩短车联网身份认证过程的时延。实验验证了不同假名请求数量与时延的关系,结果如图10所示,与传统PKI模式、文献[14]的假名授权身份认证方案进行比较,随着假名请求量的增加,

本文方案匿名身份认证方法时延增长最慢,更为高效。

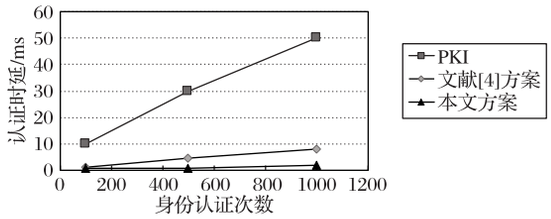

图10 时延对比

Fig. 10 Comparison of delay

3.2 方案安全性分析

3.2.1 防伪装攻击

采用公钥密码体制EIGamal算法保证密钥安全性,有效防止伪装攻击,证明如下:

OBU生成私钥 $S_{vi} < q-1$,计算公钥 $P_{vi} = \alpha^{S_{vi}} \bmod q$。设明文 X,随机选择整数 $y < q$。

公钥加密:$Y = (P_{vi})^y \bmod q$;

$C1 = a^y \bmod q$;

$C2 = YX \bmod q$。

私钥解密:$Y = (C1)^{S_{vi}} \bmod q$;

$X = (C2Y^{-1}) \bmod q$

攻击者为了恢复私钥,会计算 $S_{vi} = d\log_{\alpha,q}(P_{vi})$;或为了恢复一次性密钥 Y,选择随机数 y 计算离散对数 $y = d\log_{\alpha,q}C1$。基于离散对数难题,当 $q \geqslant 300$,$q-1$ 至少有一个大的素因子时无法推算出私钥;没有合法车辆的 P_{Token} 私钥无法伪造身份,致使无法进行Token注册。同理没有RSU私钥无法伪装RSU认证车辆身份。

3.2.2 有条件的匿名性

利用联盟区块链创建账户的自发性特性,车辆可以自行生成多个Token,进行多身份混淆,一定程度上实现匿名。联盟区块链采用分布式存储,实现车辆身份数据的永久存储,同时区块内部信息由车辆签名,不可否认,便于身份的追溯,具体说明如下:

方案使用 P_{Token} 代替用户与真实身份相关联的公钥进行通信。除RSU外无人知道车辆公钥信息。若遇到恶意车辆,RSU可以激活智能合约revoke()函数,将其对应公钥加入撤销列表,使之无法注册Token进行通信。对于违规车辆(如超速、压线等,但仍然有权利生成Token),RSU通过智能合约的Search()函数找到对应公钥并上交至TA,TA可以查询到车辆的真实身份,实现追溯性。最坏情况下:车辆公钥泄露,因为RSU不存储车辆的真实身份也不会导致车主身份隐私的泄露。

3.2.3 通信数据和存储数据的完整性和保密性

1)通信数据的保密性和完整性证明。

OBU用自己的私钥签名消息 X。OBU先计算Hash值:$x = H(X)$,OBU选取随机整数 r_i,满足 $1 \leqslant r_i \leqslant q-1$ 且 $\gcd(r_i, q-1) = 1$。

a)计算 $S1 = \alpha^{r_i} \bmod q$;

b)计算 $r_i^{-1} \bmod (q-1)$;

c)计算 $S2 = r_i^{-1}(m - S_{vi}S1) \bmod (q-1)$;

d)签名为(S1,S2)。

RSU可用OBU的公钥解密:

a)计算:$V1 = \alpha^x \bmod q$;

b)计算:$V2 = (P_{vi})^{S1}(S1)^{S2} \bmod q$。

若 $V1=V2$,签名合法。证明如下:

假设 $V1=V2$

$\alpha^x \bmod q = \alpha^{S_{vi}S1}\alpha^{r_iS2} \bmod q$

$\alpha^{x-S_{vi}S1} \bmod q = \alpha^{r_iS2} \bmod q$

$x - S_{vi}S1 \equiv r_iS2 \bmod (q-1)$

$x - S_{vi}S1 \equiv r_ir_i^{-1}(x - S_{vi}S1) \bmod (q-1)$

只有拥有私钥的OBU才可以对消息签名,用OBU公钥即可验证,保证消息的完整性。OBU使用RSU公钥加密消息,加密过程同上,仅拥有私钥的RSU才可解密消息,故保证消息的保密性。

2)存储数据的保密性和完整性分析。

联盟区块链中数据除可信节点RSU可知外,链外节点没有权限无法访问,实现了车辆身份信息的保密性存储;

联盟区块链技术利用哈希函数不可逆和极难碰撞的特性,将区块用哈希指针进行串连,实现链中数据的无法篡改,保证链中存储的车辆身份信息的完整性。

3.2.4 防重放攻击

车与车通信过程使用询问-握手的方式,通信消息附上时间戳和随机数,并将相关参数保存在本地,通过验证时间戳和随机数来保证消息是最新且未被篡改的。

4 结语

身份认证是车联网技术的基础,隐私保护是车联网的关键。本文提出基于区块链的快速匿名身份认证方案,方案基于PKI体制——TA为车辆、RSU颁发证书,保证通信双方的真实性;利用分布式体系结构实现匿名性——车辆可自行生成多个 P_{Token} 代替与真实身份关联的公钥进行服务请求和通信,P_{Token} 由全网认证,保证其有效性;采用智能合约的自动化——RSU认证完车辆的身份后,触发智能合约打包Token和车辆公钥映射数据,Token过期后触发智能合约删除映射关系;利用区块链不可篡改、可追溯、鲁棒性等特性——区块链上保存Token与车辆的身份映射,保证数据的可追溯性和完整性。此外,区块使用MPT树形数据结构缩短检索区块使用时间;利用实用拜占庭容错共识机制提高共识效率;通信过程采用非对称密码体系,保证数据在传输过程中的安全性。车联网跨域认证也可以基于相同的思路实现,限于篇幅,没有展开论述。

参考文献(References)

[1] 杨南,康荣保. 车联网安全威胁分析及防护思路[J]. 通信技术,2015,48(12):1421-1426.(YANG N, KANG R B. Security-threat analysis and defense strategy of IoV [J]. Communications Technology, 2015, 48(12): 1421-1426.)

[2] 姜建,卢丹. 车联网构架与安全问题分析[J]. 电信网技术,2016(2):38-41.(JIANG J, LU D. Analysis on the architecture and security problems of IoV [J]. Telecommunications Network Technology, 2016(2): 38-41.)

[3] 王良民,李婷婷,陈龙. 基于车辆身份的车联网结构与安全[J].

网络与信息安全学报, 2016, 2(2): 41-54. (WANG L M, LI T T, CHEN L. Security issues and system structure of internet of vehicles [J]. Chinese Journal of Network and Information Security, 2016, 2(2): 41-54.)

[4] 吕凌浩. 基于区块链技术的数字证书处理构想[J]. 中国信息化, 2019(5): 91-92. (LYU L H. Conception of digital certificate processing based on blockchain technology [J]. China Informatization, 2019(5): 91-92.)

[5] 林璟锵,荆继武,张琼露,等. PKI技术的近年研究综述[J]. 密码学报, 2015, 2(6): 487-496. (LIN J Q, JING J W, ZHANG Q L, et al. Recent advances in PKI technologies [J]. Journal of Cryptologic Research, 2015, 2(6): 487-496.)

[6] JIANG W, LI H, XU G, et al. PTAS: privacy-preserving thin-client authentication scheme in blockchain-based PKI[J]. Future Generation Computer Systems, 2019, 96: 185-195.

[7] 郭侠云. 车联网安全通信中的隐私保护研究方案[D]. 沈阳:沈阳航空航天大学, 2017: 19-31. (GUO X Y. Research on the privacy preservation in security communication for VANET [D]. Shenyang: Shenyang Aerospace University, 2017: 19-31.)

[8] 翟苗. 车联网安全寻址与通信技术研究[D]. 沈阳:沈阳航空航天大学, 2013: 23-30. (ZHAI M. Security addressing and communication technology research for vehicle network [D]. Shenyang: Shenyang Aerospace University, 2013: 23-30.)

[9] 冯中华,曾梦岐,陶建军. 5G时代车联网安全和隐私问题研究[J]. 通信技术, 2017, 50(5): 1010-1015. (FENG Z H, ZENG M Q, TAO J J. Security and privacy issues of 5G VANETs [J]. Communications Technology, 2017, 50(5): 1010-1015.)

[10] 张磊. 车载自组织网络安全认证与隐私保护的研究和实现[D]. 合肥:安徽大学, 2016: 24-28. (ZHANG L. Research and implementation of VANETs secure authentication and privacy protection[D]. Hefei: Anhui University, 2016: 24-28.)

[11] 温靖宇. 车联网中匿名认证方案与安全协议的研究[D]. 合肥:安徽大学, 2017: 18-28. (WEN J Y. Research of anonymous authentication scheme and secure protocol in VANET[D]. Hefei: Anhui University, 2017: 18-28.)

[12] 崔永泉,曹玲,张小宇,等. 格基环签名的车联网隐私保护[J]. 计算机学报, 2019, 42(5): 980-992. (CUI Y Q, CAO L, ZHANG X Y, et al. Ring signature based on lattice and VANET privacy preservation[J]. Chinese Journal of Computers, 2019, 42(5): 980-992.)

[13] 梅颖. 车联网隐私保护研究[D]. 武汉:华中科技大学, 2014: 30-36. (MEI Y. Research on the privacy preservation for VANETs [D]. Wuhan: Huazhong University of Science and Technology, 2014: 30-36.)

[14] 李国建,陈莹. 基于票据的车联网安全和隐私保护方案[J]. 通信技术, 2015, 48(7): 855-859. (LI G J, CHEN Y. VANET security and privacy protection based on tickets [J]. Communications Technology, 2015, 48(7): 855-859.)

[15] 刘伎昭. 车载自组网络安全关键技术研究[D]. 西安:西安电子科技大学, 2016: 61-69. (LIU J Z. Research on security in vehicular ad hoc networks[D]. Xi'an: Xidian University, 2016: 61-69.)

[16] 汤春明,张永乐,于翔. 基于BlockChain的车联网数据交换系统设计[J]. 天津工业大学学报, 2018, 37(2): 84-88. (TANG C M, ZHANG Y L, YU X. Design of vehicle networking data exchange system based on Bloc Chain [J]. Journal of Tianjin Polytechnic University, 2018, 37(2): 84-88.)

[17] 刘勇,李飞,高路路,等. 基于区块链技术的车联网汽车身份认证可行性研究[J]. 汽车技术, 2018(6): 17-22. (LIU Y, LI F, GAO L L, et al. Feasibility study of automotive identity based on blockchain technology [J]. Automobile Technology, 2018(6): 17-22.)

[18] SHRESTHA R, BAJRACHARYA R, SHRESTHA A P, et al. A new type of blockchain for secure message exchange in VANET [J]. Digital Communications and Network, 2020, 6(2): 177-186.

This work is partially supported by the Science and Technology Project of Nantong (JC2018131).

CHEN Weiwei, born in 2000. Her research interests include network and information security.

CAO Li, born in 1974, M. S., associate professor. His research interests include network and information security.

SHAO Changhong, born in 1997. His research interests include network communications.