文章编号:1671-6833(2022)01-0103-08

基于区块链的车联网安全信息共享机制设计

李永强, 刘兆伟

(烟台大学 计算机与控制工程学院,山东 烟台 264005)

摘 要:针对车联网中车辆共享信息的安全性及隐私性问题,提出了一种基于区块链的安全信息共享机制。在该机制中,共享信息和车辆的信誉值通过基于 DAG 结构的区块链进行存储,减轻了车辆存储负担。通过基于双重过滤的信誉机制排除网络中的恶意信息。此外,引入了一种基于用户隐私需求的假名替换策略,将车辆行驶目标和驾驶员隐私保护需求参数化,并提出一种假名替换间隔计算方法,重新定义假名更换频率。实验结果表明:当网络中恶意节点达到 30%时,车辆接收信息的准确率仍在 91%以上,该机制可以有效地提升车联网中信息共享的安全性和可靠性。

关键词:区块链;车联网;多重签名;信誉评估;隐私保护

中图分类号:U495;TP309.2 **文献标志码**:A **doi**:10.13705/j.issn.1671-6833.2022.01.005

0 引言

现如今,随着车辆中各类传感器、通信模块和人工智能技术的发展,车辆将变得更加智能。由各类基础设施和智能车辆组成的车联网将是 5G 通信时代的一个重要应用场景[1]。在该场景下,车联网借助于车-基础设施通信(V2I)、车-路通信(V2R)和车-车通信(V2V)等方式,促进车辆间的信息共享,提升道路安全性和运输效率,为人们提供舒适的驾驶体验[2]。

然而,车联网的高机动性和波动性等特性使其容易遭受到各种类型的攻击,该网络的隐私性、安全性和可靠性仍需进一步增强:一方面,由于担心上传的数据会暴露隐私,用户可能不会主动分享收集到的交通数据;另一方面,由于车辆的高速移动性和位置的不确定性,与陌生车辆建立信任关系具有一定的挑战性,车辆间的不信任性将严重影响数据流通,甚至会形成“数据孤岛”,阻碍车联网的进一步发展[3-4]。

现阶段,人们认为区块链技术有极大的潜力应对上述问题,并将彻底改变整个车联网的技术格局。区块链具有抗篡改和去中心化的特性,参与者的所有活动、身份信息和共享数据都将被写入不可伪造的分布式账本中,这些特征有利于在车联网中构建理想的数据共享平台[5]。然而,由于区块链的公开性和透明性,存储的数据可以被网络中的每一个参与者查看,攻击者通过分析网络中车辆的历史行为可以追溯到其真实身份。

为了更好地提升车联网中共享信息的可靠性,一些安全验证方案已被提出。Behfarnia 等[6]提出建立基于贝叶斯博弈模型的投票机制,该机制通过对可疑节点的周边节点发起局部投票来排除恶意节点。Liu 等[7]提出了一种基于区块链的信任管理模型以实现信息的可信性,该模型采用基于逻辑回归的信任计算提高了对恶意车辆信誉值的敏感性。然而,上述方案对于网络中的所有信息采用一致的验证方法,没有考虑网络中信息多样性和时效性的不同。

车辆隐私的保护是另一个关键的挑战,因为这将直接影响用户加入车联网的意愿,车辆的敏感信息不应暴露在网络之中。为了更好地保护车联网中的私有数据,Feng 等[8]提出了一种称为区块链辅助隐私保护认证系统的新型框架,不需要任何在线注册中心,允许跟踪和动态撤销行为不端的车辆。Tan 等[9]提出了一种车辆与路边单元

收稿日期:2021-05-19;**修订日期**:2021-07-28

基金项目:国家自然科学基金资助项目(62072391);烟台市重点研发计划(2020XDRH092);烟台大学博士启动基金(JS19B77)

通信作者:刘兆伟(1979—),男,山东烟台人,烟台大学副教授,博士,主要从事机器学习和区块链研究,E-mail:lzw@ytu.edu.cn。

之间的无证书认证协议,实现了车辆的身份认证。然而,该机制的实现依赖于可信的第三方,不能提供分布式的安全保护。

鉴于此,本文针对车联网中车辆间存在的信任和隐私问题,提出了一种基于区块链的车联网安全信息共享机制。为进一步提升网络中信息的可靠性,该机制采用了基于信誉的双重过滤技术,考虑多因素对于车辆信誉的影响,使得车辆的恶意行为可以准确和全面地反映在信誉上。此外,通过引入基于用户隐私需求的假名替换策略,重新定义假名更换频率。

1 区块链技术

区块链被认为是一种由复杂密码技术和共识模型支持的去中心化的分布式账本或数据库,能够有效解决信息不对称问题,实现多个主体间的信任与协作,具有极高的应用价值。

然而,目前的区块链系统每年需要耗费数十太瓦时的能源用于挖矿,这对于资源受限的车辆来说是无法接受的。此外,传统的区块链主要采用链式的存储结构,这种链式设计导致区块和交易都是按顺序处理的,严重影响了区块生成效率。显然,传统的链式结构区块链已无法满足车联网中海量数据的实时性存储需求。如图1所示,本文采用了一种基于有向无环图(directed acyclic graph, DAG)结构的IOTA[10]来提升系统的稳定性。

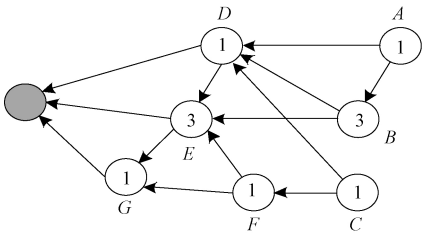

图1 基于DAG结构的区块链

Figure 1 Structure of the DAG-based blockchain

DAG结构的区块链不再受单一主链和区块大小的限制,这些特点使其能在车联网场景中获得更好的应用,如更高的吞吐量和更短的交易确认时间。在车联网应用场景中,由于车辆众多,发送和接收信息也十分频繁,故本文采用IOTA作为数据存储工具。

2 安全模型

本文从安全性和隐私性角度出发,提出了一种基于区块链的车联网安全信息共享机制。本节将着重讨论所提机制中涉及的实体。

如图2所示,该机制主要包含5种不同类型的实体,即:路边基站、车辆、交通管理部门、追踪部门和执法部门。

(1)路边基站(roadside unit, RSU)。路边基站配备了存储、处理和无线通信模块,主要负责接收和传递车辆发出的交通信息。

(2)车辆。本文中出现的车辆可分为3种类型。

诚实车辆:能够诚实地发送车辆收集到的交通信息并对接收到的信息进行及时反馈。

恶意车辆:车联网中可能存在部分恶意车辆,为了自身利益试图干扰其他车辆的正常行驶。

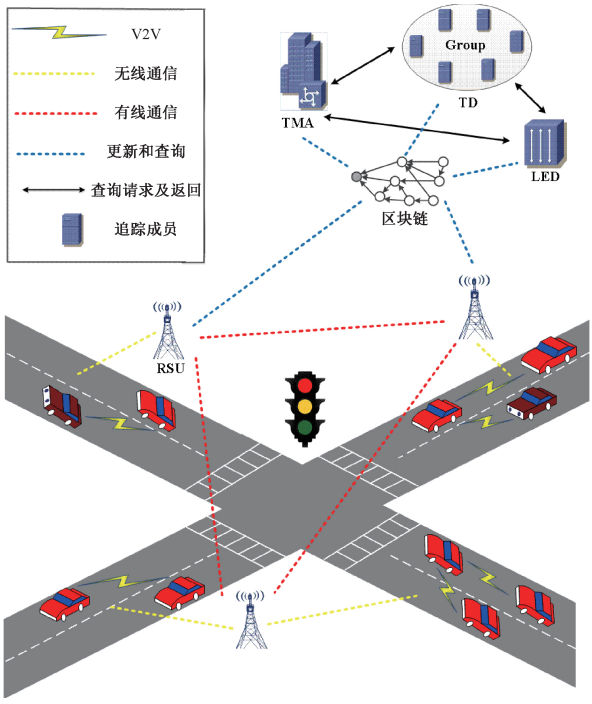

图2 本机制的主要结构框架

Figure 2 Main structural framework of the mechanism

临时中心节点:主要作用是根据组内车辆的反馈信息完成车辆信誉的更新并将其上传至区块链。

(3)交通管理部门(traffic management authority, TMA)。交通管理部门负责核验车辆初始信息和真实身份,掌管车辆假名和证书的发放。

(4)追踪部门(tracers department, TD)。追踪部门由多个追踪小组构成,追踪小组中的追踪成员由TMA和网络中的车辆联合选出。

(5)执法部门(law enforcement department, LED)。如果发现虚假公告信息,执法部门可根据

信息发布者的历史作恶记录来对其进行惩罚。

3　机制运行方案

本节将详细介绍所提出的方案,主要包含 5 个阶段:机制的初始化、车辆登记、假名分发、隐私保护和信息验证。

3.1　机制的初始化

公钥密码体制是实现信息安全传输的重要技术之一,尤其是椭圆曲线公钥密码体制(elliptic curve public-key cryptosystem, ECC),具有安全性高、密钥长度短、计算速度快、节省通信带宽和存储空间等优势。在所提出的机制中,每个实体都可以通过 ECC 方案获得一对私钥和公钥。

3.2　车辆的登记与假名分发

为了跟踪和惩罚网络中的恶意车辆,车辆需要在注册时向 TMA 提交自己的公钥和身份信息进行验证。如果有效,TMA 将公钥和身份信息的映射关系存储在区块链中。为保护身份隐私,车辆 V 可向 TMA 发送带有自身签名的假名申请请求。如果签名有效,TMA 将向 V 发送用于通信的假名。

3.3　隐私保护

与其他移动自组织网络相比,车联网的拓扑变化频繁、网络规模庞大,车辆更容易受到隐私威胁。假名技术使车辆与外部进行通信时,可以通过 TMA 颁发的临时身份代替其真实身份。然而,当网络中存在持续检测的攻击时,攻击者将共享信息与车辆的假名相结合,可以推断出车辆的真实身份。为解决上述挑战,本文采用了一种基于用户隐私需求的假名替换策略。

3.3.1　道路状况

在车辆进入道路之前,驾驶员需要将行程的目的地发送给 TMA。假设车辆起始位置为 S_0,目的地为 S_j,则 C 表示车辆从 S_0 行驶到 S_j 的路况。计算方法如式(1)所示:

$$C = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{length_i}\cdot p_i \cdot L_i\right)。\tag{1}$$

式中:n 为出行路径中包含的道路段数;$length_i$ 为车辆经过的第 i 段道路的长度;p_i 为路段上车辆共享交通信息的概率,该概率是 TMA 对道路历史数据进行分析后获得的;L_i 为某路段的车道时间占用率,为 RSU 获取的实时道路数据。

3.3.2　用户隐私要求

考虑到不同用户对车辆的隐私要求不同,本文规定车辆需要在出发前将本次行程的隐私要求发送给 TMA,以获得每段道路所对应的隐私保护级别 pv,表示为$[pv_1, pv_2, pv_3, \cdots, pv_i]$。TMA 通过权重 ψ 来参数化驾驶员隐私需求,如表 1 所示。

表 1　参数化隐私需求

Table 1　Parameterized privacy requirements

隐私需求	pv	ψ
不需要	1~10	0.1
轻微需要	11~30	0.2
一般需要	31~60	0.3
需要	61~80	0.4
十分需要	81~100	0.5

驾驶员隐私需求 P_{pri} 的计算如式(2)所示:

$$P_{\text{pri}} = \psi_1 pv_1 + \psi_2 pv_2 + \psi_3 pv_3 + \cdots + \psi_i pv_i。\tag{2}$$

3.3.3　假名变更间隔

为避免被追踪,车辆需要定期更改其假名,替换间隔被定义为 T_{lag},随 C 和 P_{pri} 的变化而动态改变。根据多元线性回归方程,可以预测假名的替换时间 T_{lag} 的计算如式(3)所示:

$$T_{\text{lag}} = \alpha_0 + \alpha_1\frac{C}{\bar{v}}S_{\text{dir}} + \frac{\alpha_2}{P_{\text{pri}}} + \mu,\quad \mu \sim N(0,\sigma^2)。\tag{3}$$

式中:α_0、α_1 和 α_2 为权重因子,可以通过最小二乘法计算获得;$\bar{v}$ 为车辆的平均速度;μ 为误差;S_{dir} 为车辆运动方向在旅程中需要改变的次数,设 d_t 和 d_{t+1} 分别表示 t 时刻和 $t+1$ 时刻车辆的移动方向,d_t 与 d_{t+1} 之间的夹角为 θ,如果 θ 大于预定义的阈值,则认为车辆的运动方向发生改变。

本文将影响车辆假名替换间隔的上下限阈值定义为 T_{upper} 和 T_{lower}。当 T_{lag} 在上下阈值之间时,将车辆加入假名更换队列 Q_{wait},即假名更换时间已到,需要尽快更换假名。为避免因使用同一假名时间过长而被跟踪,当 T_{lag} 高于 T_{upper} 时,增加车辆在 Q_{wait} 中的优先级,强制更改假名;若 T_{lag} 低于 T_{lower},表明车辆请求过于频繁,将车辆加入候选队列 Q_{cand}。当车主再次申请时更改车辆假名。

3.4　信息验证

本文采用基于双重过滤的信誉机制来完成信息的验证,该机制的运行过程如图 3 所示,当车辆的传感器模块检测到异常信息时,该车辆将通过通信模块将异常信息发送至周围车辆,接收到异常信息的车辆依据发送车辆的信誉值、近期综合信誉表现和活跃度等因素完成对接收信息的验证;随后,车辆将根据实际情况对所接收信息的真实性进行评估,并将评估信息临时存储在本地;信息发送者和接收者建立一

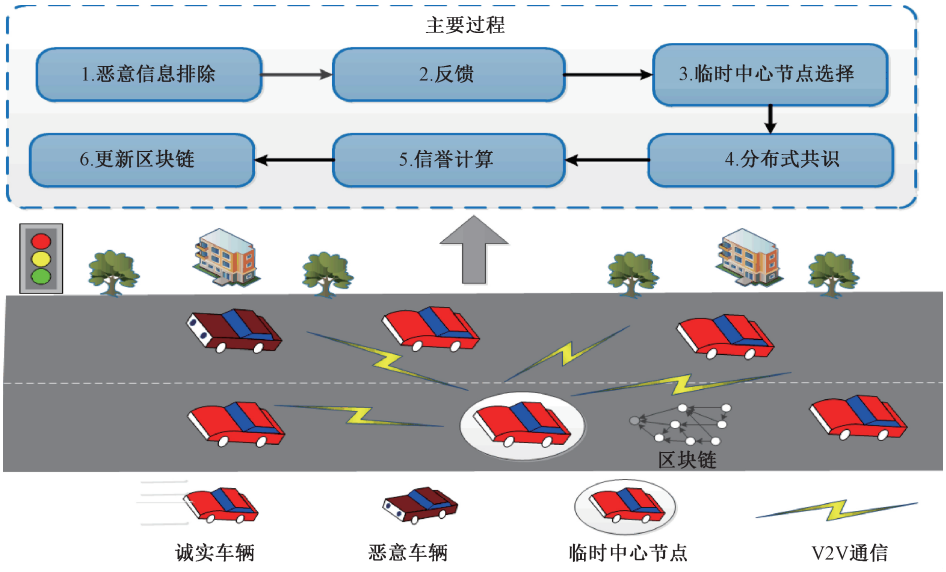

图3 基于车辆信誉的后验机制

Figure 3 Posteriori method based on vehicle reputation

个临时的小组并选出组内的临时中心节点,负责达成小组内对于评估信息的共识;最后,临时中心节点通过获取的反馈信息完成车辆信誉的更新并将其上传至区块链。

车联网中信息服务种类繁多,由于各类信息在车联网中所发挥的重要程度不同,因此车辆主动发送不同类型共享信息对自身信誉的影响也将是不同的。本文中设定车辆的信誉由两部分构成,即紧急信息信誉 R_{Em} 和非紧急信息信誉 R_{Nem},信誉的计算如式(4)所示:

$$R=\beta_1 R_{\mathrm{Nem}}+\beta_2 R_{\mathrm{Em}}。\tag{4}$$

式中:参数 β_1 和 β_2 分别为非紧急信息信誉和紧急信息信誉所占的权重,$\beta_1+\beta_2=1$。该机制将根据式(4)对车辆的总信誉进行更新。

3.4.1 信息筛选

当接收到从车辆 V_1 发送来的紧急信息后,首先查看 V_1 的信誉值,若其信誉值高于设定的阈值 RTH,便可以认为该信息通过了初步的筛选,进入下一验证阶段。

第二阶段主要考虑 V_1 的近期(一般默认为20 d,可根据实际情况进行调整)综合信誉 R_{com},当 R_{com} 较大时,则认为 V_1 的近期表现较好,接受该紧急信息;反之,抛弃该紧急信息。车辆的近期综合信誉与近期信誉表现(R_{rec})、活跃度(V_{liv})和信誉值(R)相关,具体计算如式(5)所示:

$$R_{\mathrm{com}}=\lambda_1 R_{\mathrm{rec}}+\lambda_2 V_{\mathrm{liv}}+\lambda_3 R。\tag{5}$$

式中:R_{rec}、R_{liv} 和 R 的权重分别为 λ_1、λ_2 和 λ_3,且 $\lambda_1+\lambda_2+\lambda_3=1$。其部分参数说明如下。

近期信誉表现(R_{rec})。车辆的近期行为将比历史总体行为更能体现该车辆当前的行为趋势。因此本文使用了衰减因子 S_l 来体现 R_{rec} 随时间的变化情况,表示为 $S_l=t_l/\sum_{l=1}^{n}t_l$,其中 $t_l=T_l-T_1$,T_1 为近期内车辆发送的第一条紧急类信息的时间。车辆发送共享信息的时间距当前时刻越近,其权重越大,即 $S_1<S_2<\cdots<S_n$。从区块链中获取车辆的历史信誉 H,即可通过式(6)计算车辆的近期信誉表现 R_{rec}:

$$R_{\mathrm{rec}}=\sum_{i=1}^{n}H_l S_l。\tag{6}$$

近期活跃度(V_{liv})。近期活跃度是衡量某一时间段内车辆发送的紧急信息的数目,单位时间内发送的信息数目越多,车辆的活跃度越高:

$$V_{\mathrm{liv}}=\frac{sum}{T_{\mathrm{rec}}}。\tag{7}$$

式中:sum 为近期内车辆发送的共享信息数目;T_{rec} 为所提出机制规定的时间段。

经过上述过程的筛选后,如果 V_1 所发送的紧急信息符合要求,则认为该信息是可靠的,车辆将给予驾驶员行驶提醒。算法具体步骤如下。

算法1 恶意信息筛选算法(MMF algorithm)。

输入:异常数据;

输出:信誉评估信息 D_{RE}。

①abnormal data detection;

②**if** $V_j.data$ ==false **then** /*检测到异常数据*/

③Determine the type of message and verification;

④**for** $i\leftarrow 1$, $n-1$ **do**

⑤ $V_i\leftarrow\{M_{\mathrm{Em}}, Reputation\ data, S_j, Cer_v\}$;

/* M_{Em}为紧急信息,S_j为车辆 V_j 对 M_{Em}的签名 */
⑥**end for**
⑦ **end if**
⑧ Verify the validity of the reputation data;
⑨**if** $R_j \geqslant RTH$ **then**
⑩　Calculate R_{com} according to equation (5);
/* R_{rec}和 V_{liv}分别根据式(6)和(7)获得 */
⑪　**if** $R_{com} \geqslant RTH_1$ **then**
⑫　Receive emergency messages;
⑬　**if** M_{Em} = = true **then**
⑭　Set *message* = 1;
⑮　**else**
⑯　Set *message* = −1;
⑰　**end if**
⑱　**else**
⑲　throw *message*;
⑳　**end if**
㉑**end if**
㉒**return** D_{RE}

在车辆生成信誉评估信息后,为达成共识,系统将紧急信息发送车辆和信息接收车辆组建成一个临时小组,并赋予小组内车辆一个临时的 *ID*。所提出的临时中心节点选择方案如下:

$$\text{Hash}(ID, time, R) < A。\tag{8}$$

式中:*time* 为车辆参与选举时信息输入的时间;*A* 是对车辆信誉的量化,车辆的历史信誉越好,*A* 表示的哈希阈值范围越大,车辆被选为临时中心节点的概率越高。

3.4.2　车辆信誉更新

被选为临时中心节点的车辆将把本地存储的信誉评估信息发送给组内的成员,该成员根据本地信息对所接收到的信息进行反馈,最后由临时中心节点根据反馈情况判定信誉评估信息的可靠性并上传至区块链。算法具体步骤如下。

算法 2　信誉更新算法(RVU algorithm)。

输入:信誉评估信息 D_{RE};

输出:更新后的车辆信誉值 R。

① **Call** algorithm MMF;
② V_T send message to V_i;
/* 临时中心节点发送信誉评估信息给组内车辆 */
③　**for** $i \leftarrow 1, n-1$ **do**
④　$V_i \leftarrow \{ D_{RE}, S_T \}$;
/* S_T 为临时中心节点对发送的信息的签名 */
⑤　**if** D_{RE} &&S_T = = true **then**
⑥　$Sum \leftarrow Sum + 1$;
⑦　**end if**
⑧　**end for**
⑨ **if** $Sum/(n-1) \geqslant 70\%$ **then**
⑩　update reputation value;/* 信誉值上升 */
⑪ **else if** $Sum/(n-1) \leqslant 50\%$ **then**
⑫　update reputation value and punishment;
⑬**else**　delayed rating;
⑭ **end if**
⑮ **return** reputation value

当车辆发送恶意信息时,会降低车辆的信誉值,且处罚力度与时间相关,会随着车辆作恶次数增加而逐渐加重,其定义如式(9)所示:

$$\theta = \sum_{k=1}^{n} \alpha \cdot \frac{\Delta T}{t - t_k}。\tag{9}$$

式中:θ 为对恶意车辆的惩罚程度;α 为惩罚系数;ΔT 为一个时间单元;t 为当前的时间;t_k 为车辆发送恶意信息的时间。

车辆作恶次数被记录在区块链当中,当达到指定的阈值时,TMA 将注销该用户信息并将其放入黑名单中。

4　实验分析

本节在计算机上依据所提算法进行实验仿真和分析。该实验硬件环境为 Intel AMD Ryzen 7 4800H CPU、主频 2.9 GHz 和内存 16 GB,操作系统为 64 位 Windows10,编程语言为 Go 和 Python,集成开发环境为 GoLand2019 和 Pycharm2019。

本文将实验场景设定在由 6 × 6 街区组成的正方形模拟街道上,每个街区的大小为 600 m×600 m。模拟场景中车辆的数目为 200 辆,车辆的平均速度为 110 km/h,车辆的无线通信距离为 300 m,RSU 部署在街区的交叉路口处,非恶意车辆产生错误信誉评估信息的概率为 5%,使用的哈希算法为 SHA-256。

本文用接收信息的准确率(*MAR*)来评判算法的性能,其定义如式(10)所示:

$$MAR = \frac{TP + TN}{s}。\tag{10}$$

式中:*TP* 表示车辆在接收到信息后,获取真实信息的数量;*TN* 表示排除恶意信息的数量;*s* 表示在该段时间内接收到的信息总量。

图 4 显示的是当模拟实验中存在 30 辆恶意车辆时,不同 *RTH* 取值对车辆接收信息准确率的

影响情况。从图4中可以看出,当*RTH*较低时,由于大量恶意信息不能被排除,*MAR*值较低;随着*RTH*的升高,*MAR*值也随之提升,当*RTH*为5时,车辆接收信息的准确率达到最高值0.92;当*RTH*继续增大时,由于高信誉值的车辆占少数,大量真实信息因无法满足预设的*RTH*而被排除,*MAR*值随之急剧下降。

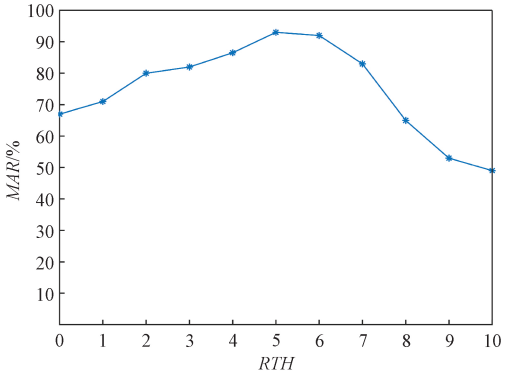

图4 *RTH*对信息准确率的影响

Figure 4 Influence of *RTH* on the accuracy of information detection

为进一步验证本文所提出方案的有效性,将其与VARS算法[11]、Vcash算法[12]和文献[13]中提出的算法进行实验对比。根据上述实验所得结果,将实验场景中*RTH*设为5,对比各方案在恶意车辆占比率(*MR*)不同时,所接收信息准确率的情况,实验结果如图5所示。

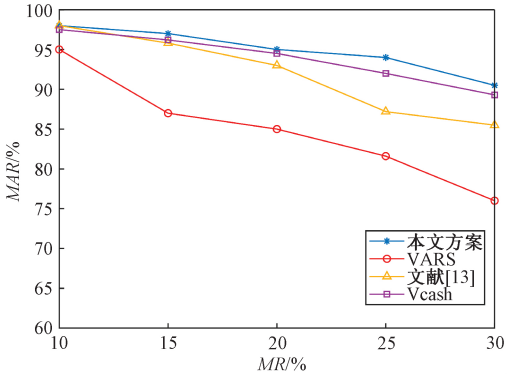

图5 不同恶意车辆占比时接收信息的准确率

Figure 5 Influence of malicious cars on the accuracy of information detection

从图5中可以看出,随着网络中恶意车辆的增多,本文所提出的机制相比其他两种方案对于恶意信息的排除率更高,曲线较为平缓,受网络中恶意信息的影响最小。当实验中恶意车辆节点占比为30%时,本文所提方案接收信息的准确率仍然大于91%。这是由于本文所使用的信誉机制不仅依靠*RTH*排除恶意信息,而且还通过车辆活跃度和近期信誉表现等多种因素进行二次过滤。在相同的恶意车辆节点占比下,该方案的*MAR*明显高于其他3种算法。

车联网中恶意车辆的存在对网络中信息的安全性危害极大,因此对网络中恶意车辆进行有效排除是十分重要的。假设模拟实验中恶意车辆仍为30辆,比较本文所提出方案与其他3种算法随运行时间对恶意车辆的排除情况。恶意车辆排除率(*MCR*)的定义如式(11)所示:

$$MCR = \frac{sum_{mal}}{sum_{all}}。\tag{11}$$

式中:sum_{mal}为被检测出的恶意车辆的数量;sum_{all}为实验中恶意车辆的总数。

图6显示的是上述4种方案对恶意车辆的排除情况,在实验运行初期(30 s之前),由于网络中恶意信息的数量较少,车辆所受到的惩罚相对较轻,*MCR*值较低;在实验运行中期(30~90 s),排除率迅速上升,且本文提出方案的上升趋势明显高于其他3种算法;在运行至90 s时对于恶意车辆的排除率已达95%以上。这是由于本文所提出的算法对于接收信息的评估需要先在小组内达成共识,该机制能够有效防止部分车辆对于所接收信息的误判,提升对于恶意信息判断的准确率。同时,该方案还采用了基于时间的惩罚机制,在短时间内随着车辆恶意行为的增多,恶意车辆受到的惩罚也将累积增长。

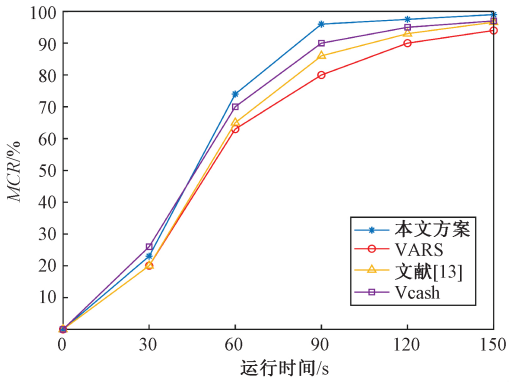

图6 恶意车辆排除率对比图

Figure 6 Comparison chart of malicious vehicle exclusion rate

图7中显示的是上述4种算法对于恶意车辆的排除数量随时间的变化情况,从图7中可以清晰地看出在整个实验过程中本文所提方案对恶意车辆的排除情况整体优于其他3种方案,完全排

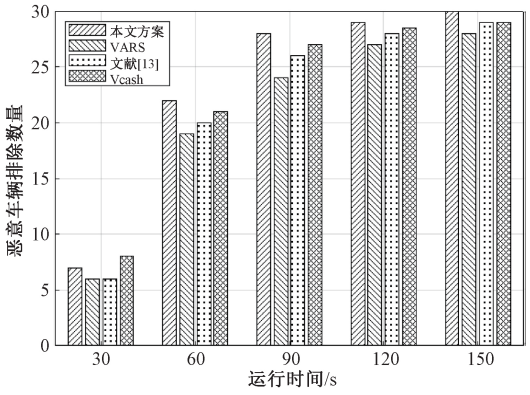

图 7　恶意车辆排除数量对比柱状图

Figure 7　Comparison histogram of malicious vehicle exclusion number

除恶意车辆所用时间也相对较短。

5　结论

车联网中恶意节点的存在会严重影响网络中共享信息的安全性,为此本文提出了一种基于区块链的车联网信息安全共享机制,该机制通过基于车辆信誉的后验方案来保证车辆接收信息的可靠性,使用基于用户隐私需求的假名替换策略来保护用户隐私。理论分析和仿真实验表明,该机制可有效地提升车联网中共享信息的安全性和可靠性。

参考文献:

[1] BELGHITI I D, MABROUK A. 5G-dynamic resource sharing mechanism for vehicular networks: congestion game approach[C]//2018 International Symposium on Advanced Electrical and Communication Technologies (ISAECT). Piscataway: IEEE, 2018: 1-5.

[2] HOSSAIN M, HASAN R, ZAWOAD S. Trust-IoV: a trustworthy forensic investigation framework for the Internet of vehicles (IoV)[C]//2017 IEEE International Congress on Internet of Things (ICIOT). Piscataway: IEEE, 2017: 25-32.

[3] 王华,何晓宇,徐静,等.融合交通心理学的车辆群组运动仿真研究综述[J].郑州大学学报(工学版),2020,41(1):83-90.

[4] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for Internet of Things: a survey[J]. IEEE Internet of Things journal, 2019, 6(5): 8076-8094.

[5] LI L, LIU J Q, CHENG L C, et al. CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE transactions on intelligent transportation systems, 2018, 19(7): 2204-2220.

[6] BEHFARNIA A, ESLAMI A. Local voting games for misbehavior detection in VANETs in presence of uncertainty[C]//2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Piscataway: IEEE, 2019: 480-486.

[7] LIU X C, HUANG H P, XIAO F, et al. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs[J]. IEEE Internet of Things journal, 2020, 7(5): 4101-4112.

[8] FENG Q, HE D B, ZEADALLY S, et al. BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks[J]. IEEE transactions on industrial informatics, 2020, 16(6): 4146-4155.

[9] TAN H W, CHOI D, KIM P, et al. Secure certificateless authentication and road message dissemination protocol in VANETs[J]. Wireless communications and mobile computing, 2018, 2018(99): 1-13.

[10] YANG S, CHEN Z T, CUI L Z, et al. CoDAG: an efficient and compacted DAG-based blockchain protocol[C]//2019 IEEE International Conference on Blockchain (Blockchain). Piscataway: IEEE, 2019: 314-318.

[11] DOTZER F, FISCHER L, MAGIERA P. VARS: a vehicle ad-hoc network reputation system[C]//Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. Piscataway: IEEE, 2005: 454-456.

[12] TIAN Z H, GAO X S, SU S, et al. Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles[J]. IEEE Internet of Things journal, 2020, 7(5): 3901-3909.

[13] YANG Z, ZHENG K, YANG K, et al. A blockchain-based reputation system for data credibility assessment in vehicular networks[C]//2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). Piscataway: IEEE, 2017: 1-5.

Blockchain-based Secure Data Sharing Mechanism Design in the Vehicular Networks

LI Yongqiang, LIU Zhaowei

(School of Computer and Control Engineering, Yantai University, Yantai 264005, China)

Abstract: A secure data sharing mechanism based on blockchain was proposed aiming at the security and privacy issues of vehicle sharing information in the Internet of Vehicles. In this mechanism, the shared message and reputation value were stored through the blockchain based on the DAG structure, and the storage burden of the vehicle would be reduced. The malicious information in the network was excluded through the reputation mechanism. In addition, a pseudonym substitution strategy based on user privacy needs was introduced, which parameterize vehicle driving goals and driver privacy protection needed. A calculation method for the replacement interval of pseudonyms was proposed, which redefined the frequency of pseudonym replacement. Experiments showed that when the malicious nodes in the network reached 30%, the accuracy of the vehicle receiving information was higher than 91%, the mechanism could effectively improve the safety and reliability of information sharing in the Internet of Vehicles.

Keywords: blockchain; Internet of Vehicles; multi-signature; reputation assessment; privacy protection

---

(上接第102页)

Research on Current Harmonic Suppression Strategy of the LCL Grid-connected Inverter

LIU Haiyang, DONG Lianghui, GAO Jinfeng, WANG Yaoqiang, HUANG Wenjian

(School of Electrical Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: The increasing number of nonlinear devices increased the harmonic content of grid voltage background and led to the grid-connected current distortion of inverter. In order to suppress grid-connected current harmonics, an improved grid voltage proportional-feedforward control strategy was proposed. The influence of inverter side inductance and filter capacitance on grid voltage proportional-feedforward control strategy of LCL grid-connected inverter was analyzed, and the optimal selection method of inverter side inductance and filter capacitor was obtained. That was to say, according to the performance requirements and equipment safety requirements of the inverter, the range of inductance and filter capacitor on the inverter side of LCL grid-connected inverter was determined, and the appropriate inductance value was determined accordingly. Then the harmonic content of grid-connected current was reduced by selecting a smaller capacitance value. Finally, the effectiveness of the control strategy and optimization method was verified in the prototype of LCL grid-connected inverter. The experimental results showed that the total harmonic distortion rate of grid-connected current of LCL grid-connected inverter was reduced from 4.04% to 2.58%, and the third and fifth harmonics with higher harmonic content were reduced from 2% to less than 1%, which improved the performance of the inverter.

Keywords: LCL filter; resonant frequency; grid-connected inverter; feedforward control of grid voltage; parameter design