计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
2025,34(4):136−145 [doi: 10.15888/j.cnki.csa.009820] [CSTR: 32024.14.csa.009820]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于私有链的自动驾驶汽车速度咨询框架①

谢义莎, 訾玲玲, 姚家鹏

(重庆师范大学 计算机与信息科学学院, 重庆 401331)
通信作者: 谢义莎, E-mail: 1695419083@qq.com

摘　要: 在使用共识速度咨询系统 (consensus speed advisory system, CSAS) 为车队推荐速度时, 常面临服务不可信以及车辆之间发送不正确数据的问题. 此外, 现有研究多集中于平坦道路的速度咨询场景, 如果使用平坦道路的速度推荐, 车辆在斜坡上可能会消耗更多的能量, 无法实现最小能耗优化目标. 为了解决上述问题, 本文提出了一种基于区块链的斜坡共识速度咨询框架. 该框架是将现有的共识速度咨询系统扩展至道路斜坡场景, 以进一步解决了自动驾驶车辆在道路斜坡上的能耗最小的优化问题. 同时, 引入了私有区块链和加密原语, 以确保服务可信以及车辆之间数据传输的隐私性. 通过以太坊私有区块链和 Truffle 来实现该框架, 实验结果表明, 此框架能够在斜坡场景下提供可信的共识速度推荐, 并有效地降低车辆能耗.

关键词: 区块链; 数据隐私; 速度咨询; 道路斜坡

引用格式: 谢义莎,訾玲玲,姚家鹏.基于私有链的自动驾驶汽车速度咨询框架.计算机系统应用,2025,34(4):136–145. http://www.c-s-a.org.cn/1003-3254/9820.html

Private-blockchain-based Speed Advisory Framework for Autonomous Vehicles

XIE Yi-Sha, ZI Ling-Ling, YAO Jia-Peng

(College of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China)

Abstract: When using a consensus speed advisory system (CSAS) to recommend speeds for vehicle fleets, challenges often arise regarding the untrustworthiness of the service and the transmission of incorrect data among vehicles. Additionally, existing research mainly focuses on speed advisory scenarios for flat roads. If the speed recommendations for flat roads are applied to sloped roads, vehicles may consume more energy, failing to achieve the optimization goal of minimum energy consumption. To address these issues, this study proposes a blockchain-based consensus speed advisory framework for sloped roads. This framework extends existing CSAS to sloped road scenarios, further solving the problem of optimizing the minimum energy consumption for autonomous vehicles on sloped roads. At the same time, private blockchains and cryptographic primitives are introduced to ensure the trustworthiness of the service and the privacy of data transmission among vehicles. By implementing this framework with Ethereum private blockchains and Truffle, experimental results show that the framework can provide trustworthy consensus speed recommendations in sloped road scenarios and effectively reduce vehicle energy consumption.

Key words: blockchain; data privacy; speed advisory; road slope

随着交通运输越来越复杂, 面临着交通拥堵、环境污染和能源消耗过高等严重问题[1,2]. 车辆的能源消耗过高对能源资源造成了巨大压力, 发展新能源汽车、优化交通流量、推广节能驾驶等方法能够降低能

① 基金项目: 重庆市教育科学规划重点课题 (K22YE205098); 重庆师范大学博士科研启动基金 (21XLB030, 21XLB029)
收稿时间: 2024-09-20; 修改时间: 2024-10-23; 采用时间: 2024-11-12; csa 在线出版时间: 2025-02-28
CNKI 网络首发时间: 2025-03-03

源消耗, 提高交通系统的能源利用效率[3−5]. 其中, 共识速度咨询系统 (consensus speed advisory system, CSAS) 作为智能速度咨询系统 (intelligent speed advisory, ISA) 的一种特殊类型, 为同一路段或方向上行驶的一组车辆推荐共识的速度[6−8], 可以带来减少排放、降低能耗、增加交通吞吐量以及提高安全和健康的好处[9,10].

如今, CSAS 的研究在 ISA 领域迎来了重大的发展[11−13]. 然而, 随着对数据隐私性关注的增加, 最近的一些研究开始着重考虑如何在保护数据隐私的前提下获得最优速度[14−16]. 不过这些研究都是基于集中式架构, 要求车辆将私人数据发送到中央服务器上以计算最优速度. 如果中央服务器或者提供商存在不可信, 那么就可能发生私人数据泄露问题, 影响数据的安全性. 除此之外, 这些研究中还忽视了车辆成员间可能发送不正确数据的情况, 导致了速度推荐的失败. 因此, 本文旨在解决确保服务可信性以及车辆成员间发送数据是否正确的问题.

以往的 CSAS 研究主要集中在平坦道路场景, 但美国国家可再生能源实验室 (NREL) 的研究发现, 道路坡度可能会影响轻型汽车的能耗, 占比可达 1%–3%[17]. 其他研究也表明, 道路坡度对车辆的能源效率有着显著影响[18−21]. 在文献[22]中, 提出了标准化能耗最小策略以提高车辆在道路坡度上的能源效率, 通过动能转换因子将能耗降至最低, 该策略节省了 5.9% 的能耗. 另一文献[23]中, 提出了一种用于电动汽车的预测性节能控制方法, 通过自动调整重量系数, 使得车辆在道路坡度上的节能率达到最高. 因此, 道路坡度对车辆的经济性能影响重, 尤其在提高车辆能源效率方面尤为重要. 然而, 目前道路坡度上的速度咨询研究并未明确考虑自动驾驶车辆在此条件下提高能源效率的问题. 此外, 文献[24]中指出道路安全是一个严重的社会和技术问题, 车辆不遵循安全约束可能会导致碰撞事故, 从而构成潜在风险, 也限制了 CSAS 的实际部署. 因此, 提高道路斜坡场景上的能源效率问题也是至关重要的.

本文针对的是道路斜坡上的车队场景, 提出了私有链的自动驾驶汽车共识速度咨询框架, 这个框架部署在私有区块链上, 旨在提供安全可信和保护隐私的方法, 为车队提供共识速度推荐并确保车队的安全. 本文采用以太坊私有区块链作为 CSAS 的去中心化骨干, 可以有效地解决信任问题. 此外, 本文还使用了 (n, t, n) 可验证秘密共享方法, 该方法不仅可以保护车辆的数据隐私, 还可以验证所传输的数据的正确性. 同时, 本文根据文献[25]去制定了安全约束问题, 以确保道路安全. 因此, 本文在降低车队能耗的同时, 保证了道路安全.

总而言之, 本文的主要贡献可以总结为以下几点.

提出了基于私有区块链自动驾驶汽车的速度咨询框架, 该框架能够为自动驾驶车辆在斜坡道路上推荐共识速度, 并提供了服务信任和数据隐私的保障, 为解决道路斜坡上车辆能源效率问题提供了新的解决方案.

通过车辆能耗模型, 本文得出了适用于道路斜坡上的优化目标, 为解决斜坡道路上车辆能耗优化问题提供了理论基础. 同时使用了隐私保护方法在速度咨询时将数据进行保护.

在以太坊平台上实现所提出的 CSAS 原型, 并进行详细的评估, 实验结果表明, 所提出的 CSAS 在斜坡道路实时速度推荐方面具有良好的性能表现.

1 相关工作

在本节中, 将分别根据共识速度咨询系统的设计目标和推荐场景, 对共识速度咨询系统、隐私保护方法和道路斜坡解决方法进行了综述.

1.1 共识速度咨询系统

共识速度咨询系统 (CSAS) 是通过向一组车辆推荐相同的速度来降低能耗. 文献[8]采用分布式共识算法使电动汽车队获得最佳推荐速度, 最大限度地提高了车队的能源效率. 文献[11]提出了一种基于智能速度自适应系统的应用, 通过优化高速公路限速共识去降低车辆的排放. 文献[7]提出了一种分层自动驾驶其次导航架构, 由车道和速度咨询系统与轨迹跟踪模块组成, 在考虑乘客舒适度的同时减少了行程时间, 也降低了能耗. 文献[13]考虑到共识速度咨询系统会无意中增加车辆的能源使用, 阻碍车辆的参与, 所以提出了信任感知的共识速度推荐方案, 使用了多权重主观逻辑模型对声誉值进行计算, 会根据声誉的变化来推荐速度, 以此来车辆能耗增加的潜在抑制作用. 以上是不同于以往的研究向单个车辆发送速度建议, 而是使用了共识速度建议的方法去降低了车队能耗.

1.2 隐私保护方法

在 CSAS 可以降低车辆能耗后逐渐出现了一些研究, 试图以隐私保护的方式去实现速度咨询, 比如基于推导的隐私保护的共识速度咨询系统[15], 和基于多方计算的速度咨询系统[14]. 尤其是在文献[15]中, 提出的

系统是将推荐的过程将其划分为一组迭代, 在迭代中, 车辆会将特定速度下的成本函数导数显示给基站, 以计算出最优速度. 由于只使用导数值作为隐含信息, 可以很好地保护车辆的隐私. 文献[14]提出了一种基于多方计算的速度咨询方法. 是将车辆在一定速度下的排放值分成几部分, 其中一部分保存在本地, 另一部分与其他车辆交换. 每辆车都会汇总本地和接收到的排放值, 并将信息发送到基站, 车辆之间交换部分数据, 对多方持有的数据集进行隐私保护计算, 以获得最优速度.

但是, 上述隐私保护研究是基于中心化架构的, 会遇到所提出的服务信任问题. 文献[12]提出了使用区块链技术和基于 Shamir 秘密共享方法, 虽然解决了服务信任问题, 但该方法中会出现车辆成员之间所发送的数据不真实. 然而本文所设计的系统在保护隐私和实时性的范围内很好地解决这个问题.

1.3 道路斜坡解决方法

适当地控制速度, 可以促使交通道路的安全驾驶, 避免道路事故的发生. 文献[26]提出了一种多智能体 RL (reinforcement learning) 算法 CommPPO, 用于控制车辆列队, 以提高交通振荡中的能源效率. 该方法中的车辆会及时对前方车辆做出反应, 避免紧急减速. 因此, 此方法与多智能体 RL 算法和 MPC (multiparty computation) 算法相比, 可以减少交通干扰和油耗.

文献[27]提出了两种实时能源导向的驾驶策略去降低电动汽车在具有坡度的公路上的能耗, 首先将车辆动能转换为电池能耗, 通过最小化归一化总能耗去计算出面向能量的车辆控制序列. 其次, 开发了改进的模型预测控制去实现了优化和计算效率的平衡.

文献[28]提出了一种两层控制架构, 第 1 层是通过交通信号灯和道路坡度信息去优化领导车辆的长期运动剖面, 第 2 层是短期适应, 车辆之间保持安全距离. 两者采用牛顿算法去解决. 降低了车辆避红灯的概率, 提高了燃油效率. 上述研究中考虑了单个车辆在斜坡上的能耗问题, 但面对车队时, 该如何解决整个车队的总能耗问题并未考虑.

CSAS 的目标是降低自动驾驶车队在高速公路或城市道路上行驶的总体能耗. 本文的共识速度咨询系统旨在以最小的跟随距离和最大的道路速度限制作为安全状态约束, 最大限度地减少道路斜坡场景下的能源消耗. 然后从设计目标和推荐场景的角度分析了速度推荐的相关工作.

表 1 列出了一些这方面的相关研究.

表 1 不同文献中的设计目标和推荐的场景

参考文献	设计目标				推荐场景	
	道路斜坡	安全	生态驾驶	隐私保护	单个车辆	车辆队
[15]	×	×	√	√	×	√
[8]	×	×	√	√	×	√
[14]	×	×	√	√	×	√
[6]	×	×	√	√	×	√
[26]	√	√	√	×	×	√
[27]	√	√	√	×	√	×
[28]	√	√	√	×	√	×
[22]	×	√	√	×	√	×
本文	√	√	√	√	×	√

2 速度咨询框架

在本节中, 将描述本文中提出的框架. 首先, 介绍了该框架的架构设计. 然后, 描述了本文所要求的优化目标. 最后, 将解释如何保护数据隐私, 以及如何获得速度建议.

2.1 架构设计

首先, 将介绍拟议的速度咨询系统的总体框架, 并解释该框架内的核心概念. 该框架的体系结构如图 1 所示.

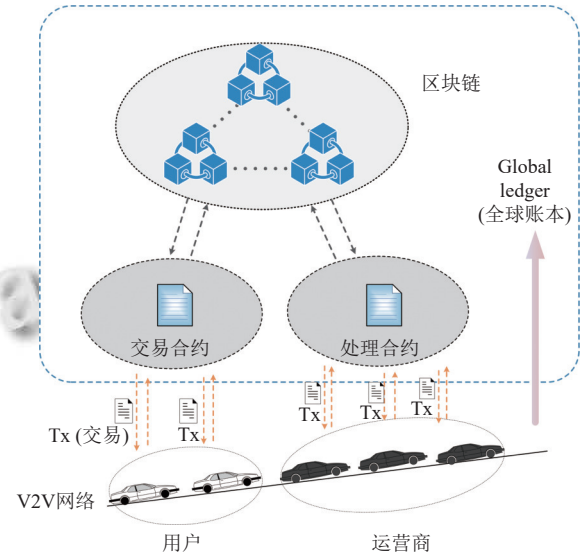

图 1 速度咨询框架

在该框架中, 首先输入车辆参数和速度, 其中参数为车辆的相应参数, 如第 2.2 节中式 (4) 所示. 然后, 在满足目标范围内的约束条件的同时, 使用最优化的目标方程. 接下来, 使用隐私保护方法对数据进行保护, 最终生成与最小能耗相关的速度为输出.

用户和运营商: 本文中, 自动驾驶车辆既代表用户也代表运营商. 用户会参与到该服务中去得到速度推

荐. 运营商则需要帮助用户去计算推荐速度来获得奖励, 并且将从运营商中随机选取一位领导者去收集速度交易后放入区块, 领导者由此可以获得奖励.

道路类型: 本文中考虑的道路类型是具有一定坡度的道路, 车辆在该道路上去获得速度推荐.

交易合约: 用户通过交易合约发起速度交易, 所谓交易就是用户向该服务发送传输映射的过程. 交易合约由两部分组成. 首先是需要将用户发起的速度交易进行收集, 其次是该合约需要向用户返回处理合约计算出的推荐速度.

处理合约: 运营商将计算的结果发送到合约中来验证, 并更新车队的推荐速度. 智能合约一旦被定义了, 就会自发执行响应的某些触发事物.

车队: 车队是本文中的一组用户, 会参与本文的速度咨询服务来推荐共同的速度.

激励: 在本文中为了鼓励车队积极参与该服务而提供的奖励. 使用一种资产的形式去奖励, 在该服务中用户和运营商都会使用一个地址公钥来启动事务, 用户需要向该服务支付一定费用才能使用推荐服务. 那么, 运营商只有正确计算出总能耗值并获得最优速度, 它才能获得一定的费用奖励, 这笔费用会发送到该运营商的账户中.

私有区块链: 私有区块链对数据具有严格的访问控制, 同时在车队速度推荐中处理速度更快, 能够实时响应速度推荐请求. 当运营商在处理合约中完成计算并验证结果后, 该结果会被添加到私有区块链中. 由于私有区块链的出块时间可以灵活调整, 因此可以通过缩短出块时间来提高交易处理速度, 从而满足本文的性能需求.

共识机制: 共识机制是采用随机选择实现的, 因为所要计算的任务不复杂, 参与计算的算子完成计算的概率很大, 将会从中随机选择一名算子来担任领导者, 如果计算正确, 那么领导者获得相应的奖励. 随机选择可以大幅简化共识过程, 提升相应的速度.

因此, 通过缩短出块时间和调整共识机制, 私有区块链能够将系统延迟控制在 1 s 以内, 正如文献[12]和后文实验结果所示, 这是满足的.

在本框架中, 速度咨询的工作流程如图 2 所示. 首先用户会通过本文的隐私保护方法来将速度-能耗映射进行保护. 其次, 用户需要共享该映射去添加到交易合约中去执行交易. 操作员将从交易合约中下载交易, 计算在安全状态约束下的速度所对应的总能耗. 然后, 找到最小能耗的速度发送给处理合约, 这时, 操作员中会随机选择一位领导, 该合约对领导和其他操作员的计算结果进行验证. 验证通过, 领导者将获得奖励. 最后, 交易合约从处理合约中获得推荐的速度, 用户的速度将更新为交易合约返回的推荐速度.

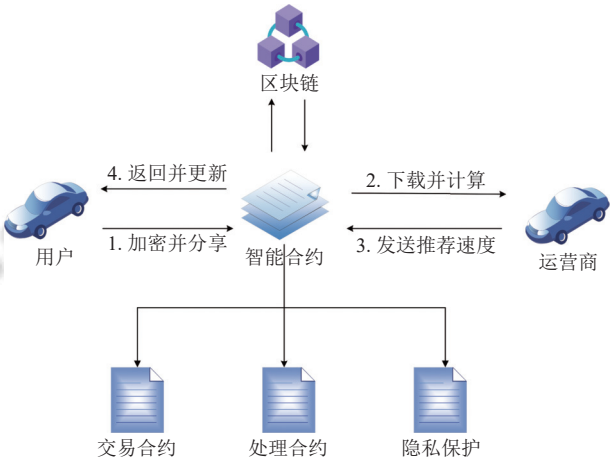

图 2 工作流程

2.2 优化目标

在这一部分中, 将描述整个框架的优化目标. 在框架中需要得到一个速度和能耗的相关公式, 输入数据会通过此公式得到车队最小能耗对应的速度, 将该速度向车队进行推荐达到降低能耗的目的, 在速度咨询的过程中会采用隐私保护方法对数据进行保护.

首先将根据文献[29]中提出的能耗模型来得到速度能耗的目标, 如式 (1) 所示:

$$p = p_n + p_h + p_l \tag{1}$$

其中, $p_n = \dfrac{rR^2}{K^2}\left(ma + Av^2 + f_r mg + mg\sin\theta\right)^2$ 是电机的功率, r (以Ω为单位) 表示导体的电阻; K 是电枢常数 K_a和磁通量ϕ_d的乘积; R是轮胎的半径; m是车的重量; g 为重力加速度$\left(g = 9.81\ \text{m/s}^2\right)$; $A = \dfrac{\rho C_D A_f}{2}$ 是空气动力阻力常数, 由空气密度ρ决定 (单位为kg/m^3)、车辆正面区域A_f和阻力系数C_D; f_r是滚动阻力系数, v是车辆的速度, θ表示道路坡度; $p_h = v(Av^2 + f_r mg + mg\sin\theta)$是由于行驶过程中阻力引起的功率; 并且 $p_l = mav$是从加速 (或减速) 中获得的可能能量. p是上述 3 个功率的总和. 假设加速度为$2\ \text{m/s}^2$. 本文的道路坡度根据文献[21]来设置, 考虑了平均坡度为 4% 的缓坡情景. 本文不考虑辅助能耗 (比如空调).

应用安全约束的目标是最大限度地减少自动驾驶车队的能量消耗, 同时通过允许车辆遵守道路速度限制并避免碰撞来保证其安全. 根据采用文献[24]中的安全约束如下所示:

$$d_1 = v_i - v_{\max} \tag{2}$$

$$d_2 = L_i - (L_{ei} - \tau_{\min}) \tag{3}$$

其中, L和L_e分别表示当前车辆和前一车辆的位置.

接着将根据上述提供的能耗模型和约束条件来得到所需的优化目标. 在这里, 将进行简单描述本文的问题. 假设有 M 辆自动驾驶汽车沿同一方向行驶在一段禁止行人或其他社会车辆的斜坡道路上, 其中 $M = \{1,2,\cdots,M\}$表示索引车辆的集合. 设$v_i(k)$为第i自动驾驶汽车在时隙k时的推荐速度, $v(k) = [v_1(k), v_2(k), \cdots, v_M(k)]^{\mathrm{T}}$为所有自动驾驶汽车的推荐速度矢量. 此外, 假设每个车辆都与一个能耗成本函数B相关联, 该函数对车辆i在速度$v_i(k)$下的能耗进行建模, 并将$(v_i(k), B_i(v_i(k)))$转换为速度-能耗映射. 因此, 本文速度咨询的优化目标可以描述如下:

$$\begin{cases} Y_{\min} = \sum_{i=1}^{m} B_i = \sum_{i=1}^{m} \int_t^{t'} p_i \mathrm{d}t / H \\ \quad = \sum_{i=1}^{m} \left(\alpha v_i^3 + \beta v_i^2 + \omega v_i + \lambda + \dfrac{\gamma}{v_i} \right) \\ \text{s.t. } d_1 \leqslant 0, d_2 \leqslant 0 \end{cases} \tag{4}$$

式 (4) 是从式 (1) 中得出的速度和能耗相关的函数. 式中的$\alpha,\beta,\omega,\lambda,\gamma$都是由式 (1) 里的公式得到的参数, H是车辆行驶的距离, t和t'是车辆行驶过程中的起始和终止时间, 这里的约束条件d_1是车辆的运行速度低于最大限制速度, d_2是车辆之间的距离不应该小于最小跟随距离. 本文的目标是最小化车队的总能耗Y. 在推荐过程中, 车队中的每辆车都需要满足约束条件, 当车辆从初始速度行驶到推荐速度时要保证道路安全. 因此, 通过本节中的速度-能耗计算公式, 可以计算出在该路段下能耗最低的推荐速度, 并将该速度推荐给车辆. 首先, 将公式中涉及车辆的参数和速度数据代入到该公式中; 接着, 根据输入的数据就可以求出车辆在该路段的最低能耗值, 而这个最低能耗所对应的速度就是推荐速度; 最后将这个推荐速度提供给车队. 这样, 车辆通过遵循推荐速度, 在满足安全约束的同时能够实现最低能耗的行驶状态, 从而实现整个车队在该路段上的能耗优化.

2.3 速度咨询的隐私保护

在进行速度咨询的过程中采用了隐私保护方法对数据进行保护, 那么该部分将介绍此框架中如何使用隐私保护方法来对数据进行保护. 本文使用的是 (n, t, n) 可验证秘密共享方案[30]来保护数据隐私. 具体来说, 方案中的份额生成和分发的过程中所有成员都会参与其中, 从而使得该方案不需要一个互信的第三方作为份额的分发者, 这一点解决了 Shamir 的方案需要依赖分发者的局限. (n, t, n) 秘密共享方案中的 3 个参数分别代表了分发者的个数、方案的门限值和成员的个数. 加入可验证机制后的 (n, t, n) 可验证秘密共享方案因为不需要可信分发者的参与, 保证了秘密只能被拥有有效份额的诚实成员才能重构, 所以该方案具有安全重构的性质. 为了保护车辆之间的数据隐私, 将使用该方案去解决此问题, 如图 3 所示是该方案的实施说明.

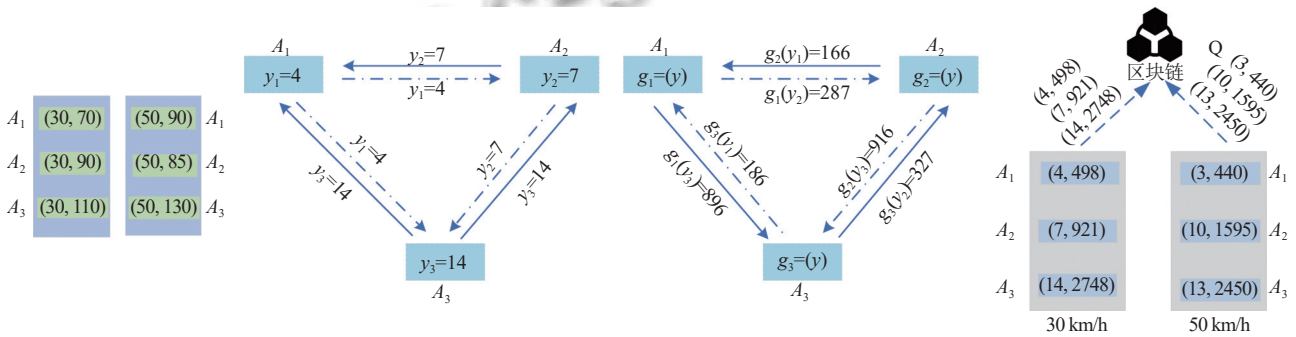

图 3 隐私保护方法

首先假设该方案中有 3 辆车分别为A_1、A_2和A_3, 在这里, 给出车速为 30 km/h 和 50 km/h 的能耗值. 在这个框架中需要找出在可能的情况下哪个速度可以使得能耗值最低. 主要有以下步骤.

(1) 随机数和多项式的生成: A_1、A_2和A_3在 30 km/h 速度下的速度-能耗映射分别为 (30, 70)、(30, 90) 和

(30, 110). 车速所对应的总能耗是本文所要保护的秘密, 可以看出总能耗为 270. 能耗值$B_i(v_i), i\{1,2,3\}$在速度发射映射中被认为是秘密共享. 这里的$B_1(v_1)=70$, $B_2(v_2)=90, B_3(v_3)=110$. 对于 3 辆车首先生成 3 个随机数和随机多项式 $g_1(y)$, $g_2(y)$, $g_3(y)$, $g_i(y)=c_1\times y^2+c_2\times y+B_i(v_i)$, c_1 和c_2 是随机数. 这里假设$c_1=4, c_2=3$.

(2) 随机数共享: 3 辆车之间彼此相互发送它们的随机数. 比如说A_1发送y_1给A_2, 然后从A_2那里接收y_2.

多项式结果共享: 3 辆车之间相互接收随机数, 然后使用随机多项式进行计算得到相应的结果, 并公开承诺信息$U_{ij}=f^{c_{ij}}$, 再将结果彼此之间相互发送. 比如说A_1从A_2接收y_2, 计算$g_1(y_2)$并将结果发送给A_2, 相应地其他车辆也是如此.

(3) 多项式结果验证: 车辆得到相互发送的多项式结果后会将其进行结果验证是否有效.

$$p^{g_j(y_i)}=\prod_{j=0}^{2}U_{ij}^{y_i^j} \tag{5}$$

如果等式成立, 那么车辆认定该结果有效. 否则车辆会给其他车辆去验证, 如果其他车辆验证后认定该结果是无效的, 就会要求该车辆重新发送正确的结果.

(4) 本地聚合和上传: 当 3 辆车验证完彼此之间发送的多项式结果有效后, 对于每辆车A_i将在本地执行$G_i(y)=\sum_{j=1}^{3}g_j(y_i)$. 然后将共享映射$(y_i, G_i(y))$发送到区块链去进行最后的速度推荐. 在本文的例子中, A_1, A_2和A_3发送 (4, 498), (7, 921), (14, 2748). 最后 3 辆车的数据如图 3 所示.

(5) 隐私保护计算: 完成以上步骤后, 区块链Q已经收到了A_1, A_2和A_3上传的共享映射. 之后, 处理合约中的运营商会下载这些映射, 将使用拉格朗日插值进行计算 30 km/h 和 50 km/h 的总能耗. 已知$k+1$个点的多项式函数, 假设任意两个点互不相同, 那么使用拉格朗日插值为:

$$U(y)=\sum_{j=1}^{k}w_jG_j(y)=G_j(y)\prod_{i=1,i\neq j}^{k}\frac{y-y_i}{y_j-y_i} \tag{6}$$

根据该公式, 运营商就可以得到在 30 km/h 速度下的 3 辆车的总能耗为 270 Wh/km.

(6) 结果输出: 通过上述步骤, 运营商得到 30 km/h 和 50 km/h 速度下的总能耗分别为 270 Wh/km 和 305 Wh/km. 然后比较所有速度的能耗, 运营商可以得到推荐的速度, 以达到最小的能耗. 这样车辆就能得到 30 km/h 的推荐速度. 因为该方法是车辆之间相互发送随机数, 随机多项式的系数也是随机生成的, 所以车辆是无法从发送的数据中获得任何有价值的信息, 并且在得到多项式的结果后车辆会进行验证是否有效, 更加确保了数据的真实性和安全性. 因此, 上述车辆的隐私性能得到很好的保护. 当然车辆也能通过只向区块链Q发送共享映射来对私有信息进行保护.

算法 1. 隐私保护方法

输入: 车辆$A=\{A_i|i=1,2,3,\cdots,M\}$.
输出: 推荐速度.

1) 初始化: $(y_i, g_i(y_i))$.
2) for speed in SPEED do
3) // 发送随机速度
4) for i in *range*(M) do
5) for j in *range*(M) do
6) if $i\neq j$ then
7) 车辆A_i从A_j接收随机数y_j.
8) 车辆A_i接收到$(y_i, g_i(y_j))$后计算并生成信息公开承诺$U_{ij}=f^{c_{ij}}$
9) // 发送 $g_i(y)$并验证结果.
10) for i in *range*(M)do
11) for j in *range*(M) do
12) if $i\neq j$ then
13) 车辆A_i获取结果并使用$p^{g_j(y_i)}=\prod_{j=0}^{2}U_{ij}^{y_i^j}$进行有效验证.
14) 车辆A_i从车辆A_j接收一个随机多项式的值$g_j(y_i)$, 并保存在本地.
15) 收集完其他车辆的随机多项式值后, 计算$G_i(y)=\sum_{j=1}^{M}g_j(y_i)$.

根据上面的描述, 可以得出算法 1 中的核心隐私保护方法. 在算法 1 中 M 是车辆数量, 也就是用户, SPEED 是速度范围. 第 4–8 行是随机数的共享和公开承诺信息的过程, 第 9–14 行是结果共享验证是否有效和隐私计算的过程.

综上所述, 本节重点介绍了本文框架中的架构设计、优化目标以及在本框架中所使用的隐私保护方法.

3 评价方法与结果

通过模拟对本文的共识速度咨询系统进行了详细的实验评估. 在本节中, 首先介绍实验设置, 然后从评估指标中去展示实验结果.

3.1 实验设置与评价指标

本文的实验是在 64 位 Intel(R) Core(TM) i3-8100 CPU@3.60 GHz, 8 GB RAM 的 Windows 操作系统上部署了一个具有 4 个处理器和 4 GB 内存的 Linux 虚

拟机, 并安装了 Ubuntu 22.04.2 操作系统上完成的.

(1) 能耗成本函数: 根据上述的能耗模型得到能耗的成本函数如图 4 所示.

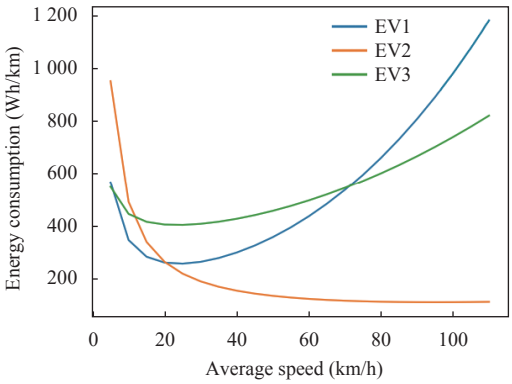

图 4 能耗成本函数曲线

(2) 车辆类型: 车辆类型的参数根据文献[29,31]得到, 如表 2 所示.

表 2 电动汽车类型参数

汽车类型	车辆1	车辆2	车辆3
m (kg)	350	100	1 266
R (m)	0.23	0.17	0.5
r (Ω)	0.08	0.06	0.11
K	4.56	0.75	10.08
A	1.26	0.027	1.3
f_r	0.006	0.003	0.006

(3) 车队: 使用 Python 3.10.9 来模拟车队场景. 在本测试中, 车队的数量设置为 10–100, 车辆数量间隔为 10. 每种车辆的类型根据图 4 中的来随机指定, 车辆的初始位置也是随机指定的.

(4) 区块链仿真: 本文的框架实现是由以太坊私有区块链和 Truffle. 私有区块链中引入隐私保护机制, 使用 UDP 协议在车辆之间进行数据传输.

本文采用节能率作为评价车辆能耗优化效果的指标, 节能率越高, 表示车辆的能耗降低效果越好, 反之, 节能率越低, 则意味着能耗优化效果较差.

3.2 仿真与结果

为了验证本研究所提议的速度咨询框架, 将使用评价指标对其进行评估.

本文中的车队以随机速度行驶的车辆的总能耗与以该研究给出的推荐速度行驶的车辆的总能耗进行对比. 结果如图 5 所示. 从中可以得出结论, 如果车队以随机速度行驶将会增加车辆的总能耗, 反之使用该研究推荐的速度将降低车队的总能耗.

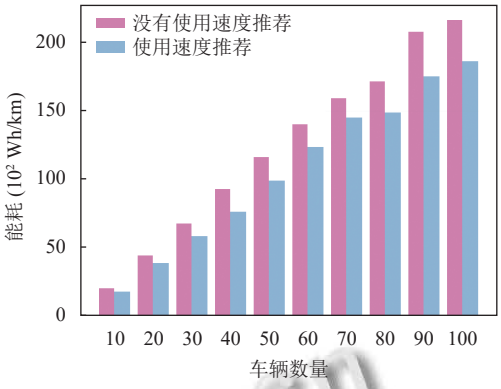

图 5 随着车辆数量的增加, 使用和未使用该服务的比较

表 3 显示不同方法的节能比较, 将本文的方法与文献[26,27,32,33]中的方法进行节能比较. BiCNet 和 PS-PPO 方法在节能上分别为 2.79% 和 3.45%, CommPPO 可以节省能耗为 11.6%, NCMS 和 IMPC 两种策略分别节省能耗为 8.23% 和 11.64%. 然而, 本文的方法在节省能耗上为 11.77%. 显然, 本文的方法在节省能耗上表现更好.

表 3 不同方法的节能比较

算法	节能率 (%)
BiCNet	2.79
PS-PPO	3.45
CommPPO	11.6
NCMS	8.23
IMPC	11.64
REACC	11
本文	11.77

在本研究的速度咨询中, 车辆的不断增加, 处理事务需求也在不断增加, 一轮速度推荐的开销也逐渐增加. 这是因为以太坊私有区块链网络和计算资源有限造成的. 可以通过缩短以太坊私有区块链的出块时间和调整共识机制, 就可以将延迟控制在 1 s 以内. 一轮速度推荐的时间成本如图 6 所示. 图 6 中可以看出当车辆数量 100 时, 时间成本在 900 ms 左右, 这是可以接受的.

本文的速度-能耗映射被当作是秘密, 运营商只有车队特定速度下才能计算总的能耗值. 该方法的随机多项式保护了能耗的成本函数 B_i' 的隐私性, 使用函数 $f(B_i)=s\times B_i+t$ 来映射 B_i'. 如图 7 所示, 此方法在不影响原始问题的最优解的情况下, 还能很好的保护局部和总能耗的隐私.

本文图 8 对比了有无隐私保护下的时间开销和能耗. 结果显示, 无隐私保护的时间开销变化幅度较大,

导致系统性能不稳定, 而有隐私保护的时间开销则趋于平稳. 此外, 使用无隐私保护速度推荐的能耗高于有隐私保护速度推荐的能耗. 这表明, 使用隐私保护不仅提升了系统的稳定性, 还有效降低了能耗.

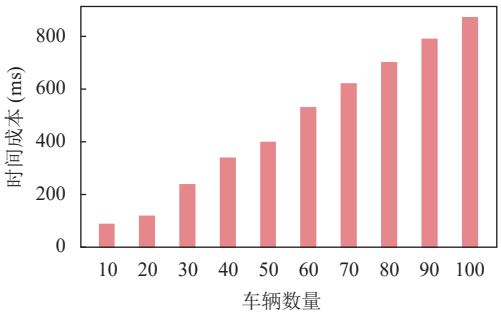

图 6 随着车辆的不断增加, 1 轮推荐速度的时间成本

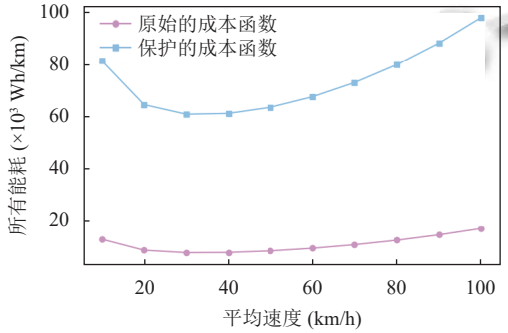

图 7 30 辆车原始和保护的成本函数总能耗

在以太坊智能合约中, 数据传输都需要一定量的 gas, 因此 gas 消耗来评估区块链上执行操作的开销. 图 9 显示了链上操作的 gas 消耗量, 可以看出在接收交易映射时 gas 消耗量较高外, 其他操作不超过 3 万单位气量. 这是因为在接收交易映射时交易合约需要存储交易细节.

在这里, 本文测试了以下函数的吞吐量和延迟的性能如图 10 所示, 是随着发送速率从 20 不断的增加到 100 的情况下相应的函数的吞吐量和延迟. 显而易见, 随着速率的增加吞吐量也在线性增加; 但延迟不随速率增加而波动, 并稳定得保持在 60 ms 以内.

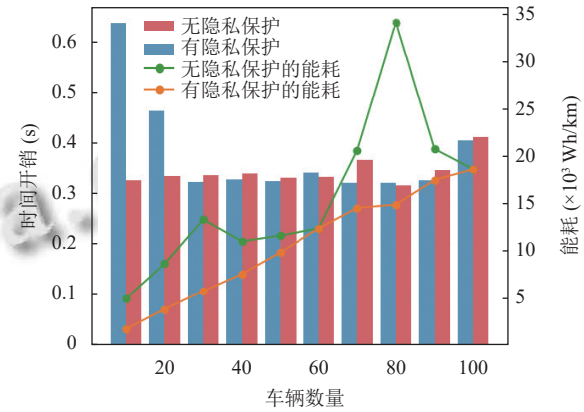

图 8 有无隐私保护对比

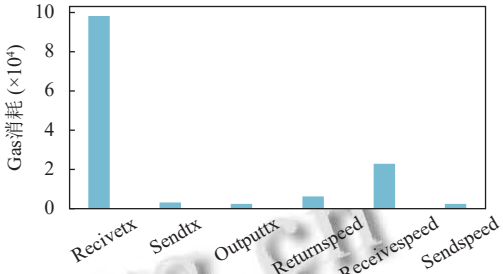

图 9 Gas 消耗

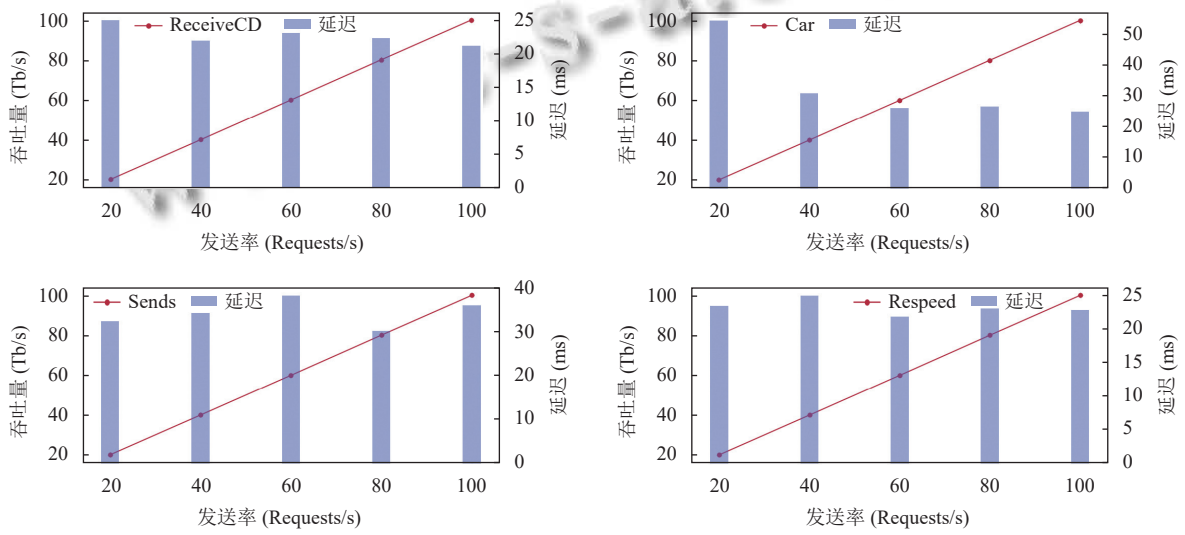

图 10 延迟和吞吐量性能

4 结论与展望

在本文中, 提出了一种基于私有区块链的安全共识速度咨询框架. 与以往不同的是, 本框架专注于道路斜坡上的自动驾驶车辆队的能耗优化. 引入安全状态约束可以避免车辆间发生碰撞且遵守了交通规则. 除此之外, 为了保证服务信任和保护数据隐私, 在私有区块链架构中引入了 (n, t, n) 可验证秘密共享方法. 本文具体介绍了共识速度咨询框架的详细设计、工作流程和评估实验结果. 通过仿真平台的实验结果表明, 此框架能够以可信和隐私的方式去实现速度推荐, 并确保自动驾驶车辆队的安全, 从而降低了自动驾驶车辆队的能耗. 在未来的研究中, 将探索道路上存在其他社会车辆的情况. 特别是, 在燃油车辆和电动车辆的混合场景下, 将研究如何实现实时的速度推荐, 进一步优化道路交通的能源效率.

参考文献

1 Sun XL, Li ZG, Wang XL, *et al*. Technology development of electric vehicles: A review. Energies, 2019, 13(1): 90. [doi: 10.3390/en13010090]

2 Fiori C, Arcidiacono V, Fontaras G, *et al*. The effect of electrified mobility on the relationship between traffic conditions and energy consumption. Transportation Research Part D: Transport and Environment, 2019, 67: 275–290. [doi: 10.1016/j.trd.2018.11.018]

3 Al-Rubaye S, Conrad C, Tsourdos A. Communication network architecture with 6G capabilities for urban air mobility. Proceedings of the 2024 IEEE International Conference on Consumer Electronics (ICCE). Las Vegas: IEEE, 2024. 1–6.

4 Sharma GP, Patel D, Sachs J, *et al*. Toward deterministic communications in 6G networks: State of the art, open challenges and the way forward. IEEE Access, 2023, 11: 106898–106923. [doi: 10.1109/ACCESS.2023.3316605]

5 Nguyen VL, Hwang RH, Lin PC, *et al*. Toward the age of intelligent vehicular networks for connected and autonomous vehicles in 6G. IEEE Network, 2022, 37(3): 44–51.

6 Griggs W, Russo G, Shorten R. Leader and leaderless multi-layer consensus with state obfuscation: An application to distributed speed advisory systems. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(3): 711–721. [doi: 10.1109/TITS.2017.2700199]

7 Tariq FM, Isele D, Baras JS, *et al*. SLAS: Speed and lane advisory system for highway navigation. Proceedings of the 61st IEEE Conference on Decision and Control (CDC). Cancun: IEEE, 2022. 6979–6986.

8 Liu MM, Ordónez-Hurtado RH, Wirth FR, *et al*. An intelligent speed advisory system for electric vehicles. Proceedings of the 2015 International Conference on Connected Vehicles and Expo (ICCVE). Shenzhen: IEEE, 2015. 84–88.

9 Krause J, Thiel C, Tsokolis D, Samaras Z, Rota C, Ward A, Prenninger P, Coosemans T, Neugebauer S, Verhoeve W.Eu road vehicle energy consumption and CO_2 emissions by 2050 —Expert-based scenarios. Energy Policy, 2020, 138: 111224. [doi: 10.1016/j.enpol.2019.111224]

10 Smith SW, Kim Y, Guanetti J, *et al*. Balancing safety and traffic throughput in cooperative vehicle platooning. Proceedings of the 18th European Control Conference (ECC). Naples: IEEE, 2019. 2197–2202.

11 Gu YQ, Liu MM, Crisostomi E, *et al*. Optimised consensus for highway speed limits via intelligent speed advisory systems. Proceedings of the 2014 International Conference on Connected Vehicles and Expo (ICCVE). Vienna: IEEE, 2014. 1052–1053.

12 Li JB, Li SK, Cheng L, *et al*. BSAS: A blockchain-based trustworthy and privacy-preserving speed advisory system. IEEE Transactions on Vehicular Technology, 2022, 71(11): 11421–11430. [doi: 10.1109/TVT.2022.3189410]

13 Li SK, Li JB, Liang Y, *et al*. TD-SAS: A trust-aware and decentralized speed advisory system for energy-efficient autonomous vehicle platoons. IEEE Transactions on Intelligent Vehicles, 2023. [doi: 10.1109/TIV.2023.3347870]

14 Liu M, Cheng L, Gu Y, Wang Y, Liu Q, O'Connor NE. MPC-CSAS: Multi-party computation for real-time privacy-preserving speed advisory systems. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(6): 5887–5893. [doi: 10.1109/TITS.2021.3052840]

15 Liu MM, Ordóñez-Hurtado RH, Wirth F, *et al*. A distributed and privacy-aware speed advisory system for optimizing conventional and electric vehicle networks. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1308–1318. [doi: 10.1109/TITS.2015.2502063]

16 谭朋柳, 徐滕, 杨思佳, 等. 区块链隐私保护技术研究综述. 计算机应用研究, 2024, 41(8): 2261–2269.

17 Wood E, Burton E, Duran A, *et al*. Contribution of road grade to the energy use of modern automobiles across large datasets of real-world drive cycles. Golden: National Renewable Energy Laboratory, 2014.

18 Liu K, Yamamoto T, Morikawa T. Impact of road gradient

on energy consumption of electric vehicles. Transportation Research Part D: Transport and Environment, 2017, 54: 74–81. [doi: 10.1016/j.trd.2017.05.005]

19 Ahiska K, Ozgoren MK, Leblebicioglu MK. Energy optimality in electric vehicles along uphill-downhill roads. IEEE Transactions on Intelligent Vehicles, 2021, 6(3): 390–405. [doi: 10.1109/TIV.2020.3033287]

20 Yang Z, Chen H, Dong SY, *et al*. Energy management strategy of hybrid electric vehicle with consideration of road gradient. Proceedings of the 2020 Chinese Control and Decision Conference (CCDC). Hefei: IEEE, 2020. 2879–2885.

21 Zhang J, Jin H. Optimized calculation of the economic speed profile for slope driving: Based on iterative dynamic programming. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(4): 3313–3323. [doi: 10.1109/TITS.2020.3035610]

22 Qu LH, Zhuang WC, Chen N. Instantaneous velocity optimization strategy of electric vehicle considering varying road slopes. Proceedings of the 2019 Chinese Control and Decision Conference (CCDC). Nanchang: IEEE, 2019. 5483–5488.

23 Wu DM, Lin ZF, Du CQ, *et al*. Real-time predictive energy-saving control for electric vehicle based on road slope prediction. International Journal of Energy Research, 2023, 2023(1): 4049672.

24 吕能超, 王玉刚, 周颖, 等. 道路交通安全分析与评价方法综述. 中国公路学报, 2023, 36(4): 183–201. [doi: 10.3969/j.issn.1001-7372.2023.04.016]

25 Li S, Li J, Pei J, Wu S, Wang S, Cheng L. Eco-CSAS: A safe and eco-friendly speed advisory system for autonomous vehicle platoon using consortium blockchain. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7802–7812. [doi: 10.1109/TITS.2022.3232851]

26 Li M, Cao ZH, Li ZB. A reinforcement learning-based vehicle platoon control strategy for reducing energy consumption in traffic oscillations. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(12): 5309–5322. [doi: 10.1109/TNNLS.2021.3071959]

27 Li BB, Zhuang WC, Zhang H, *et al*. A comparative study of energy-oriented driving strategy for connected electric vehicles on freeways with varying slopes. Energy, 2024, 289: 129916. [doi: 10.1016/j.energy.2023.129916]

28 Wang Y, Su R, Wang W, *et al*. Distributed eco-driving algorithm of vehicle platoon using traffic light and road slope information. arXiv:2104.12499, 2021.

29 Wu XK, Freese D, Cabrera A, *et al*. Electric vehicles' energy consumption measurement and estimation. Transportation Research Part D: Transport and Environment, 2015, 34: 52–67. [doi: 10.1016/j.trd.2014.10.007]

30 Harn L, Lin CL. Strong (*n, t, n*) verifiable secret sharing scheme. Information Sciences, 2010, 180(16): 3059–3064. [doi: 10.1016/j.ins.2010.04.016]

31 Tanaka D, Ashida T, Minami S. An analytical method of EV velocity profile determination from the power consumption of electric vehicles. Proceedings of the 2008 IEEE Vehicle Power and Propulsion Conference. Harbin: IEEE, 2008. 1–3.

32 Li BB, Zhuang WC, Zhang H, *et al*. Traffic-aware ecological cruising control for connected electric vehicle. IEEE Transactions on Transportation Electrification, 2024, 10(3): 5225–5240. [doi: 10.1109/TTE.2023.3325403]

33 Yu S, Pan X, Georgiou A, *et al*. A real-time robust ecological-adaptive cruise control strategy for battery electric vehicles. IEEE Transactions on Transportation Electrification, 2024, 10(3): 7389–7404. [doi: 10.1109/TTE.2023.3340670]

(校对责编: 张重毅)