区块链架构下具有条件隐私的车辆编队跨信任域高效群组认证研究

夏莹杰[1]，朱思雨[1]，刘雪娇[2]

（1. 浙江大学计算机科学与技术学院，浙江 杭州 310027；2. 杭州师范大学浙江省密码技术重点实验室，浙江 杭州 311121）

摘 要：为了均衡车辆编队跨信任域身份认证的安全和效率，提出了区块链架构下具有条件隐私的车辆编队跨信任域高效群组认证方案。设计了面向车辆编队身份认证的新型区块结构 BM-Tree，通过多信任域间链上认证参数共享为跨信任域群组认证提供支撑；采用动态匿名进行车辆身份隐私保护，通过双线性映射进行信任域参数变换，实现了具有条件隐私的跨信任域群组认证；提出了基于 BM-Tree 的高效群组认证协议，实现了车辆编队批量身份认证和重认证。所提方案在安全性和计算开销方面明显优于现有跨信任域认证方法，相比 BLA、MDPA 和 BBA，整体认证时延平均减少了 29%、25%和 53%。

关键词：车辆编队；跨信任域；区块链；隐私保护；群组认证

中图分类号：TP393

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023048

Research on efficient cross trust-domain group authentication with conditional privacy of vehicle platoon under blockchian architecture

XIA Yingjie[1], ZHU Siyu[1], LIU Xuejiao[2]

1. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China

2. Zhejiang Province Key Laboratory of Cryptography Technology, Hangzhou Normal University, Hangzhou 311121, China

Abstract: In order to balance the security and efficiency of vehicle platoon cross trust-domain identity authentication, an efficient cross trust-domain group authentication scheme with conditional privacy of vehicle platoon under blockchian architecture was proposed. A novel block structure BM-Tree was designed for vehicle platoon identity authentication, which provided support for efficient cross trust-domain group authentication by sharing the group authentication parameters on the blockchain. Dynamic pseudonym was used for vehicle identity privacy-preserving and bilinear mapping was used to transform the trust-domain parameters, which realized cross trust-domain group authentication with conditional privacy. An efficient group authentication protocol based on BM-Tree was proposed, which realized batch identity authentication and re-authentication of vehicle platoon. The proposed scheme has better performance than existing cross trust-domain authentication methods in terms of security and computational overhead. Experimental result shows that the authentication delay is reduced by 29%, 25% and 53% on average, respectively compared with BLA, MDPA and BBA.

Keywords: vehicle platoon, cross trust-domain, blockchain, privacy-preserving, group authentication

0 引言

车辆编队（VP, vehicle platoon）作为提高资源效率和道路安全的有效方案引起了学术界和工业界的广泛关注[1]，被认为是未来智能交通系统（ITS, intelligent transportation system）不可或缺的一部分。车辆编队一般为长距离高速公路运输，其行驶路线将跨越不同区域[2]。由于车联网快速的动态拓扑变化，身份认证是保障车联网安全的基础[3]。可信机构（TA, trust authority）负责管理和验证移动车辆的合法身份，其通信范围被认为是相互独立的信任域。在车辆编队跨信任域身份认证过程中，当前域可信机构需要向注册域可信机构

收稿日期：2022−10−25；**修回日期：**2023−01−11

基金项目：国家自然科学基金资助项目（No.61873232）；浙江省自然科学基金资助项目（No.LZ22F030004）

Foundation Items: The National Natural Science Foundation of China (No.61873232), The Natural Science Foundation of Zhejiang Province (No.LZ22F030004)

获取编队车辆的合法身份凭证，无法直接对外域车辆进行身份认证。传统车联网跨信任域认证研究主要包括基于共享会话密钥和基于代理重加密签名两类方案，但此类方法依赖于提供跨域转化工作的第三方机构正常运行，车辆身份凭证的跨域共享存在数据不可信问题。区块链技术[4]具有去中心化和难以篡改的特点，在车联网分布式架构下的数据共享场景中被广泛提及，以保证数据的安全性和可靠性[5-6]。在此基础上，许多研究工作提出将车辆身份凭证上链，可信机构通过链上认证参数对外域车辆合法身份进行验证，实现车辆跨信任域身份认证。

编队跨域行驶过程中，通过车辆–基础设施（V2I, vehicle to infrastructure）通信与外域边缘计算服务器（ECS, edge computing server）交换实时路况信息，进行编队成员车辆的协同控制，保证道路通行安全。编队与边缘计算服务器建立安全通信之前，边缘计算服务器需要快速地进行编队成员车辆的批量身份认证。由于开放的无线通信环境，编队与边缘计算服务器之间的广播消息容易遭受窃听攻击[7]。恶意攻击者通过链接车辆真实身份，能够分析通信消息中的敏感信息，如加速、刹车等协同控制指令，对编队正常行驶产生潜在的威胁。同时由于编队移动的群组特性，编队成员车辆集中地向边缘计算服务器发起身份认证请求。因此，设计一种保护车辆身份隐私和具有低认证时延的群组认证方案是车辆编队跨信任域身份认证研究的重点。基于区块链的跨信任域群组认证研究主要通过假名证书、群签名和环签名等技术实现车辆身份隐私保护。基于假名证书的认证方案确认假名撤销列表的时间开销随着假名数量增加而上升[8]；基于群签名和环签名的认证方案由于群成员数量的增长会产生高昂的验证开销[9]。

综上，为了兼顾车辆编队跨信任域身份认证的隐私保护和认证效率需求，本文提出了区块链架构下具有条件隐私的车辆编队跨信任域高效群组认证方案，主要贡献包括以下 3 个方面。

1) 提出了面向跨信任域群组认证的扩展区块链模型。设计了新型区块结构 BM-Tree（binary Merkle tree），利用分布式边缘计算服务器构建联盟链，通过多信任域间链上认证参数共享为高效的跨信任域群组认证提供支撑。

2) 提出了具有条件隐私的跨信任域群组认证方法。采用随机生成的动态匿名保护车辆身份隐私，同时能够实现匿名可追踪；通过双线性映射进行信任域参数的变换，实现了车辆编队跨信任域匿名身份认证。

3) 提出了基于 BM-Tree 的高效群组认证协议。采用二进制思想对车辆编队认证参数进行编码，动态适应编队群组结构，实现了车辆编队批量身份认证，同时有效减少了批量身份认证失败时重新认证的计算开销。

1 相关工作

1.1 车联网跨信任域认证研究

车联网认证体系下，身份认证是基于对第三方可信机构的信任。由于分布式可信机构之间形成了相互独立的信任域，研究者针对如何在跨信任域场景下实现一致的车辆身份认证展开了广泛研究。

传统车联网跨信任域认证研究包括基于共享密钥和基于代理重加密签名两类方案。Kerberos[10]协议基于共享会话密钥实现用户身份认证，被广泛应用于分布式认证服务中。Moustafa 等[11]提出了基于 Kerberos 的车联网通信认证模型，车辆通过票据授权服务器发布的授权票据向其他信任域的认证服务器获取服务授权票据，但是中心式架构容易产生单点故障问题。为解决共享密钥泄露造成的安全问题，基于公钥密码体制的跨信任域认证方案被广泛研究。杨小东等[12]和 Zhang[13]提出了基于代理重签名的跨信任域认证方案，通过重签名密钥实现跨域证书转化，但是转化工作显著地增加了系统的通信负荷和计算开销。

随着区块链技术在分布式架构中的广泛应用，大量研究将区块链技术与车联网跨信任域认证相结合，主要分为车辆公钥管理方案和车辆证书管理方案。Lei 等[14]和 Yao 等[15]将验证成功的车辆公钥上链，维护了多信任域间一致的合法车辆公钥列表，实现了跨域消息签名验证。魏松杰等[16]设计了区块链证书，实现了移动用户与外域可信机构之间的会话密钥协商。Yang 等[17]将车辆公钥及对应证书上链，实现了具有隐私保护的跨域消息认证方案。除上述两类主流方案之外，还有学者[18-19]提出了基于区块链的跨域认证参数共享方案，Liu 等[18]在此基础上结合同态加密技术保护链上认证参数不被泄露，进一步保证跨域车辆身份认证的安全性。综上所述，基于区块链的车联网跨信任域认证已经成为车联网安全领域的研究热点。

1.2 车联网群组认证研究

为了满足车联网群组认证的隐私保护需求，大量研究提出了基于群签名和基于环签名的群组认证方案。

Chaum 等[20]于 1991 年首次提出群签名，合法群成员可以在不泄露身份信息的情况下通过群签名证实自己属于某个特定的群，同时群管理员可以利用追踪密钥获得签名者的真实身份。Wang 等[21]采用 5G 基站维护群集合和分发群密钥，实现了车辆之间的消息认证。Wang 等[22]引入移动边缘计算架构，提出了全局撤销列表和本地撤销列表结合的双重撤销机制，建立了群集合容量与列表长度的映射模型，将本地撤销列表长度控制在一定阈值内以降低验证群签名的时延。

为了解决群管理员的可信问题，相关研究提出将环签名应用于车联网认证过程中。环签名没有群管理员，签名者可以选择任意环集合，通过自身私钥和其他成员的公钥构建环签名进行身份认证。Liu 等[23]通过路侧单元（RSU, road side unit）构造并广播环成员集合，车辆随机选择集合内一定数量的车辆公钥构造环签名对消息进行签名，该方案实现了无条件的车辆身份隐私保护。Cai 等[24]提出了基于身份的环签名方案，实现了车辆之间的匿名通信，同时能够追踪恶意车辆身份。但是由于环成员的不可区分性，当车辆出现恶意行为时，可信机构需要对所有环成员公钥逐一验证，难以快速地通过签名追踪到该车辆的真实身份。

2　系统模型

本节首先详细地介绍了系统架构和威胁模型，然后描述了本文方案的主要内容。

2.1　系统架构

本文方案的系统架构如图 1 所示，由可信机构（TA）、边缘计算服务器（ECS）、路侧单元（RSU）、车辆编队（VP）和区块链（BC）这 5 个部分组成。

1) 可信机构。TA 是信任等级最高的实体，其通信范围为独立的信任域，域内包含一定数量的边缘计算服务器、路侧单元和移动车辆。TA 负责域内实体的身份注册，为其生成用于认证的合法身份凭证。

2) 边缘计算服务器。ECS 负责通信范围内车辆编队的接入认证工作。它是半可信的，能够完全按照协议的流程执行，但试图从中间结果推导车辆的真实身份。

3) 路侧单元。RSU 部署在道路两侧，计算和存储能力有限。RSU 与邻近 ECS 进行安全的有线通信，与车辆进行无线通信。

4) 车辆编队。VP 由编队领航（PL, platoon leader）车辆和编队跟随（PF, platoon follower）车辆组成，PL 和 PF 均为编队成员车辆。PL 作为队首，负责编队与外部实体的通信；PF 接收 PL 发送的协同控制指令，实现安全跟车行驶。

5) 区块链。BC 是由分布式 ECS 构建的联盟链，可基于公钥密码体制实现 ECS 节点的管理、认证和授权。只有授权的 ECS 节点才能进行数据读写和交易上链操作。

2.2　威胁模型

系统在运行过程中可能会面临多种恶意攻击，

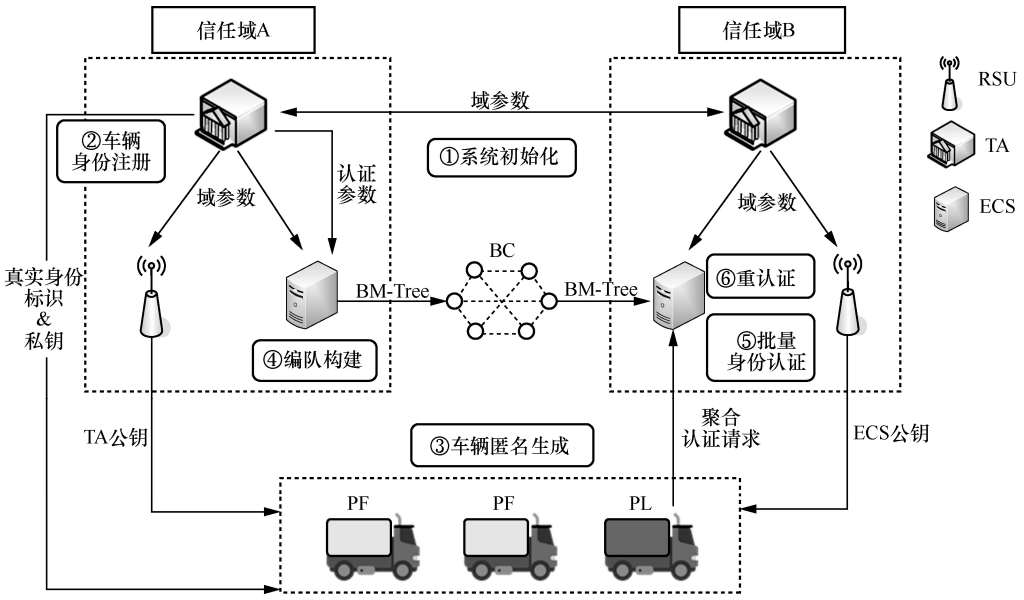

图 1　本文方案的系统架构

本文威胁模型考虑的潜在威胁如下。

1) 恶意攻击者伪装成编队成员车辆，将编队成员车辆的身份认证请求替换成自己生成的身份认证请求，试图非法地通过车辆编队批量进行身份认证。

2) 恶意攻击者通过常见的攻击方式，如伪造攻击、仿冒攻击和重放攻击等，试图伪装成合法车辆欺骗边缘计算服务器。

3) 恶意攻击者在车辆编队与边缘计算服务器通信过程中通过窃听攻击和身份链接攻击推测编队成员车辆的真实身份。

2.3 方案概述

针对车辆编队跨信任域身份认证的需求，本节首先设计了基于 BM-Tree 的扩展区块链模型，并在此基础上提出了具有条件隐私的跨信任域群组认证协议。

1) 扩展区块链模型包括 BM-Tree 构建过程和区块共识过程 2 个部分。BM-Tree 构建过程介绍了基于二进制思想的车辆编队认证参数编码方法和新型区块 BM-Tree 的详细结构。区块共识过程实现了基于拜占庭容错的 BM-Tree 共识上链，保证了链上车辆编队认证参数的合法性和不可篡改性。

2) 群组认证协议包括系统初始化、车辆身份注册、车辆匿名生成、编队构建、批量身份认证、重认证 6 个阶段，其主要工作流程如图 1 所示。在系统初始化和车辆身份注册阶段，TA 进行各信任域及域内实体的初始化和注册工作。在车辆匿名生成阶段，车辆生成用于编队构建阶段的注册匿名和用于批量身份认证阶段的认证匿名，通过动态匿名实现车辆身份隐私保护。ECS 在编队构建阶段通过车辆编队认证参数构建 BM-Tree 并进行共识上链，并在批量身份认证阶段采用编队组标识检索链上区块，通过 BM-Tree 中存储的车辆编队认证参数进行批量身份认证。如果车辆编队批量身份认证失败，ECS 执行重认证方法得到合法编队成员车辆集合。

3 基于 BM-Tree 的扩展区块链模型

本节首先介绍了新型区块 BM-Tree 的构建过程，然后实现了基于拜占庭容错的区块共识机制。基于 BM-Tree 的扩展区块链模型实现了多信任域间车辆编队认证参数共享，为高效的跨信任域群组认证提供支撑。

3.1 BM-Tree 构建过程

BM-Tree 基于二进制思想编码车辆编队认证参数，具体实现细节如下。索引值 $2^i(i\in1,2,\cdots)$ 的节点存储区间范围 $[1,2^i]$ 的编队车辆身份认证参数，其他索引值节点根据二进制思想进行子区间长度划分。如图 2 所示，索引值 8 的节点子区间长度序列为 $\left(\frac{8}{2^1},\frac{8}{2^2},\frac{8}{2^3}\right)=(4,2,1)$，则索引值 4 的节点区间范围为 $[1,4]\rightarrow$ 节点存储值为 5+0+8+1=14，索引值 6 的节点区间范围为 $[5,6]\rightarrow$ 节点存储值为 $2+9=11$，索引值 7 的节点区间范围为 $[7]\rightarrow$ 节点存储值为 1。

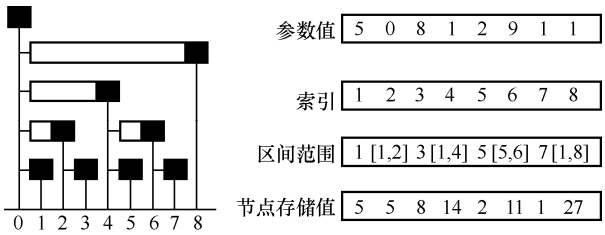

图 2 基于二进制思想的编码结构

基于二进制思想的车辆编队认证参数编码过程如算法 1 所示。

算法 1 车辆编队认证参数编码过程

输入 车辆编队容量 N，编码序列节点数量 M，编队认证参数 $\mathrm{AP}=\{\mathrm{HC}_i,\mathrm{VPK}_i\},i\in\{1,\cdots,N\}$ // HC_i 为编队成员车辆身份哈希码，VPK_i 为编队成员的合法车辆公钥

输出 车辆编队认证参数编码序列 seq

1) $M=2^{\lceil \mathrm{lb}N\rceil}$；//计算编码序列长度
2) 遍历所有编队成员车辆 $i=1:1:N$；
3) $\mathrm{idx}=i$；
4) 当 $\mathrm{idx}\leqslant M$ 循环；
5) $\mathrm{HC}[\mathrm{idx}]=\mathrm{HC}[\mathrm{idx}]+\mathrm{HC}_i$；
6) $\mathrm{VPK}[\mathrm{idx}]=\mathrm{VPK}[\mathrm{idx}]+\mathrm{VPK}_i$；
7) $\mathrm{idx}=\mathrm{idx}+(\mathrm{idx}\ \&\ (-\mathrm{idx}))$；
8) 循环结束；
9) 遍历结束；
10) 遍历 $k=1:1:M$；
11) $\mathrm{seq}_k=\{\mathrm{HC}[k],\mathrm{VPK}[k]\}$；
12) 遍历结束；
13) 返回车辆编队认证参数编码序列 seq。

将编码序列作为默克尔树叶子节点，计算根哈希值并记录在区块头中，保证链上认证参数的不可篡改性，基于 BM-Tree 的扩展区块链模型如图 3 所示。区块头中各字段的含义如下。

① $\mathrm{Hash}_{\mathrm{PB}}$：前一个区块的哈希值，防止区块数据被恶意篡改。

② GID：编队组标识。边缘计算服务器通过编队组标识检索链上区块。

③ SIG_k：车辆注册域的可信机构签名。边缘计算服务器向可信机构请求车辆编队认证参数，通过对应的可信机构签名保证链上认证参数的合法性。

④ ID_{domain}：车辆注册域标识。在区块共识阶段，边缘计算服务器根据域标识得到车辆注册域可信机构公钥，验证记录在区块头中的签名合法性。

⑤ $Hash_{MTR}$：默克尔树根哈希值，防止区块体中交易数据被恶意篡改。

⑥ VaildTime：车辆编队认证参数的有效时间。

3.2　区块共识过程

拜占庭容错采用少数服从多数的原则，假设区块链网络中所有边缘计算服务器数量为 M，若少数不一致节点数量为 f，则 M=3f+1。区块共识过程包括区块广播、区块有效性验证、验证结果比较和一致性确认。除 ECS_j 之外，其他边缘计算服务器均为共识节点。

1) 区块广播。当产生新区块时，ECS_j 通过全网广播将该区块发送给共识节点。

2) 区块有效性验证。共识节点收到新区块后，首先验证区块头中的 $Hash_{PB}$ 和 $Hash_{MTR}$ 以判断区块的有效性；然后根据 ID_{domain} 检索可信机构公钥来验证签名 SIG_k 的合法性；最后将验证结果全网广播。

3) 验证结果比较。共识节点收到其他 $M-2$ 个共识节点的区块验证结果，然后结合自己的验证结果将大于或等于 $2f+1$ 数量的验证结果作为当前节点的最终验证结果，同时将该结果全网广播。

4) 一致性确认。共识节点收到其他 $M-2$ 个共识节点的最终验证结果，然后结合自己的最终验证结果将大于或等于 $2f+1$ 数量的最终验证结果作为一致性结果反馈给 ECS_j。如果 ECS_j 收到大于或等于 $2f+1$ 的一致性结果为同意该区块，则区块上链成功。

4　具有条件隐私的跨信任域群组认证协议

为了实现车辆编队跨信任域身份认证，本文提出了区块链架构下具有条件隐私的车辆编队跨信任域高效群组认证方案。在扩展区块链模型的基础上，本节详细地介绍了具有条件隐私的跨信任域高效群组认证协议。

跨信任域认证场景的形式化表述如下。多方可信机构 $TA_k(k\in\{1,\cdots,K\})$ 及其管辖区域 $domain_k$，不同信任域采用不同的系统参数 $Param_k$；边缘计算服务器 $ECS_j(j\in\{1,\cdots,M\})$ 部署在不同信任域内；编队车辆 $V_i(i\in\{1,\cdots,N\})$ 的

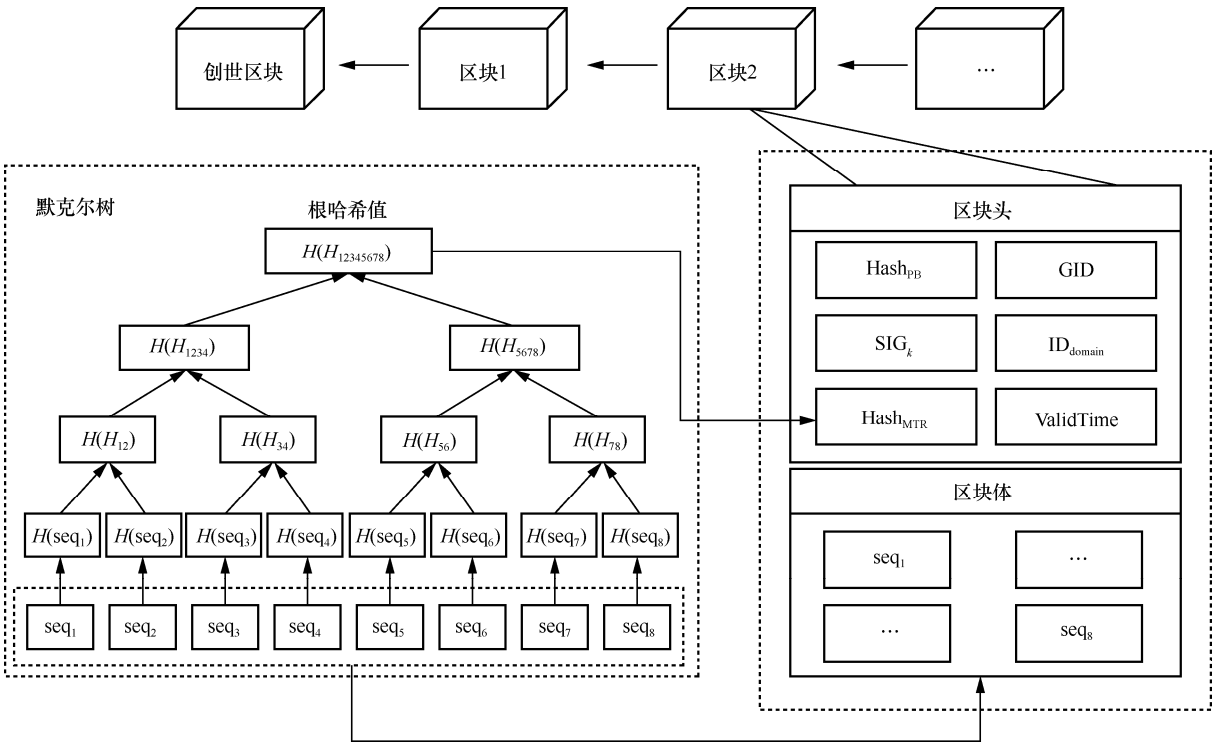

图 3　基于 BM-Tree 的扩展区块链模型

注册域是相同的，注册域和认证域的公开参数分别记为 domain_a 和 domain_b，协议流程的详细步骤如下。

4.1 系统初始化

1) 信任域参数设置

① 系统设置 p 和 q 这 2 个大素数。TA_k 通过有限域 $\mathbb{F}_p$ 上的椭圆曲线 $E_p(a,b)$ 生成阶数为 q 的循环加法群 G_k，生成元为 P_k 且 $P_k \neq \mathcal{O}$；选择 $s_k \in Z_q^*$ 作为域私钥，生成对应域公钥 $\text{TPK}_k = s_k P_k$；选择哈希函数 $h_k^0 : \{0,1\}^* \to Z_q^*$ 和 $h_k^1 : \{0,1\}^* \to \{0,1\}^C$，其中 C 表示字符串长度为常数。

② TA_k 向其他可信机构广播本域的系统参数 $\text{Param}_k = (G_k, q, P_k, h_k^0, h_k^1, \text{TPK}_k)$。因此，注册域的公开参数为 $\text{Param}_a = (G_a, q, P_a, h_a^0, h_a^1, \text{TPK}_a)$，认证域的公开参数 $\text{Param}_b = (G_b, q, P_b, h_b^0, h_b^1, \text{TPK}_b)$。

2) 边缘设施部署

①部署 ECS_j 时，TA_k 随机选择 $m_j \in Z_q^*$ 作为私钥 ECS_j，生成公钥 $\text{EPK}_j = m_j P_k$ 并采用域私钥 s_k 对公钥 ECS_j 进行签名 $\text{SIG}_k(\text{EPK}_j)$。部署完成后，$\text{ECS}_j$ 保存 $\{m_j, \text{EPK}_j, \text{SIG}_k(\text{EPK}_j), \text{Param}_k\}$，其中 $k \in \{1,\cdots,K\}$。

②部署 RSU 时，TA_k 将 RSU 邻近的边缘计算服务器公钥 ECS_j 安全保存在 RSU 存储设备中。

4.2 车辆身份注册

1) TA_a 采用车辆车牌号码 VN_i、驾驶员姓名 NA_i、驾驶员生物特征 BF_i 和域私钥 s_a 生成车辆身份标识 $\text{RID}_i = h_a^1(\text{VN}_i \| \text{NA}_i \| \text{BF}_i \| s_a)$。

2) TA_a 随机选择 $w_i \in Z_q^*$，通过域私钥 s_a 生成车辆密钥 $\text{VRK}_i = h_a^0(\text{RID}_i \| s_a \| w_i)$。

身份注册完成后，车辆安全保存 $\{\text{RID}_i, \text{VRK}_i, \text{Param}_k\}$，其中 $k \in \{1,\cdots,K\}$，TA_a 将 $\{\text{RID}_i, \text{VRK}_i\}$ 秘密存储在本地车辆身份列表中。

4.3 车辆匿名生成

1) 注册匿名生成

① V_i 随机选择 $r_i^{\text{reg}} \in Z_q^*$，生成 $\text{PID}_{i,1}^{\text{reg}} = r_i^{\text{reg}} P_a$。

② V_i 通过车辆身份标识 RID_i 和注册域公钥 TPK_a 生成 $\text{PID}_{i,2}^{\text{reg}} = \text{RID}_i \oplus h_a^0(r_i^{\text{reg}} \text{TPK}_a)$。

③ V_i 的注册匿名为 $\text{PID}_i^{\text{reg}} = (\text{PID}_{i,1}^{\text{reg}}, \text{PID}_{i,2}^{\text{reg}})$。

2) 认证匿名生成

① PL 向 RSU 请求 ECS_j 公钥，根据可信机构公钥 TPK_b 和 $< \text{EPK}_j, \text{SIG}_b(\text{EPK}_j) >$ 验证 EPK_j 的合法性，若验证通过，则将 $< \text{Param}_b, \text{EPK}_j >$ 分发给 PM。

② V_i 选择随机数 $r_i^{\text{auth}} \in Z_q^*$ 且 $\text{PID}_{i,1}^{\text{auth}} = r_i^{\text{auth}} P_b$。

③ V_i 通过身份哈希码 HC_i 和边缘计算服务器公钥 EPK_j 生成 $\text{PID}_{i,2}^{\text{auth}} = \text{HC}_i \oplus h_b^0(r_i^{\text{auth}} \text{EPK}_j)$。

④ V_i 的认证匿名为 $\text{PID}_i^{\text{auth}} = (\text{PID}_{i,1}^{\text{auth}}, \text{PID}_{i,2}^{\text{auth}})$。

车辆身份注册时保存了注册域公钥 TPK_a，并且可以通过 RSU 获取邻近 ECS 的公钥 EPK_j，所以能够提前生成注册匿名和认证匿名，进一步减少认证时间开销。

4.4 车辆编队构建

车辆组成编队之前，通过注册域边缘计算服务器进行编队构建。

1) V_i 选择注册匿名 $\text{PID}_i^{\text{reg}} = \left(\text{PID}_{i,1}^{\text{reg}}, \text{PID}_{i,2}^{\text{reg}}\right)$ 并将其发送给领航车辆 PL。

2) PL 生成编队构建请求 $\left\langle \text{PID}_1^{\text{reg}}, \cdots, \text{PID}_N^{\text{reg}} \right\rangle$ 并由邻近 ECS 将该请求转发给 TA_a。

3) TA_a 采用域私钥 s_a 和注册匿名 $\text{PID}_i^{\text{reg}}$ 计算 $\text{SP}_i = s_a \text{PID}_{i,1}^{\text{reg}}$ 和 $\text{RID}_i' = \text{PID}_{i,2}^{\text{reg}} \oplus h_a^0(\text{SP}_i)$，并通过 RID_i' 检索本地存储的 $\{\text{RID}_i, \text{VRK}_i\}$。

4) TA_a 随机选择 γ_i 生成编队成员车辆身份哈希码 $\text{HC}_i = h_a^1(\text{RID}_i \oplus \gamma_i)$，并且通过 SP_i 对车辆身份哈希码 HC_i 进行加密 $\text{EHC}_i = \text{ENC}_{\text{SP}_i}(\text{HC}_i)$；根据车辆密钥生成公钥 $\text{VPK}_i = \text{VRK}_i P_a$，将 HC_i 保存到车辆身份列表 $\{\text{RID}_i, \text{VRK}_i, \text{HC}_i\}$ 中。

5) TA_a 采用域私钥 s_a 对编队认证参数 $\text{AP} = \{\text{HC}_i, \text{VPK}_i\}$ 签名，将 $\left\langle \text{AP}, \text{SIG}_a(\text{AP}), \left\{\text{PID}_i^{\text{reg}}, \text{EHC}_i\right\}\right\rangle$ 返回 ECS，其中 $i \in \{1,\cdots,N\}$。

6) ECS 采用编队成员车辆身份哈希码计算编队组标识 $\text{GID} = h_a^1(\text{HC}_1 \| \cdots \| \text{HC}_N)$，根据算法 1 构建区块 BM-Tree 并共识上链。

7) ECS 将 $\left\langle \left\{\text{PID}_i^{\text{reg}}, \text{GID}, \text{EHC}_i\right\}\right\rangle$ 返回 PL，由 PL 分发给其余 PM，其中 $i \in \{1,\cdots,N\}$。

8) V_i 计算 $\text{SP}_i = r_i^{\text{reg}} \text{TPK}_a$，解密得到车辆身份哈希码 $\text{HC}_i = \text{DEC}_{\text{SP}_i}(\text{EHC}_i)$。

4.5 批量身份认证

当 PL 行驶到信任域 Domain_b 通信范围时，认证域边缘计算服务器 ECS_j 进行外域车辆编队批量身份认证，具体过程如图 4 所示。

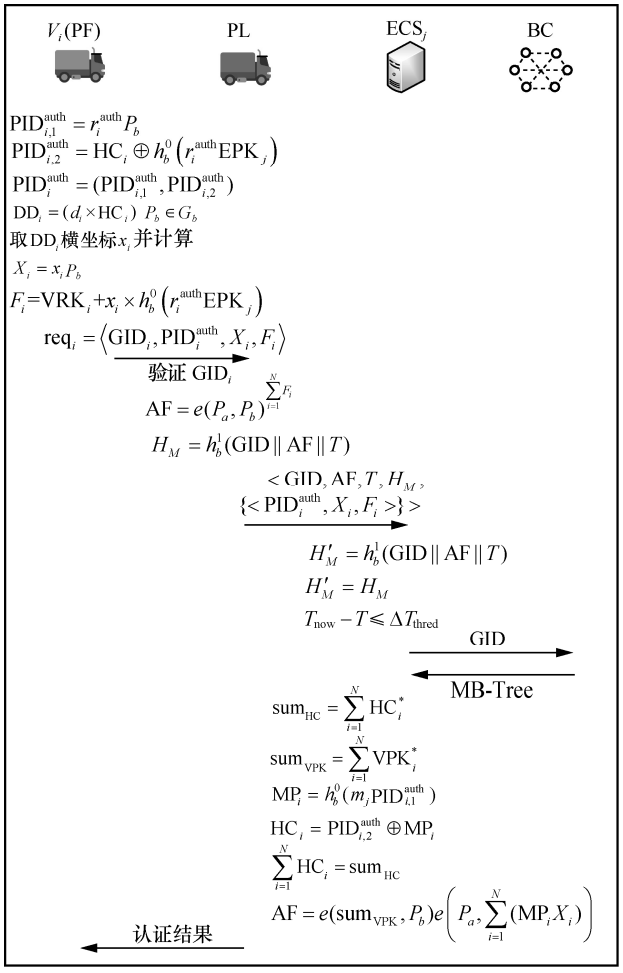

图 4　批量身份认证过程

1) 聚合认证请求生成

①V_i 选择认证匿名 $PID_i^{auth} = (PID_{i,1}^{auth}, PID_{i,2}^{auth})$，随机选择 $d_i \in Z_q^*$ 计算 $DD_i = (d_i \times HC_i)P_b$，其中，×表示素数群上的乘法，取 DD_i 横坐标 $x_i \in Z_q^*$ 并计算 $X_i = x_i P_b$；生成车辆身份验证字段 $F_i = VRK_i + x_i \times h_b^0(r_i^{auth} EPK_j)$；最后将认证请求 $req_i = \left\langle GID_i, PID_i^{auth}, X_i, F_i \right\rangle$ 发送给 PL。

②PL 验证组标识 GID_i 的合法性，进行重排序以保证成员车辆身份请求列表与编队构建阶段一致；生成 $AF = e(P_a, P_b)^{\sum_{i=1}^{N} F_i}$ 和 $H_M = h_b^1(GID \| AF \| T)$，其中 T 为聚合认证请求生成时间戳；将聚合认证请求 $< GID, AF, T, H_M, \{< PID_i^{auth}, X_i, F_i >\} >$ 发送给 ECS_j，其中 $i \in \{1, \cdots, N\}$。

2) 编队批量身份认证

①ECS_j 计算 $H'_M = h_b^1(GID \| AF \| T)$，通过 $H'_M = H_M$ 验证请求消息的完整性，通过 $T_{now} - T \leqslant \Delta T_{thred}$ 验证请求消息的即时性对抗重放攻击，其中 T_{now} 表示系统当前时间，ΔT_{thred} 表示系统可以容忍的传输时延阈值。若消息完整性或即时性验证失败，批量身份认证失败。

②ECS_j 通过编队组标识 GID 检索链上区块 BM-Tree，并通过 VaildTime 判断车辆编队认证参数是否处于有效期，然后计算 $sum_{HC} = \sum_{i=1}^{N} HC_i^*$ 和 $sum_{VPK} = \sum_{i=1}^{N} VPK_i^*$。

③ECS_j 采用私钥 m_j 和认证匿名 PID_i^{auth} 计算得到 $MP_i = h_b^0(m_j PID_{i,1}^{auth})$ 和 $HC_i = PID_{i,2}^{auth} \oplus MP_i$，通过等式 $\sum_{i=1}^{N} HC_i = sum_{HC}$ 批量验证所有编队成员车辆身份哈希码的合法性。

④若等式 $\sum_{i=1}^{N} HC_i = sum_{HC}$ 不成立，则批量身份认证失败，需进行重认证；反之，说明成员车辆身份哈希码均合法，进一步通过等式 $AF = e(sum_{VPK}, P_b) e\left(P_a, \sum_{i=1}^{N} (MP_i X_i)\right)$ 批量验证编队成员车辆密钥的合法性。

⑤若等式 $AF = e(sum_{VPK}, P_b) e\left(P_a, \sum_{i=1}^{N} (MP_i X_i)\right)$ 不成立，则批量身份认证失败，需进行重认证；反之，编队身份认证成功。

4.6　基于 BM-Tree 的重认证

编队行驶过程中，成员车辆可能会由于故障等原因离开编队，造成批量身份认证失败。为了快速验证所有合法的编队成员车辆身份，本节提出基于 BM-Tree 的重认证方法。首先定义 ReqInsert 操作并给出一个简洁示例。

假设车辆编队容量为 4 且 3 号车辆离队，则车辆请求列表为 $\{req_1, req_2, req_4\}$。重认证过程中，3 号车辆的身份认证参数 $\{HC_3, VPK_3\}$ 和 req_4 无法满足身份验证等式，则在 req_3 位置插入 NULL，请求列表转化为 $\{req_1, req_2, NULL, req_4\}$。基于 BM-Tree 的重认证过程如算法 2 所示。

算法 2　基于 BM-Tree 的重认证过程

输入　编队成员车辆的身份认证请求列表 $RL = \{req_1, req_2, \cdots, req_N\}$，BM-Tree 节点 seq_j，节点包含的车辆编号区间范围 [st,ed]；//其中 req_i 为 $< PID_i^{auth}, X_i, F_i, MP_i >$，$seq_j = \{HC[j], VPK[j]\}$

输出 合法车辆集合 VaildSet

1) 如果 $\sum_{i=\mathrm{st}}^{\mathrm{ed}}\mathrm{HC}_i=\mathrm{HC}[j]$ 且 $e(P_a,P_b)^{\sum_{i=\mathrm{st}}^{\mathrm{ed}}F_i}=e(\mathrm{PK}[j],P_b)e(P_a,\sum_{i=\mathrm{st}}^{\mathrm{ed}}(\mathrm{MP}_iX_i))$ 成立；

2) 则 $\mathrm{VaildSet}\leftarrow\{\mathrm{PID}_{\mathrm{st}}^{\mathrm{auth}},\cdots,\mathrm{PID}_{\mathrm{ed}}^{\mathrm{auth}}\}$ 并停止递归；

3) 如果 seq_j 区间长度为 1；// $\mathrm{st}=\mathrm{ed}$

4) 则在 RL 的 j 位置执行 ReqInsert 操作并停止递归；

5) $\mathrm{sum}_{\mathrm{HC}}=0,\ \mathrm{sum}_{\mathrm{VPK}}=0$；

6) 循环 seq_j 的所有子区间；

7) $k=\mathrm{st}+\left\lceil\frac{\mathrm{ed}-\mathrm{st}}{2}\right\rceil$；

8) $\mathrm{sum}_{\mathrm{HC}}=\mathrm{sum}_{\mathrm{HC}}+\mathrm{HC}[k]$；

9) $\mathrm{sum}_{\mathrm{VPK}}=\mathrm{sum}_{\mathrm{VPK}}+\mathrm{VPK}[k]$；

10) 算法2$(\mathrm{RL},\mathrm{seq}_k,[\mathrm{st},k])$；//递归验证子区间包含的成员车辆合法身份

11) $\mathrm{st}=k+1$；//下个子区间的起始编号

12) 结束循环；

13) 如果 $\mathrm{HC}_{\mathrm{ed}}=\mathrm{HC}[\mathrm{ed}]-\mathrm{sum}_{\mathrm{HC}}$ 且 $e(P_a,P_b)^{F_{\mathrm{ed}}}=e(\mathrm{PK}[\mathrm{ed}]-\mathrm{sum}_{\mathrm{VPK}},P_b)e(P_a,(\mathrm{MP}_iX_{\mathrm{ed}}))$ 成立；

14) 则 $\mathrm{VaildSet}\leftarrow\{\mathrm{PID}_{\mathrm{ed}}^{\mathrm{auth}}\}$；

15) 否则，在 RL 的 ed 位置执行 ReqInsert 操作

16) 返回 VaildSet

4.7 车辆匿名追踪

当编队成员车辆出现异常行为时，边缘计算服务器在注册域可信机构的帮助下快速对异常车辆进行匿名追踪。

1) ECS_j 通过计算自身私钥 m_j 和车辆认证匿名 $(\mathrm{PID}_{i,1}^{\mathrm{auth}},\mathrm{PID}_{i,2}^{\mathrm{auth}})$，得到异常行为车辆的身份哈希码 $\mathrm{HC}_i'=\mathrm{PID}_{i,2}^{\mathrm{auth}}\oplus h_b^0(m_j\mathrm{PID}_{i,1}^{\mathrm{auth}})$，并将 HC_i' 提交给注册域可信机构 TA_a。

2) TA_a 通过 HC_i' 检索本地存储的车辆身份列表 $\{\mathrm{RID}_i,\mathrm{VRK}_i,\mathrm{HC}_i\}$，得到异常行为车辆的真实身份标识 RID_i，实现匿名追踪。

5 安全性分析

本节首先介绍了车辆编队跨信任域身份认证过程中的安全目标，然后对本文方案进行了正确性证明和安全性证明。

5.1 安全目标

系统在运行过程中可能会面临多种恶意攻击，这些攻击行为会对车联网安全造成极大的危害。本文的安全目标如下。

1) 当且仅当所有编队成员车辆同时进行身份认证且均为合法车辆时，批量身份认证成功。

2) 能够抵抗车辆身份认证过程中常见的恶意攻击，如伪造攻击、仿冒攻击和重放攻击等。

3) 防止恶意攻击者在车辆编队与边缘计算服务器通信过程中通过窃听攻击和身份链接攻击窃取编队成员车辆身份隐私。

5.2 正确性证明

边缘计算服务器收到了来自领航车辆的聚合身份认证请求 $<\mathrm{GID},\mathrm{AF},T,H_M,\{<\mathrm{PID}_i^{\mathrm{auth}},X_i,F_i>\},i\in\{1,\cdots,N\}>$。由于认证匿名 $(\mathrm{PID}_{i,1}^{\mathrm{auth}},\mathrm{PID}_{i,2}^{\mathrm{auth}})=(r_i^{\mathrm{auth}}P_b,\mathrm{HC}_i\oplus h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j))$，并且 $r_i^{\mathrm{auth}}\mathrm{EPK}_j=r_i^{\mathrm{auth}}(m_jP_b)=m_j\mathrm{PID}_{i,1}^{\mathrm{auth}}$，因此车辆身份哈希码 $\mathrm{PID}_{i,2}^{\mathrm{auth}}\oplus h_b^0(m_j\mathrm{PID}_{i,1}^{\mathrm{auth}})=\mathrm{HC}_i\oplus h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)\oplus h_b^0(m_j\mathrm{PID}_{i,1}^{\mathrm{auth}})=\mathrm{HC}_i$。当车辆提交的身份哈希码和区块存储的编队成员车辆身份哈希码一致时，$\mathrm{sum}_{\mathrm{HC}}=\sum_{i=1}^{N}\mathrm{HC}_i^*=\sum_{i=1}^{N}\mathrm{HC}_i$ 成立。

车辆通过身份哈希码导出 x_i，并将 $X_i=x_iP_b$ 提交给边缘计算服务器用于身份认证。

$$\begin{aligned}&e(\mathrm{sum}_{\mathrm{VPK}},P_b)=e\left(\sum_{i=1}^{N}(\mathrm{VRK}_i^*P_a),P_b\right)=\\&e\left(\left(\sum_{i=1}^{N}\mathrm{VRK}_i^*\right)P_a,P_b\right)=e(P_a,P_b)^{\sum_{i=1}^{N}\mathrm{VRK}_i^*}\end{aligned}\tag{1}$$

$$\begin{aligned}&e\left(P_a,\sum_{i=1}^{N}(\mathrm{MP}_iX_i)\right)=\\&e\left(P_a,\sum_{i=1}^{N}(h_b^0(m_j\mathrm{PID}_{i,1}^{\mathrm{auth}})(x_iP_b))\right)=\\&e\left(P_a,\sum_{i=1}^{N}(h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)(x_iP_b))\right)=\\&e\left(P_a,\sum_{i=1}^{N}((x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j))P_b)\right)=\\&e\left(P_a,\left(\sum_{i=1}^{N}P_bx_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)\right)P_b\right)=\\&e(P_a,P_b)^{\sum_{i=1}^{N}x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)}\end{aligned}\tag{2}$$

$$e(\mathrm{sum}_{\mathrm{VPK}},P_b)e\left(P_a,\sum_{i=1}^{N}(\mathrm{MP}_iX_i)\right)=$$
$$e(P_a,P_b)^{\sum_{i=1}^{N}\mathrm{VRK}_i^*}e(P_a,P_b)^{\sum_{i=1}^{N}x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)}=$$
$$e(P_a,P_b)^{\sum_{i=1}^{N}\mathrm{VRK}_i^*+\sum_{i=1}^{N}x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)}=$$
$$e(P_a,P_b)^{\sum_{i=1}^{N}\mathrm{VRK}_i^*+x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)}=$$
$$e(P_a,P_b)^{\sum_{i=1}^{N}F_i}=\mathrm{AF}\tag{3}$$

若式(1)~式(3)成立，则当且仅当车辆密钥与区块中存储的编队成员车辆公钥一一对应时，车辆编队批量身份认证成功。

5.3　安全性证明

本文方案与文献[15,17,19,25]方案的安全性对比如表 1 所示。其中，Y 表示满足该特性，N 表示不满足该特性。

表 1　　**各方案安全性对比**

方案	不可伪造性	不可仿冒性	抗重放攻击	条件匿名	不可链接性
文献[15]	Y	Y	N	Y	N
文献[17]	Y	Y	Y	Y	N
文献[19]	Y	Y	Y	N	N
文献[25]	Y	N	N	Y	N
本文方案	Y	Y	Y	Y	Y

1) 不可伪造性

可信机构负责车辆身份的注册和管理，根据哈希函数的抗强碰撞性，恶意攻击者在不知道域私钥 s_a 的情况下，无法生成合法的车辆身份标识 RID_i 和车辆密钥 VRK_i。车辆编队认证参数上链需要进行区块共识，所有边缘计算服务器根据注册域可信机构的公钥验证区块头中签名 SIG_k 的合法性，只有多数边缘计算服务器同意才能将区块上链。在恶意攻击者无法伪造可信机构合法签名的前提下，伪造合法车辆身份来欺骗边缘计算服务器是困难的。

2) 不可仿冒性

车辆编队认证参数存储在由边缘计算服务器构建的联盟链上，只有授权的区块链节点才可以读写链上认证参数。在批量身份认证过程中，验证等式 $\mathrm{AF}=e(\mathrm{sum}_{\mathrm{VPK}},P_b)e\left(P_a,\sum_{i=1}^{N}(\mathrm{MP}_iX_i)\right)$ 成立，则所有编队成员车辆身份认证成功。由于 $X_i=x_iP_b$ 由车辆身份哈希码一一导出，恶意攻击者难以通过仿冒合法的编队成员车辆完成批量身份认证。

3) 抗重放攻击

在编队批量身份认证开始阶段，边缘计算服务器通过计算 $H_M=h_b^1(\mathrm{GID}\|\mathrm{AF}\|T)$ 验证聚合认证请求消息的完整性，并通过 $T_{\mathrm{now}}-T\leqslant\Delta T_{\mathrm{thred}}$ 验证请求消息的即时性，所以恶意攻击者无法通过重放合法车辆编队的聚合身份认证请求通过批量身份认证。

4) 条件匿名

恶意攻击者可以通过拦截、窃听等攻击方式获取车辆编队与边缘计算服务器之间的通信消息。给定 $\mathrm{PID}_{i,1}^{\mathrm{reg}}=r_i^{\mathrm{reg}}P_a$ 和 $\mathrm{TPK}_a=s_aP_a$，根据计算性 Diffie-Hellman 问题可知，计算 $(s_ar_i^{\mathrm{reg}})P_a$ 是困难的，进一步通过 $\mathrm{PID}_{i,2}^{\mathrm{reg}}$ 提取车辆身份标识 RID_i 是难以实现的。同理，恶意攻击者难以根据车辆认证匿名 $\mathrm{PID}_i^{\mathrm{auth}}$ 和边缘计算服务器公钥 EPK_j 提取车辆身份哈希码 HC_i。同时，$F_i=\mathrm{VRK}_i+x_i\times h_b^0(r_i^{\mathrm{auth}}\mathrm{EPK}_j)$ 是一个不定方程，恶意攻击者无法从 F_i 直接获取任何车辆身份信息。

当编队成员车辆出现异常行为时，边缘计算服务器通过 m_j 和 $\mathrm{PID}_i^{\mathrm{auth}}$ 计算身份哈希码 HC_i。由于 $r_i^{\mathrm{auth}}\mathrm{EPK}_j=(r_i^{\mathrm{auth}}m_j)P_b=m_j\mathrm{PID}_{i,1}^{\mathrm{auth}}$，因此 $\mathrm{HC}_i=\mathrm{PID}_{i,2}^{\mathrm{auth}}\oplus h_b^0(m_j\mathrm{PID}_{i,1}^{\mathrm{auth}})$。可信机构可以通过边缘计算服务器提交的异常车辆身份哈希码 HC_i 检索车辆身份列表得到车辆真实身份标识 RID_i。

综上，编队与边缘计算服务器的通信过程不会泄露成员车辆的身份隐私，并且能实现匿名可追踪。

5) 不可链接性

编队构建时，编队成员车辆收到加密的身份哈希码 $\mathrm{EHC}_i=\mathrm{ENC}_{\mathrm{SP}_i}(\mathrm{HC}_i)$，通过对称密钥 SP_i 解密得到 $\mathrm{HC}_i=\mathrm{DEC}_{\mathrm{SP}_i}(\mathrm{EHC}_i)$。给定 $\mathrm{PID}_{i,2}^{\mathrm{reg}}=r_i^{\mathrm{reg}}P_a$ 和 $\mathrm{TPK}_a=s_aP_a$，根据计算性 Diffie-Hellman 问题可知，计算 $\mathrm{SP}_i=r_i^{\mathrm{reg}}\mathrm{TPK}_a=r_i^{\mathrm{reg}}s_aP_a$ 是困难的。所以，恶意攻击者解密车辆身份哈希码 HC_i 是难以实现的。即使车辆身份哈希码 HC_i 不小心被泄露，根据哈希函数的抗强碰撞性，恶意攻击者也无法推测得到车辆真实身份标识 RID_i；同时链上认证参数超过有效期会及时更新，进一步抵抗身份链接攻击。

6　性能仿真分析

本节评估了批量身份认证阶段、重认证阶段和区块共识过程的性能开销，并进行了对比分析。

6.1 实验设置

仿真实验请求端和认证端的环境参数如下：Ubuntu 18.04.6 LTS，处理器为 Intel(R) Core(TM) i7-9700 CPU @ 3 GHz，内存为 4 GB，磁盘为 100 GB。由于编队认证参数编码序列长度为 $M=2^{\lceil \mathrm{lb}N \rceil}$，则车辆编队容量 N 设置为 8、16、24、32、40、48。

1) 批量身份认证阶段的仿真实验采用 C++的配对密码库（PBC）实现了本文方案和对比方案的认证协议，并对比分析了各方案批量身份认证阶段的通信开销和计算开销。3 种对比方案介绍如下。

①BLA（block-assisted lightweight anonymous）[15] 实现了基于区块链的车辆公钥管理方案，采用拉格朗日插值方法进行认证消息的加解密，通过验证唯一的车辆身份标识实现跨域认证。

②MDPA[17]实现了基于区块链的车辆有效证书管理方案，通过外域证书进行跨域认证。

③BBA（block chain-based batch authentication）[19] 实现了基于区块链的跨域认证参数共享方案，在此基础上提出了基于双线性映射的批量认证协议。

2) 重认证阶段的仿真实验面向不同离队车辆比例情况，评估了认证端完成所有合法编队成员车辆身份认证所需的时间开销。对比方法为二分搜索验证（BSV, binary search validation）方法，该方法在本文协议的基础上采用二分搜索树进行离队车辆定位，实现重认证。

3) 区块共识过程发生在编队构建阶段，是影响认证参数跨信任域共享效率的关键因素。区块共识过程的仿真实验通过不同区块链网络规模和车辆编队容量下的区块共识平均时间，评估车辆编队认证参数跨信任域共享效率。

6.2 批量身份认证阶段

1) 通信开销分析

本节讨论车辆编队容量为 N 时，编队进行跨信任域群组认证所需要的通信次数。

首先，N 辆编队成员车辆各自生成请求 $\mathrm{req}_i=<\mathrm{GID}_i,\mathrm{PID}_i^{\mathrm{auth}},X_i,F_i>$；然后，领航车辆生成编队聚合认证请求 $<\mathrm{GID},\mathrm{AF},T,H_M,\{<\mathrm{PID}_i^{\mathrm{auth}},X_i,F_i>\}>$，$i\in\{1,\cdots,N\}$；最后，该请求由路侧单元转发给边缘计算服务器。完成车辆编队批量身份认证之后，认证结果由路侧单元转发给编队领航车辆，领航车辆将其分发给跟随车辆。如表 2 所示，本文方案具备较少的通信次数。

表 2 各方案通信次数

方案	通信次数
BLA	$4N$
MDPA	$3N+1$
BBA	$2N+2$
本文方案	$2N+4$

2) 计算开销分析

动态车联网环境下，车辆编队跨信任域身份认证效率是一个重要的指标。本节分别采用符号 T_{A}、T_{M}、T_{B}、T_{P} 表示椭圆曲线上的加法运算、椭圆曲线上的数乘运算、双线性配对运算和乘法群上的指数运算。在 6.1 节设置的仿真实验参数下，4 种运算执行 1 000 次的平均时间开销为 0.008 ms、1.672 ms、1.538 ms、0.041 ms。

表 3 对比了各方案批量身份认证阶段的计算开销。其中，请求端计算开销为生成群组认证请求的时间；认证端计算开销为验证 N 条编队成员车辆身份认证请求的时间。

本文方案通过领航车辆生成编队聚合身份验证字段，减轻了边缘计算服务器在批量身份认证过程中的计算开销和通信负荷，车辆请求端引入的额外计算开销为 $T_{\mathrm{B}}+T_{\mathrm{P}}\approx 1.579$ ms，整体的计算开销为 $3T_{\mathrm{M}}+T_{\mathrm{B}}+T_{\mathrm{P}}\approx 6.595$ ms。BLA 请求端计算开销为 $4T_{\mathrm{A}}+6T_{\mathrm{M}}\approx 10.064$ ms，BBA 请求端计算开销为 $3T_{\mathrm{A}}+5T_{\mathrm{M}}\approx 8.384$ ms，MDPA 在认证请求生成阶段仅涉及哈希运算和模乘法运算，其请求端计算开销几乎可以忽略不计。由表 3 可知，相比于 BLA 和

表 3 各方案批量身份认证阶段的计算开销

方案	请求端计算开销/ms	认证端计算开销/ms	
		同信任域	跨信任域
BLA	$4T_{\mathrm{A}}+6T_{\mathrm{M}}\approx 10.064$	$N(2T_{\mathrm{A}}+3T_{\mathrm{M}})+2(T_{\mathrm{A}}+T_{\mathrm{M}})\approx 5.032N+3.36$	$N(2T_{\mathrm{A}}+3T_{\mathrm{M}})+2(T_{\mathrm{A}}+T_{\mathrm{M}})\approx 5.032N+3.36$
MDPA	≈ 0	$N(4T_{\mathrm{A}}+3T_{\mathrm{M}})\approx 5.048N$	$N(4T_{\mathrm{A}}+3T_{\mathrm{M}})\approx 5.048N$
BBA	$3T_{\mathrm{A}}+5T_{\mathrm{M}}\approx 8.384$	$N(6T_{\mathrm{A}}+5T_{\mathrm{M}})+3T_{\mathrm{B}}\approx 8.408N+4.614$	$N(6T_{\mathrm{A}}+5T_{\mathrm{M}})+3T_{\mathrm{B}}+T_{\mathrm{M}}\approx 8.408N+6.286$
本文方案	$3T_{\mathrm{M}}+T_{\mathrm{B}}+T_{\mathrm{P}}\approx 6.595$	$N(T_{\mathrm{A}}+2T_{\mathrm{M}})+2T_{\mathrm{B}}\approx 3.352N+3.076$	$N(T_{\mathrm{A}}+2T_{\mathrm{M}})+2T_{\mathrm{B}}\approx 3.352N+3.076$

BBA，本文方案请求端具有更低的时延。

本文方案支持同信任域场景和跨信任域场景下的车辆编队批量身份认证，其认证端计算开销均为 $N(T_{\mathrm{A}}+2T_{\mathrm{M}})+2T_{\mathrm{B}}\approx 3.352N+3.076$ ms。同信任域和跨信任域场景下，BLA 认证端计算开销均为 $N(2T_{\mathrm{A}}+3T_{\mathrm{M}})+2(T_{\mathrm{A}}+T_{\mathrm{M}})\approx 5.032N+3.36$ ms；MDPA 认证端开销均为 $N(4T_{\mathrm{A}}+3T_{\mathrm{M}})\approx 5.048N$ ms。同信任域场景下，BBA 认证端计算开销为 $N(6T_{\mathrm{A}}+5T_{\mathrm{M}})+3T_{\mathrm{B}}\approx 8.408N+4.614$ ms；跨信任域场景下，由于跨信任域认证参数转化带来的额外开销，BBA 认证端计算开销为 $N(6T_{\mathrm{A}}+5T_{\mathrm{M}})+3T_{\mathrm{B}}+T_{\mathrm{M}}\approx 8.408N+6.286$ ms。本文方案认证端计算开销明显优于其他 3 种方案。

如图 5 所示，虽然 MDPA 请求端计算开销比较低，但是本文方案的整体认证过程具有更低时延。这是因为本文方案随着车辆编队容量增加，认证时延增长更缓慢。在跨信任域场景下，相比于 BLA、MDPA 和 BBA，本文方案整体认证过程时延平均减少了 29%、25%和 53%。

6.3　重认证阶段

为了评估重认证效率，本节通过仿真实验对比了本文重认证方案和 BSV 方案的计算开销。2 种方案离队车辆比例均为 12.5%、25%、37.5%和 50%。

如图 6 所示，本文重认证方案相比于 BSV 方

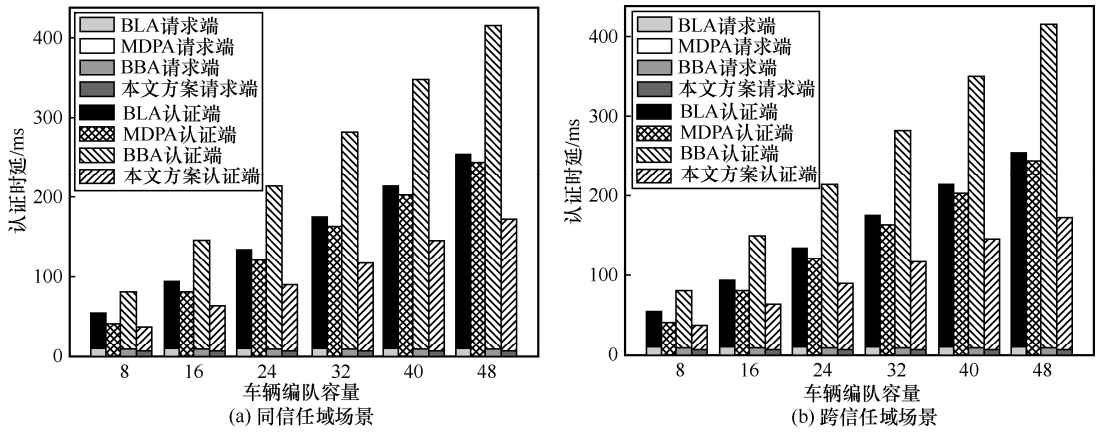

图 5　各方案批量身份认证阶段的认证时延

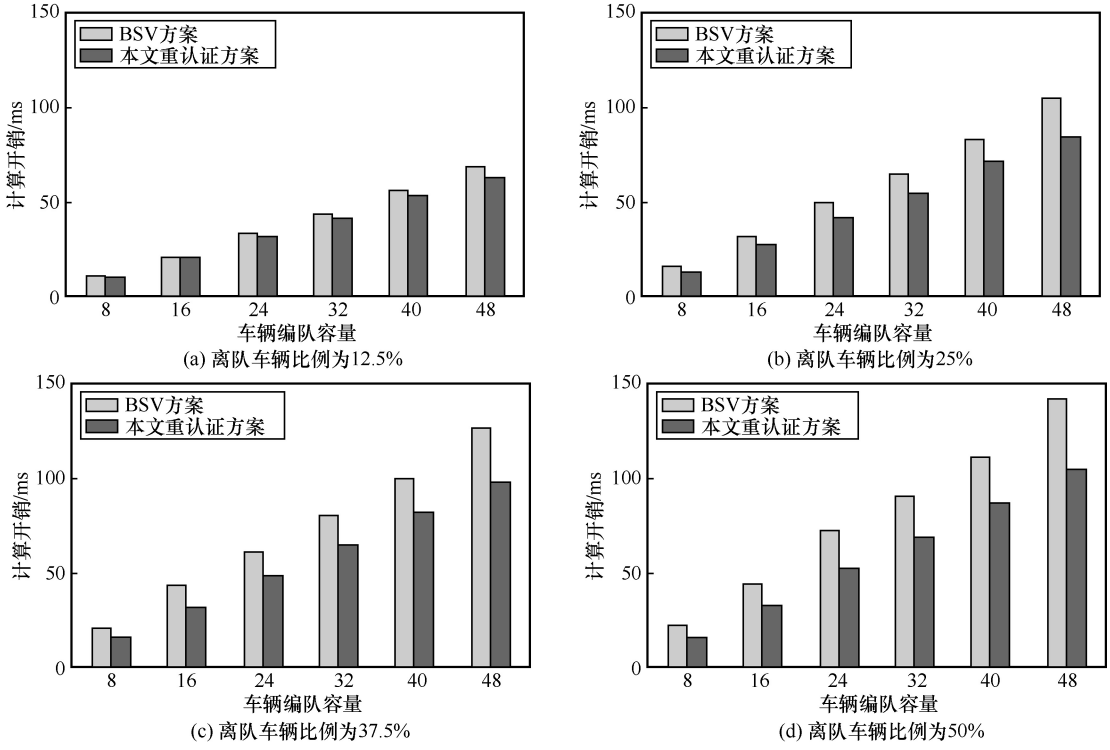

图 6　重认证阶段的计算开销

案一直具有更低的时延。随着车辆编队容量增加，两者时间开销的差距增大；随着离队车辆比例增加，两者时间开销的差距进一步增大。当车辆编队容量为 48 时，本文重认证方案的效率提升最显著，在 4 种离队车辆比例下分别比 BSV 方案降低了 7.6%、20.0%、22.8%和 26.3%的计算开销。

本文重认证方案的计算开销随车辆编队容量的增长趋势更平缓。其原因是重新划分验证车辆范围时，BSV 方案均采用二分方法，而本文重认证方案基于二进制编码思想，当部分车辆重认证成功时，后续划分的范围变小，有效减少定位离队车辆的迭代次数和计算开销。

6.4 区块共识过程

为了评估区块共识过程引入的额外时延，本文在 Hyperledge 平台上部署基于 Go 语言编写的区块共识链码，通过并发测试方法提交区块上链请求，计算区块共识平均时延。

图 7 展示了区块共识平均时延随边缘计算服务器数量和车辆编队容量变化的趋势。当边缘计算服务器数量达到 20 且车辆编队容量为 48 时，区块共识平均时延最高，约为 878 ms。在该时间范围内，高速行驶的车辆编队（行驶速度约为 100 km/h）未驶离当前 ECS 的通信范围，所以该时延在编队构建阶段是可接受的。

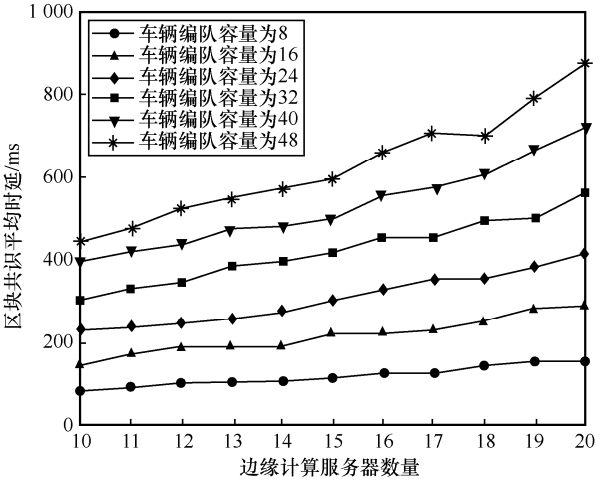

图 7 区块共识平均时延随边缘计算服务器数量和车辆编队容量变化的趋势

7 结束语

为了兼顾车辆编队跨信任域身份认证的隐私保护和认证效率需求，本文提出了区块链架构下具有条件隐私的车辆编队跨信任域高效群组认证方案。设计了新型区块结构 BM-Tree，实现了多信任域间链上认证参数共享，为高效的跨信任域群组认证提供支撑；采用动态匿名保护车辆身份隐私，通过双线性映射进行信任域参数变换，实现了具有条件隐私的跨信任域群组认证；提出了基于 BM-Tree 的高效群组认证协议，实现了批量身份认证和重认证。本文方案在安全性和计算开销方面优于 3 种对比方法，相比 BLA、MDPA 和 BBA，整体认证时延平均减少了 29%、25%和 53%。

本文方案在保护车辆身份隐私的同时实现了异常成员车辆的匿名可追踪，但是目前匿名追踪工作的实现主要依赖于注册域可信机构本地存储的车辆身份列表，外域可信机构无法独立实现异常车辆的匿名可追踪。下一步将围绕多信任域场景下更加灵活、高效的跨域异常车辆追踪问题展开研究。

参考文献：

[1] LESCH V, BREITBACH M, SEGATA M, et al. An overview on approaches for coordination of platoons[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(8): 10049-10065.

[2] HOEF V D S, JOHANSSON K H, DIMAROGONAS D V. Fuel-efficient en route formation of truck platoons[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(1): 102-112.

[3] LI X H, CHEN T, CHENG Q F, et al. Smart applications in edge computing: overview on authentication and data security[J]. IEEE Internet of Things Journal, 2021, 8(6): 4063-4080.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[5] LIU L, FENG J, PEI Q Q, et al. Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor-critic learning approach[J]. IEEE Internet of Things Journal, 2021, 8(4): 2342-2353.

[6] XIAO T T, CHEN C, PEI Q Q, et al. Consortium blockchain-based computation offloading using mobile edge platoon cloud in Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(10): 17769-17783.

[7] ZHOU H B, XU W C, CHEN J C, et al. Evolutionary V2X technologies toward the Internet of vehicles: challenges and opportunities[J]. Proceedings of the IEEE, 2020, 108(2): 308-323.

[8] BOUALOUACHE A, SENOUCI S M, MOUSSAOUI S. A survey on pseudonym changing strategies for vehicular ad-hoc networks[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 770-790.

[9] 汤永利, 李元鸿, 张晓航, 等. 格上基于身份的群签名方案[J]. 计算机研究与发展, 2022, 59(12): 2723-2734.
TANG Y L, LI Y H, ZHANG X H, et al. Identity-based group signatures scheme on lattice[J]. Journal of Computer Research and Development, 2022, 59(12): 2723-2734

[10] NEUMAN B C, TS'O T. Kerberos: an authentication service for computer networks[J]. IEEE Communications Magazine, 1994, 32(9): 33-38.

[11] MOUSTAFA H, BOURDON G, GOURHANT Y. Providing authentication and access control in vehicular network environment[C]// Security and Privacy in Dynamic Environments. Berlin: Springer, 2006: 62-73.

[12] 杨小东, 安发英, 杨平, 等. 云环境下基于代理重签名的跨域身份认证方案[J]. 计算机学报, 2019, 42(4): 756-771.
YANG X D, AN F Y, YANG P, et al. Cross-domain authentication scheme based on proxy re-signature in cloud environment[J]. Chinese Journal of Computers, 2019, 42(4): 756-771.

[13] ZHANG J H. Improvement of ID-based proxy re-signature scheme with pairing-free[J]. Wireless Networks, 2019, 25(7): 4319-4329.

[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(6): 1832-1843.

[15] YAO Y Y, CHANG X L, MIŠIĆ J, et al. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.

[16] 魏松杰, 李莎莎, 王佳贺. 基于身份密码系统和区块链的跨域认证协议[J]. 计算机学报, 2021, 44(5): 908-920.
WEI S J, LI S S, WANG J H. A cross-domain authentication protocol by identity-based cryptography on consortium blockchain[J]. Chinese Journal of Computers, 2021, 44(5): 908-920.

[17] YANG Y H, WEI L J, WU J, et al. A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network[J]. IEEE Internet of Things Journal, 2022, 9(11): 8078-8090.

[18] LIU J, LI X H, JIANG Q, et al. BUA: a blockchain-based unlinkable authentication in VANETs[C]//Proceedings of 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-6.

[19] BAGGA P, SUTRALA A K, DAS A K, et al. Blockchain-based batch authentication protocol for Internet of Vehicles[J]. Journal of Systems Architecture, 2021, 113: 101877.

[20] CHAUM D, HEYST E. Group signatures[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer, 1991: 257-265.

[21] WANG P, CHEN C M, KUMARI S, et al. HDMA: hybrid D2D message authentication scheme for 5G-enabled VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(8): 5071-5080.

[22] WANG Q P, GAO D Y, FOH C H, et al. Protocols design and area division for privacy-preserving delay-aware authentication in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(11): 11129-11144.

[23] LIU J H, YU Y, JIA J W, et al. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks[J]. Tsinghua Science and Technology, 2019, 24(5): 575-584.

[24] CAI Y, ZHANG H, FANG Y G. 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.

[25] VIJAYAKUMAR P, AZEES M, KOZLOV S A, 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.

[作者简介]

夏莹杰（1982− ），男，浙江宁波人，博士，浙江大学研究员，主要研究方向为智能交通和信息安全。

朱思雨（1998− ），女，湖南邵阳人，浙江大学硕士生，主要研究方向为车联网安全和区块链技术。

刘雪娇（1984− ），女，河南安阳人，博士，杭州师范大学副教授，主要研究方向为网络安全和车联网安全。