文章编号:1007-5321(2022)06-0140-07 **DOI**:10.13190/j.jbupt.2022-142

结合区块链的车联网隐私保护可信预测缓存架构

刘 琨[1], 王圆洁[2], 申自浩[2], 王 辉[1], 刘沛骞[1]
(1.河南理工大学 软件学院, 焦作 454000; 2.河南理工大学 计算机科学与技术学院, 焦作 454000)

摘要: 第 6 代移动通信系统提供的高效通信技术促进了车联网的快速发展。车联网中已发布数据中的位置和查询请求等敏感信息容易遭到恶意攻击,使隐私泄露。对此,根据认知引擎感知用户需求,提出一种基于区块链的可信预测缓存架构(TPCAB)。首先,基于深度学习方法提出一种请求预测模型以预测用户需求,从而提高缓存命中率;其次,采用信任机制评估信任值解决与不同邻居通信时交互不可信的问题;最后,基于区块链的特性将交易过程中生成的大量信任数据和交易数据存储在区块中。仿真实验结果表明,用 TPCAB 能够有效提高缓存命中率,防止数据被篡改,可达到隐私保护的效果。

关 键 词: 认知车联网; 缓存; 隐私保护; 区块链; 信任机制
中图分类号: TP393 **文献标志码**: A

Trusted Predictive Cache Architecture for Internet of Vehicles Privacy Protection Combined with Blockchain

LIU Kun[1], WANG Yuanjie[2], SHEN Zihao[2], WANG Hui[1], LIU Peiqian[1]
(1. School of Software, Henan Polytechnic University, Jiaozuo 454000, China;
2. School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: The efficient communication technology provided by the sixth generation of mobile communications system has promoted the rapid development of the Internet of vehicles. Sensitive information such as location and query request of published data in the Internet of vehicles is vulnerable to malicious attacks, which will leak privacy. In this regard, a trusted prediction cache architecture based on blockchain (TPCAB) is proposed by sensing user needs through the cognitive engine. First, a request prediction model based on deep learning technology is proposed to predict user's demand, thus improving the cache hit rate. Second, the trust mechanism is used to evaluate the trust value and solve the problem of untrustworthy interaction caused by communication with different neighbors. Finally, based on the characteristics of blockchain, a large number of trust data and transaction data generated in the transaction process are stored in the block. The simulation results show that TPCAB can effectively improve the cache hit rate and prevent data from being tampered with, which can achieve the effect of privacy protection.

Key words: cognitive Internet of vehicles; cache; privacy protection; blockchain; trust mechanism

收稿日期: 2022-06-08
基金项目: 河南省高等学校重点科研项目(23A520033); 河南理工大学博士基金项目(B2022-16)
作者简介: 刘 琨(1978—), 女, 副教授, 硕士生导师。
通信作者: 申自浩(1980—), 男, 副教授, 硕士生导师, 邮箱: szh@hpu.edu.cn。

车联网中的传感网络技术、无线通信技术和卫星定位技术为用户提供了诸多基于位置的服务，如交通路况预警、天气预报、导航、服务查询等[1]。利用车联网使用户得到更好驾驶体验的同时也使位置和查询请求等数据激增。目前，由于中心化架构的传统车联网中处理大量数据的能力有限，不能满足用户的个性化服务，容易导致隐私泄露。因此，Qian 等[2]将认知服务与车联网相结合构建了认知车联网（CIoV，cognitive Internet of vehicle）以满足用户的个性化需求。第 6 代移动通信系统具有传输数据快和低延迟的特点，可快速传输车联网中产生的大量数据，使 CIoV 快速对数据进行处理。

车联网用户从位置服务提供商（LSP，location service provider）获取服务时，需要提交位置和查询请求等信息。然而，LSP 作为不完全可信实体，攻击者容易根据 LSP 泄露的位置信息推断出车辆轨迹，导致用户的家庭住址、工作地点等敏感信息泄露。车辆的高速移动使匿名区在短时间内难以构建成功[1]。采用椭圆曲线加密算法[3]需要耗费大量计算和存储资源，但是车辆和路边单元（RSU，roadside unit）的计算和存储资源有限，不能满足加密对资源的高要求。车辆基数大，用差分隐私[4]技术无法为每辆车分配合适的隐私预算。鉴于上述方法的局限性，缓存技术受到学者的关注。利用缓存技术能够提前缓存查询结果，减少向 LSP 提交查询请求的次数，但是传统缓存技术无法正确预测用户的查询请求。Wang 等[5]提出一种 CIoV 框架，用认知引擎解决资源分配和数据包调度的问题，但不适用于请求预测模型。长短期记忆（LSTM，long short-term memory）网络[6]可用于预测内容流行度。但是，基于年龄、星期、设备类型等多个属性预测模型与预测位置服务无大关系，且未考虑信任问题。Ahmad 等[7]提出了一种混合信任管理方案，其中，每辆车需要维护 2 个数据库，第 1 个数据库用来跟踪遇到的所有车辆，第 2 个数据库用来维护各自的信任评级。车载容量的限制使得车辆无法长时间存储和维护 2 个数据库。

为了解决传统缓存技术缓存命中率低的问题，认知引擎可利用车辆的历史请求信息，基于深度学习方法预测车辆的查询请求。请求者（RV，requestor vehicle）从周围邻居获取服务时，两者通信会导致用户隐私泄露。该问题可通过以下方式解决：①将成为服务提供商的 RSU 和车辆（PVs，provider vehicles）的数据进行广播；②结合信任机制和区块链技术选择可信服务提供商。区块用来存储 RV 完成的服务请求和历史信任信息，信任机制和区块链存储数据以实现信任值评估。笔者的主要贡献如下：

1）为了减少向 LSP 提交查询请求的次数，提出一种基于区块链的可信预测缓存架构（TPCAB，trusted prediction cache architecture based on blockchain），服务提供商通过广播缓存数据，实现隐私保护；

2）区别于传统的缓存方法，认知引擎基于 LSTM 模型感知车辆用户的需求，获取车辆所需的缓存数据；

3）引入信任机制解决与不同邻居通信时的交互不可信问题，结合区块链技术记录交易过程中生成的大量信任数据和交易数据，防止攻击者恶意篡改数据。

1　基于区块链的可信预测缓存架构

1.1　CIoV 架构设计

CIoV[5]架构中融合了深度学习方法，在传统车联网上实现智能认知、智能化车辆部署和资源配置等功能，以满足车辆用户的个性化要求并提供高质量的服务。CIoV 由认知引擎、云数据中心、边缘数据中心和车辆组成。认知引擎是运行在云数据中心或边缘数据中心的一套软件系统，用来预测用户请求，构建请求预测模型。如图 1 所示，CIoV 架构共分为 3 层：底层车辆、路边单元、基于云数据中心的 LSP 和认知引擎。

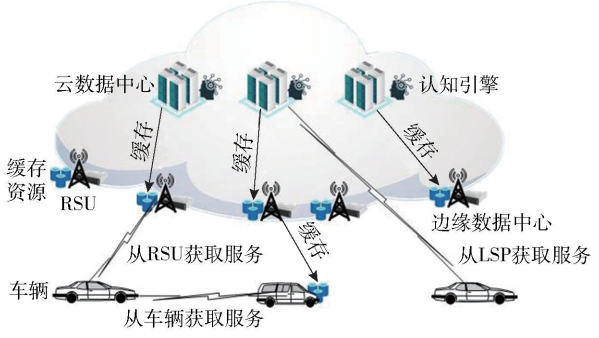


图 1　认知车联网的缓存架构

1）底层车辆。底层车辆通过与 PVs 通信获取其缓存的数据，同时，装载大量传感器收集的数据并将数据上传到云端，用认知引擎进行数据分析。

2）路边单元。认知引擎先将查询请求结果传

递给 RSU。在 RSU 通信范围内,底层车辆与 RSU 通信,获取数据,RSU 构成边缘数据中心。

3) 基于云数据中心的 LSP 和认知引擎。认知引擎基于 LSTM 网络与 Zipf[8] 模型根据 RV 上传到云端的历史请求信息预测下一时间段的查询请求,并将请求结果缓存到 PVs 和 RSU,解决 LSP 引起的时间延迟和用户隐私泄露问题。

1.2 基于 LSTM 网络和 Zipf 模型的请求预测

定义 1 请求概率即每个请求内容被广播的概率。在缓存技术的研究中,根据 Zipf 模型计算缓存内容,内容 q_i 的请求概率为

$$p_i = \frac{o_i^{-\varphi}}{\sum_{i=1}^{|Q|} o_i^{-\varphi}} \tag{1}$$

其中:$|Q|$ 为请求内容的数量,o_i 为内容存储库中 q_i 根据数量的排序,$\varphi(0<\varphi\leqslant 1)$ 为 Zipf 模型的参数,φ 越大表明内容越受欢迎。

定义 2 二进制矩阵 $\boldsymbol{A}_{|Q|\times(N_p+N_r)}$ 为缓存决策存储矩阵,表示每个请求内容是否被缓存。其中,N_p 和 N_r 分别为 PVs 和 RSU 的数量,RV 的请求内容 $Q=\{q_1,q_2,\cdots,q_{|Q|}\}$。令 $a_{i,j}, a_{i,N_p+j}$ 为 $\boldsymbol{A}_{|Q|\times(N_p+N_r)}$ 的元素,表示 q_i 是否被第 j 个 PVs 和 RSU 缓存。$a_{i,j}=0$ 表示 PVs 未缓存,$a_{i,j}=1$ 表示 PVs 已缓存;$a_{i,N_p+j}=0$ 表示 RSU 未缓存,$a_{i,N_p+j}=1$ 表示 RSU 已缓存,即

$$a_{i,j}, a_{i,N_p+j} \in \{0,1\} \tag{2}$$

定义 3 缓存命中率即查询请求内容命中的概率,用 H 表示。根据定义 2,用缓存命中率描述缓存效果,则 PV 的缓存命中率为

$$H_{PV} = \sum_{i=1}^{|Q|} p_i a_{i,j} \tag{3}$$

其中:$P_r=\{p_1,p_2,\cdots,p_{|Q|}\}$ 为下一时间段查询请求的概率,可通过定义 1 求出。类似地,RSU 的缓存命中率为

$$H_{RSU} = \sum_{i=1}^{|Q|} p_i a_{i,N_p+j} \tag{4}$$

则总缓存命中率为

$$H = \sum_{j=1}^{N_p} H_{PV} + \sum_{j=1}^{N_r} H_{RSU} \tag{5}$$

通过事先缓存流行度较高的查询请求结果能够减少提交查询请求的次数,保障用户隐私。但是内容热度随时间变化,仅依靠历史请求数量作为 Zipf 模型的输入,获取的内容流行度不准确。用户请求在一定时间段内存在规律,可以结合深度学习算法,根据历史请求数量预测下一时间段的请求数量,将结果作为预测下一时间段请求流行度的标准和 Zipf 模型的输入。

LSTM 网络作为一种优化的循环神经网络,由遗忘门、输入门、更新门和输出门 4 个神经网络单元组成,能够降低网络梯度消失和梯度爆炸的概率,从而保持梯度稳定并利于模型训练。因此,利用 LSTM 网络挖掘数据间的时间相关性,建立请求预测模型。用 LSTM 网络的 4 种门能够处理具有时间特性的数据,从而预测用户下一时间段内查询请求的数量。网络输入为 $t-1$ 时间段内的请求数量,输出为 t 时间段内的请求数量,则预测后每个查询请求的数量为 $Y^*(t)=\{y_1^*(t),y_2^*(t),\cdots,y_{|Q|}^*(t)\}$。对 $Y^*(t)$ 中的元素排序,获得每个查询请求的排序为 $O=\{o_1,o_2,\cdots,o_{|Q|}\}$。最终将 O 作为 Zipf 模型的输入,求得查询请求的概率为

$$P_r=\{p_1,p_2,\cdots,p_{|Q|}\} \tag{6}$$

根据服务提供商的缓存容量限制执行缓存决策,利用 LSTM 网络和 Zipf 模型求出在该缓存决策下的 H,如算法 1 所示。

算法 1 基于 LSTM 网络和 Zipf 模型的缓存命中率

输入:$t-1$ 时间段内的查询请求数量

输出:t 时间段内的缓存命中率 H

1 通过 LSTM 网络预测请求数量 $Y^*(t)$;

2 对 $Y^*(t)$ 中的元素排序,获得 $O=\{o_1,o_2,\cdots,o_{|Q|}\}$;

3 通过式(1)求 P_r;

4 根据 $\boldsymbol{A}_{|Q|\times(N_p+N_r)}$ 计算 H。

1.3 基于 Beta 的信任值评估

恶意服务提供商发布的广播数据经常包含恶意数据,或会主动探测 RV 的敏感信息,所以选择可信服务提供商至关重要。引入信任机制,PVs 和 RSU 可根据其广播数据是否为恶意计算信任值。若 PVs 和 RSU 经常广播恶意数据或拒绝参与服务,可通过实施惩罚降低其信任值。RV 常会优先考虑具有较高信任值的邻居。

定义 4 信任值表示对车辆的可信度。可根据可信度选择服务提供商,用 T_i 表示。先统计第 i 个提供服务车辆广播的真实数据和恶意数据的数量 u_i 和 m_i,再计算信任值,即

$$\mathrm{Beta}(u_i,m_i)=\frac{\Gamma(u_i,m_i)}{\Gamma(u_i)\Gamma(m_i)}P_{\mathrm{b}}^{u_i-1}(1-P_{\mathrm{b}})^{m_i-1} \tag{7}$$

其中：P_{b} 为车辆广播数据的概率，$0\leqslant P_{\mathrm{b}}\leqslant 1$。发送真实数据时，$u_i=u_i+1$；发送恶意数据时，$m_i=m_i+1$。易推导得出车辆 V_i 的信任值为

$$T_{i_0}=\mathrm{Beta}(u_i+1,m_i+1) \tag{8}$$

针对 $\Gamma(n)=(n-1)!$，考虑 n 为整数的情况，Beta[9] 函数的期望值为 $E[\mathrm{Beta}(u_i,m_i)]=u_i/(u_i+m_i)$。式(8)的期望值即信任值，为使 V_i 的信任值最大为 1，T_{i_1} 表示为

$$T_{i_1}=\frac{1+u_i}{1+u_i+m_i} \tag{9}$$

T_{i_1} 的取值在 0～1 之间，当 $u_i\geqslant 1$，$m_i=0$ 时，T_{i_1} 总为 1。说明：V_i 总是或经常广播可信数据，信任值就越高；若经常发送恶意数据，信任值会随 m_i 的增加逐渐降低。r_i 为 V_i 拒绝参与服务的次数，可通过利用惩罚机制对发送恶意数据和拒绝参与服务的提供商实施惩罚，惩罚因子为

$$d_i=\frac{m_i+r_i+1}{u_i+m_i+r_i+1} \tag{10}$$

以 d_i 对 T_{i_1} 实施惩罚，则 V_i 的信任值 T_i 为

$$T_i=\begin{cases}T_{i_1}-d_i, & d_i<T_{i_1}\\ 0, & d_i\geqslant T_{i_1}\end{cases} \tag{11}$$

利用阈值 δ 可判断可信服务提供商。当 $T_i\geqslant\delta$ 时，服务提供商可信；否则，服务提供商不可信。

算法 2 给出了信任值的计算方法。

算法 2　信任值计算

输入：参与服务提供商的 δ,u_i,m_i,r_i 和数量 g

输出：可信服务提供商数量 Num

```
Num = 0
for i = 0; i < g; i++ do
    计算 T_{i_1}
    计算 d_i
    计算 T_i
    if T_i ≥ δ then
        Num++
    else
        Num 值不变
    end if
end for
```

1.4　基于假名的数据广播

服务提供商通过真实身份广播 RV 所需的数据，容易被攻击者推断出真实身份等敏感信息。值得信赖的权威机构能为 PVs 和 RSU 分配假名 $K_{i,N_{\mathrm{p}}}$ 和 $K_{i,N_{\mathrm{r}}}$，从而打破服务提供商与真实身份之间的联系，防止攻击者通过窃取的广播数据，识别出用户的真实身份，进而使敏感信息泄露。K_i 表示第 i 个服务提供商的假名。假名分配过程如算法 3 所示。

算法 3　假名分配算法

输入：$N_{\mathrm{p}},N_{\mathrm{r}}$

输出：K_i

```
max = 0;
if N_p ≥ N_r then
    max = N_p;
else
    max = N_r;
for i = 0; i < max; i++ do
    Initialize K_{i,N_p};
    Initialize K_{i,N_r};
end for
```

1.5　基于区块链的信任数据管理

TPCAB 将完成的服务请求视为一个完整的交易，并将交易记录在区块中。区块由区块头和区块体组成。区别于传统的区块链，TPCAB 中的区块头除了包含散列、时间戳、Merkle root 和区块 ID，还增加了新数据，新增数据如表 1 所示。

表 1　TPCAB 区块头新增数据描述

名称	描述
R_i	提交查询请求车辆的 ID
C_i	提供服务的 PVs 和 RSU 的 ID 集合
(u_i,m_i,r_i)	V_i 作为服务提供商时，可信数据、恶意数据和拒绝参与服务的次数
B_i^{last}	上一次更新(u_i,m_i,r_i)的区块 ID
块索引	区块链的块索引副本，包含数据{B_ID,R_i,…,C_i}

B_ID 为区块 ID。在区块体中，对 C_i 集合中服务提供商所对应的 3 个参数(u,m,r)进行哈希变化，从而构建 Merkle 树。在一次交易完成时，需在创建新区块时更新 C_i 对应的(u,m,r)。可通过搜索块索引，在每个区块头保存的 C_i 的 ID 集中找到服务提供商的 ID 和 R_i，从而查找他们的历史变化，快速形成临时数据库以更新(u,m,r)。

1.6　TPCAB

TPCAB 包括认知引擎数据分析、车辆注册、数

据广播和接收、内容交易,如图2所示。

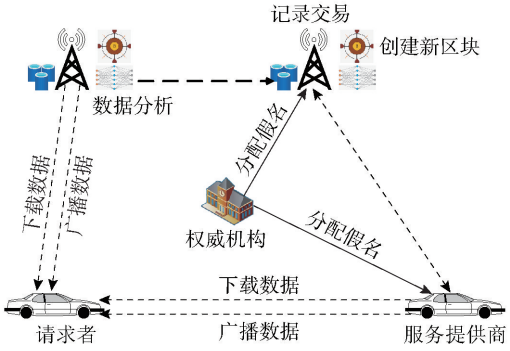


图2 TPCAB组成

1)认知引擎数据分析。对于不同时间、不同地点提交的查询请求,认知引擎可基于历史请求采用LSTM网络预测用户的查询请求并将结果缓存到PVs和RSU,以满足车辆用户实时获取服务的需求。

2)车辆注册。每辆车在交易过程中扮演请求者或服务提供商的角色。车辆扮演的角色并非固定,可在请求者和服务提供商之间转换身份。在未来时间内注册为请求者的车辆接收服务提供商共享的数据,注册为服务提供商的车辆为请求者提供服务。

3)数据广播和接收。权威机构首先为RSU和PVs分配假名;然后RSU和PVs广播缓存数据以满足RV需求,达到保护车辆隐私的效果。

4)内容交易。RV和服务提供商之间完成的数据共享被视为一个完整的交易,即车辆与RSU之间、车辆之间的数据共享。TPCAB通过RSU创建新区块记录交易,认知引擎具备较高的计算能力和存储容量,被用来存储和维护区块。

2 TPCAB安全分析

2.1 缓存与广播对隐私的保护

缓存命中率的提高能减少提交查询请求的次数,使车辆隐私得到保障。与文献[1]相比,为了提高缓存命中率,在TPCAB中根据请求者的历史请求采用LSTM网络预测下一时间段的查询请求。此外,用户请求服务时不再提交查询请求,而是通过RSU和PVs广播缓存数据,满足用户需求。缓存命中率的提高和服务提供商广播数据的方式,能够阻止攻击者窃取车辆隐私。

2.2 区块链防止信任数据被篡改

TPCAB中,以区块形式存储信任数据而区块链以链表表示。因此,当存储在区块中的信任数据被篡改时,链接在本区块后面的数据也必须被修改。很明显,区块链中存储数据的区块越多,篡改成本也就越高。假设有 i 个车辆请求服务,区块 e 后面有 j 个区块,那么所需篡改的区块的数量为

$$F_e = i + i^2 + \cdots + i^j = \frac{i^{j+1} - i}{i - 1} \tag{12}$$

3 实验仿真与结果分析

3.1 实验设置

使用Python3.8对所提方案进行仿真实验,参数设置如表2所示。仿真实验采用文献[10]中的数据集。该数据集包含了电信、天气、社交网络和电力等10个方面的内容请求数据。

表2 实验参数设置

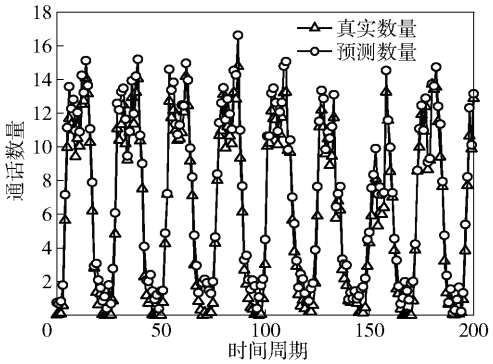
参数	默认值
车辆数量 w_v	40
服务提供商数量 s_p	1~20
Zipf模型的参数 φ	0.2,0.4,0.6,0.8,1.0
信任值阈值 δ	0.2,0.5,0.8
服务提供商不诚实的概率 l/%	30

3.2 实验结果分析

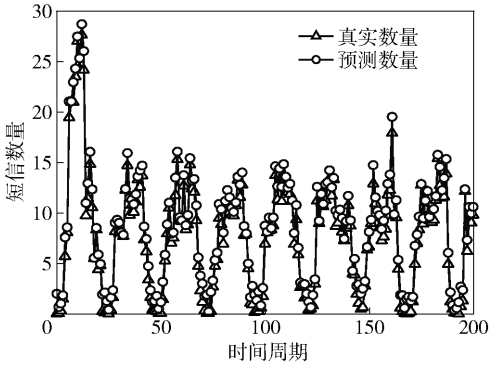
考虑数据集中的实际数据量,使用的数据量为1 000个,间隔时间为10 min。将800个数据作为训练集,其余200个数据作为测试集。用训练集训练LSTM网络,使用训练后的LSTM网络可求出预测后的数据。

查询请求预测结果如图3所示。预测数量越准确,预测效果越好。不难发现,本方案的预测结果与真实数据非常接近,具有很好的预测效果。

基于缓存的隐私保护技术中,缓存命中率越高,隐私泄露的概率越低。图4所示为TPCAB与位置隐私保护方案(LPPS, location privacy preservation scheme)[11]、基于缓存的位置隐私保护(LPP-cache, cache-based location privacy preserving)[12]方案和盲第三方(BTP, blind third party)[13]方案的缓存命中率对比结果。可以看出,缓存命中率随着Zipf模型参数的增大而增加。这是因为参数越大,热度越高,缓存命中率越大。实验结果表明,TPCAB具有更高的缓存命中率;尽管使用LPP-cache方案能够依次缓存受欢迎程度高的查询请求,但未考虑缓存数据是否符合用户需求;使用LPPS方案虽然缓存命中



(a) 查询请求1的预测结果



(b) 查询请求2的预测结果

图 3　查询请求的预测结果

率较高,但是仅根据位置的受欢迎程度提高缓存命中率,忽略了基于位置的不同查询请求;BTP 方案只依赖用户的真实查询缓存查询结果,因此缓存命中率较大。

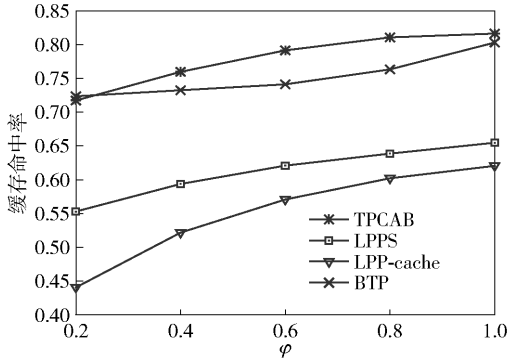


图 4　不同方案下缓存命中率随 φ 的变化

不诚实的服务提供商在通信时会生成大量恶意回复,导致恶意数据增多,进而使隐私泄露概率增加。在 TPCAB 中采用基于周期的方式计算恶意数据的数量,并在每个周期随机选择 RV。

恶意数据的数量随周期的变化如图 5 所示。根据设定的服务提供商不诚实的概率 l,假设诚实的服务提供商总是提供可信数据,不诚实的服务提供商总是提供恶意数据。LPPS 和 LPP-cache 方案中未作信任处理,所以恶意数据较多。可见,TPCAB 在抑制发送恶意数据方面优于 LPPS 和 LPP-cache 方案,意味着信任机制对 LPPS 和 LPP-cache 方案至关重要。

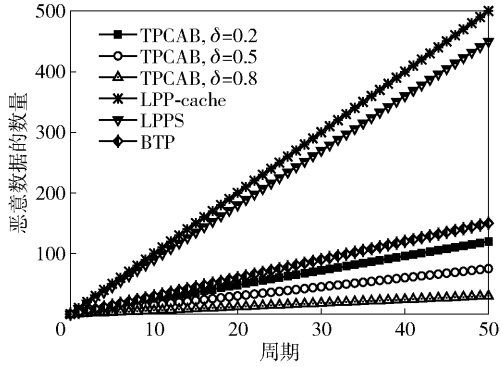


图 5　恶意数据的数量随周期的变化

从图 5 可看出,TPCAB 在 $\delta = 0.8$ 时表现最好。用 BTP 方案能通过加密查询信息防止隐私泄露,但不能阻止第三方与 LSP 的串通和第三方本身被攻击,因此会产生恶意数据。

实验中,将 δ 设为 0.8。区块链存储的信任机制中的相关数据能反映 PVs 的信任值,而 u_i,m_i 和 r_i 的改变会影响可信度。因此,将数据的篡改数量表示为 u_i,m_i 和 r_i 被篡改数量的总和,数据被篡改的数量越多,PVs 的可信度越低。如图 6 所示,LPPS 和 LPP-cache 方案中数据被篡改的数量大,因为未引入信任机制的不可信 PVs 多。BTP 方案通过加密防止数据被篡改,但不能阻止第三方与 LSP 的串通和第三方本身被攻击,因此数据也会被篡改。而 TPCAB 中引入区块链技术存储相关信任数据,能够防止数据被篡改。

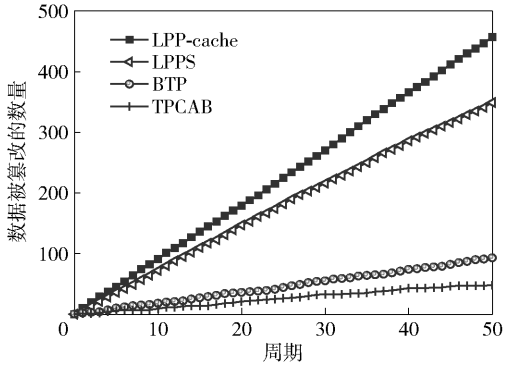


图 6　u_i,m_i 和 r_i 被篡改数量的总和随周期的变化

通信时间表示完成一次查询请求所需要的时间。如图7所示,采用 w_v 和 s_p 两个参数,通过计算通信时间衡量整体效果。TPCAB 的通信时间随着请求车辆 w_v 和 s_p 的增加而增加。这是因为虽然单个车辆的请求时间少,但请求车辆越多,整体请求的时间就会变长。s_p 越多,计算信任值和分配缓存资源的时间会加长,因此整体请求的时间会变长。

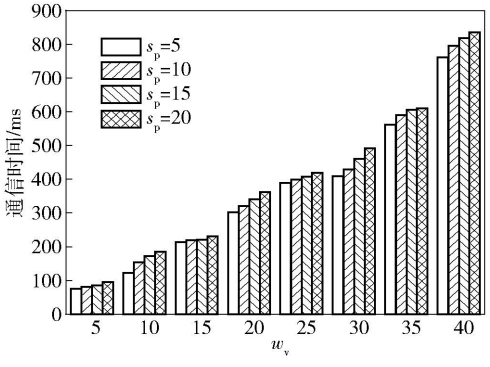


图7 通信时间随 w_v 和 s_p 的变化

4 结束语

预测缓存技术是解决车联网隐私保护的一种有效手段,而用所提基于区块链的可信预测缓存架构可以准确预测用户的查询请求,解决车联网用户间的信任问题,防止信任数据被篡改。未来将致力于研究车辆与 RSU 间服务提供商具有自主决策能力的协同缓存决策,改善认知车联网在服务获取延迟和缓存命中率方面的性能。

参考文献:

[1] 崔杰, 陈学峰, 张静, 等. 基于公交车缓存的车联网位置隐私保护方案[J]. 通信学报, 2021, 42(7): 150-161.
CUI J, CHEN X F, ZHANG J, et al. Bus cache-based location privacy protection scheme in the Internet of vehicles[J]. Journal on Communications, 2021, 42(7): 150-161.

[2] QIAN Y F, JIANG Y, HU L, et al. Blockchain-based privacy-aware content caching in cognitive internet of vehicles[J]. IEEE Network, 2020, 34(2): 46-51.

[3] ZHANG M Y, ZHOU J L, ZHANG G X, et al. EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of vehicles[J]. Journal of Systems Architecture, 2021, 117: 1-10.

[4] SUN Y E, HUANG H, YANG W J, et al. Toward differential privacy for traffic measurement in vehicular cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2022, 18(6): 4078-4087.

[5] WANG Y, WANG X, HUANG Z B, et al. Joint optimization of dynamic resource allocation and packet scheduling for virtual switches in cognitive Internet of vehicles[J]. Eurasip Journal on Advances in Signal Processing, 2022(1): 1-21.

[6] LI L X, XU Y, YIN J Y, et al. Deep reinforcement learning approaches for content caching in cache-enabled D2D networks[J]. IEEE Internet of Things Journal, 2020, 7(1): 544-557.

[7] AHMAD F, KURUGOLLU F, KERRACHE C A, et al. NOTRINO: a novel hybrid trust management scheme for Internet-of-vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(9): 9244-9257.

[8] ZHOU F S, WANG N, LUO G Y, et al. Edge caching in multi-UAV-enabled radio access networks: 3D modeling and spectral efficiency optimization[J]. IEEE Transactions on Signal and Information Processing over Networks, 2020, 6: 329-341.

[9] SONG Z D, SUN H G, YANG H, et al. Reputation-based federated learning for secure wireless networks[J]. IEEE Internet of Things Journal, 2022, 9(2): 1212-1226.

[10] BARLACCHI G, DE NADAI M, LARCHER R, et al. A multi-source dataset of urban life in the city of Milan and the province of Trentino[J]. Scientific Data, 2015, 2(1): 1-15.

[11] CHEN M, LI W Z, CHEN X, et al. LPPS: a distributed cache pushing based k-anonymity location privacy preserving scheme[J]. Mobile Information Systems, 2016: 1-16.

[12] HU L, QIAN Y F, CHEN M, et al. Proactive cache-based location privacy preserving for vehicle networks[J]. IEEE Wireless Communications, 2018, 25(6): 77-83.

[13] YAMIN M, ALSAAWY Y, ALKHODRE A B, et al. An innovative method for preserving privacy in Internet of things[J]. Sensors, 2019, 19(15): 1-24.