基于区块链和时空特征融合的车联网信誉评估方法

田　钊[1,2], 周　政[1,2], 牛亚杰[1,2], 鲁豪杰[1,2], 刘　炜[1,2], 宰光军[1,2]

(1.郑州大学 网络空间安全学院,河南 郑州 450002;2.郑州大学 郑州市区块链与数据智能重点实验室,河南 郑州 450002)

摘　要:针对车联网中节点恶意攻击与自私行为导致交互数据不可信,且现有方法易引发信誉贬值的问题,提出一种基于区块链与时空特征融合的信誉评估方法。首先,引入高斯朴素贝叶斯算法融合时间与空间特征,旨在提高动态环境下信誉评估的准确性;其次,以事件确认度为依据更新信誉,实现更可靠的信誉聚合;最后,在智能合约中部署基于信令博弈的奖惩与税收机制,用于维持全局信誉动态平衡。仿真结果表明,本方法的识别精确度与召回率保持在82%和81%以上;面对高隐蔽性的恶意开关攻击,可在2.5 min内将攻击节点信誉清零。该方法有效抑制了复杂网络攻击与理性自私行为,从机制上避免了系统信誉贬值,保障了车联网数据交互的安全。

关键词:智能交通; 区块链; 人工智能; 车联网; 信誉评估

中图分类号:TP389.1　　**文献标志码**:A　　**doi**:10.13705/j.Issn.1671-6833.2026.06.008

5G技术的迅速发展进一步提升了车联网在低延迟、高可靠性的性能。随着城市发展向智能化和互联化转型,交通事件报告与管理的智能化和自动化变得尤为重要。这些发展对于增强智能驾驶技术、提高运营效率以及改善交通服务具有关键意义[1]。现有研究表明,5G网络技术为车联网处理海量数据提供了坚实基础,增强了通过路侧单元(road side unit, RSU)向智能车辆传递实时交通信息和路况预警的能力,从而显著提升了车联网的信息交互能力。这一技术支持多种未来的应用,如道路交通状态监测[2]、自动驾驶防撞预警[3]和车辆服务信息共享[4]等。在智能交通应用中,车辆通常会将感知到的信息报告给附近的基站,基站再将信息与其他车辆共享。然而,在信息上报过程中可能会出现人为的恶意攻击[5]或自私行为[6]。一方面,恶意攻击者可能使车辆发送虚假信息,从而干扰系统的正常运行;另一方面,自私的用户可能拒绝承担信息上报的责任。为了确保智能交通应用的有效性,如何抵御恶意攻击和抑制自私行为是一个重要的安全挑战。基于密码学[7-8]的方案可以保证报告信息的机密性、完整性和可用性,但不能判断信息内容的真实性。为了鼓励车辆主动报告真实信息,为其分配信誉值并建立相应的信誉评估方法[9]是一个具有前瞻性的想法。近年来,区块链技术和深度学习模型在车联网信誉评估领域的融合应用已取得显著进展。基于区块链的解决方案主要聚焦于分布式信任管理体系的构建。Hussain等人[10]利用机器学习提出的分布式信誉框架通过智能合约实现车辆交互记录的不可篡改存储。为了抵抗恶意攻击和抑制自私行为,Dempster-Shafer理论[11]提出了一种车辆信誉评估方法。深度学习技术的引入为解决动态环境下的信誉评估提供了新思路。Mao等[12]开发的HHTM方案结合LSTM网络处理时序行为数据。Xiao[13]提出的VehicleRank模型采用图神经网络捕捉车辆交互的拓扑特征。

尽管这些方法已被用于评估车辆的信誉和信息

收稿日期:2026-04-29;**修订日期**:2026-05-28

基金项目:河南省科技攻关项目(252102210185);综合交通运输大数据应用技术交通运输行业重点实验室开放课题(2022B1201)

作者简介:田钊(1985—),男,郑州大学副教授,博士,主要从事信息安全、区块链、智能交通等方面的研究,E-mail:tianzhao@zzu.edu.cn。

通讯作者:宰光军(1979—),男,郑州大学副教授,主要从事信息安全、软件工程、金融信息系统等方面的研究,E-mail:zaiguangjun@zzu.edu.cn。

的真实性,但仍面临一些挑战。首先,先前的研究很少关注智能车辆在对抗能力方面的提升。恶意车辆可以通过状态切换来避免被系统驱逐,而自私车辆则可以选择性地报告信息。其次,现有研究未考虑信誉值的流通和长期管理,许多节点在获得较高信誉值后,会选择不再报告信息,同时,太多高信誉值的节点可能会导致信誉贬值,从而诱发恶意攻击和自私行为。

车联网网络拓扑结构的高动态性、移动性且不可预测性增加了其安全性的复杂性。车联网呈现自组织网络特性,车辆需要与陌生节点进行交互,网络的拓扑结构变化频繁,车辆与其它节点交互存在安全风险,未知或恶意来源的数据注入可能导致虚假信息的传播,甚至引发灾难性事故。因此,在车联网通信中,识别恶意车辆节点和虚假信息,对车联网的安全[14]至关重要。

因此,针对车联网环境,本文提出了 1 种基于区块链的分布式时空特征感知融合的信誉管理方法,该方法结合了车辆节点的历史和实时行为对信誉评估的影响,并考虑车辆信誉值的流通管理,提出了车辆事件报告的奖惩机制和信誉值税收机制。本文的主要贡献如下:

(1)构建了时空特征融合的动态信誉评估方法。引入空间衰减因子与时间衰减因子,结合高斯朴素贝叶斯分类计算直接与间接信誉的聚合。

(2)提出了去中心化信誉评估平衡机制。针对车联网长期运行中难以避免的信誉贬值难题,将税收调控与信令博弈引入区块链智能合约。通过定义惩罚边界与信誉通缩规则,实现了对恶意开关攻击与理性自私行为的抑制。

1 方法设计

1.1 方法结构

本文提出了基于区块链的去中心化信誉管理方法,网络结构如图 1 所示。该方法主要包括基于融合时空特征感知的信誉评估算法,奖惩机制和税收机制。在物理感知层,车辆作为终端用户,从传感器设备收集本地数据用以计算信誉值和上报事件信息,并将其上传到附近的 RSU。在通信层,RSU 组成网络集群,每辆车与最近的 RSU 进行通信,各 RSU 共同维护一个区块链网络。所提出方法的关键要素如下。

(1)RSU:在车联网中,RSU 是部署在道路旁边或交通枢纽的设备,用于提供通信和相关应用服务,由于 RSU 具有丰富的计算资源,其在系统中主要负责收集信任评级和管理信任值。

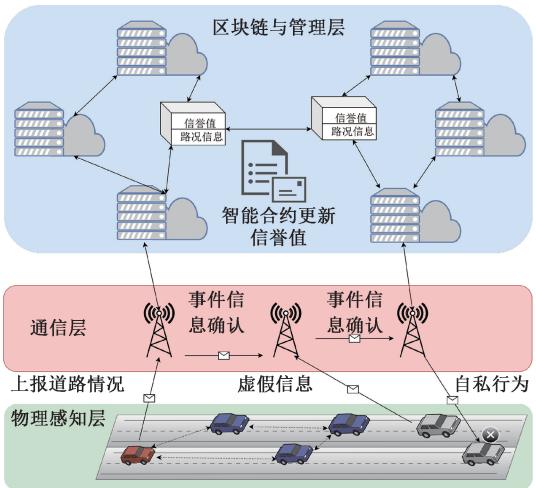

图 1 网络结构

Figure 1 Network Structure

信任评级收集:车辆的信誉值由其它车辆节点进行评估,这些信息无法长期存储或管理在本地。因此,车辆会定期将其评估结果上传到附近的 RSU。

信任值管理:RSU 根据收集到的信誉评价信息和车辆报告的事件信息来计算特定车辆的信任值。一旦信任值计算完成,其它车辆可以在需要时随时查询这些数据。

(2)车辆节点:在车联网网络中,每个车辆节点都配备了一个车载单元(OBU),该单元实现车辆通信。这些 OBU 具有通信、计算、存储和导航等功能。

1.2 设计目标

为了实现智能交通场景下车辆的信誉管理,本文将系统的设计目标总结为以下几个方面。

(1)抵抗恶意攻击。恶意攻击(malicious attack, MA)是指车辆向路边基站发送虚假信息,干扰智能交通系统的正常运行。

(2)抵制自私行为。自私行为(selfish behaviors)表现为车辆节点选择不向 RSU 报告感知到的信息。通过这种方式,自私车辆可以避免行驶过程中在计算、通信和能源方面的开销。

(3)抵抗智能恶意攻击和理性自私行为。恶意开关攻击是 MA 的升级变种。通过长期主动报告积累了良好口碑的车辆可能会在某些情况下启动 MA,并在攻击结束后立即切换回正常模式。此外,理性自私行为车辆一般情况下不会上报任何信息。只有当它发现难以继续存在于系统中,车辆才会切换回正常模式。

(4)避免信誉贬值。信誉贬值是指信誉管理系统长期运行后,由于主动上报真实信息,大多数车辆

的信誉值趋近于上界的现象。在这种情况下,任何基于车辆信誉值建立的信任关系都可能会变得不可靠。因此,需要从整个系统的角度来管理信誉值,实现信誉值在不同实体之间的流通。

1.3 信誉值计算

本文提出了基于时空特征感知的信誉评估方法。该方法使用空间传递性来评估车辆节点的间接信誉,使用时间连续性来评估其历史信誉。然后将这些评估合并成综合信誉值,该值包含了时间和空间维度。在空间维度上,考虑了丢包率(PLR)、包转发率(PFR)和可信交互率(TIR)三个关键指标。时间维度主要考虑节点的历史信誉值。信誉值更新流程如图 2 所示。

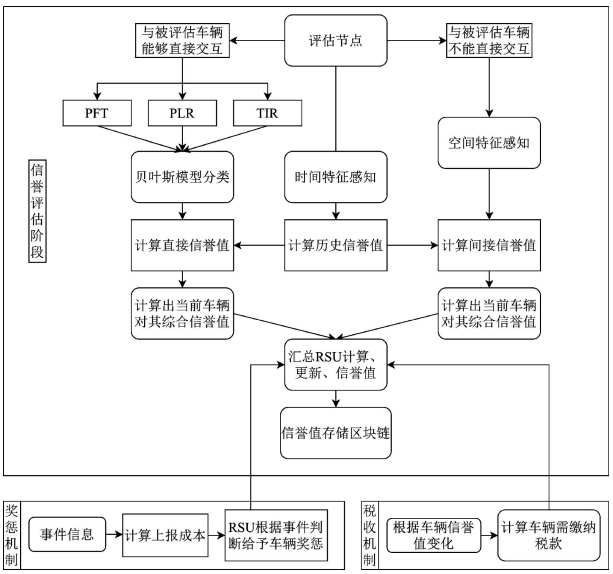

图 2 信誉值更新流程

Figure 2 Reputation value update process

1.3.1 直接信誉值计算

本文采用高斯朴素贝叶斯算法和 β 分布来确定车辆之间的直接信任。根据车辆节点在 $[t-\Delta t,t]$ 内的交互情况,预测 t 时刻交互成功概率,本文将节点 i 和 j 在 t 时刻的交互成功概率用于计算直接信誉值,通过模拟训练集训练高斯朴素贝叶斯分类器。通过监测节点行为来评估节点,训练集中主要包含三个关键评估因子:丢包率(PLR)、包转发率(PFR)和可信交互率(TIR),并将分类器输出的预测概率值作为车辆交互成功率。

恶意节点会降低链路的可靠性并且增加丢包率,IR 表示接受节点接收报文数,IS 表示发送节点发送报文数。可计算为

$$PLR = IR/IS。 \tag{1}$$

在车联网中,车辆间的数据传输依赖中间节点转发实现。恶意节点可能为了干扰车联网的正常运行而截断报文转发。PFR 可以作为车辆交互满意度的重要评价指标,其中 IN 表示节点接收到的数据包数量,IF 表示节点转发的数据包数量,可计算为

$$PFR = IF/IN。 \tag{2}$$

本文方案将 TIR 定义为在事件期间内受信任的交互与成功交互的比率。其中 $Iuntru$ 表示不可信交互的数量,$Itru$ 表示可信交互的数量,可计算为

$$TIR = Iuntru/(Iuntru + Itru)。 \tag{3}$$

在本文方案中,用模拟训练集将预先训练好的贝叶斯模型的输出值作为交互成功率,训练集主要特征为:PLR、PFR、TIR,将数据进行标注,判定正常和恶意节点,其中恶意节点的判断为 $PLR>0.5$ 持续 3 个周期,或 $PFR<0.4$ 且 $TIR<0.3$。对数据的预处理过程中,存在部分无交互记录节点,会填充默认值 $PLR=0$,$PFR=1$,$TIR=1$。同时剔除异常值:$PLR=1$ 且 $PFR=0$ 和理想节点:$PFR=1$,$TIR=1$。最后进行训练集的划分和模型构建。将上述三种指标输入贝叶斯模型:

$$S_i = \text{Gaussian}(PLR,PFR,TIR)。 \tag{4}$$

如果输出的值大于 0.5,认为交互成功,如果输出的值小于 0.5,则认为交互失败。设 S 表示两个节点之间交互成功的次数,F 表示交互失败的次数。节点 i 对 j 的直接信誉评价公式为

$$D_{ij}^{t} = (S+1)/(S+F+2)。 \tag{5}$$

1.3.2 基于空间车辆间的数据传输依赖中间节点转发实现特征感知的间接信誉评价

在实际的车联网场景中,节点之间往往难以计算直接信誉值。因此,本文引入了间接信誉,同时为了建立更真实的信誉评估方法,提高信誉评价的准确性,引入了信誉空间衰减因子来调整。间接信誉的计算可表示为

$$SP_{ij}^{t} = e^{-\lambda_1 n} D_{ij} (0 \leqslant n \leqslant 4)。 \tag{6}$$

式中:$e^{-\lambda_1 n}$ 表示间接节点总数为 n 的信誉链的信誉衰减程度;λ_1 为空间衰减率;信誉链可表示为 $L=[i,v_1,\cdots v_n]$;D_{ij} 表示节点 i 和节点 j 的直接信誉。

1.3.3 基于时间特征感知的历史信誉评价

在车联网场景下,车辆信誉评估还需要考虑历史信誉值对当前的影响。因此,本文在信誉评估方法中加入了历史信誉评估模块。为了确保信誉的动态变化并准确计算其值,本文在该模块中引入了信誉时间衰减因子。历史信誉值可以计算为

$$His_j^t = \sum_{m=1}^{n} e^{-\lambda_2 (t-t_m)} Tru_j^{t_m}。 \tag{7}$$

式中:His_j^t 表示节点 j 在当前时刻 t 的历史信誉;$e^{-\lambda_2(t-t_m)}$ 表示时刻 t_m 的信誉衰减程度;λ_2 为时间衰减率,取值在 0 到 1 之间,根据不同场景调整其值。

1.3.4 综合信誉评价

综合信誉由直接信誉、间接信誉和历史信誉 3 部分构成。当节点 i 与节点 j 能够建立直接的信誉关系时,则节点 i 对节点 j 的综合信誉评价为

$$T_{ij}^t = \delta_1 D_{ij}^t + \delta_2 His_j^t。 \tag{8}$$

否则为

$$T_{ij}^t = \delta_3 SP_{ij}^t + \delta_2 His_j^t。 \tag{9}$$

式中:δ_1、δ_2 和 δ_3 分别代表直接信誉、间接信誉和历史信誉的权重。三者应满足 $\delta_1 + \delta_2 = 1$, $\delta_3 + \delta_2 = 1$。直接交互时,直接信誉评估和历史信誉评估构成完备事件空间,符合概率可加性公理。间接交互场景下,由于需依赖信誉链,经过衰减后可得

$$\delta_3 = \delta_1 e^{-\lambda_1 n}。 \tag{10}$$

由此可得的约束条件还有 $\delta_3 < \delta_1$。为满足不同场景需求,在城市拥挤路段中,可以将 δ_1 的数值适时调高,在空旷道路,可以将的数值适时调低。本文将它们的值设置为 0.5。

车辆将对该节点的信誉值上报给 RSU,RSU 负责计算节点的综合信誉值,车辆节点 j 的综合信誉值为

$$Tru_j^t = \frac{1}{|V|}\sum_{i\in V} T_{ij}^t。 \tag{11}$$

1.4 奖惩机制

本文提出了 1 种信誉值奖惩机制。车辆在报告事件信息时,需要在报告中添加确认值 e,e 表示车辆对其报告信息的确认度。较高的 e 表示车辆对所上报事件具有更高确认度。RSU 接收到报告后,虽然事件信息的真实性尚未验证,但可以通过 e 值进行初步判断。此外,车辆需要从其账户中扣除一部分信誉值,作为上报一条信息的成本 C。函数 $C(e,Tru_j^t)$ 是计算成本 C 的,$C(e,Tru_j^t)$ 需要满足三个属性。首先,车辆应该为每一个报告信息支付成本。其次,发送信息时确认度高的车辆应该支付更多成本。最后,在同样的情况下,信誉值较高的车辆应该支付更少成本。基于此,相关描述如下:

$$\forall e, Tru_j^t, C(e,Tru_j^t) \in [e, Tru_j^t]; \tag{12}$$

$$\forall Tru_j^t, C(0,Tru_j^t) = 0; \tag{13}$$

$$\frac{\partial C(e,Tru_j^t)}{\partial e} > 0; \tag{14}$$

$$\frac{\partial C(e,Tru_j^t)}{\partial Tru_j^t} < 0。 \tag{15}$$

为满足三个性质,将 $C(e,Tru_j^t)$ 定义为

$$C(e,Tru_j^t) = e^2/(\alpha Tru_j^t)。 \tag{16}$$

式中:α 是针对不同场景下的调优参数集。由于车辆在信誉值变为 0 后应该被排除系统,因此本文评估方法中的信誉值总是大于 0。根据公式,当 $e = Tru_j^t/\sqrt{\alpha}$ 时,$C(e,Tru_j^t)$ 达到最大值 Tru_j^t。

RSU 可以通过监控等方式进行事件真实性验证,验证后需要对上报事件的车辆进行奖励或惩罚。函数 $W(e)$ 是计算奖励值 w 的公式,一方面,w 的值要高于车辆之前支付成本。另一方面,发送信息时设置较高 e 的车辆应获得更多奖励。此外,设计了函数 $P(f)$ 用于惩罚信誉值的计算。在验证信息为假之后,会按一定比例扣除车辆当前信誉值的一部分。由于所有报告活动都记录在链上,因此可以计算车辆执行恶意攻击次数 f,并且惩罚值随着 f 的增加而增加。根据上述分析,将 $W(e)$ 和 $P(f)$ 需要满足的属性总结如下:

$$\forall e, Tru_j^t, W(e) > C(e,Tru_j^t); \tag{17}$$

$$\frac{\partial W(e)}{\partial e} > 0; \tag{18}$$

$$\frac{\partial P(f)}{\partial f} > 0。 \tag{19}$$

为了实现上述性质,分别在式(20)和式(21)中定义 $W(e)$ 和 $P(f)$。与 α 一样,式(20)中的 β 为应用场景相关参数。在奖励函数 $W(e) = \beta e$ 中,参数 β 表示确认度对应的信誉奖励强度。由于真实上报的期望收益需要高于沉默行为,即 $\beta e > C(e,Tru_j^i)$,代入式(12)中可得

$$\beta > e/(\alpha Tru_j^i)。 \tag{20}$$

由于可能存在设备故障等错误,RSU 应该能够允许车辆报告错误信息。只有当发现车辆恶意攻击次数超过一定次数,才应该将其从系统中移除。因此,$P(f)$ 被设计为分段函数。只有当 f 大于阈值 Wrn 时,车辆的信誉值才会降为 0。

$$W(e) = \begin{cases} 0, & r = \text{false}; \\ \beta e, & r = \text{true}。 \end{cases} \tag{21}$$

$$p(f,Tru_j^t) = \begin{cases} Tru_j^t, & f > Wrn; \\ (1-0.5^f)Tru_j^t, & f \leqslant Wrn。 \end{cases} \tag{22}$$

1.5 税收机制

对于车辆信誉值的长期管理,本文提出了一种税收机制。当一个管理周期结束时,根据下述公式计算管理账号支出的信誉值 S:

$$S = W - P - C = \sum_i^m w_i - \sum_i^n p_i - \sum_i^l c_i。 \tag{23}$$

式中:W 为诚实上报信息的车辆获得的信誉值总

和;P 为执行恶意攻击的车辆被扣除的信誉值总和;C 为上报信息的车辆所支付的总成本;l 为一个时间段内所有车辆上报信息的总次数;m 为调查结果为真次数;n 为调查结果为假次数。

如果 S 大于 0,则管理方信誉值为净支出,将向车辆收取信誉值作为税。函数 $T(R,\delta)$ 是用于计算车辆应缴纳的税额,并满足以下 3 个性质。根据车辆在最近管理周期内的信誉变化 δ,将其划分为信誉值增加、减少与不变 3 类状态。其次,无论信誉值是增加还是减少,车辆所缴纳的税都随着绝对值的增加而增加。如果信誉值保持不变,则车辆所缴纳的税款与信誉值呈正相关。根据上述分析,$T(R,\delta)$ 定义为

$$T(R,\delta)=\begin{cases} T_1\delta \Big/ \sum_{j=1}^{n_1}\delta_j, & \delta>0;\\ T_2|\delta| \Big/ \sum_{j=1}^{n_2}|\delta|_j, & \delta<0;\\ T_3 Tru \Big/ \sum_{j=1}^{n_3} Tru_j^t, & \delta=0。 \end{cases} \tag{24}$$

式中:n_1、n_2、n_3 分别为 3 个子集的车辆数量;T_1、T_2、T_3 分别为 3 个子集中的车辆应缴纳的税款。

1.6 基于区块链的数据存储

为了防止攻击者恶意篡改数据,设计了基于区块链的数据存储方案。首先,将信誉值的奖惩机制和税收机制计算流程写入智能合约,以确保 RSU 按照正确的方法计算事件报告车辆的信誉值。然后,将信誉值和事件报告中的路况信息存储到区块链中,当车辆请求路况信息和其它车辆的信誉值时从区块链获取。

(1)智能合约。本文方法将信誉值的奖惩机制和税收机制的计算过程写入智能合约并部署在区块链上。智能合约一旦部署到区块链上就无法更改。当 RSU 计算信誉值时,只需要调用智能合约中的算法。伪代码如算法 1 所示:

算法 1 奖惩机制智能合约

输入:车辆 j 的上报信息

输出:信誉值更新

①if 车辆上报事件属实 then
②　计算奖励值 $W(e)$
③　更新车辆 j 的信誉值
④else
⑤　计算惩罚值 $P(f)$
⑥　更新车辆 j 的信誉值
⑦if 更新后的数值<0 或者>1
⑧　return false;
⑨else
⑩　return true;

根据算法 1,首先获取车辆事件报告,查询指定车辆的当前信誉值。然后,根据结果计算对车辆的奖励或处罚。最后,检查更新后的数值是否合理,并将信誉值和事件信息存储在区块链中。如果确认新的信誉值正确,则返回 true,否则返回 false。

算法 2 税收机制智能合约

输入:车辆的信誉变化值

输出:信誉值更新

①if $\delta>0$
②　then 分类至信誉值增加子集中
③else if $\delta<0$
④　then 分类至信誉值减少子集中
⑤else 分类至信誉值不变子集中
⑥　计算 $T(R,\delta)$,更新车辆 j 的信誉值
⑦　if 更新后的数值<0 或者>1
⑧　return false;
⑨else
⑩　return true;

根据算法 2,首先计算管理者和车辆在最近一个管理周期内的变化,然后根据其类别计算指定车辆的税收,最后核对扣除税款后的信誉值。如果更新后的信誉值正确,则返回 true。否则返回 false。

(2)数据存储。在区块链中,一个区块通常含有一个唯一标识且具有前一个区块的哈希值。这种区块的加密链接确保了链中记录信息的不可篡改,使得数据更加可靠和安全。

(3)共识算法。Raft 算法的交易延迟稳定低于 1 秒,假设 RSU 节点为可信节点,无需应对拜占庭攻击,Raft 算法在车联网场景下具有实时性高,资源需求低等优势。

2 实验分析

为评估本文提出的方法,在 Ubuntu20.04 操作系统中使用 Veins、Sumo、OMNET++模拟器和 Python 语言相结合模拟真实的车联网场景。模拟区域为郑州市部分区域真实路况,纬度从 34.788 11°到 34.780 75°,经度从 113.652 15°到 113.676 27°。仿真参数如表 1 所示。

2.1 安全性分析

(1)抵抗恶意攻击。在车辆进行事件报告时,依据公式要求车辆支出事件报告成本。如果车辆上报的信息属实,则可以获得信誉值奖励,奖励值必须

大于成本值。相反,如果车辆上报虚假信息,无论它恶意攻击次数是否超过阈值,都会扣除信誉值,从而可以抵抗恶意攻击。

表 1　仿真参数
Table 1　Simulation parameters

仿真参数	参数数值	单位
RSU 数量	2	个
车辆数量	150	个
恶意车辆占比	[0,50%]	
车辆速度交通流量模型	[5,20]随机均匀分布	m/s
通信距离	200	m
传输功率	20	dBm
权重 δ_1、δ_2、δ_3	0.5	
阈值 Wrn	10	

(2)抵制自私行为。对于有自私行为的车辆,根据公式(23),由于车辆的信誉值没有变化,因此税收只与车辆当前的信誉值有关。由于信誉值是非负的,因此有自私行为的车辆的信誉值变化是小于等于 0。如果车辆保持沉默,则在每个管理期结束时将其信誉价值的一部分作为税收扣除。在信誉值清零之后,该车辆将被排除在系统之外。

(3)抵抗智能恶意攻击和自私行为。对于恶意开关攻击,本文从两个方面采取了抵抗措施,首先,本文公式中为车辆执行的恶意攻击次数设置了一个阈值,超过阈值时,车辆信誉值会直接归 0,并被排除在系统之外。其次,所有事件报告都会上报在区块链上,这些记录无法被篡改,管理者可以通过查询获得车辆恶意行为的准确数值。对于理性自私的车辆,本文方法通过税收机制在每个周期后征收信誉值。由于车辆的信誉值不断减少,具有理性自私行为的车辆必须通过报告真实信息来留在系统内。

2.2　性能分析

在第一个对比实验中,随机将 30%的节点设置为具有恶意攻击行为的车辆(VMAB),其余 70%的节点设置为具有诚实行为的车辆(VNB)。此外,还选择[15]中采用的经典线性信誉管理方法(LRM)进行比较。

图 3(a)显示了两种不同评估方法下 VMAB 的信誉值变化。由于文本方法和 LRM 都是通过扣除信誉值惩罚 VMAB,因此信誉值的变化趋势是相似的。虽然两者均通过扣除信誉值进行惩罚,但机制存在本质差异。LRM 按固定比例扣除,惩罚力度随信誉降低而减弱,且无法彻底清零;本文方法的惩罚力度则随攻击次数递增,一旦超过阈值便直接将节点信誉清零并剔除出系统。

图 3(b)显示了恶意开关攻击(VMOAB)在两种不同评估方法下的信誉值变化。虽然这两种评估方法都降低了 VMOAB 的信誉值,但它们的表现不同。LRM 通常在一定程度上降低信誉值,但不能判断 VMOAB 是否是恶意开关攻击。本文方法可以快速将 VMOAB 的信誉值赋值为 0。

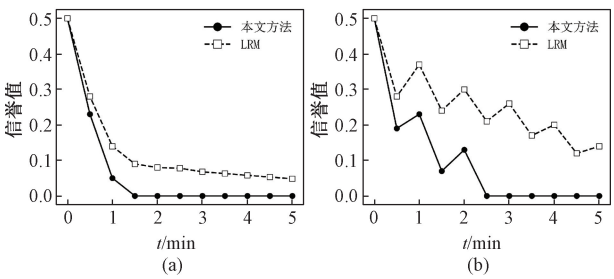

图 3　不同方法下 VMAB 和 VMOAB 的信誉值变化
Figure 3　Variation of reputation values of VMAB and VMOAB under different methods

选择文献[16]作为一组对比实验,该方法利用了强化学习区分恶意节点,在图 4 中该方法可以识别出具有恶意攻击行为的节点并降低其信誉值,但其并不能识别具有恶意开关攻击行为的车辆节点,这种类型车辆的信誉值呈现出时高时低的状态。

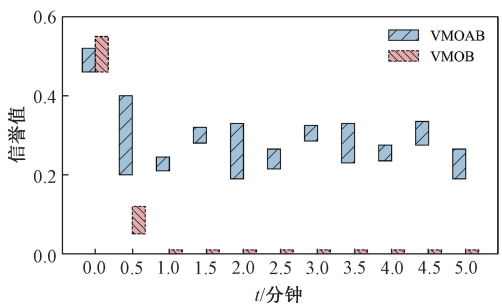

图 4　2 种车辆在文献[16]中信誉值变化
Figure 4　Variation of reputation values for two types of vehicles in reference[16]

最后,比较了两种方法对两种自私行为的抵抗能力。在实验中,30%的节点随机设置为自私行为的车辆(VSB),30%的节点随机设置为理性自私行为的车辆(VRSB),其余节点设置为 VNB。根据实验设置,当 VRSB 的信誉值低于 0.25 时,它会从自私转向主动上报。如图 5(a)所示,随着时间的推移,自私车辆的信誉价值逐渐降低。一旦车辆再次选择主动上报信息,其信誉值迅速增加。LRM 不能检测车辆的自私行为。如图 5(b)所示,在实验过程中,VSB 和 VRSB 的信誉值几乎没有变化。在 LRM 中,VNB 的信誉值在累计后可以达到上界。一旦出现这种情况,VNB 可能会因为无法继续积累其信誉价值而转向自私行为。本文方法一方面,VNB 在每笔交易中获得的奖励随着其信誉值的增加而逐渐减

少。另一方面,所有车辆都会定期扣除一部分信誉价值来缴税。因此,如图 5(b)所示,VNB 可以保持较高的信誉,但无法达到预设的上限。

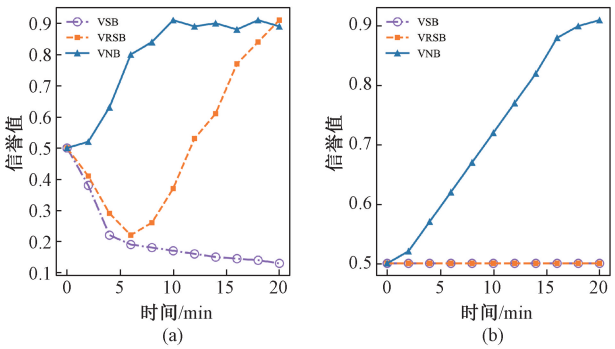

图 5　3 种车辆在本方法和 LRM 中信誉值变化

Figure 5　Variation of reputation values for three types of vehicles under this method and LRM

同时为了验证本文提出的评估方法在车联网中识别恶意节点的性能,使用精确度 P 和召回率 R 来评估本文提出方法的准确性。同时本文提出的方法将与 HHTM[12]和 IWOT-V[13]进行对比。

$$P = \frac{\text{检测到的真正恶意节点总数}}{\text{报告的恶意节点总数}}; \tag{22}$$

$$R = \frac{\text{检测到的真正恶意节点总数}}{\text{真正的恶意节点总数}}。 \tag{23}$$

图 6 对比了在车辆网中不同车辆节点数量下的方法性能,与 HTTM 方法相比,由于本文采用了基于时空特征融合的信誉值算法,随着节点数量的增加,本文方法可以避免因车联网变得复杂而导致的识别率下降,因此本文方法的精确度和召回率相比于其它两个方法更好。

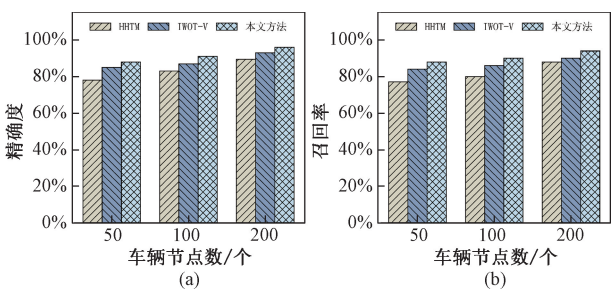

图 6　不同车辆节点数量的精确度和召回率

Figure 6　Accuracy and recall rate with different numbers of vehicle nodes

图 7 中,与两种对比方案相比,本文方法的精确度更好,当网络中的恶意节点占比较低时,本文方法与其他方法并无明显性能差异。图中显示的召回率也高于两个对比方案,随着恶意节点占比的增加,性能呈现下降的趋势,因为在网络中恶意节点占比较高的情况下,更难从附近车辆接收到真实的交通信息,并且通信更加困难导致评估车辆信誉的难度增大,更难识别出恶意车辆。

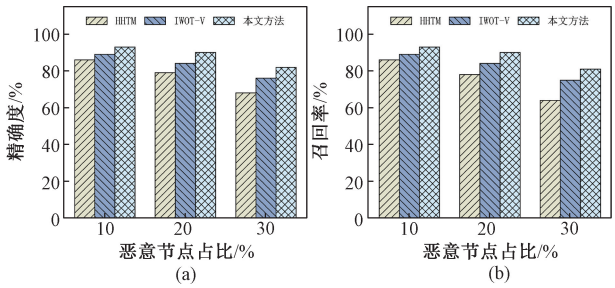

图 7　不同恶意节点占比的精度和召回率

Figure 7　Accuracy recall rate with different proportions of malicious nodes

3　结论

本文提出了 1 种基于区块链和时空特征感知融合的车联网信誉管理方法。基于丢包率、转发率和可信交互来评估节点的信誉。间接信誉使用空间传递性进行评估,而历史信誉利用时间连续性进行评估。在车辆事件报告方面,不仅要求只有经过验证的信息才能作为信誉计算的依据,而且还提出了 2 种不同的机制来防御车辆的恶意攻击和自私行为。最后,通过理论分析和仿真实验证明,本文提出的车辆信誉管理方法不仅可以有效抵御恶意攻击和自私行为,还可以应对车辆智能化带来的挑战,证实了其可靠性,优于现有解决方案。本文的方案存在一定局限性,还需增强和多样化数据集,提高识别不同类型恶意车辆的准确性。基于此,未来我们的工作主要在信任管理工作的基础上为边缘设备进行计算资源的卸载与分配。

参考文献:

[1] Liu Qiang, Chen Da, Liu Yijian, et al. Reconfigurable intelligent surface-enhanced layered division multiplexing for 5G-based MBMS over vehicle networks[J]. IEEE Transactions on Broadcasting, 2024, 70(1): 57-65.

[2] Ji Baofeng, Zhang Xueru, Mumtaz S, et al. Survey on the Internet of vehicles: network architectures and applications[J]. IEEE Communications Standards Magazine, 2020, 4(1): 34-41.

[3] Yu Cunqian, Lin Bin, Guo Ping, et al. Deployment and dimensioning of fog computing-based Internet of vehicle infrastructure for autonomous driving[J]. IEEE Internet of Things Journal, 2019, 6(1): 149-160.

[4] Cao Bin, Sun Zhiheng, Zhang Jintong, et al. Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing[J]. IEEE Transactions on Intelligent

Transportation Systems, 2021, 22(6): 3832-3840.
[5] Wang Peng, 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.
[6] Ge Chunpeng, Zhou Lu, Hancke G P, et al. A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks[J]. IEEE Internet of Things Journal, 2021, 8(16): 12481-12489.
[7] Safavat S, Rawat D B. On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based Internet of vehicles for smart cities[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(8): 5050-5059.
[8] Feng Chaosheng, Yu Keping, Aloqaily M, et al. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13784-13795.
[9] Kerrache C A, Calafate C T, Cano J C, et al. Trust management for vehicular networks: an adversary-oriented overview[J]. IEEE Access, 2016, 4: 9293-9307.
[10] Hussain R, Lee J, Zeadally S. Trust in VANET: a survey of current solutions and future research opportunities[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(5): 2553-2571.
[11] Chen Jiming, Li Tingting, Panneerselvam J. TMEC: a trust management based on evidence combination on attack-resistant and collaborative Internet of vehicles[J]. IEEE Access, 2019, 7: 148913-148922.
[12] Mao Ming, Yi Peng, Hu Tao, et al. Hierarchical hybrid trust management scheme in SDN-enabled VANETs[J]. Mobile Information Systems, 2021, 2021: 7611619.
[13] Xiao Yonggang, Liu Yanbing. BayesTrust and VehicleRank: constructing an implicit web of trust in VANET[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2850-2864.
[14] Yu Dongxiao, Zou Zongrui, Chen Shuzhen, et al. Decentralized parallel SGD with privacy preservation in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(6): 5211-5220.
[15] Ahmad F, Kurugollu F, Adnane A, et al. MARINE: man-in-the-middle attack resistant trust model in connected vehicles[J]. IEEE Internet of Things Journal, 2020, 7(4): 3310-3322.
[16] Zhao Junhui, Huang Fanwei, Liao Longxia, et al. Blockchain-based trust management model for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2024, 11(5): 8118-8132.

A Reputation Assessment Method for Vehicular Networks Based on the Fusion of Spatiotemporal Features and Blockchain

TIAN Zhao[1,2], ZHOU Zheng[1,2], NIU Ya Jie[1,2], Lu Hao Jie[1,2], LIU Wei[1,2], ZAI Guang Jun[1,2]

(1. School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450002, China; 2. Zhengzhou Key Laboratory of Blockchain and Data Intelligence, Zhengzhou 450002, China)

Abstract: Aiming at the problem of untrusted interaction data caused by malicious attacks and selfish behaviors of nodes in the Internet of Vehicles (IoV), and the issue that existing methods are prone to cause reputation depreciation, a reputation assessment method fusing blockchain and spatiotemporal features was proposed. First, the Gaussian Naive Bayes algorithm was introduced to fuse temporal and spatial features, aiming to improve the accuracy of reputation assessment in dynamic environments. Second, reputation was updated based on the event confirmation degree to achieve more reliable reputation aggregation. Finally, a reward and punishment mechanism and a taxation mechanism based on signaling games were deployed in smart contracts to maintain the dynamic balance of global reputation. Simulation results showed that the identification precision and recall of the proposed method remained above 82% and 81%, respectively. Facing highly concealed malicious switching attacks, it could reduce the reputation of attacking nodes to zero within 2.5 minutes. This method effectively suppressed complex network attacks and rational selfish behaviors, mechanically avoided system reputation depreciation, and guaranteed the security of data interaction in the IoV.

Keywords: intelligent transportation; blockchain; artificial intelligence; internet of vehicles; reputation assessment