

基于区块链的智能网联车队协同轨迹预测系统

王仁生, 吴天昊, 张琳, 朱孔林

(北京邮电大学信息与通信工程学院, 北京 100876)

摘要: 自动驾驶汽车技术近年来得到了广泛研究与快速发展,但在复杂的交通场景下,自动驾驶汽车面对突然出现的行驶车辆并不能及时避让。针对此问题,基于区块链技术提出智能网联车队的协同轨迹预测系统,智能网联车队中的各个节点与路边基础设施通过长短时记忆网络(LSTM)模型对周边车辆的运动轨迹进行预判,并将得到的结果进行分享,利用区块链技术,智能网联车队与路边基础设施可以对其接收到的信息进行评分,并将汇总后的评分以区块的形式加入存储信誉评分的区块链中。通过该评分,智能网联车队中的车辆可以根据车队中其他节点的信誉值来判断其是否可信,低信誉值节点传来的信息将不予理睬,从而实现了协同驾驶。实验分析表明,所提LSTM模型能够较为准确地预测周边车辆5 s内的行驶轨迹,而所提的系统在提升智能网联车队的行驶安全上起到了明显的效果。

关键词: 智能网联车队; 轨迹预测; 长短时记忆网络; 信任管理机制; 区块链

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020015

Cooperative trajectory prediction system for intelligent and automated connected convoy based on blockchain

WANG Rensheng, WU Tianhao, ZHANG Lin, ZHU Konglin

School of Information and Communication Engineering, Beijing University of Posts and Telecommunication, Beijing 100876, China

Abstract: Autonomous vehicles have been extensively researched and developed rapidly in recent years. However, these vehicles may be not able to avoid collision with vehicles that appear suddenly. To solve this problem, a cooperative trajectory prediction system for intelligent and automated connected convoy based on blockchain was proposed. In the proposed system, each node in the intelligent and automated connected convoy and roadside infrastructure predict the trajectory of vehicles around them with the LSTM model, and they share the information they get. Using blockchain, the intelligent and automated connected convoy and roadside infrastructure rate the received messages. The summarized rating will be stored as a block in the blockchain that stores the trust values. Vehicles in

收稿日期: 2019-05-20; 修回日期: 2019-07-08

通信作者: 王仁生, wangrensheng@bupt.edu.cn

基金项目: 国家重点研发计划基金(2016YFB0100902)

Foundation Item: The National Key R&D Program of China (2016YFB0100902)

论文引用格式: 王仁生, 吴天昊, 张琳, 等. 基于区块链的智能网联车队协同轨迹预测系统[J]. 网络与信息安全学报, 2020, 6(3): 78-87.

WANG R S, WU T H, ZHANG L, et al. Cooperative trajectory prediction system for intelligent and automated connected convoy based on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 78-87.

the intelligent and automated connected convoy are able to judge whether the other nodes in the Conroy are credible according to their trust value, and messages from the low trust value sender will be ignored, thus achieving cooperative driving. Experiment shows that the proposed system plays a significant role in improving driving safety of the intelligent connected platoon.

Key words: intelligent and automated connected convoy, trajectory prediction, LSTM, trust management, blockchain

1 引言

自动驾驶汽车技术在过去 10 年取得了长足进步, 部分自动驾驶汽车已经进入测试阶段。目前, 自动驾驶汽车的避撞系统主要依赖于摄像头配合毫米波雷达, 从而对汽车行驶路径上的障碍物进行识别和避撞。然而, 由于真实的交通环境往往比较复杂, 自动驾驶汽车在行驶过程中时常会与其他行驶车辆产生交互, 因为遮挡和盲区等, 这些车辆的行驶轨迹有时并不能被提前观察到, 交通事故往往是在这种复杂的交通环境中发生的。因此, 如何规避行驶的车辆是自动驾驶汽车必须解决的问题。

为了能够安全有效地驾驭复杂的交通环境, 自动驾驶汽车需要有预判周围车辆未来行驶轨迹的能力。然而, 在真实的交通场景中, 不同的驾驶员有着不同的驾驶风格, 且车辆轨迹在较长时间范围内往往是高度非线性的, 这使自动驾驶汽车识别行驶意图具有很大的挑战性。

车辆轨迹预测的方法有很多种, 如卡尔曼滤波、高斯混合模型、动态贝叶斯网络等, 最近, 一些学者将长短时记忆网络 (LSTM, long short term memory network) 应用到了车辆的轨迹预测中, 并取得了较好的效果。LSTM 是一种特殊的循环体结构, 它靠一些“门”的结构让信息有选择性地影响循环神经网络中每个时刻的状态, 适合于处理和预测时间序列中间隔和延迟相对较长的重要事件。目前, LSTM 已经在科技领域有了多种应用, 包括翻译语言、控制机器人、图像分析、语音识别、图像识别、手写识别、合成音乐等任务, 将 LSTM 应用于车辆轨迹预测, 可以有效地根据车辆之前的行驶轨迹预判其行驶意图。

对于单车而言, 其意图识别系统可以提前感知周围可能要发生的车辆路径冲突问题。然而, 受限于遮挡和盲区, 其能够进行意图识别的视野区域并不够宽广, 这也为自动驾驶汽车的安全问

题埋下了隐患。借助车载网络, 自动驾驶汽车可以获得附近车辆的视野, 也可以从路边的基础设施中得到路况信息, 这在极大程度上解决了以上问题。但由于网络的高移动性和可变性, 邻近的车辆往往是陌生人, 并不能完全信任, 尤其当网络中存在恶意车辆时, 自动驾驶汽车可能收到恶意的欺骗信息, 路边的基础设施也有受到攻击的可能, 这使问题变得更加严重。研究出一套智能网联车队的安全交互机制将大大改善车联网中的安全隐患, 这也是本文的重点。

随着未来越来越多的网联汽车上路, 网联汽车节点数量呈现出较快的增长趋势, 这将给中心化的安全系统带来许多问题。首先, 中心化的安全系统需要在车的维护上付出高昂的成本; 其次, 海量的接入将会给网络带来较大的扩容压力, 使中心化平台存在性能瓶颈; 此外, 一旦中心节点被攻破, 整个中心化安全系统将遭到无法估量的打击。

近年来, 由于区块链具有去中心化、公开透明等特点, 受到了人们广泛的关注。区块链技术又被称为分布式账本技术, 是一种去中心化、去信任化、集体维护分布式账本的技术方案, 其利用块链式数据结构来验证与存储数据, 其本质是由多个节点集体参与, 通过多方存储、多方计算的方式来实现数据不可篡改、计算结果可信的分布式数据库系统。借助区块链, 本文可以在智能网联车队中建立一个分布式的信任管理机制, 从而解决参与各方的互信问题。

本文提出了一种智能网联车队中安全协同的意图识别系统, 其模型如图 1 所示。利用车对外界的信息交换 (V2X, vehicle to everything) 技术在距离较近的车辆间形成智能网联车队, 车队中的各个节点与路边基础设施通过长短时记忆网络模型对周边车辆的运动轨迹进行预判, 并将得到的结果进行分享。利用区块链, 智能网联车队与路边基础设施可以对其接收到的信息进行评分, 并将汇总后的评分以区块的形式加入存储信誉评

分的区块链中。通过这种去中心化的方式,有效解决了参与各方的互信问题,实现了智能网联车队的协同驾驶。实验表明,本文的智能网联车队中安全协同的意图识别系统可以大大降低自动驾驶汽车在行驶过程中的安全隐患。

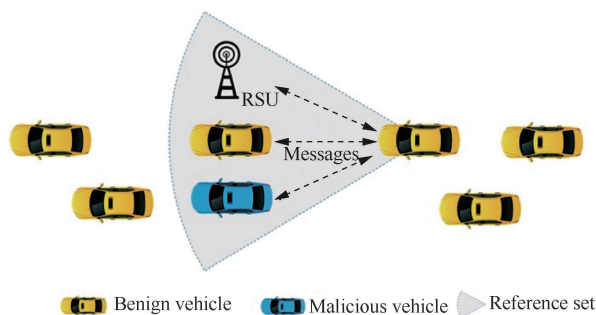


图1 智能网联车队协同意图识别模型
Figure 1 Model of the collaborative intent identification by intelligent and automated connected convoy

2 相关工作

2.1 车辆轨迹预测

为了达到车辆轨迹预测的目的,学者提出了很多方法。传统的方法有卡尔曼滤波以及扩展卡尔曼滤波^[1],然而这种方式的模型过于简单,当车辆在较为复杂的环境下运动时,它们对于车辆较长一段时间内的轨迹预测并不够准确。为了改进这种缺陷,一些更为复杂的模型被提出,如高斯混合模型、动态贝叶斯网络(DBN)等^[2]。使用高斯混合模型学习动态车辆的驾驶行为模式并用于驾驶行为意图检测,最后将动态车辆驾驶行为意图与运动模型结合进行轨迹预测。而动态贝叶斯网络^[3]则使用图形模型来描述各种影响车辆行驶轨迹的潜在因素,并以此为基础为轨迹预测提供了较为灵活的模型。这两种方法虽然有着较高的复杂度,但它们的模型忽略了周边环境对于车辆运动轨迹的影响,在复杂的交通环境下,仅仅考虑车辆自身的运动状态是不够的。

由于运动任务可以被视为序列分类或序列生成任务,因此近年来,研究人员提出了许多基于递归神经网络(RNN)的方法,用于机动分类和轨迹预测。Lee在文献[4]中利用递归神经网络提出了可以预测出车辆行驶意图的方法,其模型在预测时不仅参考车辆自身的行驶轨迹,还考虑车

辆周边物体对其运动的影响,使其可以较为准确地预测出车辆在较短时间内的行驶意图。Kim^[5]则基于长短时记忆网络提出了可以预测出在接下来0.5 s、1 s以及2 s内车辆位置的模型。然而,仅预测出车辆在短时间内的行驶意图并不能规避车辆之间碰撞的危险,本文基于LSTM模型提出了可以预测出行驶车辆5 s内行驶意图的模型。

2.2 车联网中的信任管理机制

中心化的网联车队信任管理机制在业内已经被广泛提出,文献[6]提出了中心服务器的概念,利用中心服务器,系统可以收集并处理数据,从而得到所有车辆的信任值,而这些信任值也被存储在中心服务器中。然而,这一类系统都是建立在中心服务器足够可靠的基础上,如果服务器受到攻击,整个信任管理机制都将瘫痪。为了解决此类问题,一些去中心化的智能网联车队信任管理机制被提出。文献[7]中每个节点首先分析信息的关键词,并将信息据此进行分类,然后根据信息内容的相似度和内容之间的冲突对信息进行评分。这种方法在很大程度上摆脱了对中心服务器的依赖,然而,每个车辆节点都需要自己计算并存储信任值,由于单个节点的计算能力以及观察条件有限,其打分的精确度可能受到较大的限制。

针对此种情况,一些研究者提出了将区块链应用于智能网联车队的想法^[8-9],文献[8]基于区块链技术为车载网络提出了一种新的分散式信任管理方案。借助该系统,车辆可以从自己的邻近车辆获得路况信息,并能够对所接受到的信息进行评级,该评级会在路边的基础设施汇总并生成一个最终的得分。这种方法既避免了中心化带来的限制,也解决了单个节点计算能力和观察条件有限的问题。然而,对于每一车辆的信任值更新,路边基础设施间都需要进行“矿工”选举,在车辆数量较大的情况下,对于路边基础设施的运算能力是不小的挑战。

3 系统结构

3.1 轨迹预测

3.1.1 问题定义

本文将轨迹预测问题定义为根据车辆之前的

行驶轨迹及其周围的环境来预测车辆接下来每 t 个时刻行驶位置的概率分布。模型的输入为车辆的历史轨迹。

$$X=[x^{(t-t_n)}, \dots, x^{(t-1)}, x^{(t)}] \quad (1)$$

其中, $x^{(t)}$ 为被预测车辆在 t 时刻的坐标, 而模型的输出则为一段概率分布。

$$Y=[y^{(t+1)}, \dots, y^{(t+t_f)}] \quad (2)$$

其中, $y^{(t)}$ 为被预测车辆在 t 时刻的坐标。

本文的模型估计条件分布 $P(X|Y)$, 为了让模型产生多重模态分布, 本文在动机 m_i 上进行扩展。

$$P(Y|X) = \sum_i P_{\Theta}(Y|m_i, X)P(m_i|X) \quad (3)$$

$$\Theta=[\Theta^{(t+1)}, \dots, \Theta^{(t+t_f)}] \quad (4)$$

其中, m_i 表示车辆的具体动机, 本文的车辆动机包括向左变道、直行和向右变道, Θ 为车辆的位置在未来每个时间点的高斯分布参数, 对应于未来位置的均值和方差。

3.1.2 模型架构

本文的 LSTM 模型包括 LSTM 编码器、卷积交互池化层、LSTM 解码器。

首先, 本文使用 LSTM 编码器来学习车辆运动状态, 对于每个瞬间, 最近 t 帧的历史轨迹片段传递给 LSTM 编码器以预测车辆及其周围车辆的运动轨迹。每个车辆的 LSTM 状态会逐帧更新, 该状态可以用来预测每辆车的运动状态, 而用于每辆车的 LSTM 相互分享彼此的权重, 这使所有车辆的 LSTM 状态之间存在直接相关性。

当 LSTM 编码器捕获车辆运动状态时, 它无法捕捉场景中所有车辆运动的相互依赖性。文献[10]中提出的交互池化 (social pooling) 通过将预测目标周围的所有物体的 LSTM 状态汇集到交互张量中来解决这个问题。这是通过在预测目标周围定义空间网格并基于场景中代理的空间配置用 LSTM 状态填充网格来完成的, 除了预测目标的 LSTM 状态之外, 还使用交互张量作为模型的输入, 已经证明此方法可以提高未来轨迹预测的准确性^[10]。

然而, 所有之前的交互池化文献^[10-11]实例都

将全连接层应用于交互张量, 但这种做法破坏了交互张量的空间结构。由于全连接层的存在, 在空间中彼此相邻单元之间的相互作用等同于完全连接层中彼此远离的单元, 这可能导致对测试集的泛化问题, 特别是物体可以处于各种不同的空间配置中。例如, 假设训练集在交互张量的空间位置 (m, n) 没有 LSTM 状态的单个实例, 当在测试集中遇到这样的实例时, 模型将无法泛化。特别地, 即使在空间网格位置 $(m+1, n)$ 和 $(m, n+1)$ 处存在 LSTM 状态的训练实例, 这仍将成立。

为了解决这种问题, 本文在交互张量上使用卷积层和池化层, 简称卷积交互池化, 其模型如图 2 所示。卷积层的等效性有助于学习交互张量的空间网格内的局部有用特征, 并且最大池化层可以添加局部平移不变性, 这两者都有助于解决上述问题。

本文通过定义基于车道的网格来建立交互张量。首先, 在被预测的车辆周围定义 13×3 空间网格, 其中每列对应于单个车道, 每行保持 4.7 m 的距离, 其大约等于一个车辆长度, 而交互张量是通过将该网格与周围的汽车位置一起填充而形成的。然后, 本文将两个卷积层和一个池化层应用于交互张量, 如图 2 所示, 以获得上下文编码。此外, 为了获得车辆动力学编码, 预测车辆的 LSTM 状态会交给全连接层处理。这两种编码连接在一起形成完整的轨迹编码, 然后传递给解码器。

为了提升训练模型时的速度, 加快收敛过程, 本文在每一层卷积层后加入了批标准化 (batch normalization), 即对网络每一层的输出都做了归一化处理。有了 Batch Normalization, 本文不需要考虑为每一层加入随机失活 (dropout), 因为 Batch Normalization 本身就是一种防止过拟合的正则化表达式。通过这种方法, 对模型参数的初始化要求有所降低, 学习率相比之前有所增大, 这大大简化了调参的过程。

本文使用基于 LSTM 的解码器为接下来 t 帧的运动轨迹生成预测分布。本文通过之前描述的每一个动机类分布以及每个动机类的概率来解决驾驶员行为的固有多模态。解码器具有两个 softmax 层, 其输出横向和纵向操纵概率, 而把这

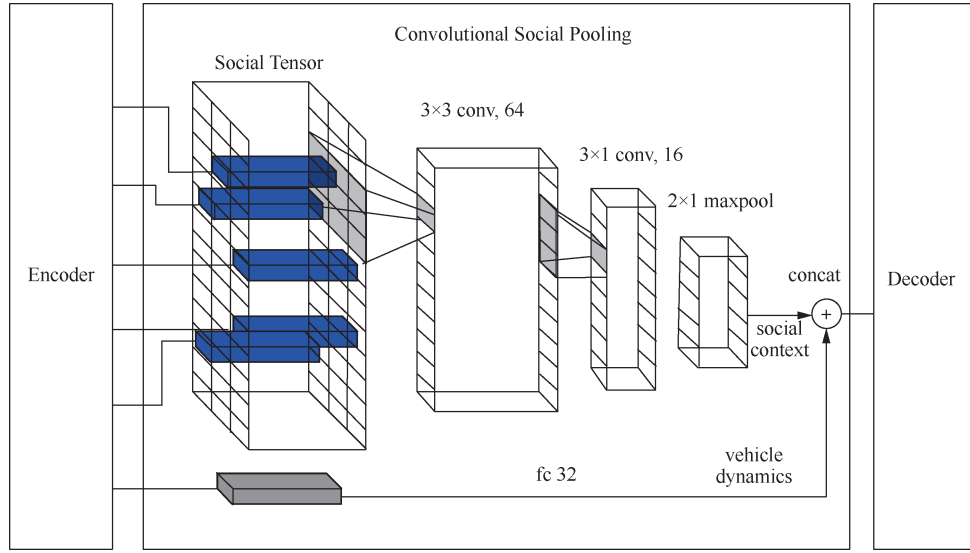


图 2 卷积交互池化模型
Figure 2 Convolutional social pooling model

些概率相乘就可以得到 $P(m_i|X)$ 的值。此外, LSTM 可以用于生成超过 t 帧的双变量高斯分布参数, 以给出车辆运动的预测分布。

3.1.3 训练及参数细节

本文采用端到端的方式训练模型, 首先, 将损失值定义为

$$-\log\left(\sum_i P_{\Theta}(Y|m_i, X)P(m_i|X)\right) \quad (5)$$

其中, 每一个点的概率分布由式(3)给出。由于每个训练例只提供一个行驶动机的实例, 本文将所有训练例中的总损失值定义为

$$-\log(P_{\Theta}(Y|m_{\text{true}}, X)P(m_{\text{true}}|X)) \quad (6)$$

其中, m_{true} 表示每一个训练实例对应的结果, 包括向左变道、直行、向右变道。

本文采用 Adam^[12]的方法来训练所提模型, 起始的学习率为 0.001, 训练到 20 000 步后, 学习率会降低到 0.000 1。本文的 LSTM 编码器是 64 维的, 而 LSTM 解码器为 128 维。而接受车辆动态编码的全连接层有 32 个输入。本文使用 leaky-ReLU 作为每一层的激活函数, 将其激活函数参数 α 值设置为 0.01。

3.2 基于区块链的信任管理机制

借助车载网络, 自动驾驶汽车可以获得附近车辆的视野, 也可以从路边的基础设施中得到路

况信息。然而, 周围的网络并不一定是安全的, 当网络中存在恶意车辆时, 自动驾驶汽车可能收到恶意的欺骗信息, 路边的基础设施也有受到攻击的可能。针对该问题, 本文提出了基于区块链的信任管理机制, 利用区块链去中心化和不可篡改的特性, 能够在一定程度上抵御上述恶意攻击。

3.2.1 相关技术介绍

分布式账本技术 (DLT, distributed ledger technology) 作为去中心化自治交易的底层技术, 使对某一节点或机构的信任转化为对计算机协议的信任, 这加快了去信任化 (trust-free) 对等网络的发展^[3]。区块链是分布式账本技术的一个子集, 其工作机制符合分布式账本技术的共性, 而分布式账本的数据结构会形成区块链的架构基础。因此, 区块链是一种单链数据结构。在区块链上, 除去创世区块 (genesis block), 其他每一区块都包含块头和块身。区块头含有对前一区块的哈希值 (hash function, 又称散哈希数, 是一种从任何数据中创建“指纹”的方法), 将其作为身份证明 (identification), 从而实现对前一区块的链接。区块中的交易记录以默克尔树 (Merkle tree) 的结构进行排列^[5], 而前后区块则按照时间顺序进行排列, 否则前一区块的哈希值是未知的, 这一技术设置在很大程度上解决了重复支付的问题^[6], 并能通过对连续区块的 ID 追踪实现对区块

链上的交易按时间回溯的功能。

3.2.2 系统架构

本文去中心化的智能网联车队信任管理模型主要包括路边基础设施(RSU)以及智能网联汽车两部分。

(1) 路边基础设施

在本文的信任管理机制中,路边基础设施不会成为系统的中心服务器,它会以一个普通参与者的身份将自己捕获到的交通信息分享给智能网联车队中的车辆。通过这种去中心化的方式,系统不会过度依赖于路边基础设施,不仅减小了通信时延,也保证了数据的安全性和可靠性,因为即使路边基础设施受到了恶意攻击,也不会对整个系统的运营造成太大影响。

(2) 智能网联汽车

每一辆智能网联汽车都配备有车载传感器、计算机和通信设备,用于进行数据的收集、处理和共享。

借助车载设备,车辆可以自动检测与交通相关的事件,并使用车辆间通信标准向其他人发送警告信息,如LTE-V2V、DSRC等。然而,并非所有消息都有用。例如,如果车辆已经通过了特定事件的位置,则有关此事件的报告将不再具有价值。因此,每个车辆需要保持参考集,其参考集与目标车辆的交通安全性高度相关。在本文系统中,每个车辆的参考集由在一定距离内前行的相邻车辆组成。使用从参考集发送的消息,车辆可以及时了解交通状况并响应可能的事件。

3.2.3 攻击模型

在本文的模型中,路边基础设施与智能网联汽车都被视为容易受到攻击的对象,而这两者中的任一个受到恶意攻击者操控都将对本文智能网联车队的行驶安全造成巨大的影响。因此,本文的攻击模型主要包括恶意车辆以及受到攻击的路边基础设施。

(1) 恶意车辆

智能网联车队中可能存在许多恶意车辆,它们通常有特定的动机,会在特定的时间对周围的车辆和路边基础设施发动信息安全攻击,而这种行为可能会严重危害交通的安全和效率。本文主要考虑消息欺骗攻击以及选票攻击。

在消息欺骗攻击中,攻击者可能故意播放虚假信息,从而达到危害交通安全或降低交通效率的目的。例如,恶意车辆检测到前方一辆汽车要进行向左变道的操作,但它向周围车辆广播向右变道的信息,从而对后面车辆的行驶进行干扰。

在投票攻击中,恶意车辆对上传了可靠信息的车辆进行低分评价,使本应该受其他车辆信任的信息分享者没有得到应有的评分,从而破坏了智能网联车队的信息分享。

(2) 受到攻击的路边基础设施

路边基础设施沿着道路分布,有时也会受到一些攻击者的攻击,而一旦路边基础设施被入侵,攻击者就能够更改其数据,使其发送恶意欺骗信息给附近的车辆,因此,路边基础设施也是不能完全信任的。由于网络运营商的定期安全检查,受到攻击的路边基础设施不可能长时间地被控制,因此本文假定攻击者只能在较短时间内破坏路边基础设施。

3.2.4 设计目标

本文重点评估智能网联车队中信息的可靠性,并致力于解决以上几种攻击。本文的信任管理机制的主要目标如下。

(1) 去中心化

随着智能网联汽车的快速增长,中心化的信任管理机制越来越不切实际,此外,中心化管理系统对中心服务器的过度依赖也使信息的安全性和可靠性受到了威胁。因此,信任管理机制需要充分利用分布式节点,即路边基础设施和智能网联汽车。通过去中心化的管理方式,确保任一节点在受到攻击时都不会对本文的信任管理机制造成致命的危害。

(2) 可用性

在本文的方法中,所有的信任信息存储在每一辆智能网联汽车中,当需要查询某一辆车的信誉信息时,智能网联汽车只需查询自身的存储信息即可,因此不存在信誉信息被篡改的可能性,但存储在每一辆智能网联汽车中的信任值需要保证可靠有效。

(3) 及时性

信任值表示基于其历史行为的特定车辆的总体评价。由于该车辆发送的消息的可信度可能随

时间而变化,因此存储在智能网联汽车中的信任值需要及时更新。

3.2.5 主要步骤

本文的信任管理机制主要由以下几个步骤实施:信息分享、处理及评分、“矿工”选举、生成新的区块,如图3所示。

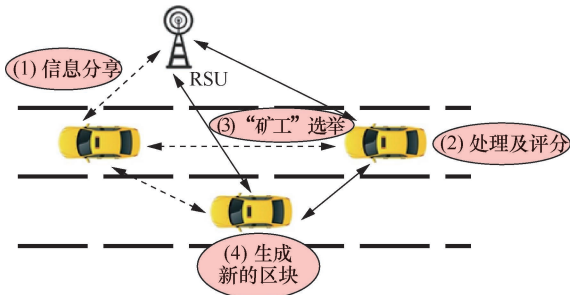


图3 基于区块链的信任管理机制系统设计
Figure 3 System design of trust management mechanism based on blockchain

(1) 信息分享

在本文的系统中,距离较近的智能网联汽车利用 V2X 技术组成智能网联车队,该车队与路边基础设施形成区块链网络,该网络中每个节点的初始信誉度为 0。区块链网络中的各个节点通过摄像头采集路面交通状况的图像,并对图像中的车辆进行物体检测。检测到的车辆将被进行持续的图像跟踪,并由其过往的行驶轨迹预测出该车辆的下一步行驶意图。本文采用 YOLO^[13]的方法对道路上的车辆进行物体检测,采用 deepSort^[14]的方法对检测到的车辆进行目标跟踪。当智能网联汽车或者路边基础设施预测到交通事件时,会将自己拍摄到的图像以及自己的预测结果在区块链网络中广播。本文中的交通事件包括左右变道、左转、右转、变道、加速、制动。

(2) 处理及评分

智能网联汽车接收到事件信息后,结合信息发送者的位置以及信誉值对事件进行处理。智能网联汽车首先判断该发送者是否在自己的参考集内,如果不在,则针对此次时间信息不予理睬。反之,智能网联汽车会参考信息发送者的信誉值,当发送者的信誉值大于或等于 0 时,智能网联汽车根据其提供的事件信息,提前做出减速或变道等避让行为;当发送者的信誉值小于 0 时,智能网联汽车将不采取避让措施。不论信息发送者的

信誉值是多少,只要其在智能网联汽车的参考集内,智能网联汽车都将对时间信息中车辆与自身摄像头捕获车辆进行比对。这里,本文采用 RA-CNN^[15]方法对车辆进行细粒度分类,如果得到的细粒度分类结果相同,则认为事件信息中的车辆与自身摄像头中的车辆一致。进一步地,本文将事件信息进行评分。这里,本文借鉴文献[1]中的评分方式,当信息中的事件与实际事件相符合时,给信息评分为 1;反之,评分为-1。此外,本文给予信息发送者一些容错空间,当错误信息中的交通事件方向与真实的交通事件方向一致时,本文给错误信息的评分为 0。例如,信息中的交通事件为左转,而真实的交通事件为向左变道或掉头,本文则认为信息的发送者只是预判出现了偏差,但同样起到了给车辆良性的警示作用,所以不会给其过低的评分。

(3) “矿工”选举

由于去中心化的网络结构,区块链网络中并没有恒定的中心,因此,需要定期选出一个“矿工”节点来生成新的区块。在本文的系统中,每当有智能网联汽车对某一车辆进行连续 3 次的评分后,区块链网络就会发起对于该车辆评分的“矿工”选举。选举发起后,区块链网络中每一个对于该车辆有过评分的节点会将自己对其的评分求平均值,而该网络中的所有节点都将申请选举“矿工”。每一个进行“矿工”选举的节点会将自己计算的评分、自己在区块链中记录的信誉值以及自己的实时位置打包成数据包进行广播。其他节点在收到该数据包后比对数据包中的信誉值与区块链中记录的该车辆信誉值是否一致,如果不相符,则丢弃该数据包。最终,“矿工”选举者中评分最高的节点会成功当选。

当“矿工”选举者中出现信誉度相同的节点时,附近车辆更多的节点会当选“矿工”。具体地,每辆收到数据包的智能网联汽车会计算信誉度最高的评分节点到其余各节点距离的平方和 S ,评分节点中 S 值更小的一方会当选“矿工”。该平方和的距离定义如下。

$$S = \sum_{i=1}^n (x_i - x_k)^2 + (y_i - y_k)^2 \quad (7)$$

其中, n 表示该区块链网络中节点的数量, x_i 表示第

i 个节点的经度值, x_k 表示平分节点的经度值, y_i 表示第 i 个节点的纬度值, y_k 表示平分节点的纬度值。

通过这种方式, 信誉值最高的节点会当选“矿工”, 这在较大程度上保证了“矿工”节点的可靠性。如果出现并列的信誉值最高节点, 则从评分节点中选出 S 值最小的当选“矿工”, 这样选出的“矿工”节点在智能网联车队中车辆更为密集的区域, 从而保证“矿工”节点在生成新的区块后能够以较小的时延广播给其他节点。

(4) 生成新的区块

在区块链网络中, 针对某一节点, “矿工”节点会收到若干个关于它的评分, “矿工”节点通过计算可以得到一个关于该节点的最终信任值, 其计算方法如下。

$$\text{credit} = \frac{\sum_{i=0}^n c_i r_i + \lambda c_{\text{block}}}{\sum_{i=0}^n c_i + \lambda} \quad (8)$$

其中, n 表示对该事件进行评分的节点数量, c_i 表示评分节点自身的信誉值, r_i 表示该节点对事件的评分, c_{block} 表示被评分的节点在存储信誉信息的区块链中最近一次存储的评分。 λ 为调节因子, λ 的大小代表区块链之前存储的信誉值在新一轮评分中所占的权重, 其默认值为 1。计算完成后, 节点会将自己更新的信誉信息添加到存储信任值的区块链中, 并将添加的区块广播到区块链网络的其他节点中。

一旦从“矿工”节点接收到块, 智能网联汽车需要检查其有效性, 然后将其添加到区块链中。有时, 智能网联汽车可能同时接收多个块, 在这种情况下, 区块链开始分叉。本文采用分布式共识方案解决此问题, 每个智能网联车队选择一个 block 并继续在其后添加新块。随着时间的推移, 由最大数量的智能网联车队承认的分支增长速度快于其他分支, 最后, 最长的一个链成为网络的分布式共识, 而其他链被丢弃。此外, 每个区块链节点需要收集自己在丢弃的分叉中生成的块, 并尝试将其添加到区块链中。通过这种方式, 所有智能网联汽车都存储相同版本的区块链, 从而确保网络的一致性。

4 实验与评估

4.1 轨迹预测效果

本文在 PyTorch 上使用公开的 NGSIM US-10 和 I-80 数据集^[16]进行实验。每个数据集包含 45 min 时间跨度内以 10 Hz 捕获的实际高速公路交通的轨迹, 每个数据集由 15 min 的轻度拥挤、中度拥挤和拥挤交通状况组成。本文将完整的数据集拆分为训练集和测试集, 测试集包括来自 US-101 和 I-80 数据集的 3 个子集。

本文将能通过 5 s 内预测轨迹与真实轨迹的均方误差 (RMSE) 用来衡量模型的准确性, 同时, 将本文的模型与以下几个模型进行对比。

(1) 卡尔曼滤波 (KF) 模型

通过对输入输出数据进行观测, 排出噪声和干扰, 输出较为线性的结果。

(2) 高斯混合模型 (VGMM)

学习动态车辆的驾驶行为模式并用于驾驶行为意图检测, 最后将动态车辆驾驶行为意图与运动模型结合进行轨迹预测。

(3) 递归神经网络 (RNN)

利用递归神经网络预测出车辆行驶意图, 在预测时不仅参考车辆自身的行驶轨迹, 还考虑车辆周边物体对其运动的影响。

表 1 展示了本文的 LSTM 模型与以上几个参考模型的效果对比。相比于其他几种模型, 由于本文的 LSTM 能够更多地考虑周边环境对于车辆运动状态的影响, 所以能够更加准确地预测 5 s 内车辆的行驶轨迹, 且具有更低的 RMSE 值, 尤其随着预测时间越来越久, LSTM 的优势变得越来越明显。

表 1 不同模型的均方根误差
Table 1 MSE of different models

预测时间/s	KF	VGMM	RNN	LSTM
1	0.76	0.68	0.62	0.60
2	1.79	1.60	1.35	1.27
3	3.16	2.75	2.24	2.08
4	4.78	4.24	3.29	3.10
5	6.72	5.98	4.78	4.32

4.2 安全性能分析

4.2.1 对抗恶意车辆

恶意车辆可能会向附近的邻居车辆广播虚假

的消息,这会导致严重的交通事故或拥堵。在本文的系统中,每辆智能网联汽车中都存有其他车辆的信誉值,智能网联汽车可以根据该信誉值选择性地对接收到的信息采取相应的措施。如果信息发送者的信誉值过低,那么智能网联汽车的驾驶行为将不会做出任何改变,这大大保证了所用信息的可靠性。此外,一些恶意车辆可能会对一些信息进行不公平的评分,如对良好的信息发送者给予过低的评价。在本文的体系中,每个评分者在最终的信誉值生成中都享有一个权重,而该权重与评分者自身的信誉值直接相关,由于恶意车辆数量较少,且评分往往较低,所以其恶意评分很难影响到本文的信任管理机制。

4.2.2 对抗受损 RSU

如果以路边基础设施为中心服务器,那么一些恶意用户将很有可能对其发动攻击,而一旦路边基础设施被攻陷,整个系统都将瘫痪。在本文的信任管理机制中,路边基础设施不会成为系统的中心服务器,它会以一个普通参与者的身份将自己捕获到的交通信息分享给智能网联车队中的车辆。通过区块链技术,系统不会过度依赖路边基础设施,不仅减小了通信时延,也保证了数据的安全性和可靠性,因为即使路边基础设施受到恶意攻击,也不会对整个系统的运营造成太大影响。

4.3 系统效率

为了验证本文系统的效率和及时性,本文基于 Matlab 搭建了车联网及区块链仿真平台,并对系统中区块的生成时间及信息利用率进行了相应的仿真。

4.3.1 区块生成

评分完成后,区块链网络会进行“矿工”节点的选举,而当选的“矿工”节点需要汇总各个节点的评分,并最终以此生成新的区块。本文对这一过程进行了仿真实验,并与文献[1]中的方法进行了对比,得到了在不同数量的智能网联汽车环境下,两种方法从“矿工”选举到生成区块所用的时间,如图4所示。

可以看出,由于文献[1]中的区块链网络由所有的路边基础设施组成,该方法将大部分的计算任务以及区块生成任务交由路边基础设施完成,路边基础设施需要计算每一辆车的信誉评分并为其生成区块。因此,随着该区域内汽车数量的增加,路边

基础设施会处于超负荷的状态,其区块生成所需时间较大。相比于文献[1]中的方法,本文中的区块链由路边基础设施与智能网联车队所有的节点组成,路边基础设施与智能网联车队中任一车辆一样,只是区块链网络中的一个节点,大量任务被下放到了各个智能网联汽车中。因此,相较于文献[1]中提出的方法,随着交通环境中车辆数量的增长,本文方法生成区块所用的时间增加较少,这使生成区块具有较好的及时性,也保障了系统的工作效率。

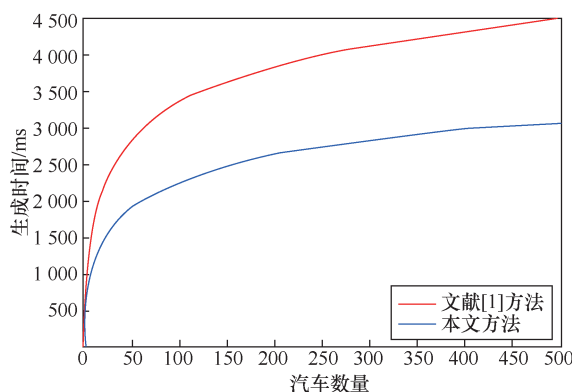


图4 不同方法生成区块的时间
Figure 4 Time to generate blocks by different methods

4.3.2 信息利用率

同样地,当智能网联车队中车辆的节点数量不同,其接收信息的利用率也会有所不同,本文针对这一特点进行了仿真,结果如图5所示。

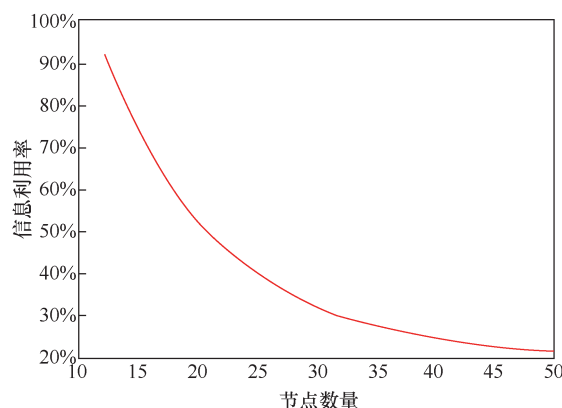


图5 不同节点数量下的信息利用率
Figure 5 Information utilization ratio under different number of nodes

可以看出,随着智能网联车队中节点数量的增加,每辆车接收到信息的利用率会降低。这一结果与逻辑相吻合,当车队过于庞大时,距离相隔较远的车辆增多,每辆车接收到信息所描述的交通事件

与自身关系不大。然而，现实中距离较近车辆的数量往往没有那么庞大，因此，本文所建立车队的节点数量一般在 5~30，从图中可以看出，在该范围内，信息利用率相当可观。

5 结束语

本文提出了智能网联车队中安全协同的意图识别系统，利用 LSTM 模型，路边基础设施与智能网联车队中的每一个节点都可以对周围车辆的行驶轨迹进行预判，并将预测结果进行分享。借助区块链技术，智能网联汽车可以对接收到的信息进行评分，而这些评分被汇总后存储到区块链中。通过这种方式，智能网联汽车既能通过自己的轨迹预测模型进行车辆避让，又可以选择性地利用其他节点分享的信息，从而实现协同驾驶。

参考文献：

- [1] BARRIOS C, MOTAI. Improving estimation of vehicle's trajectory using the latest Y global positioning system with Kalman filtering[J]. IEEE Trans on Instru and Meas, 2011, 6(12): 3747-3755.
- [2] 黄如林. 无人驾驶汽车动态障碍物碰撞关键技术研究[D]. 合肥: 中国科学技术大学, 2017.
HUANG R L. Research on key technologies of dynamic obstacle avoidance for autonomous vehicle[D]. Hefei: University of Science and Technology of China, 2017.
- [3] GINDELE T, BRECHTEL S, DILLMANN R. Learning driver behavior models from traffic observations for decision making and planning[J]. IEEE Intelligent Transportation System Magazine, 2015, 7(1): 69-79.
- [4] LEE N, CHOI W, VERNAZA P, et al. DESIRE: distant future prediction in dynamic scenes with interacting agents[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2017: 2165-2174.
- [5] KIM B, KANG C M S, LEE H, et al. Probabilistic vehicle trajectory prediction over occupancy grid map via recurrent neural network. arXiv preprint [J]. arXiv:1704.07049, 2017.
- [6] LI Q, MALI A, MARTIN K M, et al. A reputation-based announcement scheme for VANETs[J]. IEEE Transactions on Vehicular Technology, 2012, 61(9): 4095-4108.
- [7] LI W, SONG H. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks[C]//International Conference on Network and System Security. 2013: 94-108.
- [8] YANG Z, YANG K, LEI L, et al. Blockchain based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2018.
- [9] 戴婕. 基于密钥管理和无中心化加密的网联汽车信息安全的设计与实现[D]. 北京: 北京邮电大学, 2018.
DAI J. Design and implementation of vehicular information security based on key management and decentralized encryption[D]. Beijing: Beijing University of Posts and Telecommunication, 2018.
- [10] ALAHI A, GOEL K, RAMANATHAN V, et al. Social LSTM: human trajectory prediction in crowded spaces[C]//IEEE Conference on Computer Vision and Pattern Recognition. 2016: 961-971.
- [11] DEO N, TRIVEDI M M. Multi-modal trajectory prediction of surrounding vehicles with Maneuver based LSTMs[C]//2018 IEEE Intelligent Vehicles Symposium (IV). 2018: 1179-1184.
- [12] KINGMA D P, BA J. Adam: a method for stochastic optimization[J]. arXiv preprint arXiv:1412.6980, 2014.
- [13] REDMON J, FARHADI A. YOLO9000: better, faster, stronger[J]. arXiv preprint arXiv:1612.08242, 2016.
- [14] WOJKE N, BEWLEY A, PAULUS D. Simple online and realtime tracking with a deep association metric[C]//2017 IEEE International Conference on Image Processing (ICIP). 2017.
- [15] FU J, ZHENG H, MEI T. Look closer to see better: recurrent attention convolutional neural network for fine-grained image recognition[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2017: 4476-4484.
- [16] COLYAR J, HALKIAS J. US highway 101 dataset. Federal highway Administration (FHWA)[R]. 2007.

[作者简介]



王仁生（1994-），男，山东烟台人，北京邮电大学硕士生，主要研究方向为智能网联汽车。



吴天昊（1992-），男，山东济南人，北京邮电大学博士生，主要研究方向为 C-V2X 通信技术的应用。



张琳（1974-），男，上海人，博士，北京邮电大学教授、博士生导师，主要研究方向为超宽带生物雷达成像及生命信号检测、网络信息处理、车联网。



朱孔林（1985-），男，山东临沂人，博士，北京邮电大学副教授，主要研究方向为智能网联汽车。