基于公交车缓存的车联网位置隐私保护方案

崔杰[1,2,3]，陈学峰[1]，张静[1]，魏璐[1]，仲红[1,2,3]
（1. 安徽大学计算机科学与技术学院，安徽 合肥 230601；2. 安徽省物联网安全技术工程实验室，安徽 合肥 230601；
3. 安徽大学物质科学与信息技术研究院，安徽 合肥 230601）

摘 要：为了解决车联网中车辆用户使用基于位置的服务（LBS）时真实位置的泄露问题，提出一种基于公交车缓存的位置隐私保护方案。公交车先根据其线路信息向 LBS 提供商获取兴趣点（POI）池，然后在行驶时根据其当前位置从 POI 池中挑选部分 POI 数据形成 POI 列表并广播给周围私家车。私家车在接收到广播信息后，验证公交车身份，然后将 POI 列表存储到车辆的本地缓存中。当私家车需要查询 POI 信息时，首先在本地缓存中进行检索，若缓存未命中再以 k-匿名的方式向 LBS 提供商发送查询请求。仿真实验结果表明，所提方案通过减少私家车与 LBSP 的通信次数，能够降低私家车真实位置泄露的可能性，从而有效提高私家车的位置隐私保护水平。

关键词：车联网；基于位置的服务；隐私保护；k-匿名
中图分类号：TP393.0
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021132

Bus cache-based location privacy protection scheme in the Internet of vehicles

CUI Jie[1,2,3], CHEN Xuefeng[1], ZHANG Jing[1], WEI Lu[1], ZHONG Hong[1,2,3]
1. School of Computer Science and Technology, Anhui University, Hefei 230601, China
2. Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230601, China
3. Institute of Physical Science and Information Technology, Anhui University, Hefei 230601, China

Abstract: To solve the problem of real location leakage when vehicles use location-based service (LBS) on the Internet of vehicles, a location privacy protection scheme based on bus cache was proposed. Firstly, a point of interest (POI) pool was obtained from the LBS provider based on its route information. Then the data in the POI pool was selected form a POI list while driving. Finally, the POI list was broadcast to surrounding private vehicles. After the private vehicle received the broadcast data, it verified the identity of the bus and then stored the POI list in the vehicle's local cache. When a private vehicle needed to query POI information, it would first retrieve it in the local cache, and if the cache was missed, it would send a query request to the LBS provider using the k-anonymity method. The simulation experiment results show that the proposed scheme can reduce the possibility of leakage of the real location of the private vehicle by reducing the number of communications between the private vehicle and the LBSP, thereby effectively improving the privacy protection level of the private vehicle.

Keywords: Internet of vehicles, location-based service, privacy protection, k-anonymity

1 引言

作为传统车载自组织网络（VANET, vehicular ad-hoc network）的超集，车联网（IoV, Internet of vehicles）是 5G 网络的重要应用之一[1]。IoV 是一种集成和开放的网络系统[2]，除了包含异构网络、用户以及车辆以外，还包括车辆持续感知、计算和存储能力。不同类型的车辆使用统一的通信协议与

收稿日期：2020−09−17；**修回日期**：2020−12−15
基金项目：国家自然科学基金资助项目（No.61872001）；国家自然科学基金国际（地区）合作交流项目（No.62011530046）
Foundation Item: The National Natural Science Foundation of China (No.61872001), The National Natural Science Foundation of China International (Regional) Cooperation and Exchange Project (No.62011530046)

相邻车辆或基础设施进行无线通信。目前，有 2 种无线通信协议在 IoV 中被广泛使用，分别是专用短程频谱协议（DSRC, dedicated short-range spectrum）和蜂窝车辆对一切协议（C-V2X, cellular vehicle-to-everything）[3]。这 2 种协议都支持车辆对一切（V2X, vehicle-to-everything）通信，包括车辆对车辆、车辆对行人和车辆对基础设施通信[4]。

通过区分数据在各个实体之间流动的方向，可将 IoV 中的应用程序分成 2 类，分别为安全应用和娱乐应用[5]。安全应用根据道路信息及时做出响应，例如碰撞检测、行人避让等。娱乐应用则是为了提高车辆行驶时的用户体验，常见的娱乐应用有导航、音乐和视频等。基于位置服务（LBS, location-based service）的应用作为重要的娱乐应用之一，被广泛应用于 IoV 中。

在 LBS 中，私家车首先向 LBS 提供商（LBSP, location-based service provider）发送查询请求消息，其中包含车辆当前位置和能够反映车辆兴趣的查询关键字。然后，LBSP 返回基于关键字的响应消息，其中包含与车辆位置及查询关键字相关的 POI（point of interest）（例如餐馆、加油站、停车场等）的信息。正如硬币有正反两面一样，虽然 LBS 给用户带来了很多的好处和便利，但是也出现了很多重要的安全和隐私问题。例如，当车辆的请求数据（如位置数据）被泄露时，敌手可以重建其行车轨迹并推断出车辆用户的隐私信息，如家庭地址、工作单位以及健康状况等。这些隐私信息的泄露可能会导致发生危害用户人身安全的行为[6]。因此，LBS 中的位置隐私保护得到了学者的关注[7-8]。

近年来，为了解决上述问题，学者先后提出了许多方案[9-11]。其中，基于缓存策略的方案相对容易实现。它的主要思想是使用缓存来减少 LBSP 获取私家车的真实位置的次数，从而降低位置隐私泄露的可能性。在某些方案中[6,11]，使用路边单元（RSU, road side unit）为其覆盖范围内的车辆提供 POI 缓存数据。然而，在 IoV 中大规模部署 RSU 的费用高昂，还可能发生物理攻击 RSU 的情况，造成额外的损失[12-13]。而公交车具有相对固定的移动轨迹以及移动模式，可以用来作为 POI 数据的缓存节点。因此，本文使用公交车作为对 POI 数据进行缓存、广播以及更新的边缘节点，相比于大规模部署 RSU，使用公交车在成本上更具有竞争力，并且可以更广泛地分布在 IoV 中。

综上所述，本文主要的创新点可以总结为以下 3 个方面。

1) 本文提出了一种安全的基于广播的位置隐私保护方案，在该方案中，公交车充当边缘节点，周期性地从 LBSP 中预先获取大量的 POI 数据，在其中挑选部分数据并将其广播给私家车。

2) 当发生缓存未命中时，车辆可以使用 k-匿名技术向 LBSP 发送包含其真实位置的查询，以确保为车辆提供更好的服务。本文在用户体验和位置隐私之间取得了一个较好的平衡。

3) 针对缓存失效问题，本文提出了一种基于主动推送的缓存数据更新算法，该算法可减少 LBSP 网络流量并更好地保护车辆位置的隐私。仿真实验结果表明，本文提出的方案具有较低的网络开销和计算开销。

2　相关工作

随着 IoV 的普及，车辆位置隐私问题引起了许多学者的关注。目前，针对 LBS 的位置隐私保护方案主要可分为以下 3 类。

1) 基于密码学的方案。此类方案可以提供可证明的安全性和隐私性。Yi 等[14]提出了一种基于差分隐私的位置隐私保护方案，该方案使用 Paillier 同态加密技术以实现地理不可区分性的 s-差分位置隐私。Paulet 等[15]提出了一种最近邻搜索方案，该方案使用茫然传输（OT, oblivious transfer）和私有信息检索（PIR, private information retrieval）等密码学技术在不损害位置隐私的情况下向 LBSP 查询 POI 信息。然而，使用重量级密码学技术来提供可证明的位置隐私保护的开销过大。因此，此类方案不适合资源受限的移动设备。

2) 基于混淆的方案。Beresford 等[16]提出了混合区域的概念，将混淆的思想引入位置隐私保护中。它通过不断改变用户在这个区域内的假名来保护用户的位置隐私。然而，混合区域对区域内的用户数量有严格的要求，导致在实际环境下中很难实现这个方法。k-匿名作为混合区域的补充方法被提出，其前提条件是用户的真实位置不能与其他 $k-1$ 个虚拟位置区分。为实现 k-匿名，Gruteser 等[17]引入了一个第三方可信实体（通常被称为匿名服务器[10,18]），该方案通过在私家车的查询请求被发送到 LBSP 之前，混淆请求内的位置信息，从而保护用户的位置隐私。然而，匿名服

务器很容易被黑客攻击，造成单点故障，从而降低用户服务质量。为了解决这一问题，Chow 等[19]提出了一种方案，每个用户首先与其他 $k-1$ 个用户合作，形成一个没有第三方可信实体的群，然后利用群里其他成员的位置作为虚拟位置实现 k-匿名。Cui 等[20]提出了一种位置隐私保护方案，车辆根据周围车辆的状态动态生成虚拟位置，并将混淆后的位置数据发送给 LBSP。然而基于混淆的方案往往会忽略敌手拥有的背景知识（如道路拓扑、查询概率、移动模式）[21]。因此，敌手可以很容易地使用基于机器学习的算法[22]从私家车提交的 k 个位置中过滤一些没有被精心设计的，甚至是随机生成的虚拟位置，从而降低 k-匿名方案的隐私保护程度。

3) 基于缓存方法的方案。近年来，一些学者还提出了基于缓存的方案，为用户提供位置隐私保护。在此类方案中，用户可以在本地缓存中检索所需的内容，而不需要向 LBSP 发送查询。Amini 等[23]提出了一种隐私保护方案，通过在用户到达特定区域之前，预先下载该区域内的所有 POI 数据来保护用户的位置隐私。然而，该方案要求用户具有特定的移动轨迹且用户的移动设备上具有很大的存储空间。Shokri 等[24]提出了一种被称作 MobiCrowd 的方案。在移动用户从 LBSP 请求所需的 POI 数据之前，首先向邻居用户请求 POI 数据，以减少真实位置泄露的可能性。然而，该方案没有考虑邻居是恶意用户的情况。Niu 等[25]提出了 2 种虚拟位置生成算法来保护用户位置隐私，但该算法需要群内用户之间进行协作。Peng 等[26]提出了一种通过移动用户之间的协作缓存来保证连续位置隐私的方案。Zhang 等[27]提出了一种通过缓存和均匀网格来增强位置隐私的方案，该方案可以避免不同的用户在同一区域中发送相同查询。Liu 等[11]和 Hu 等[6]提出使用主动缓存在车联网中对车辆的位置隐私进行保护，然而它们都依赖于 RSU。

3 问题描述

本节将简要介绍本文所需的预备知识、系统模型、威胁模型以及安全性目标。表 1 中列出了本文所使用的符号和描述。

3.1 椭圆曲线密码体制

下面，简要介绍椭圆曲线密码体制（ECC, elliptic curve cryptosystem）的基本知识和 3 个相关的性质[28]。

表 1 本文所使用的符号和描述

符号	描述
TA	可信机构
LBSP	位置服务提供商
POI	车辆感兴趣的位置点
OBU	车载单元
p,q	大质数
E	椭圆曲线方程
G	q 阶加法群
P	加法群 G 的生成元
PK	公钥
sk	私钥
TPK	临时公钥
σ	消息的签名
$\oplus$	异或操作
$\|\|$	消息连接操作
RID	车辆的真实身份
PID	车辆的假名身份
PWD	车辆所使用的密码
id	公交车的线路编号
PV	私家车
BUS	公交车
ECDSA	椭圆曲线数字签名算法
ECIES	椭圆曲线集成加密方案
H	安全哈希函数
T	时间戳
PP	POI 池
PL	POI 列表
BM	公交车广播的信息

F_p 是一个有限域，它是由一个大质数 p 所决定的。在 F_p 上有一个椭圆曲线 E： $y^2 = x^3 + ax + b(\mathrm{mod}\ p)$，其中 $a,b \in F_p$ 且 $(4a^3 + 27b^2) \bmod p \neq 0$。设有无穷远点 O，椭圆曲线 E 上所有的点和 O 共同组成一个阶为大质数 q、生成元为 P 的加法椭圆曲线群 G，其具有以下性质和困难性假设。

加法运算。设 P 和 Q 是群 G 上的 2 个点，如果 $P \neq Q$，可得 $R = P + Q$，其中 R 是曲线 E 与一条连接 P、Q 直线的交点；如果 $P = Q$，可得 $R = 2P$；如果 $P = -Q$，可得 $P + Q = O$。

标量点乘运算。设 $P \in G$， $m \in Z_q^*$，则 E 上的点乘被定义为 $m \cdot P = P + P + \cdots + P$（$m$ 个 P）。

椭圆曲线离散对数问题（ECDLP, elliptic curve discrete logarithm problem）。该问题是椭圆曲线密码体制中的一个困难问题，即对于在椭圆曲线 E 上给定的任意 2 个点 $P, Q \in G$，其中 $Q = xP$，$x \in Z_q^*$，在多项式时间内计算出 x 的值是困难的。

3.2　系统模型

IoV 系统模型如图 1 所示，主要包含 4 种实体，即可信中心（TA, trusted authority）、LBSP、基站以及车辆。

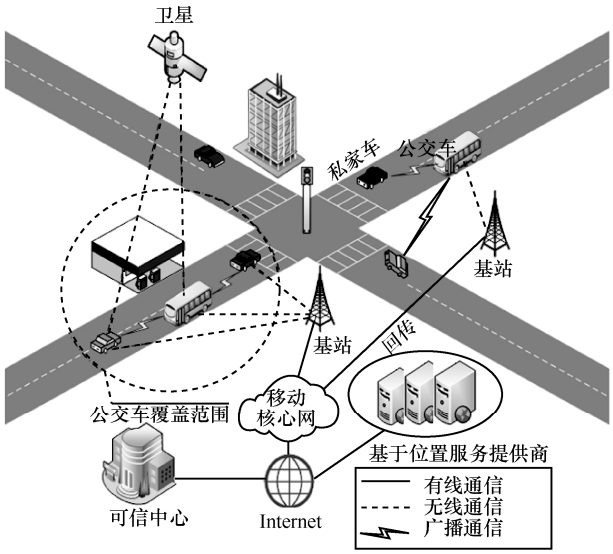


图 1　IoV 系统模型

在本文中，每种实体的主要功能和前提假设介绍如下。

1) TA。该实体由交通管理部门负责管理，通常可被视为是完全可信的。TA 具有强大的计算能力和足够的存储容量且配备防篡改设备（TPD, tamper proof device），可以利用足够的资源来防御各种网络攻击以及物理攻击。TA 还负责为所有实体分配公私钥对。

2) LBSP。该实体负责响应来自公交车或私家车的请求，并将最新的 POI 数据主动推送给公交车。它根据车辆发送的位置信息和关键字返回相应的 POI 数据，例如车辆可以向 LBSP 获取离车辆最近的加油站的相关信息。

3) 基站。该实体属于公共基础设施，通常由运营商负责部署和维护，它仅负责为车辆提供蜂窝网络接入[29]。因为它不进行任何加解密计算，所以即使被攻击，它也不会泄露任何有价值的信息。正在广泛普及的 5G 技术可以为车辆提供足够的带宽和超低的时延。

4) 车辆。车辆内置车载单元（OBU, onboard unit），OBU 的计算和存储能力有限。车辆还配备多个传感器、TPD 以及通信模块。车辆通常使用 C-V2X 或 DSRC 协议与其他基础设施或者车辆进行通信。在本文中，车辆分为 2 种：私家车和公交车。与私家车相比，公交车的 OBU 具有更加强大的计算能力和更充足的存储空间。私家车在道路上的行驶模式通常不可预测，公交车具有相对固定的行驶轨迹和发车间隔且所有用户都可以提前获知。车辆在首次登记或者年审时都会从 TA 获取一个最新的真实身份 RID 以及密码 PWD 。

3.3　威胁模型

本文使用全局敌手（GA, global adversary）模型作为威胁模型[30]。GA 不仅可以通过窃听消息来追踪特定区域中的目标车辆，还可以篡改消息中的内容。GA 的主要目的是通过跟踪目标车辆的真实位置和行驶轨迹来获取车主的敏感数据以及生活方式。敌手可以通过攻击 LBSP 和公交车来获取用户隐私数据，因此 LBSP 和公交车通常被认为是半可信的，即它们会执行相应的功能，但是可能泄露其中的数据。本文仅考虑基于有线和无线通信的攻击[31]，不考虑基于计算机视觉的攻击，比如车辆重识别追踪。

3.4　安全性目标

安全性是本文方案的基本属性，必要的安全性目标如下。

1) 消息完整性。为了抵抗女巫攻击，车辆和其他实体需要验证彼此的身份。此外，参与实体之间交换的消息应得到完整性保护。

2) 匿名性。私家车使用假名与除 TA 以外的其他实体进行通信。

3) 不可链接性。任何第三方都不能将窃听到的消息链接到同一辆车上。

4) 可追溯性。当发生交通事故时，TA 有权通过消息中的假名揭露相关车辆的真实身份。

5) 抗攻击性。本文不仅可以抵抗女巫攻击，还可以抵抗其他常见的网络攻击，例如中间人攻击和重放攻击。

4　基于公交车缓存的位置隐私保护方案

4.1　概述

本文旨在设计一种安全有效的位置隐私保护

方案应用于 IoV 中。其基本思想是使用公交车作为特殊的缓存节点来缓存 POI 数据，并在公交车行驶过程中将它们广播给周围的私家车。私家车通过接收来自公交车的广播，可以在没有 LBSP 的情况下获得其所需的 POI 数据，从而减少私家车泄露其真实位置的次数，降低敌手获取私家车真实位置的可能性。

本文方案的数据流[32]如图 2 所示，其中，阴影矩形表示 POI 数据（不同灰度的阴影表示不同内容的 POI 数据），白色矩形表示查询请求。LBSP 首先根据公交车的线路信息将其沿路所经过的 POI 数据预先发送给公交车，公交车在行驶过程中再根据其当前位置选择部分 POI 数据广播给私家车，私家车接收广播的数据并存储到本地缓存中。若私家车在本地缓存中没有检索到想要的 POI 数据，则通过 k-匿名的方式向 LBSP 发送查询请求，LBSP 根据查询请求返回相应的数据。

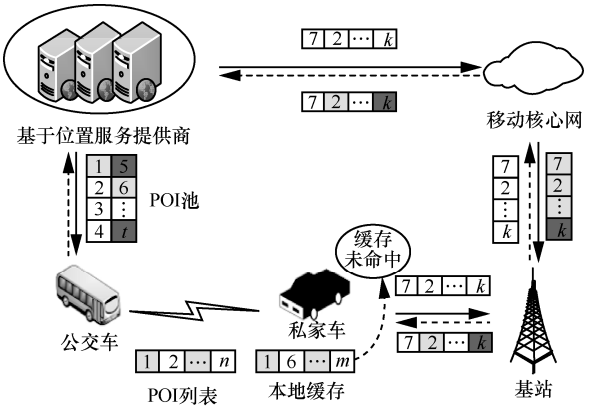


图 2 本文方案的数据流

4.2 初始化阶段

1) TA 预先为所有车辆分配公私钥对，且已经预装在所有车辆的 TPD 中。TA 选择一个随机数 $\mathrm{sk}_{\mathrm{TA}} \in Z_q^*$ 作为 TA 的一个私钥并且计算出它所对应的公钥 $\mathrm{PK}_{\mathrm{TA}}=\mathrm{sk}_{\mathrm{TA}}P$。TA 再选择 2 个哈希函数 $H_1: G \to Z_q$ 和 $H_2: \{0,1\}^* \to Z_q$。最后 TA 将系统安全参数 $\psi=\{p,q,\mathrm{PK}_{\mathrm{TA}},P,H_1,H_2\}$ 发送给全体车辆。

2) 公交车在每天发车前会首先使用其私钥 $\mathrm{sk}_{\mathrm{BUS}_i}$ 对其公交车的真实身份 RID 和密码 PWD 进行签名 $\sigma_A=\mathrm{ECDSA}(\mathrm{RID},\mathrm{PWD})$，然后使用 $\mathrm{PK}_{\mathrm{TA}}$ 去加密它们，生成密文 $A=\mathrm{ECIES}(\mathrm{RID},\mathrm{PWD},\sigma_A)$，并将 A 发送给 TA。

3) 当 TA 收到公交车发送的密文 A 后，首先使用其私钥 $\mathrm{sk}_{\mathrm{TA}}$ 对 A 进行解密，并核对 BUS_i 的 RID 和 PWD，核对成功后使用 BUS_i 的公钥 $\mathrm{PK}_{\mathrm{BUS}_i}$ 验证签名 σ_A。如果验证通过，则 TA 生成一个随机数 r_i，作为 TA 与 BUS_i 之间共享的秘密参数，并计算出公交车的临时公钥 $\mathrm{TPK}_i=r_i \oplus \mathrm{RID}$ 用于之后广播消息。然后，TA 生成一个随机数 x_i，留作后续步骤使用。最后，TA 将这些参数 (TPK_i,r_i,x_i) 存储到本地，并且发送密文 $B=\mathrm{ECIES}_{\mathrm{PK}_{\mathrm{BUS}_i}}(\mathrm{TPK}_i, x_i, \mathrm{ECDSA}_{\mathrm{sk}_{\mathrm{TA}}}(\mathrm{TPK}_i,x_i))$ 给公交车。

4) 当私家车 PV_j 首次进入公交车 BUS_i 的广播范围时，首先向公交车获取其临时公钥 TPK_i，然后连同私家车的 RID 和 PWD 一起使用 $\mathrm{sk}_{\mathrm{PV}_j}$ 生成签名 $\sigma_C=\mathrm{ECDSA}(\mathrm{RID},\mathrm{PWD},\mathrm{TPK}_i)$，再使用 $\mathrm{PK}_{\mathrm{TA}}$ 加密它们生成密文 $C=\mathrm{ECIES}(\mathrm{RID},\mathrm{PWD},\sigma_C)$，并通过公交车将密文 C 发送给 TA。

5) 当 TA 收到密文 C 后，首先使用自己的私钥 $\mathrm{sk}_{\mathrm{TA}}$ 对 C 进行解密，并检查私家车 PV_j 的 RID 和 PWD 是否正确，检查无误后使用 PV_j 的公钥 $\mathrm{PK}_{\mathrm{PV}_j}$ 验证签名 σ_C。如果能够验证通过，TA 则能够使用 TPK_i 在本地存储中检索到参数 x_i，作为公交车 BUS_i 与 PV_j 之间共享的秘密参数。然后，TA 发送密文 $D=\mathrm{ECIES}_{\mathrm{PK}_{\mathrm{PV}_j}}(\mathrm{TPK}_i,x_i,\mathrm{ECDSA}_{\mathrm{sk}_{\mathrm{TA}}}(\mathrm{TPK}_i,x_i))$ 给公交车，让其转发给私家车。

6) 当公交车收到密文 B 和 D 之后，使用私钥 $\mathrm{sk}_{\mathrm{BUS}_i}$ 解密 B，得到临时公钥 TPK_i 和秘密参数 x_i。公交车验证签名 $\mathrm{ECDSA}_{\mathrm{sk}_{\mathrm{TA}}}(\mathrm{TPK}_i,x_i)$ 成功以后，计算出秘密参数 $r_i=\mathrm{TPK}_i \oplus \mathrm{RID}$，将密文 D 转发给私家车 PV_j。

7) 私家车收到来自公交车转发的密文 D 后，使用私钥 $\mathrm{sk}_{\mathrm{PV}_j}$ 解密 D，然后使用 $\mathrm{PK}_{\mathrm{TA}}$ 验证其中的签名，验证通过以后能够得到公交车的临时公钥 TPK_i 和共享的秘密参数 x_i。

4.3 公交车广播阶段

公交车首先从 LBSP 获取 POI 池，并将它们存储在公交车的 OBU 中。随后，公交车在行驶过程中，基于其当前位置从 POI 池中挑选一些附近的 POI 数据以生成 POI 列表，并将它们广播给周围的私家车，具体步骤介绍如下。

1) 获取 POI 池。为了最大限度地利用缓存的 POI 数据，应该选择私家车经常访问的 POI 数据进行缓存和广播。私家车在接收公交车广播的消息之前，需要对公交车的身份进行认证。为了找到这些

流行的 POI 数据，本文假设 LBSP 具有城市中所有 POI 的历史被查询数据，其中不包含任何隐私数据。

公交车在发车前，首先向 LBSP 发送一个请求消息以获取 POI 池，其格式为{PID，route^{id}}，其中，PID 表示公交车的假名身份；id 表示公交车的线路编号，即第 id 路公交车；route^{id} 表示公交车的线路信息，即第 id 路公交车的轨迹信息。

LBSP 根据公交车线路周围 POI 的流行程度以及其他背景知识生成 POI 池，然后向公交车发送一个响应消息，其格式为 $\{\text{PID},\text{PP}^{\text{id}},T\}$，其中，$\text{PP}^{\text{id}}=(\text{POI}_1^{\text{id}},\text{POI}_2^{\text{id}},\cdots),\text{POI}_k^{\text{id}}=(L_k^{\text{id}},n_k^{\text{id}},l_k^{\text{id}},R_k^{\text{id}})$，$L_k^{id}$ 表示第 k 个 POI 的地理位置，n_k^{id} 和 l_k^{id} 分别表示 POI 的名称和类别，R_k^{id} 包括与 POI 相关的信息，例如 POI 的地址以及额外数据。LBSP 在生成 POI 池后，会将其存储起来并且定期更新其中的数据，以便能够直接响应来自同一条线路不同 RID 的公交车发送的请求。

2) 生成 POI 列表。为降低广播时的数据分组丢失率，公交车需要从 POI 池中选择部分 POI 数据，生成适合广播的 POI 列表。公交线路被车站所分隔，每个车站之间的距离大致相同。当公交车停靠在第 m 站时，从 POI 池中选择第 m 站到第 m+1 站之间公交车线路附近的 POI 生成 POI 列表。由于需要本地检索和缓存更新，公交车广播的 POI 列表格式可以定义为 $\{\text{PID},\text{PL}^{\text{id}},\sigma,T\}$，其中，$\text{PL}^{\text{id}}$ 表示第 id 路公交车广播的 POI 列表，其格式与 PP 的相同，包含 POI 的位置信息以及与 POI 相关的数据信息。

3) 广播 POI 列表。公交车在道路上行驶时，使用算法 1 周期性地广播其生成的 POI 列表。假设公交车以间隔 T_{gap} 广播 POI 列表，通常设置为 8~10 s。

算法 1　POI 列表广播算法

输入　将进行广播的公交车 BUS_i，2 次广播的最短间隔 T_{gap}，2 次广播的最短距离 D_{gap}

1) 生成随机数 s；

2) 生成广播列表 PL^{id}；

3) 计算 $\text{PID}_1=sP$；

4) 计算 $\text{PID}_2=\text{TPK}\oplus H_1(x\text{PID}_1)$；

5) 计算 $\text{PID}=(\text{PID}_1,\text{PID}_2)$；

6) 计算 PL^{id} 的签名 $\sigma=s+xH_2(\text{PID}\|\text{PL}^{\text{id}}\|T)\bmod q$；

7) while $\Delta T<T_{\text{gap}}\ \&\&\ \Delta D<D_{\text{gap}}$

8)　　广播消息 $\{\text{PID},\text{PL}^{\text{id}},\sigma,T\}$；

9)　　接收周围公交车的广播消息，将其命名为 BUS_j；

10)　　if $\text{BUS}_i^{\text{id}}==\text{BUS}_j^{\text{id}}\ \&\&\ \text{BUS}_i^T\leqslant\text{BUS}_j^T$

11)　　break;

12)　　end if

13) end while

4.4　基于主动推送的缓存更新阶段

随着交通流的变化，不同的 POI 流行程度也随之变化，因此 LBSP 需要及时更新公交车中的 POI 池缓存以保持较高的缓存命中率。例如，某地新增了一个加油站，周围的车辆经常访问这个 POI，一个新流行的 POI 就此产生。

传统的缓存更新策略要求用户主动请求服务器以更新失效的缓存数据。如果使用这种更新策略，则需要让公交车知道私家车访问哪些 POI 时发生了缓存未命中，这意味着公交车能够了解车辆的兴趣，从而根据这些信息推出车主的其他隐私信息。因此，本文设计了一种基于推送的更新算法，不需要公交车掌握车辆的缓存未命中情况，也能正常更新私家车本地缓存中无效的数据，从而更好地保护私家车的位置隐私。详细策略分为以下 3 个步骤。

1) LBSP 只更新被修改过或者新增的 POI 数据，以降低通信成本和存储开销。LBSP 分析私家车发送的查询请求并检查 POI 的更新，执行 POI 池的添加、删除和修改数据等操作。假设 LBSP 以 U_{gap} 的间隔推送更新补丁，通常设置为 1~3 h，这取决于在此期间 POI 池 PP^{id} 中发生变化的 POI 的数量。LBSP 生成补丁后，将更新补丁以消息 $\{\text{id},\text{diff},T\}$ 的格式发送给公交车，其中，diff 表示增量更新补丁，其为 unix-diff 格式。

2) 公交车接收来自 LBSP 的缓存更新消息，并将其中的增量更新补丁合并到存储在公交车上的 PP^{id} 中。POI 池中的时间戳将被更新补丁中的时间戳替换，以表示 PP^{id} 中的数据是最新的。

3) 如果私家车的本地缓存中已经存储了来自同一条线路公交车的广播数据，那么比较广播消息中的时间戳。然后从本地缓存中删除时间戳较旧的 POI 列表，并存储具有较新时间戳的 POI 列表。

4.5 私家车接收阶段

私家车在接收到公交车的广播消息 BM 后，需要对消息中的签名 σ 进行验证，具体步骤如下。

1) 设私家车接收到广播消息的时间戳为 T_v，若 BM 中时间戳为 T，若 $T_{\mathrm{PV}}-T\leqslant\Delta T$ 则消息无效，其中 ΔT 为系统预设的可容忍的传输时延。

2) 验证签名能否满足 $\sigma P=sP+hxP$，其中 $h=H_2(\mathrm{BM}\,\|\,\mathrm{PID}\,\|\,T)$。若等式成立，则说明 BM 有效，然后私家车提取 BM 中的 $\mathrm{PL}^{\mathrm{id}}$ 放入本地缓存中。

3) 否则，说明 BM 无效，私家车丢弃 BM。

若私家车想要同时验证来自多辆公交车 $\mathrm{BUS}_1,\mathrm{BUS}_2,\cdots,\mathrm{BUS}_n$ 的广播消息 $\mathrm{BM}_1,\mathrm{BM}_2,\cdots,\mathrm{BM}_n$，可以通过以下步骤去进行验证。

1) 验证时间戳 $T_1,T_2,\cdots,T_n$ 是否有效。

2) 随机选择小指数向量 $\boldsymbol{v}=\{v_1,v_2,\cdots,v_n\}$，$v_i\in[1,2^t]$，为了降低计算开销，$t$ 应该取一个非常小的正整数。

3) 验证签名能否满足

$$\left(\sum_{i=1}^{n}v_i\sigma_i\right)P=\left(\sum_{i=1}^{n}v_i\left(s_i+x_ih_i\right)\right)P=$$
$$\left(\sum_{i=1}^{n}v_i\left(s_iP+x_ih_iP\right)\right)=$$
$$\left(\sum_{i=1}^{n}v_i\left(\mathrm{PID}_{i1}+x_ih_iP\right)\right)=$$
$$\sum_{i=1}^{n}\left(v_i\mathrm{PID}_{i1}\right)+\left(\sum_{i=1}^{n}\left(v_ih_ix_i\right)\right)P$$

其中，$h_i=H_2\left(\mathrm{BM}_i\left\|\mathrm{PID}_i\right\|T_i\right)$。若上述等式能够成立，则说明这一批广播消息 BM 均有效。私家车可以批量提取 BM 中的 $\mathrm{PL}^{\mathrm{id}}$，放入本地缓存中。

4) 否则，说明这批广播消息中有无效的消息，需要对 BM 单独进行验证。

4.6 私家车查询阶段

在私家车使用 LBS 之前，首先使用关键字在本地缓存中进行检索。如果私家车在不同的 POI 列表中检索到相同的 POI，则选择时间戳较新的那个 POI 列表中的数据。例如私家车本地缓存中有 2 个 POI 列表 PL^1 和 PL^2，其中都包含相同的兴趣点 $\mathrm{POI}_k=(L_k,n_k,l_k,R_k)$。若私家车此时想要查询关于兴趣点 k 的信息，那么其会同时在 PL^1 和 PL^2 中检索到同一个兴趣点 POI_k，此时私家车会比较 PL^1 和 PL^2 的时间戳，然后使用时间戳较新的那个 PL 中的 POI_k。若在本地缓存未检索到想要查询的 POI 数据，则通过算法 2[33]生成 $k-1$ 个虚拟位置，然后连同车辆的真实位置，一起发送给 LBSP，获取 POI 信息，其具体流程如图 3 所示。

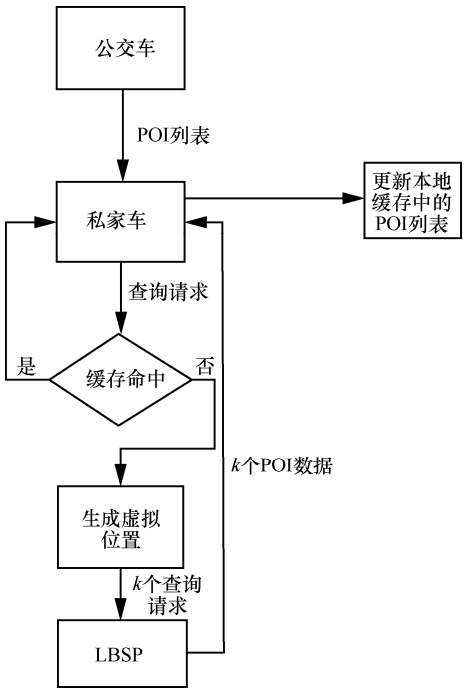


图 3 私家车查询 POI 流程

算法 2 虚拟位置生成算法

输入 真实位置，矩阵 $\boldsymbol{M}$，虚拟位置数量 T，ϵ

输出 虚拟位置 o_t

1) for t in$\{1,2,\cdots,T\}$ do
2) 将真实位置传入矩阵 $\boldsymbol{M}$ 以生成 o_t;
3) while o_t 不能满足ϵ-时空时间隐私 do
4) 调整矩阵 $\boldsymbol{M}$;
5) 重新生成 o_t;
6) end while
7) return 虚拟位置 o_t
8) end for

5 仿真实验分析

本节提出了用来评估位置隐私保护程度的性能指标，描述了本文方案所使用的仿真实验环境，并与 Hu 等[6]提出的 PAPT 位置隐私保护方案以及 Liu 等[11]提出的 LBS-CBAC 位置隐私保护方案进行了各方面的性能对比与分析。

5.1 度量指标

为了评估方案的位置隐私的能力，本文提出位

置隐私保护度作为度量标准，其由匿名集的熵和缓存命中率共同决定，具体定义如下所示。

定义 1　匿名集的信息熵表示匿名集中真实位置和虚拟位置被正确区分的不确定性。假设在匿名集 AS 中，只有一个私家车的真实位置，其余都是根据真实位置生成的虚拟位置。例如私家车使用 *k*-匿名方式，向 LBSP 发送的 *k* 个查询请求中的 *k* 个位置信息都能形成一个匿名集。设 *r* 为匿名集中的真实位置，*d* 为匿名集中的虚拟位置，则 AS 的信息熵定义为

$$E = -\sum_{d \in \mathrm{AS}} p(r,d)\mathrm{lb}(r,d) \tag{1}$$

其中，$p(r,d)$ 表示 *r* 和 *d* 被正确区分的概率。熵的值越大说明 LBSP 掌握的关于车辆真实位置的信息越多，反之越少。

定义 2　缓存命中率表示查询缓存命中的数目占总查询数的比例。缓存命中表示私家车需要查询的 POI 数据能够在本地缓存中检索到。缓存命中率具体定义为

$$H = \frac{\sum_{i=1}^{m} h_i}{\sum_{i=1}^{n} q_i} \tag{2}$$

其中，q_i 表示私家车需要查询的 POI 请求，h_i 表示缓存命中的查询请求。缓存命中率越高，表示私家车向 LBSP 发送的查询次数越少，则 LBSP 获取私家车的真实位置的可能性就越低。

定义 3　位置隐私保护度表示私家车在整个行驶过程中其位置隐私被保护的程度，具体定义为

$$D = H + (1-H)\frac{E - E_{\min}}{E_{\max} - E_{\min}} \tag{3}$$

其中，*H* 表示整个行驶过程中缓存命中率，*E* 表示当缓存未命中时向 LBSP 请求服务时的信息熵的值，$E_{\max}$ 表示信息熵的最大值，$E_{\min}$ 表示信息熵的最小值。根据最大熵模型可以计算出在本文方案中 $E_{\max} = -\sum_{d \in \mathrm{AS}} \frac{1}{|\mathrm{AS}|}\mathrm{lb}|AS|$，$E_{\min} = 0$。*D* 的值越大，则说明私家车在行驶过程中的位置隐私被保护的程度就越高。

5.2　仿真环境设置

本文方案基于 Veins 4.6 环境[34]进行仿真实验，这是一种进行车联网仿真的开源框架，其基于 2 种常用的模拟器：OMNeT++ 5.1.1 和 SUMO 0.30.0。其中，OMNeT++是一种基于事件的网络仿真模拟器，支持有线和无线网络的仿真；SUMO 是一种开源的道路交通模拟器，用于生成道路中的交通流数据。Veins 是连接 OMNeT++和 SUMO 的中间件软件。仿真环境的详细参数设置如表 2 所示。

表 2　　仿真环境的详细参数设置

参数	值
仿真区域面积	2 500 m×2 500 m
数据传输速率/(Mbit·s^{-1})	6
传输功率/mW	20
私家车最大速度/(m·s^{-1})	40
公交车最大速度/(m·s^{-1})	20
车辆加速度/(m·s^{-2})	10
敏感度/dBm	−89
热噪声/dBm	−110
信标间隔/s	1
广播间隔/s	3
模拟时间/s	300
信道	CCH
私家车最大数量/个	50
公交车最大数量/个	5
POI 最大数量/个	500
模拟器时间/s	140

5.3　性能对比与分析

本节与 PAPT 方案[6]和 LBS-CBAC 方案[11]进行了各方面的性能对比与分析。

数据分组丢失率的具体定义为

$$L = \mathrm{AVG}\left(\sum_{i=1}^{n} \frac{P_{\mathrm{lost}}^{i}}{P_{\mathrm{received}}^{i} + P_{\mathrm{lost}}^{i}}\right) \tag{4}$$

其中，AVG 表示求平均函数，$P_{\mathrm{received}}^{i}$ 表示私家车 PV_i 接收到的广播数据分组的个数，P_{lost}^{i} 表示私家车没有接收到的广播数据分组的个数。该指标可用于评价方案的广播性能，即数据分组丢失率越高，广播性能越差。

在 IoV 中，车辆在道路上行驶时为了保证行驶安全，需要向周围车辆和 RSU 广播以及接收信标数据。然而，如果广播的数据分组大小过大可能会干扰正常的信标传输，因为大量的数据下载可能会长时间占用无线信道，从而导致较高的数据分组丢失率。将本文方案与 PAPT 方案[6]和

LBS-CBAC 方案[11]进行了数据分组丢失率的比较，结果分别如图 4 和图 5 所示。

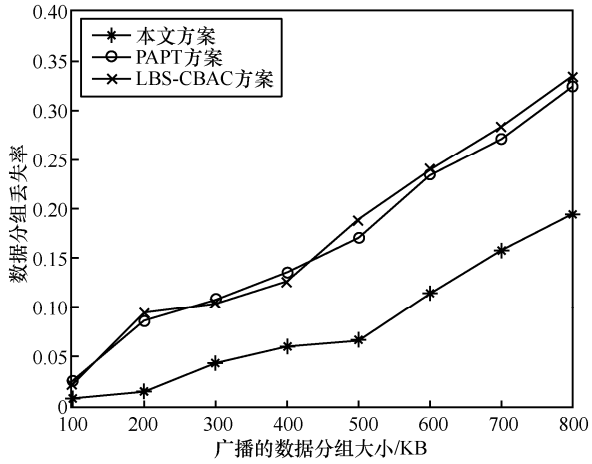


图 4 不同大小的数据分组对广播性能的影响

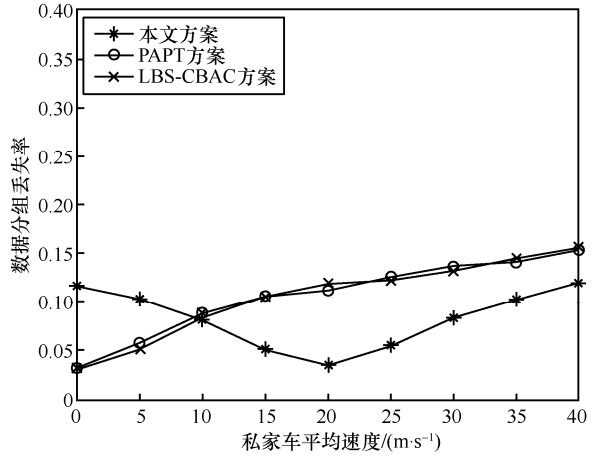


图 5 私家车不同的速度对广播性能的影响

从图 4 和图 5 可以看出，本文方案具有较低的数据分组丢失率，不会对 IoV 造成显著干扰。本文方案具有较低的数据分组丢失率的原因是本文方案中私家车直接从附近的公交车上获取 POI 数据；而公交车和同向行驶的私家车相对距离较短，相对速度较小，所以公交车与私家车之间的传输环境比 RSU 与私家车之间的传输环境更好。相比于车速变化带来的影响，广播数据分组大小的变化对数据分组丢失率的影响更显著。这是因为车辆接收较大的数据分组时需要较长时间占用的 CCH 信道，从而导致车辆需要竞争使用该信道，造成数据分组丢失率的增加。

图 6 给出了 3 种方案中不同的缓存文件大小对位置隐私保护度的影响。从图 6 可以看出，当缓存文件很小时，3 种方案的位置隐私保护度都比较低，这是因为缓存文件很小时，缓存文件中无法容纳所有的热门 POI 数据，导致私家车需要频繁地向 LBSP 获取 POI 数据，从而暴露了私家车的真实位置。缓存文件越大，私家车就可以从缓存中检索到越多的热门 POI 数据，减少了其直接向 LBSP 获取 POI 数据的次数，从而降低了私家车真实位置被泄露的可能性。随着缓存文件不断增大，它所带来的边际收益也在不断降低。因此，一个合适的缓存文件大小可以让本文方案在位置隐私保护度和广播性能之间寻找到一个较合适的平衡点。

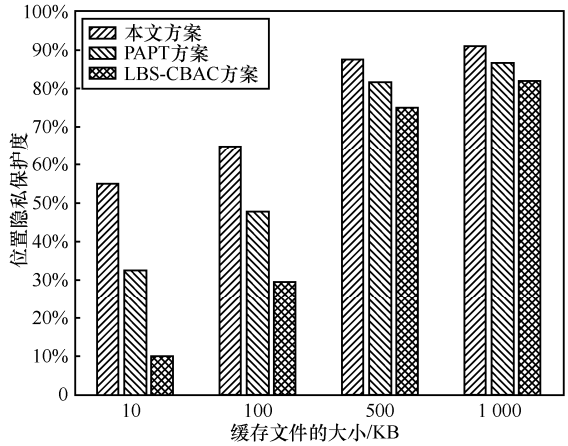


图 6 不同缓存文件的大小对位置隐私保护度的影响

不同的缓存命中率对位置隐私保护度的影响如图 7 所示。从图 7 可以看出，随着缓存命中率的增加，3 种方案的位置隐私保护度都会相应提高。因为缓存命中率越高，私家车直接向 LBSP 发送查询请求的可能性就越低。如果私家车能在缓存中检索到所有想要查询的 POI 数据，那么这 3 种方案都可以完全保护私家车的位置隐私，这是因为在整个行驶过程中，私家车没有将真实位置发送给 LBSP。然而，在实际生活中，这种情况几乎不可能发生。

从图 7 还可以看出，与 PAPT 方案和 LBS-CBAC 方案相比，本文方案在缓存命中率较低的情况下，依旧可以为用户提供较高的位置隐私保护能力。这是因为当出现缓存未命中时，PAPT 方案通过 RSU 转发包含私家车真实位置的查询请求，LBS-CBAC 方案则是私家车直接将自己的真实位置发送给 LBSP 进行 POI 查询。而本文方案则首先使用 k-匿名技术处理私家车的发送查询请求，在查询请求中加入噪声数据，从而实

现对位置信息的混淆，然后向 LBSP 发送查询请求。在本文方案中，LBSP 从单次查询中推断出私家车真实位置的概率理论上仅为 $1/k$，远小于 PAPT 方案和 LBS-CBAC 方案。

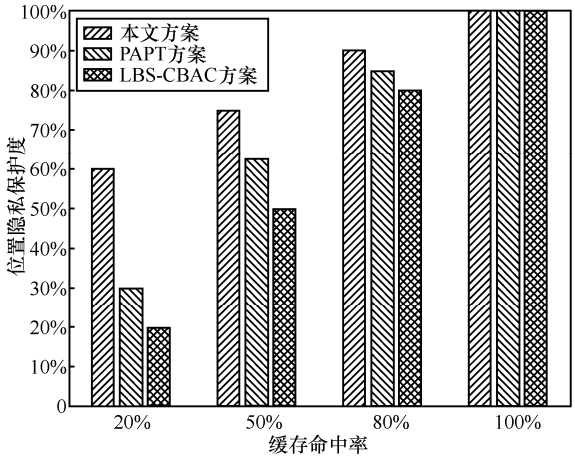


图 7　不同的缓存命中率对位置隐私保护度的影响

不同 POI 数量对缓存更新文件大小的影响如图 8 所示。从图 8 可以看出，当有大量的 POI 数据发生变化时，与 PAPT 方案和 LBS-CBAC 方案相比，本文方案可以显著降低缓存更新所需的网络开销。这就意味着，本文方案可以高效地进行缓存更新，降低了缓存更新对 IoV 的影响。

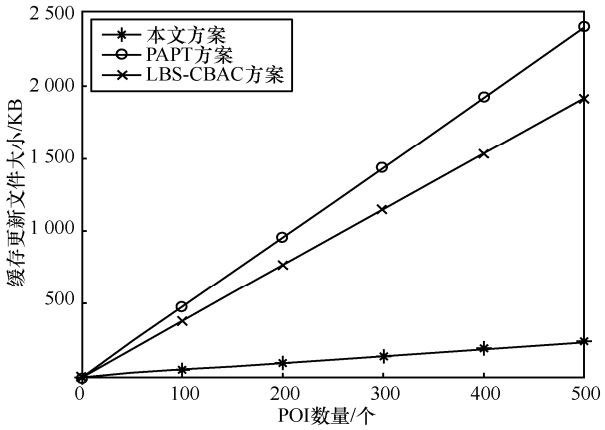


图 8　不同 POI 数量对缓存更新文件大小的影响

6　安全性分析

基于本文提出的消息认证过程和困难假设，本节进行了安全性分析，以表明本文方案可以完成本文提出的安全性目标。

1) 消息完整性。由于 ECDLP 难以在常数项时间内被解决以及单向哈希具有不可逆的特性，在随机预言模型下，敌手在自适应选择消息攻击中无法生成代表车辆的合法签名。因此，本文方案可以实现签名的不可伪造性。车辆可以对所发送的消息进行签名，从而保证了消息的完整性。

2) 匿名性。因为车联网中的广播信道是公开的，可以被敌手监听，所以车辆在和其他车辆进行通信时，使用假名身份以对车辆的真实身份进行保护。在初始化阶段，TA 与车辆共享秘密参数，车辆随后将这些参数存入 TPD 中。在行驶过程中，定期从 TPD 中取出秘密参数，生成假名。

3) 不可链接性。因为假名身份是由安全的单向哈希函数 H 生成的，所以敌手不能确定 2 个不同的假名身份是否源自同一车辆。

4) 可追溯性。TA 可以对车辆真实身份连接其他参数进行哈希，检查是否和假名身份相称，从而实现对车辆身份的可追溯性。

5) 抗攻击性。将主密钥和其他安全参数放入不会被攻破的 TPD 中，可以抵抗物理攻击；使用消息认证，可以抵抗女巫攻击；使用时间戳，可以抵抗重放攻击；使用消息签名，可以抵抗中间人攻击。

7　结束语

本文提出了一种车联网中基于公交车缓存的位置隐私保护方案。在该方案中，公交车负责进行缓存管理与广播，即公交车首先根据其线路信息向 LBSP 发送请求以获取 POI 池，然后在行驶过程中，周期性地根据其当前位置从 POI 池中挑选部分 POI 数据形成 POI 列表，广播给周围的私家车。私家车在接收到广播消息后，对消息进行认证，认证通过后将 POI 列表存储到车辆的本地缓存中。当私家车需要查询 POI 信息时，首先在本地缓存中进行检索，若在缓存中没有检索到相应的 POI 信息，则通过 k-匿名的方式向 LBSP 发送查询请求。此外，本文还基于增量更新技术设计了一种缓存更新策略，以降低缓存更新所带来的通信开销。仿真实验结果表明，本文方案在具有较高的位置隐私保护水平的同时，具有较低的通信开销；安全性分析表明，本文方案可以实现车辆通信时所需的安全性目标。

参考文献：

[1] LAI C Z, LU R X, ZHENG D, et al. Security and privacy challenges in 5G-enabled vehicular networks[J]. IEEE Network, 2020, 34(2): 37-45.

[2] ZHANG J, CUI J, ZHONG H, et al. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 722-735.

[3] LAI C Z, ZHANG K, CHENG N, et al. SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(6): 1559-1574.

[4] YANG Y, DANG S P, HE Y J, et al. Markov decision-based pilot optimization for 5G V2X vehicular communications[J]. IEEE Internet of Things Journal, 2019, 6(1): 1090-1103.

[5] HE D B, ZEADALLY S, XU B W, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[6] 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.

[7] 张文静, 刘樵, 朱辉. 基于信息论方法的多等级位置隐私度量与保护[J]. 通信学报, 2019, 40(12): 51-59.
ZHANG W J, LIU Q, ZHU H. Evaluation and protection of multi-level location privacy based on an information theoretic approach[J]. Journal on Communications, 2019, 40(12): 51-59.

[8] 叶阿勇, 孟玲玉, 赵子文, 等. 基于预测和滑动窗口的轨迹差分隐私保护机制[J]. 通信学报, 2020, 41(4): 123-133.
YE A Y, MENG L Y, ZHAO Z W, et al. Trajectory differential privacy protection mechanism based on prediction and sliding window[J]. Journal on Communications, 2020, 41(4): 123-133.

[9] LI Q Y, WU H, WU X, et al. Multi-level location privacy protection based on differential privacy strategy in VANETs[C]//2019 IEEE 89th Vehicular Technology Conference. Piscataway: IEEE Press, 2019: 1-5.

[10] ZHANG Y, TONG W, ZHONG S. On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2528-2541.

[11] LIU B, ZHOU W L, ZHU T Q, et al. Silence is golden: enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 9942-9953.

[12] CUI J, ZHANG X Y, ZHONG H, et al. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1654-1667.

[13] CHENG J J, CHENG J L, ZHOU M C, et al. Routing in Internet of vehicles: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(5): 2339-2352.

[14] YI X, PAULET R, BERTINO E, et al. Practical k nearest neighbor queries with location privacy[C]//2014 IEEE 30th International Conference on Data Engineering. Piscataway: IEEE Press, 2014: 640-651.

[15] PAULET R, KAOSAR M G, YI X, et al. Privacy-preserving and content-protecting location based queries[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(5): 1200-1210.

[16] BERESFORD A R, STAJANO F. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46-55.

[17] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[C]//The 1st International Conference on Mobile Systems, Applications and Services. Berkeley: USENIX Association, 2003: 31-42.

[18] 裴卓雄, 李兴华, 刘海, 等. LBS 隐私保护中基于查询范围的匿名区构造方案[J]. 通信学报, 2017, 38(9): 125-132.
PEI Z X, LI X H, LIU H, et al. Anonymizing region construction scheme based on query range in location-based service privacy protection[J]. Journal on Communications, 2017, 38(9): 125-132.

[19] CHOW C Y, MOKBEL M F, LIU X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service[C]//Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems. New York: ACM Press, 2006: 171-178.

[20] CUI J, WEN J Y, HAN S S, et al. Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network[J]. IEEE Internet of Things Journal, 2018, 5(5): 3491-3498.

[21] REN W T, TANG S H. EGeoIndis: an effective and efficient location privacy protection framework in traffic density detection[J]. Vehicular Communications, 2020, 21: 100187.

[22] PAN J J, LIU Y N, ZHANG W M. Detection of dummy trajectories using convolutional neural networks[J]. Security and Communication Networks, 2019, 2019: 1-12.

[23] AMINI S, LINDQVIST J, HONG J, et al. Caché: caching location-enhanced content to improve user privacy[C]//Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services. New York: ACM Press, 2011: 197-210.

[24] SHOKRI R, THEODORAKOPOULOS G, PAPADIMITRATOS P, et al. Hiding in the mobile crowd: LocationPrivacy through collaboration[J]. IEEE Transactions on Dependable and Secure Computing, 2014, 11(3): 266-279.

[25] NIU B, LI Q H, ZHU X Y, et al. Enhancing privacy through caching in location-based services[C]//2015 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2015: 1017-1025.

[26] PENG T, LIU Q, MENG D C, et al. Collaborative trajectory privacy preserving scheme in location-based services[J]. Information Sciences, 2017, 387: 165-179.

[27] ZHANG S B, CHOO K K R, LIU Q, et al. Enhancing privacy through uniform grid and caching in location-based services[J]. Future Generation Computer Systems, 2018, 86: 881-892.

[28] MENEZES A J, VANSTONE S A. Elliptic curve cryptosystems and their implementation[J]. Journal of Cryptology, 1993, 6(4): 209-224.

[29] CUI J, ZHANG X Y, ZHONG H, et al. RSMA: reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(4): 6417-6428.

[30] PETIT J, SCHAUB F, FEIRI M, et al. Pseudonym schemes in vehicular networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(1): 228-255.

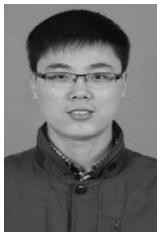
[31] LAI C Z, ZHANG M, CAO J, et al. SPIR: a secure and privacy-preserving incentive scheme for reliable real-time map updates[J]. IEEE Internet of Things Journal, 2020, 7(1): 416-428.

[32] CHENG J J, YUAN G Y, ZHOU M C, et al. A fluid mechanics-based data flow model to estimate VANET capacity[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(6): 2603-2614.

[33] CAO Y, XIAO Y H, XIONG L, et al. PriSTE: from location privacy to spatiotemporal event privacy[C]//2019 IEEE 35th International Conference on Data Engineering. Piscataway: IEEE Press, 2019: 1606-1609.

[34] SOMMER C, GERMAN R, DRESSLER F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis[J]. IEEE Transactions on Mobile Computing, 2011, 10(1): 3-15.

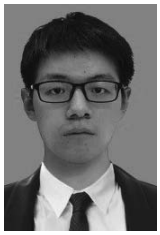
[作者简介]



崔杰（1980− ），男，河南淮阳人，博士，安徽大学教授、博士生导师，主要研究方向为车联网安全、物联网安全等。

陈学峰（1995− ），男，安徽合肥人，安徽大学硕士生，主要研究方向为车联网安全与位置隐私保护。

张静（1990− ），女，河南永城人，安徽大学博士生，主要研究方向为车联网安全、物联网安全等。



魏璐（1993− ），男，安徽安庆人，安徽大学博士生，主要研究方向为车联网安全、物联网安全等。

仲红（1965− ），女，安徽固镇人，博士，安徽大学教授、博士生导师，主要研究方向为网络与信息安全。