基于 DAG 区块链的车联网分区域信息共享方法

李一冰[1], 牛科栋[2], 曹仰杰[2], 李　颉[1,3], 庄　岩[2]

(1. 郑州大学 计算机与人工智能学院,河南 郑州 450001;2. 郑州大学 网络空间安全学院,河南 郑州 450002;3. 上海交通大学 计算机科学与工程系,上海 200030)

摘　要:针对传统区块链应用于车联网扩展性差、吞吐量低的问题,提出了一种基于轻量级有向无环图(DAG)区块链的分区域信息共享方法。首先,在此方法中充分考虑了车联网信息共享过程中的区域化特征,将车联网划分为多个子区域来及时完成车辆之间地信息共享,并且利用边缘 RSU 节点来帮助车辆进行快速的跨区域认证。其次,将区域性和时间敏感性与传统 DAG 的马尔科夫蒙特卡洛(MCMC)方法相融合,设计了新的基于信息共享相关性的提示选择算法(RTB-TSA)。另外,使用了一种基于积分值的 tip 发送速率控制方法来抵御寄生链攻击,确保 DAG 系统的安全性。最后,通过仿真实验的结果表明,在效率方面,与传统 DAG 区块链系统对比,本文提出方法的 tip 选择速率较提高了约 5%,收敛轮数降低了约 30%;与 DDB-TSA 方法对比,本文所提出方法的 tip 选择速率提高了约 1%,收敛轮数降低了约 7%;在系统稳定性和安全性方面,本文所提出方法的 DAG 账本可以保持收敛性,且可以有效抑制由恶意节点发起的寄生链攻击。

关键词:区块链; 信息共享; 有向无环图; 车联网; 分区域

中图分类号:TU528.1　　**文献标志码**:A　　**doi**:10.13705/j.issn.1671-6833.2026.03.002

将区块链技术应用于车联网构建分布式的通信网络,有效解决了信息共享过程中数据隐私、安全性和可靠性的问题[1]。但是区块链吞吐量低、可扩展性差,这给高移动性、低时延的车联网场景下的应用带来了挑战[2]。提高吞吐量和可扩展性是使区块链与车联网融合的有效方法。

图结构是解决区块链吞吐量和扩展性的有效方法。在有向无环图(directed acyclic graph,DAG)区块链中一次可以并行处理多笔交易。但在一些标准的 DAG 中,例如埃欧塔(a dag-based distributed ledger protocol for the internet of things,IOTA)[3],采用随机游走的蒙特卡洛(markov chain monte carlo,MCMC)tip 选择算法,节点每次需要从账本某一深度的粒子随机游走到 DAG 账本尖端,算法处理冲突速度较慢[4]。此外,只有一些现有工作考虑到与车联网的领域相关度,这在很大程度上影响了车联网信息共享的质量和效率[5-6]。

目前,已经有许多研究提出将 DAG 区块链应用于车联网来确保安全和可靠的信息共享。李等人[7]提出用 DAG 结构的区块链进行存储来减轻车辆的存储负担。Zhang 等[8]提出了 V-Lattice 架构,每辆车辆具有自己的账户链异步的将交易添加区块链中,并在[9]中提出了适应此架构的分片式实用拜占庭容错(practical byzantine fault tolerance,PBFT)共识算法。Yang 等[10]引入 DAG 为数据结构的区块链完成基于车载社交网络(vehicular social networks,VSNs)的信息共享。Feraudo 等[11]提出了名为基于去中心化标识符(decentralized identifier-based reputation system for secure transmission in vanets,DIVA)的分布式信誉系统来保障车联网的安全传输。Li 等[12]设计了一种基于 DAG 的相互监督算法来解决社会化车联网中车辆互不信任的问题。Li, Naipeng 等[13]提出车辆根据自己行程的需要独立的选择附近的车辆达成共识,在当前的区域对车

收稿日期:2025-06-03;**修订日期**:2025-07-26

基金项目:国家自然科学基金项目(62302458);河南省青年科学基金资助项目(242300421474);河南省科技攻关资助项目(222102310547)

作者简介:李一冰(1995—),女,河南驻马店人,郑州大学博士研究生,主要从事区块链研究,E-mail:ybing_li@163.com。

通讯作者:曹仰杰(1976—),男,河南濮阳人,郑州大学教授,博士,博士生导师,主要从事区块链,机器智能与人机交互、大数据智能处理、云计算与高性能计算研究,E-mail:caoyj@zzu.edu.cn。

辆的信誉值形成局部一致性。Cao 等[14]利用区块链的一致性特点解决联邦学习中的设备异步问题。Dong 等[15]将车辆信誉引入待确认交易选择算法(tip select algorithm,TSA)增强系统安全性。FU 等[16]提出了一个融合 DAG 区块链和现代密码学的车联网通信框架,采用博弈论来完成最优通信带宽分配策略。Li 等[17]基于 DAG 区块链和智能合约来抵抗车辆网络中的频谱感知数据伪造(spectrum sensing data falsification,SSDF)攻击。Yang 等[18]基于 DAG 区块链开发了一个分布式的可信边缘计算框架,运用 DAG-DTM 机制使移动边缘节点的信任在链上和链下保持一致。Gu 等[19]设计了一个量的 DAG 区块链架构,将车辆收集到的重要信息存储在 DAG 区块链账本中防止被篡改,并设计了决策理论 Tip 选择(decision-theoretic tip selection,DTTS)算法来选择离开当前区域的的 tip,但是此算法没有考虑到本区域的相关性且需要计算多个属性的效用值,不适应算力资源有限的车联网环境。Du 等[20]提出了一种轻量级的 DAG 区块链框架,虽然减少了共识时延,但没有充分考虑到车联网信息的区域化特征,不利于提高信息共享的质量和效率。

为此,本文提出了一个基于 DAG 区块链的分布式的信息共享框架,将车联网络划分为多个区域。本文假设区域范围足够大,车辆可以在当前所在区域完成信息共享过程。此外,为了解决共识延迟和共享信息的相关度问题,设计了一种新的 tips 选择算法,该算法在共享过程中考虑区域性特征和信息的实时性。总的来说,本文的贡献如下:

(1)本文设计了一种基于轻量级 DAG 区块链架构的区域化信息共享机制,实现车辆在局部区域内的信息分发与共享。在该机制中,道路侧单元(RSU)作为主节点负责账本的管理与维护,车辆则作为轻量节点协同参与 DAG 账本的更新与共识过程。

(2)进一步地,本文提出了一种新的 Tip 选择算法 RTB-TSA,融合了信息共享的地理区域特性与车辆行为的时空敏感性,以提升信息共享的相关性与系统的收敛效率。

1 基于 DAG 区块链的车联网分区域信息共享框架

DAG 区块链是一种轻量的区块链技术,采用有向无环图的数据结构维护区块链账本。在 DAG 区块链中,交易通过并行处理提高了扩展性。在本文中,将交易封装为记录车辆收集信息的交易,通过 DAG 区块链网络共享给其他通信实体(RSU、车辆等),保证了信息的安全性和共享效率。

1.1 信息共享方案

如图 1 所示,整个车联网被划分为多个区域。在本文的信息分享框架中,每个区域有其唯一的区域 ID。每个区域都包含一定数量的路边单元(RSU)和车辆,其中 RSU 的编号与当前区域的区域 ID 相关联。车辆在当前所在区域收集信息并生成交易,交易经过 RSU 或车辆认证后添加至 DAG 账本。在提出的信息共享框架中,大部分 RSU 是诚实的[21],由 RSU 为主节点,车辆为轻节点共同维护整个 DAG 账本。信息共享的基本流程如图 1 所示。

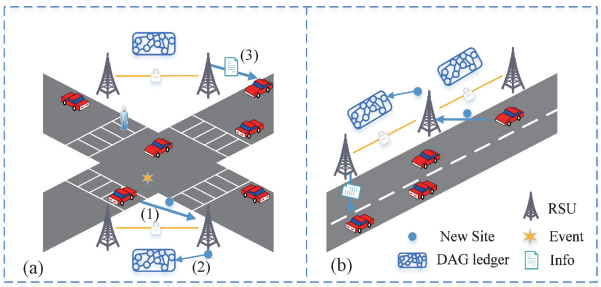

图 1 信息共享框架

Figure 1 Information sharing framework

(1)车辆身份初始化:车辆 k 在初始加入网络时需要注册合法身份。首先,车辆使用唯一的私钥(S_k)通过 SHA-256 算法生成其唯一的公钥(P_k);其次,由 P_k 生成车辆账户地址;再次,车辆通过周围 RSU 或其他车辆账户获取最新的 DAG 账本数据同步后,就可以在 DAG 网络中进行信息共享;最后,只有当车辆的身份在 RSU 维护的合法名单内时,车辆才可以用 P_k 进行信息共享。

(2)从周围环境中收集信息:首先,车辆中装有车载智能单元、红外扫描和激光雷达等智能感知设备,可以从周围环境中收集原始数据;其次,从数据中提取有助于驾驶安全和交通效率的信息,例如周围交通状况、路面情况、拥堵情况等;最后,将这些信息封装后附着在 DAG 账本中。

(3)将共享信息打包:提取的信息会被打包为交易,车辆 x 产生的典型交易本文用 S_x 表示,S_x 典型格式为式(1)

$$S_x = \{I, c, H, W, Sig, P_k\}。 \tag{1}$$

式中:I 是需要共享的信息;c 是共享信息的相关性参数,用来设计新的提示选择算法;H 是信息的哈希值,采用 SHA-256 算法生成;W 是交易自身的权重;Sig 是智能车辆用私钥生成的签名;P_k 是发布该交易车辆的公钥,即为车辆在网络中的账户地址。

(4)将交易添加至 DAG 账本并完成信息共享:如图 1 所示,该过程包括以下步骤:①车辆首先将封装的交易信息传输给邻近的 RSU;②RSU 将该交易信息纳入 DAG 账本中进行审批,包括算法验证和选择两个前驱节点;③将信息与其他车辆共享。

1.2 安全性分析与挑战

本文提出的方法采用基于 DAG 的区块链技术保证信息共享的安全性,改善了传统区块链技术可扩展性差等问题。然而,由于车辆的高移动性、车联网要求低时延性和车辆信息共享的实时性,基于 DAG 区块链的车辆信息共享仍然存在一些问题。

(1)懒惰攻击:如图 2 所示,Lazy workers 是指一些懒惰车辆总是故意批准 DAG 账本中一些已经验证过的旧交易来避免验证工作。如果懒惰站点总是这么做,虽然长时间后会因累计权重的差异而被抛弃,但在短时间内,会造成 DAG 账本尖端 tip 得不到确认,造成大量新交易聚集造成网络拥塞,降低 DAG 网络的吞吐量。

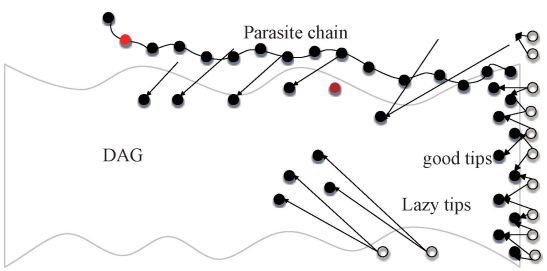

图 2 懒惰攻击和寄生链攻击

Figure 2 Lazy workers and parasitic chain attack

(2)寄生链攻击:指攻击者恶意构造子 DAG。就像图 2 中所示,红色交易是攻击者发起的交易,通过间断的引用主 DAG 来增加子 DAG 的可信度,攻击者后续不断的生成交易来批准和验证自己的交易,以此来增加子 DAG 的权重。如果攻击者使用足够算力的计算机,会发起大量的新交易到网络中,这些交易会批准攻击子 DAG,当寄生链规模足够大时,诚实节点生产的交易也会选择攻击子 DAG 进行批准和认证,此时攻击者攻击成功,车联网安全受到威胁。

(3)确认延迟高:在传统的 DAG 区块链中,采用 MCMC 的 tip 选择算法来选择尖端 tip 进行认证,每次从某一粒子深度的交易采取随机游走的方式游走到尖端 tip。随机选取的 tip 将成为待批准的候选者,MCMC 算法在在随机游走的每一步都需要花费较长时间,会导致较长的共识延迟。因此需要新的 tip 选择算法来减少 DAG 网络的共识延迟。

(4)DAG 账本的收敛性:如果支持 DAG 的区块链账本不收敛,会导致尖端 tips 数量趋向无穷大,大量未被确认的 tip 会造成网络拥塞,导致车联网延迟无限大,最终导致 DAG 系统无法正常运行。因此,在设计新的 tip 选择算法时在降低共识共识延迟的同时必须保证 DAG 账本的收敛性。

(5)DAG 账本相关性:在高移动性、快速变化的交通场景中,驾驶员在做出驾驶决策时更加倾向于选择与其车辆周围交通状况相关度高的信息。在传统的 DAG 账本中,采用 MCMC 算法随机游走选择 tip,忽略了共享信息的相关性,会造成车辆信息共享效率低下。因此,本文在设计信息共享策略时,考虑了车辆收集信息的相关性。

2 DAG 框架中解决方案分析

在本节中,针对上述存在的问题,提出了一种考虑共享信息相关性的 tip 选择算法,将信息共享与车辆当前所在区域位置和信息的实时性相结合。此外还分析了此 tip 选择算法下 DAG 账本的收敛情况。

2.1 基于地理区域和实时性的 tip 选择算法

本文根据地理位置(如街道)将车联网络划分为多个区域,每个区域生成对应的区域 ID。车辆沿道路长度为 L 的道路匀速行驶,速度为 v,位置为 $x(t)=vt$,沿道路以固定间隔 d 部署 RSU,RSU 之间通过有线连接且无线通信半径为 R,设 RSU 位置为 S_i,则单个 RSU 的的覆盖区间为 G_i,如式(2):

$$G_i=[S_i-R,S_i+R]。\tag{2}$$

车辆 x 在时刻 t 所属区域为式(3):

$$r_x=\operatorname{argmax}\{x(t)\in G_i\}。\tag{3}$$

RSU 的数量为 n,单位道路长度内的 RSU 数量 ρ 为式(4):

$$\rho=\frac{n}{L}。\tag{4}$$

RSU 有效覆盖道路长度在总长度的比例 η 的计算公式如式(5)所示:

$$\eta=1-\frac{\sum_{i-1}^{n-1}\max(0,d_i-2R)}{L}。\tag{5}$$

式中:d_i 为相邻 RSU 之间的间距。

可以推导出 RSU 的最优密度 ρ_{opt} 为式(6):

$$\rho_{\text{opt}}=\frac{1}{2R}。\tag{6}$$

在基于 DAG 的区块链中,tip 选择算法至关重要,相当于传统区块链中一种共识方法,即新生成的交易如何添加到当前 DAG 账本中。因此,为了使 DAG 区块链更好的融入车联网,定义了一个车辆信息相关度参数 C,$C=(f(r_x,r_y),g(t_x,t_y))$,$r$ 是车辆

所在地理区域,t 是信息发生的时间。在传统的 DAG 中,如果 y 批准 $x(x \rightarrow y)$,在 IOTA[3] 中选择概率 P_{xy} 表示为公式(7):

$$P_{xy} = \frac{\exp\{-\theta(w_x - w_y)\}}{\sum_{z:z\rightarrow x}\exp\{-\theta(w_x - w_z)\}}。\tag{7}$$

式中:$\theta > 0$ 是选择参数,决定了加权随机游走的程度。w 是交易的累计权重。但直接将累计权重的选择算法应用到车联网中不准确的。在 RTH-TSA[6],DDB-TSA[20] 中,相关参数可以用来加速 tip 选择算法。因此,本文将共享信息的相关度 C_{xy} 添加至选择概率,可以表示为式(8):

$$P_{xy} = \frac{\exp\{-\alpha(w_x - w_y) + \beta c_{xy}\}}{\sum_{z:z\rightarrow x}\exp\{-\theta(w_x - w_z) + \beta c_{xz}\}}。\tag{8}$$

式中:α,β 是大于 0 的权重参数;c 是两个交易之间的相关度;w 是累计权重。可以发现,在累计权重和相同的情况下,交易 x 和交易 y 的 c_{xy} 越高,选择概率 P_{xy} 越大,因此共享信息会优先选择和自己相关度高的信息。

如图 3 所示,新交易会优先选择和自身在同一区域的 tip,随着时间的推移,本文提出的 DAG 账本会形成自然分片,如区域 A 和区域 B 所示。注意红色交易 5,同时包含在两个分片中,是车辆的跨区域交易。

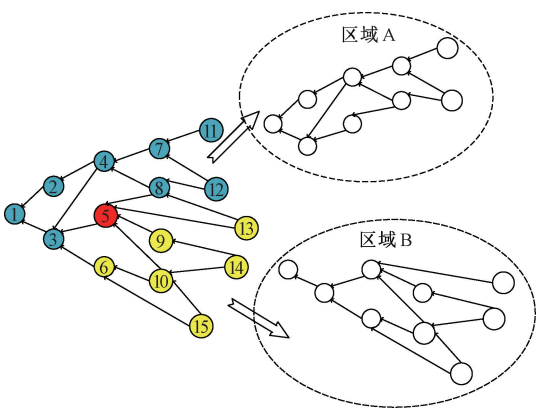

图 3　分区 DAG 逻辑账本

Figure 3　Logically partitioned DAG ledge

其组成 S_y 为式(9):

$$S_y = \{M, R_A, R_B, Sig, P_k\}。\tag{9}$$

式中:R_A 和 R_B 是 RSU_{ID},在本文的架构中,RSU_{ID} 的长度为 160 位,其组成结构如图

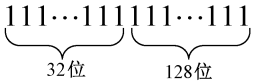

图 4　RSU_{ID} 的结构

Figure 4　The structure of RSU_{ID}

其中前 32bit 为 $Region_{ID}$,后 128bit 是随机生成的唯一字符串,这样可以确保每个 RSU 有唯一的 ID。

2.2　快速跨区域认证

当车辆要从 A 区域前往 B 区域时,边缘 RSU 互相协作完成车辆的快速跨区域认证。如图 5 中所示,区域 A 边缘 RSU_A 向车辆发送一段信息摘要 M,并用自己的私钥进行数字签名。同时,RSU_A 向 B 区域的所有边缘 RSU 发送 M。在这里本文假设 RSU 是绝对信任的且 RSU 之间通过 RSU_{ID} 通讯。车辆到达 B 区域后,将包含 M 和签名的信息发送给 B 区域的 RSU_B,RSU_B 收到信息后,用 RSU_A 的公钥(R_A)验证消息 M。如果 M 相同,车辆跨区域认证通过。RSU_B 将相关信息打包成交易附着在 DAG 账本上。

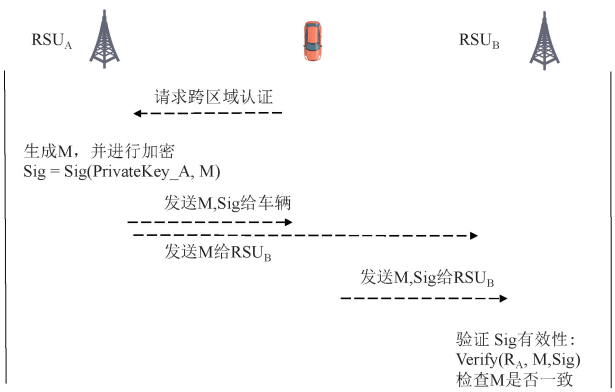

图 5　跨区域认证流程

Figure 5　Cross-regional authentication process

2.3　DAG 账本的收敛性分析

DAG 账本收敛性是区块链系统能够保持正常运行的关键,接下来本文对所提出基于 DAG 区块链框架的收敛性进行理论分析。首先设 $L(t)$ 为系统中在 t 时刻的 tips 总数。本文假设车辆以速率为 λ 的泊松点过程独立的发布交易,$L(t)$ 可表示为式(10):

$$L(t) = L(t-h) + N_h - A_h。\tag{10}$$

式中:$L(t-h)$ 是系统在 $(t-h)$ 时刻系统中的 tips 总数,N_h 式(11)为 $[t-h,t)$ 内车辆发布的新交易 s,A_h 是被 N_h 认证的 tips 数量。

$$N_h = \lambda h。\tag{11}$$

接下来分析 A_h 的数量,先来计算 A_h 事件的概率,A_h 是被 N_h 认证的 tips 数量,计算时间区间 $[t-h,t)$ 内的联合分布概率 $P(A_h,N_h)$,可表示为式(12):

$$P(A_h,N_h) = P(A_h \mid N_h) \times P(N_h)。\tag{12}$$

假设在时间区间 $[t-h,t)$ 内发生了 n 轮批准,

而且批准数量均匀的分布在多轮批准中。所以每轮批准的平均时长为 h/n ,数量为 A_h/n 。在一轮批准中,本文把在 $[0,h/n)$ 的时间内相关度为 c_m 的 tips 记为 a_m ,那么在此时间内存在的所有可能相关度 tips 总数为 $\sum_{m-1}^{M} a_m$,因此在一个批准轮次内,式(12)可以转变为:

$$P\left(c_1 = a_1, c_2 = a_2, \cdots, c_m = a_m, \sum_{m=1}^{M} a_m\right) = P\left(c_1 = a_1, c_2 = a_2, \cdots, c_m = a_m \middle| \sum_{m=1}^{M} a_m\right) \times P\left(\sum_{m=1}^{M} a_m\right)。 \tag{13}$$

在式(13)中 $a_m \geqslant 0$ 且互相独立,且 $\sum_{m-1}^{M} p_c = 1$,所以参数 $a_1, a_2, \cdots, a_n$ 服从多项分布,因此

$$P\left(c_1 = a_1, c_2 = a_2, \cdots, c_m = a_m, \sum_{m=1}^{M} a_m\right) = P\left(\sum_{m=1}^{M} a_m\right)! \prod_{m=1}^{M} \frac{\left(p_{c_m}\right)^{a_m}}{a_m!}。 \tag{14}$$

所以联合分布率式(13)变为

$$P\left(c_1 = a_1, c_2 = a_2, \cdots, c_m = a_m, \sum_{m=1}^{M} a_m\right) = \left(\sum_{m=1}^{M} a_m\right)! \prod_{m=1}^{M} \frac{\left(p_{c_m}\right)^{a_m}}{a_m!} \times \frac{\left(\frac{\lambda h}{n}\right)^{\sum a_m}}{\left(\sum a_m\right)!} e^{-\frac{\lambda h}{n}} = \prod_{m=1}^{M} \frac{\left(\frac{p_{c_m} \lambda h}{n}\right)^{a_m}}{a_m!} e^{-\frac{P_{c_m} \lambda h}{n}}。 \tag{15}$$

根据式(15)的结果,在 $[0,h/n)$,相关度参数为 c_m 的 $A_{c_m}(h/n)$ 符合参数为 $\frac{p_{c_m} \lambda h}{n}$ 的泊松分布,因此

$$E\left(A_{h/n} = \sum_{m=1}^{M} A_{c_m(h/n)}\right) = \sum_{m=1}^{M} \frac{p_{c_m} \lambda h}{n} = \frac{\lambda h}{n}。 \tag{16}$$

所以 $E(A_h) = E(nA_{h/n}) = \lambda h$,由(6)式得 $N_h = A_h$,将结果带入式(12)的可得

$$L(t) = L(t - h)。 \tag{17}$$

这个结果表明,在相隔时间 h 的时间内,tips 总数和上一个时间段保持不变,这说明本文提出的 DAG 账本是保持收敛的。

2.4 抵御攻击方法

针对提出模型易遭受的懒惰攻击和寄生链攻击,解决方法如下:

(1)抵御懒惰攻击:在本文提出的 tip 选择算法中,根据公式(3),优先选择相关度较高的 tip,即在空间距离近和时间间隔小的 tip,不会去选择时间间隔过久的 tip,因此本文的 tip 选择算法可以有效抵御懒惰攻击。

(2)抵御寄生链攻击:寄生链攻击者通过创建 DAG 子链,在短时间内发送大量 tip 附着到子 DAG,然后间接引用主链 DAG 来增加子 DAG 可信度,从而造成分叉。因此,本文提出了基于积分值的 tip 发送速率控制方法。假设正常车辆在固定时间 Δt 内发出的 tip 数量为 n ,如果车辆在 Δt 时间内发送的 tip 数量 $k \leqslant n$,那么车辆积分值保持正常;如果 $k \geqslant n$,则扣除该车辆积分,如果积分值 $\leqslant$ 积分$_{\min}$,该车辆在此时间段无法继续发送 tip。具体过程如算法 1 所示。

算法 1　基于积分值的 tip 发送速率控制算法

① 初始化 vehicle. points = Initial points
② 初始化 vehicle. sent_tips = 0
③ For each time period (Δt)每个周期执行一次:
④ # 检查积分是否足够允许发送 tip
If vehicle. points <=积分阈值 则:
　　Print ("Insufficient points")
　　continue
　　发送 tips
⑤ # 检查是否超过最大可发送 tip 数
　If vehicle. sent_tips > 最大可发送 tip 数:
　　计算超额发送数量
　　扣除积分
⑥　　#防止积分过低,强制保持在门槛值
　　If vehicle. points < 积分阈值:
　　积分回调
　　Else
　　输出"积分不足",跳出本周期
⑦ 重置周期计数器,以备下一个周期
⑧ 等待下一个周期

3　实验分析

在本节中,本文运用仿真实验评估了所提出的基于 DAG 区块链的系统。实验硬件环境为 Intel Core i5-10500 处理器@ 3. 10GHz 主频,16GB DDR4 内存,Windows 11 专业版系统,编程语言为 Java,开发环境为 VsCode2024。主要实验参数见表 1,仿真实验包括 tip 选择延迟、DAG 账本收敛轮数、DAG 账本自身收敛性、抵御寄生链攻击的效果。本文在 tip 选择延迟和 DAG 账本收敛轮数与标准 MCMC 算法[3]和 DDB-TSA[20]选择算法进行比较。本文采用

100 辆车辆在本文提出的框架中的发送信息,车辆的发布信息的过程采用泊松分布的方式。

表 1　主要实验参数

Table 1　Main experimental parameters

参数	值	参数	值
车辆数量	100	泊松分布	$\lambda = 20 \sim 100$
哈希算法	SHA-256	累计权重 cw[1]	$cw = 50 \sim 150$
交易 w 值	1	粒子深度[2]	$pd = 50 \sim 150$

注:1. 累计权重 cw 为交易本身累计的 w 值。

2. 粒子深度从 DAG 账本的某一深度开始游走的值。

3.1　加入 DAG 延迟

加入 DAG 延迟是指车辆从发送消息到 tip 加入 DAG 账本的延迟,本文评估了在粒子深度 $pd = 50$, 100,150 时 RTB 算法和传统 MCMC 算法的 tip 的加入延迟。如图 6 中所示,在 $pd = 50$ 时,RTB 选择算法 tip 选择延迟略高于 MCMC 算法和 DDB-TSA 选择算法,在 $pd = 100$,150 时,RTB 算法的 tip 选择延迟低于传统 MCMC 算法和 DDB-TSA 选择算法。这是由于本文提出的算法将 tip 相关性添加至选择算法中,新生成的 tip 优先选择相关性高的 tip。在大规模的 tips 中拥有更低 tip 选择延迟。

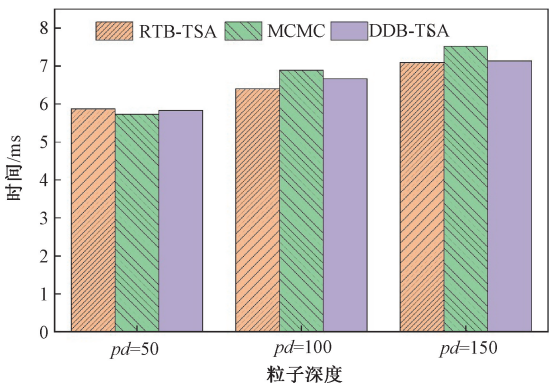

图 6　Tip 选择延迟

Figure 6　Tip selection delay

3.2　DAG 账本收敛轮数

收敛轮数是指新的 tip 加入 DAG 账本后到达某一累计权重 cw 所需要的收敛次数,在 DAG 账本中,累计权重以 $cw = \lambda w$ 的速度增长,累计权重越大,tip 的可靠性会越强。本文将所有 tip 初始自身权重设置为 1,因此累计权重的增长与 tip 的发送速率 λ 有关。如图 7 中所示,在 tip 需要到到不同的累计权重的情况下,在 λ 速率较低的情况下,由于本文提出的 DAG 账本 tip 之间的相关性更高,不同区域的 tip 会自然形成不同的分区,与传统 MCMC 算法的和 DDB-TSA 选择算法相比,在达到相同的累计权重的情况下,本文提出的方法所需收敛轮数更少。

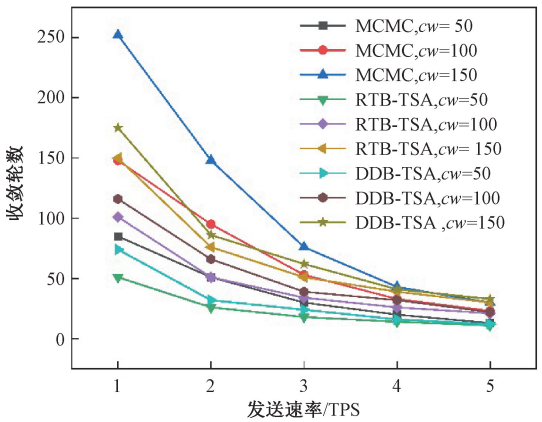

图 7　DAG 收敛轮数

Figure 7　The number of DAG convergence rounds

3.3　DAG 账本收敛性

DAG 账本的收敛性是指 DAG 账本中尖端未被确认 tip 的数量趋于一个有限值,保证 DAG 系统的安全性。图 8 显示了在不同的发送速率 λ 下,DAG 账本中未被确认的 tip 总数总会稳定在某个值附近,未被确认的 tip 数量稳定在均值±5%范围。

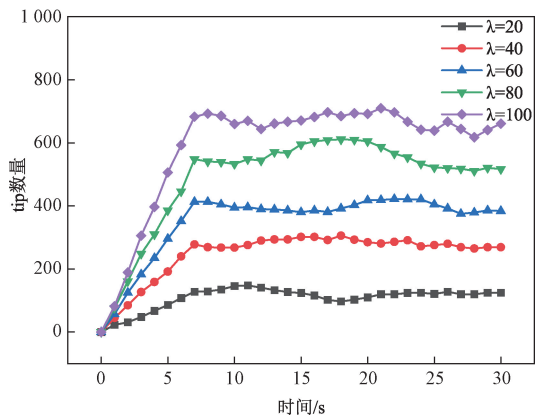

图 8　DAG 收敛轮数

Figure 8　The number of DAG convergence rounds

3.4　DAG 账本抵御寄生链攻击

寄生链攻击者需要再短时间发送大量 tips 附着到自己的子 DAG 端来增加自己子 DAG 的权重。在图 9 中模拟了正常车辆发布和恶意车辆发布 tip 的情况。攻击车辆突然发布 tip 数量大于正常发送 tip 速率,每次发送 tip 扣除账户积分值,当积分值小于最低值时,攻击车辆账户被系统拉入黑名单,并将其之前发送的 tip 逐渐变为孤儿节点不被后续 tip 附着,攻击车辆在 DAG 网络中发送的有效 tip 逐渐变为 0。

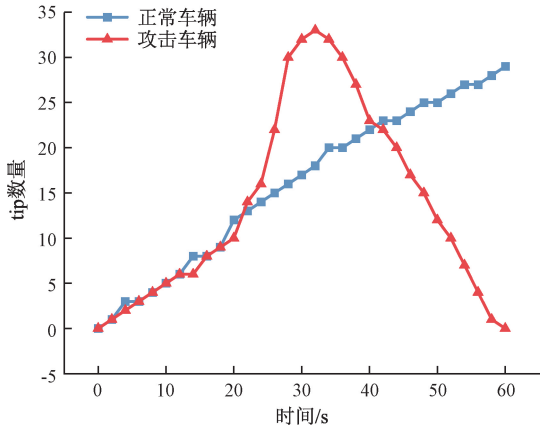

图 9　抵御寄生链攻击

Figure 9　Resist parasitic chain attacks

4　结论

传统区块链应用于车联网存在可扩展性差、效率低下的问题。本文的主要结论如下：

(1)本文提出了一种基于 DAG 区块链的分区域车辆共享信息方法,将车联网分为多个区域来进行信息共享；

(2)本文并结合分区提出了一种新的 tips 选择算法 RTB-TSA,该算法充分考虑信息共享区域化特征和时空敏感性要求；

(3)本文提出了一种基于账户积分的 tip 发送速率控制策略来抵御寄生链攻击。理论分析和仿真实验表明,本文提出方法可以提高提高车联网信息共享的相关性和收敛速度,并有效抑制寄生链攻击。

参考文献：

[1] YADAV S, SINGH K, BEZZATEEV S. Enhancing security using trusted blockchain method for Internet of vehicle [C]//2024 International Conference on Automation and Computation (AUTOCOM). Dehradun, India. IEEE, 2024: 512-518.

[2] ALLADI T, CHAMOLA V, SAHU N, et al. A comprehensive survey on the applications of blockchain for securing vehicular networks[J]. IEEE Communications Surveys & Tutorials, 2022, 24(2): 1212-1239.

[3] RAWAT A, DAZA V, SIGNORINI M. Offline scaling of IoT devices in IOTA blockchain[J]. Sensors, 2022, 22(4): 1411.

[4] CHAI H Y, LENG S P, WU F, et al. Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 14620-14631.

[5] POKHREL S R, CHOI J. Improving TCP performance over WiFi for Internet of vehicles: a federated learning approach[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 6798-6802.

[6] CHAI H Y, LENG S P, WU F. Secure knowledge sharing in Internet of vehicles: a DAG-enabled blockchain framework[C]//ICC 2021 - IEEE International Conference on Communications. Montreal, QC, Canada. IEEE, 2021: 1-6.

[7] 李永强, 刘兆伟. 基于区块链的车联网安全信息共享机制设计[J]. 郑州大学学报(工学版), 2022, 43(1): 103-110.
LI Y Q, LIU Z W. Blockchain-based secure data sharing mechanism design in the vehicular networks[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 103-110.

[8] ZHANG X D, LI R, HOU W H, et al. V-lattice: a lightweight blockchain architecture based on DAG-lattice structure for vehicular ad hoc networks[J]. Security and Communication Networks, 2021, 2021(1): 9942632.

[9] ZHANG X D, LI R, ZHAO H. A parallel consensus mechanism using PBFT based on DAG-lattice structure in the Internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 10(6): 5418-5433.

[10] YANG W H, DAI X H, XIAO J, et al. LDV: a lightweight DAG-based blockchain for vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5749-5759.

[11] FERAUDO A, ROMANDINI N, MAZZOCCA C, et al. DIVA: a DID-based reputation system for secure transmission in VANETs using IOTA[J]. Computer Networks, 2024, 244: 110332.

[12] LI Y J, TAO X F, ZHANG X F, et al. A DAG-based reputation mechanism for preventing peer disclosure in SIoV[J]. IEEE Internet of Things Journal, 2022, 9(23): 24095-24106.

[13] LI N P, GUO Y C, CHEN Y S, et al. A partitioned DAG distributed ledger with local consistency for vehicular reputation management[J]. Wireless Communications and Mobile Computing, 2022, 2022: 6833535.

[14] CAO M R, CAO B, HONG W, et al. DAG-FL: direct acyclic graph-based blockchain empowers on-device federated learning[C]//ICC 2021-IEEE International Conference on Communications. Montreal, QC, Canada. IEEE, 2021: 1-6.

[15] DONG Z X, WU H Y, LI Z Y, et al. Trustworthy VANET: hierarchical DAG-based blockchain solution with proof of reputation consensus algorithm[C]//2023 IEEE International Conference on Blockchain (Blockchain). Danzhou, China. IEEE, 2023: 127-132.

[16] FU Y, WANG S P, ZHANG Q, et al. Game model of

optimal quality experience strategy for Internet of vehicles bandwidth service based on DAG blockchain[J]. IEEE Transactions on Vehicular Technology, 2023, 72(7): 8898-8913.

[17] LI F S, LIN R Q, WANG J, et al. A fast method to defend against SSDF attacks in the CIoV network: based on DAG blockchain and evolutionary game[J]. IEEE Communications Letters, 2023, 27(12): 3171-3175.

[18] YANG W W, SHI L, LIANG H, et al. Trusted mobile edge computing: DAG blockchain-aided trust management and resource allocation[J]. IEEE Transactions on Wireless Communications, 2024, 23(5): 5006-5018.

[19] GU C, CUI X D, LI M, et al. An efficient and privacy-preserving information reporting framework for traffic monitoring in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7900-7913.

[20] DU G X, CAO Y J, LI J, et al. Secure information sharing approach for Internet of vehicles based on DAG-enabled blockchain[J]. Electronics, 2023, 12(8): 1780.

[21] LI Y B, CAO Y J, ZHUANG Y, et al. Blockchain-enabled trust management with location privacy preservation in vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2024, 11(14): 24659-24671.

Subregional information sharing method of Internet of Vehicles based on DAG blockchain

LI Yibing[1], NIU Kedong[2], CAO Yangjie[2], LI Jie[1,3], ZHUANG Yan[2]

(1. School of Computer Science and Artificial Intelligence, Zhengzhou University, Zhengzhou 450001, China; 2. School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450002, China; 3. Department of Computer Science and Engineering, ShanghaiJiaotong University, Shanghai 200030, China)

Abstract: This paper proposes a region-based information sharing method based on a lightweight Directed Acyclic Graph (DAG) blockchain to address the issues of poor scalability and low throughput in traditional blockchain applications for vehicular networks. First, the method takes into account the regional characteristics of information sharing in vehicular networks, dividing the network into multiple sub-regions for timely information sharing between vehicles. Edge RSU nodes are used to help vehicles quickly authenticate across regions. Secondly, the method integrates regional and time-sensitive features with the traditional DAG's Markov Chain Monte Carlo (MCMC) approach and designs a new Tip Selection Algorithm based on information sharing relevance (RTB-TSA). Additionally, a tip sending rate control method based on integral values is used to defend against parasitic chain attacks, ensuring the security of the DAG system. Finally, simulation results show that, in terms of efficiency, compared with traditional DAG blockchain systems, the proposed method improves the tip selection rate by approximately 5% and reduces the convergence rounds by about 30%. Compared with the DDB-TSA method, the proposed method improves the tip selection rate by about 1% and reduces the convergence rounds by about 7%. In terms of system stability and security, the proposed DAG ledger can maintain convergence and effectively suppress parasitic chain attacks initiated by malicious nodes.

Keywords: blockchain; information sharing; directed acyclic graph; internet of vehicles; region-based