

车联网环境下隐私度量研究进展

娄浩^{1,2}

(1. 佳木斯大学 信息电子技术学院;
2. 佳木斯大学 黑龙江省自主智能与信息处理重点实验室, 黑龙江 佳木斯 154007)

摘要: 在车联网环境中, 隐私保护技术的发展对于防止隐私信息泄露至关重要。隐私度量是评估隐私保护技术有效性的关键因素, 通过衡量隐私信息泄露风险可以准确反映出隐私保护方案的强度, 为构建更加可靠的隐私保护手段提供支持。因此, 如何准确度量车联网隐私保护技术水平成为当前研究中一项紧迫而重要的任务。首先, 对车联网环境中存在的隐私风险类型、隐私保护技术以及隐私度量进行概述, 给出基于车联网的隐私度量框架; 其次, 从理论和实践的角度对基于匿名、不确定性和失真3类隐私度量方法进行详细阐述, 总结各自的优缺点; 最后, 从隐私度量的过程、效果和方法3个方面指出车联网隐私度量技术的发展趋势以及亟需解决的问题, 为未来研究指明方向, 推动车联网隐私保护技术更加高效。

关键词: 车联网; 隐私度量; 隐私保护技术; 隐私安全; 隐私泄露

DOI: 10.11907/rjdk.241730

中图分类号: TP309

文献标识码: A

文章编号: 1672-7800(2025)012-0057-10

扫描二维码阅读全文:



Research Progress on Privacy Measurement in the Internet of Vehicles Environment

LOU Hao^{1,2}

(1. School of Information and Electronic Technology, Jiamusi University; 2. Key Laboratory of Autonomous Intelligence and Information Processing in Heilongjiang Province, Jiamusi University, Jiamusi 154007, China)

Abstract: The development of privacy protection technology is crucial for preventing the leakage of privacy information in the connected car environment. Privacy metrics are a key factor in evaluating the effectiveness of privacy protection technologies. By measuring the risk of privacy information leakage, the strength of privacy protection schemes can be accurately reflected, providing support for building more reliable privacy protection measures. Therefore, how to accurately measure the privacy level of the Internet of Vehicles privacy protection technology has become an urgent and important task in current research. Firstly, an overview of the types of privacy risks, privacy protection technologies, and privacy metrics present in the Internet of Vehicles environment is provided, along with a privacy measurement framework based on the Internet of Vehicles; Secondly, from both theoretical and practical perspectives, provide a detailed explanation of the three types of privacy measurement methods based on anonymity, uncertainty, and distortion, and summarize their respective advantages and disadvantages; Finally, the development trend and urgent problems of privacy measurement technology in the Internet of Vehicles are pointed out from three aspects: the process, effectiveness, and methods of privacy measurement. This provides direction for future research and promotes the evolution of privacy protection technology in the Internet of Vehicles towards a more efficient direction.

Key Words: Internet of Vehicle; privacy measurement; privacy protection technology; privacy and security; privacy disclosure

0 引言

车联网是在新一代移动通信技术的辅助下, 实现车辆内部、车辆与人、车辆与车辆、车辆与道路以及车辆与服务

平台的全方位网络连接^[1]。车联网通过车辆之间的实时通信, 使其能够相互协同, 共享交通信息^[2]。车联网数据涵盖了车辆的当前状态、位置、速度等信息, 因此在通信过程中产生的“数据指纹”可能会对用户的隐私和安全造成威胁^[3]。例如, 黑客可以通过数据挖掘技术分析收集到的

收稿日期: 2024-08-21

基金项目: 黑龙江省省属高等学校基本科研业务费优秀创新团队建设项目(2022-KYYWF-0654); 佳木斯大学国家基金培育项目(JM-SUGPZR2022-014); 黑龙江省自主智能与信息处理重点实验室开放课题(ZZXC202302)

作者简介: 娄浩(1997-), 男, CCF 学生会会员, 佳木斯大学信息电子技术学院硕士研究生, 研究方向为车联网隐私、隐私保护。

用户数据,获取有关用户的敏感信息^[4]。

隐私保护技术在保障用户权益、促进行业发展等方面具有重要意义,是实现安全、高效的车联网系统不可或缺的一部分。近年来,学者们已针对车联网隐私保护技术开展了大量研究。例如,Liu等^[5]提出一种基于分层假名的条件隐私保护认证方案,可有效保护车辆的身份与轨迹隐私,当检测到车辆出现恶意行为时又可以通过相应的假名恢复其身份。Qi等^[6]提出一种快速聚类 k -匿名隐私保护算法,通过结合区块链技术解决了在构建匿名区域时请求车辆与合作车辆之间的不信任问题,但攻击者仍可以通过位置模式、时间等信息进行分析,进而发现用户位置。Atauba^[7]使用同态加密来解决车联网数据的隐私问题,但该类加密方法的计算开销较大,可能影响实时性。

隐私度量是采用数学模型量化隐私保护强度的关键手段^[8]。现有隐私保护技术仍有隐私泄露的风险,并存在隐私保护水平评估过高的问题^[9]。建立有效的车联网隐私保护度量机制对于更精准地衡量不同隐私保护技术的强度、可信性和可行性具有重大意义。因此,本文首先阐述车联网安全存在的隐患,对隐私保护技术和隐私度

量方法进行分类与总结;其次,系统分析3种典型隐私度量方法的理论基础与研究进展;最后,总结3类隐私度量方法的评价指标以及优缺点,对其后续发展方向进行讨论。

1 车联网隐私保护与安全隐患

1.1 车联网隐私风险分类

表1从攻击者类别的角度可将车联网隐私风险分为主动攻击和被动攻击两类。主动攻击是指攻击者通过主动发送恶意代码、病毒或对网络进行攻击等方式,直接破坏车辆上的车联网系统。这种攻击通常意味着攻击者有意识地对目标进行攻击,可以针对性地破坏特定车辆的安全。被动攻击是指攻击者通过监听信息、窃取机密信息、欺骗等方式来攻击车联网系统。攻击者不直接对车辆或车联网系统进行破坏,而是利用系统本身的漏洞进行攻击,例如拦截车载通信数据包、窃取车辆和用户的隐私信息、伪装成合法用户来骗取车辆和用户的机密信息。车联网中的隐私风险类型具体如表1所示。

Table 1 Types of privacy risks in the Internet of Vehicles

表1 车联网中的隐私风险类型

攻击	攻击者类别	攻击目的
女巫攻击 ^[10]	主动	攻击者伪造多个虚假身份,并使用虚假身份发布大量虚假信息参与通信
窃听攻击 ^[11]	被动	攻击者试图非法拦截数据传输的过程,以获取用户的敏感信息
重放攻击 ^[12]	主动	攻击者在通信过程中拦截用户的合法数据,然后将数据重新在网络中广播
流量分析 ^[13]	被动	攻击者通过监控和分析网络通信流量,获取敏感信息或识别网络中的漏洞
拒绝服务 ^[14]	主动	攻击者通过不断发送大量请求,恶意占用系统资源导致系统崩溃
伪装攻击 ^[15]	主动	攻击者通过伪装或欺骗的手段,访问未授权的用户信息或执行恶意操作
消息篡改 ^[16]	主动	攻击者试图在传输过程中修改或篡改通信中的数据

1.2 车联网隐私保护技术及度量方法

1.2.1 车联网隐私保护技术

为保护车联网中的隐私信息,需使用隐私保护技术对车辆的位置、身份、数据进行处理。常用的面向车联网的隐私保护技术可以分为以下5类:①基于假名的隐私保护技术^[17-22]。该类技术使用虚假身份替换车辆的真实身份,从而保护其身份信息,但在某些情况下,攻击者仍然可以通过分析车辆的移动模式推断出其真实身份;②基于匿名的隐私保护技术^[23-28]。该类技术通过使车辆在数据处理和通信中保持匿名状态来减少潜在的隐私泄露风险。 k -匿名是常用的匿名技术,其可生成特定的匿名集合以启动查询流程,并通过整合其他车辆的位置信息构建出满足隐私保护要求的匿名区域;③基于失真的隐私保护技术^[29-33]。该类技术在原始数据中引入一定程度的噪声,在保护车辆隐私的同时仍能保持数据的可用性。噪声越大,隐私保护强度越大,数据可用性越低;④基于加密的隐私保护技术^[34-41]。该类技术通过在数据存储、传输和处理的各个环节应用加密算法来确保只有授权的用户才能够访问数据内容,代表性方法包括区块链、同态加密、联邦学习等,但计算和通信开销均较高;⑤基于缓存的隐私保护技

术^[42-44]。该类技术通过在信息存储、传输和访问过程中利用缓存来减少对敏感信息的直接暴露,进而提高车辆隐私的安全性。

1.2.2 隐私度量方法分类

常用的隐私度量方法可分为以下3类:①位置隐私度量方法。该类方法可以帮助研究人员评估位置隐私泄露风险,代表性方法为基于匿名与不确定性的度量方法,度量指标包括匿名集大小、匿名成功率、信息熵等^[45-47];②身份隐私度量方法。该类方法用于评估车辆在通信过程中的身份信息保护程度,度量指标包括信息熵、匿名集大小等^[48-49];③数据隐私度量方法。该类方法用于衡量在共享与传输过程中车辆信息的隐私保护程度,代表性方法为基于不确定性与失真的度量方法,度量指标包括信息熵、差分隐私等^[50-51]。

1.3 车联网隐私度量框架

为正确量化隐私保护技术的有效性,需综合考虑车联网环境中影响车辆隐私的各项因素间的关联,包括车辆信息、背景知识攻击、隐私保护技术、隐私度量方法等。综合考虑上述因素,本文构建出一种车联网隐私度量框架。具体如图1所示。

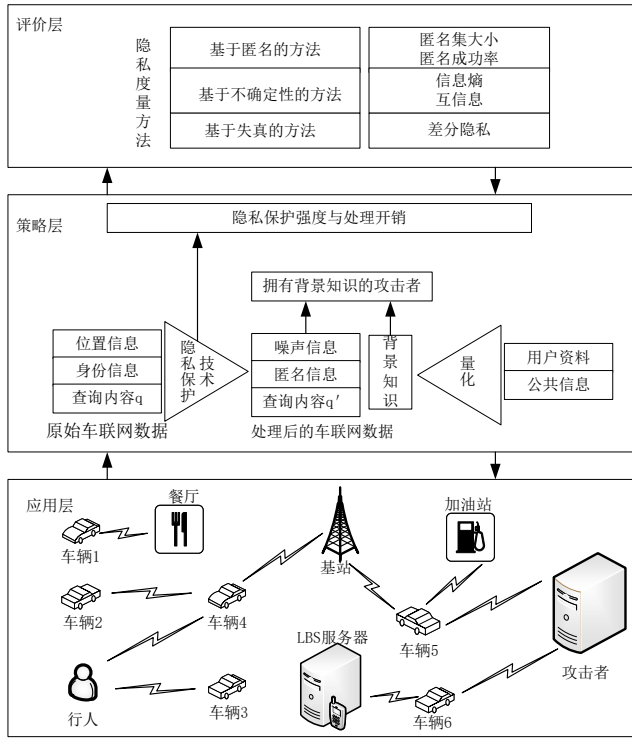


Fig. 1 Privacy measurement framework for Internet of Vehicles

图1 车联网隐私度量框架

该框架主要涵盖3个方面:①应用层。包括车辆与车辆、车辆与行人、车辆与基础设施、车辆与路旁设施之间的通信,同时考虑攻击者的存在;②策略层。涵盖应用层所使用的隐私保护技术和攻击者。车辆根据隐私需求选择适当的保护技术,而攻击者则利用背景知识来尝试披露隐私信息;③评价层。采用相应的度量方法衡量策略层中隐私保护技术的强度。

在以往研究中,文献[3, 52, 53]所提出的隐私度量框架中层与层之间都是单向传递,没有任何交互。本文提出的车联网隐私度量框架中的三层结构有效交互,即车辆的需求变化在应用层影响隐私保护技术的选择,评价层的度量方法用于评估隐私保护技术的性能,并将评价结果反馈给研究者,研究者据此重新选择与优化隐私保护技术,最终形成一个闭环,可提供更出色的隐私信息保护服务。

2 面向车联网的度量方法

2.1 基于匿名的度量方法

基于匿名的度量方法旨在量化匿名集中车辆身份或位置的难以识别程度。框架如图2所示。

2.1.1 匿名集大小

1988年,Chaum^[54]首次提出匿名集的概念,将其定义为发送与接收特定信息的用户集合。匿名集大小是用于衡量隐私保护能力的指标,其匿名程度 LP 可表示为:

$$LP = |A_u| = \log_2 N (N \geq 1) \quad (1)$$

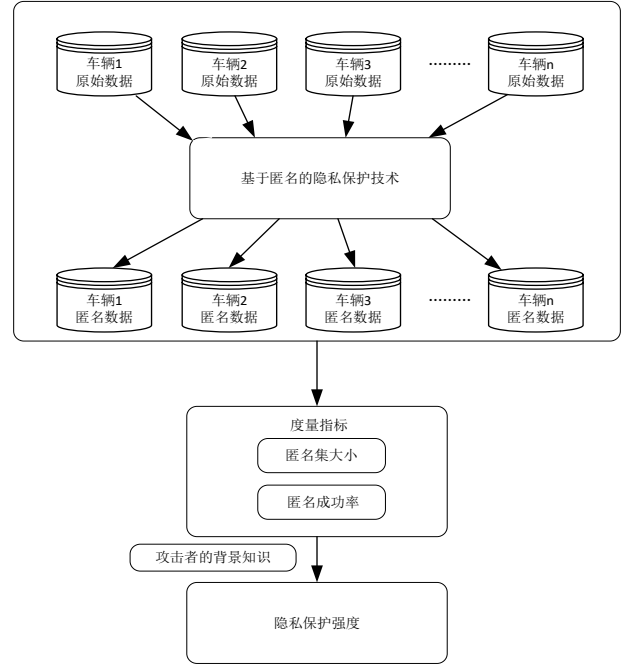


Fig. 2 Anonymity based privacy measurement framework for the Internet of Vehicles

图2 基于匿名的车联网隐私度量框架

式中: u 为用户; $|A_u|$ 为匿名集大小; N 为匿名集中用户的数量。

在车联网隐私保护中,匿名集大小描述了车辆身份难以被追踪和识别的程度。匿名集合越小,车辆的身份或位置越容易被识别,匿名程度越低。因此,车联网系统通过限制匿名集大小来提高系统的安全性。

Sweeney^[55]于2002年首次提出 k -匿名的概念,主要应用于关系数据库中个人数据的保护,也可用于衡量数据集中数据的匿名程度。其匿名程度 LP 可表示为:

$$LP = k \quad (2)$$

式中: k 为数据集中不可被识别的元组,每个元组被识别的概率均为 $1/k$ 。 k 值越大,隐私保护程度越高。

基于 k -匿名的隐私保护技术存在两种实现方案:其一为依赖匿名服务器的方案,在该方案中,匿名服务器负责生成一个匿名区域,该区域需包含查询用户以及至少 $k-1$ 个其他用户,从而确保匿名区域内至少涵盖 k 个用户^[56-57];其二为不依赖匿名服务器的方案,在该方案下,由用户自身生成至少 $k-1$ 个假位置,并将这些假位置与查询用户的真实位置进行混淆处理,之后统一发送给位置服务提供商^[58-59]。无论采用上述哪种方案,从攻击者的视角来看,其成功识别出查询用户的概率均为 $1/k$ 。

Huang等^[60]借鉴目标跟踪算法的思想^[61],根据 $t-1$ 时刻的位置计算 t 时刻车辆的预测位置,其匿名集由车辆的真实位置与预测位置构成。Wu等^[45]提出匿名集大小由车辆真实位置附近的车辆及其一起形成的偏移位置构成,通过计算匿名集中两个位置的距离之和来获得匿名集中假位置的分散程度。因此,假位置的分散程度越高,匿名

集的覆盖范围越大,匿名效果也越好。然而,如果匿名集过大,则会提高攻击者重识别匿名化位置轨迹的风险。由于车辆通常使用多个假名对其身份进行保护,Artail等^[62]认为匿名集的大小不能只考虑车辆数量,还应该考虑使用假名的数量。Babaghayou等^[48]使用车辆在行驶过程中获得的每条轨迹的最大匿名集大小来衡量其与附近其他车辆的不可区分性。Bao等^[49]认为车辆的最大匿名集大小是通过寻找与该车辆同时更改假名的最大数量的车辆来获得的,并通过计算平均匿名集大小了解整个车辆群组达到的平均匿名程度。考虑到匿名集中车辆的具体运动情况以及车辆群组随时间的变化,Nitschke等^[63]通过跟踪发送消息车辆的位置信息及其所属的群组计算每个车辆发送的消息数量与所属群组发送的所有消息数量之比,从而确定最合适的匿名集大小。

Tu等^[64]针对语义推理攻击和重识别攻击所提出的算法同时满足 k -匿名性、 l -多样性和 t -临近性,在蜂窝网络和移动端收集的两个真实移动数据集上验证了其有效性。考虑到许多模型假设攻击者拥有完整的背景知识,会高估隐私风险的问题,Bennati等^[65]提出轨迹数据隐私风险评价模型,假设攻击者不具有完整的背景知识。该模型通过构建等价区域对不同类型的攻击进行建模,使用 k -匿名性、 l -多样性和 t -临近性对模型进行评价,结果表明这些度量指标在使用真实世界数据集量化链接攻击和推理攻击时具有有效性。

2.1.2 匿名成功率

在车联网环境中,匿名成功率是指通过运用匿名技术来降低攻击者成功推断出车辆真实位置或轨迹的概率,进而衡量成功隐藏车辆真实位置或轨迹的程度^[28,66]。Xie等^[46]发现匿名成功率不仅与匿名度 k 有关,还与最小匿名区域有关。具体来说,当 k 值较小时,最小匿名区域中的车辆数量越多,匿名成功率越大;当 k 值较大时,若最小匿名区域中的车辆数量不满足 k 匿名要求,匿名区域会扩散,直到满足 k 为止。因此,在车辆数量较少的环境中形成的匿名区域更大,匿名成功率也越高。Zheng等^[67]对车辆数量与匿名成功率之间的关系进行分析,发现匿名区域内车辆数量越多,越有利于匿名执行,匿名成功率也就越高。王洁等^[68]认为匿名成功率不仅与匿名度 k 有关,而且与语义差异度 u 有关。其发现随着匿名度 k 的增加,匿名成功率会有所下降,说明满足语义差异度的位置数并不能满足匿名度 k 的要求。随着语义差异度 u 的增加,匿名成功率同样呈下降趋势,表明对语义差异度的要求越高,匿名集中的语义多样性也就越难满足。文献[45, 69]使用位置暴露概率(Probability of Exposing Real Location, PERL)表示车辆真实位置的暴露概率。匿名成功率与PERL通常是负相关的,即随着匿名成功率的增大,位置暴露概率逐渐降低。PERL的计算公式为:

$$PERL = \frac{1}{k - k'} \quad (3)$$

式中: k 表示所有匿名位置数量; k' 表示攻击者过滤出的匿名位置数量。

2.2 基于不确定性的度量方法

基于不确定性的度量方法是一种利用信息论来量化车联网中隐私泄露风险的方法,其将车联网中的数据建模为随机变量,并通过信息熵等指标来评估数据的不确定性程度,进而衡量不同隐私保护措施的效果。

2.2.1 信息熵

匿名集大小或有效匿名集的大小 k 等指标虽然被广泛应用,但存在一定不足。当匿名区域中用户出现的概率不相等时,以上指标不能很好地反映隐私保护水平^[70-71]。信息熵解决了信息的量化问题,是信息度量的有效方法。为了更加直观地度量信息熵,彭长根等^[72]将隐私保护系统形象地描述成一种通信模型。结构如图3所示。攻击者缺乏与数据信源中隐私信息相关的任何背景知识,仅通过分析数据信宿中的观察数据来揭示隐私信息。运用信息熵对数据信宿中的平均隐私信息量进行描述,隐私信息泄露的潜在风险由隐私信息的不确定性决定。因此,隐私信息泄露程度可表示为:

$$H(X) = -\sum p(x) \log p(x) \quad (4)$$

式中: $H(X)$ 表示隐私发送方的隐私不确定程度,其值越大,隐私保护程度越高。对于不同的方案, $p(x)$ 的含义有所不同。在位置熵中, $p(x)$ 与历史查询概率以及车辆位置有关^[47, 68, 73];在匿名集合熵中, $p(x)$ 与匿名集合中的车辆数量有关^[74];在语义多样性熵中, $p(x)$ 与当前车辆查询的语义类型有关^[75-77];在假名熵中, $p(x)$ 与假名的年龄等因素有关^[78];在数据熵中, $p(x)$ 表示元组 x 的概率密度函数^[50]。

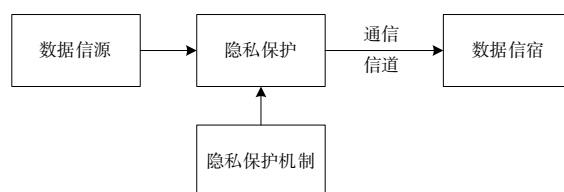


Fig. 3 Privacy protection communication model

图3 隐私保护通信模型

Xing等^[47]使用位置熵来衡量所提方案的有效性。计算公式为:

$$H_l = \frac{1}{2} (H_x + H_y) \quad (5)$$

式中: H_x 为车辆位置的横坐标熵值; H_y 为纵坐标熵值。

在车联网中,假名熵由每辆车被恶意节点攻击的概率决定,其随着被攻击概率的增加而减少。为解决由静默期导致的隐私—安全权衡问题,Babaghayou等^[48]分别在曼哈顿网格场景和高速公路场景下采用匿名集合熵评估所提隐私保护方案的有效性。Xia等^[79]基于车辆被攻击者攻击的概率,利用车辆的假名熵来实现其轨迹隐私度量。Yang等^[80]利用语义多样性熵来建立匿名集的多样性评估指标。

与直接使用匿名位置类别数量进行多样性评估不同,语义多样性熵能够反映语义整体数量对语义安全性的影响,以及每个语义类别数量对整体语义安全性的影响。该种度量方法不仅能够利用匿名位置的语义多样性来提高对真实位置的识别难度,而且能够通过时间尺度上分布每个语义类别来避免由于类别不平衡分布而引起的安全性损失。

匿名集合熵的取值范围取决于匿名集中车辆的数量。归一化熵通过除以最大熵值,将结果映射到 $[0,1]$ 区间内,提供了一种可比较的度量指标。计算公式为:

$$H_n = \frac{H(X)}{H_0(X)} \quad (6)$$

式中: $H_0(X)$ 为最大熵。

Benarous 等^[81]使用所有可能成为目标车辆的熵来量化隐私,并结合平均匿名集大小和归一化熵来提供更好的隐私保证。数据熵是衡量数据信息量的基本方法,其可以测量单个元组集的信息量。考虑到连续数据集由于样本数量有限,难以计算其概率密度函数等问题。Jiang 等^[50]使用高斯函数作为窗口函数的概率密度来估计连续数据集的数据熵。Mustafa 等^[82]将信息熵应用到决策树算法中,用于衡量某个属性对于分类的重要程度。因此,每次数据集迭代时都要计算熵值大小,选择具有较低熵值的属性作为划分依据,以验证数据是否被正确分类。针对多址边缘计算中的计算卸载决策可能会泄露用户隐私的问题,Zhao 等^[83]将基于用户计算任务卸载频率的隐私熵作为定量分析指标,从而在每个时隙度量卸载决策结果的实时隐私量。

2.2.2 互信息

互信息通过攻击者在获取隐私信息前后对原始数据不确定性减少的程度来反映隐私泄露风险^[72]。随着原始数据不确定性减少的程度增加,隐私信息泄露风险随之上升。互信息的计算公式为:

$$I(X; Y) = \sum_{x \in X} \sum_{y \in Y} p(xy) \log \frac{p(xy)}{p(x)} \quad (7)$$

式中: $I(X; Y)$ 表示隐私发送方 X 与隐私接收方 Y 之间隐私的整体泄露程度。互信息量越大,隐私保护程度越低。可以看出,互信息决定了联合分布 $p(xy)$ 与边缘分布 $p(x)p(y)$ 乘积的相似度。

Zhang 等^[84]使用互信息来判断基于 k -means 聚类生成的轨迹位置点之间的相关性,同时评估发布机制的隐私保护程度。由于先验知识和相关性在位置轨迹中是自然存在的,Zhang 等^[85]提出一种基于互信息的轨迹隐私度量方法来量化离线与在线轨迹之间的隐私泄露程度。直接计算隐私度量的复杂度会随着轨迹长度的增加而呈指数级增长。因此,其利用时间位置相关性的 Markov 结构获得轨迹隐私泄露的边界,从而提高计算效率。该研究将真实轨迹与扭曲轨迹之间的相关性视为无向的,因此在确保所需语义效用的同时无法准确量化轨迹数据隐私和语义隐私

泄露风险。为准确度量轨迹中位置之间的时空相关性以及真实轨迹与扭曲轨迹之间的因果关系所导致的数据隐私泄露风险,Zheng 等^[86]假设用户的移动轨迹遵循 r 阶的马尔可夫链,并提出基于有向信息的轨迹数据隐私度量方法来衡量因果关系和时空相关性导致的轨迹数据隐私泄露风险。此外,为量化语义感知的轨迹数据效用,其还提出基于 JS 散度的语义感知效用度量,通过求解这些度量指标构建的多目标优化问题,可更好地实现隐私与效用之间的平衡。

2.3 基于失真的度量方法

基于失真的度量方法是一种基于数据失真程度来评估车联网中隐私保护效果的方法。该方法通过向车联网中的数据添加噪声来达到保护隐私的目的,并通过量化失真程度来评估隐私保护效果。基于失真的车联网隐私度量框架如图 4 所示。

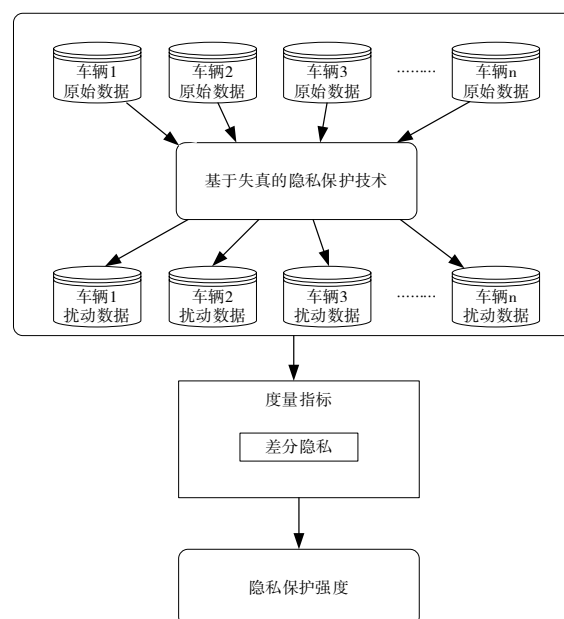


Fig. 4 Distortion-based privacy measurement framework for the Internet of Vehicles

图4 基于失真的车联网隐私度量框架

差分隐私是由Dwork^[87]提出的隐私概念,用于解决统计数据库环境下的隐私泄露问题。其对隐私保护强度进行了严格定义,任意增加或删除一条记录都不会对查询结果产生影响,而且不关心攻击者拥有的背景知识,因此得到学术界的广泛关注,迅速成为当前的研究热点^[88]。

假设有随机算法 A , $Range(A)$ 为算法 A 的值域,若算法 A 在数据集 $D1$ 和 $D2$ 上的任意输出结果 $O \in Range(A)$ 满足下列不等式,则算法 A 满足 ϵ -差分隐私保护。

$$\Pr [A(D_1 = O)] \leq e^\epsilon \times \Pr [A(D_2 = O)] \quad (8)$$

式中: $\Pr [\cdot]$ 表示隐私泄露风险,由随机算法 A 控制;数据集 $D1$ 和 $D2$ 只相差一条记录; ϵ 为差分隐私保护预算。

差分隐私不仅可以实现隐私保护,而且可以量化隐私

泄露程度。通过选择不同的隐私预算 ϵ 可划分隐私保护强度,隐私预算 ϵ 越小,添加的噪声越多,隐私保护强度越高,隐私泄露程度越低。差分隐私添加噪声的方式包括 Laplace 机制与指数机制,而添加的噪声量由全局敏感度 Δf 和 ϵ 共同确定^[89]。均匀分配与自适应分配是差分隐私预算分配的常用方法^[90]。如果有 n 个查询,均匀分配策略是将总的隐私预算 ϵ 平均分为每个查询的隐私预算 ϵ/n ,目的是确保每个查询都在相同的隐私保护下进行,不会有某个查询因获得更多的隐私预算而对隐私泄露风险产生不平衡的影响。Liu 等^[91]提出将差分隐私与匿名集大小相结合的度量方法,首先根据预测位置生成 $k-1$ 个假位置,并与用户真实位置一起构造匿名集;其次,根据差分隐私的串行组合性质对匿名集中的每个位置点均匀添加隐私预算 $\epsilon' = \epsilon/k$ 的拉普拉斯噪声,用于衡量隐私保护的有效性。均匀分配是一种简单且常见的策略,适用于当所有查询被视为同等重要或需要相同程度隐私保护的场景。然而,在某些情况下可能需要更灵活的自适应分配策略,例如根据查询的敏感性或重要性分配不同的隐私预算。考虑到隐私具有多样性,叶阿勇等^[92]的研究允许用户自定义位置敏感度,并为不同敏感程度的位置分配不同的隐私预算,有效提高了隐私预算利用率。自适应分配的关键在于根据用户查询的特性或隐私需求动态确定每个查询所需分配的隐私预算。这种策略可以使系统更灵活地满足不同查

询的隐私需求,更好地适应不同查询的复杂性,从而提高隐私保护效果。

3 各类隐私度量方法比较分析

表2为以上3种隐私度量方法的总结性比较。可以看出,每种方法都有其优缺点。基于匿名的隐私度量方法适用于小规模数据,能获得准确结果,但对于大规模的多维数据处理效率较低,应用范围存在一定局限性,可考虑采用分布式计算的方式提高效率。基于不确定性的度量方法可以根据攻击者的背景知识建立相应的隐私度量模型。该方法简单易实现,但容易受到异常值以及错误数据的影响,因此需要对数据进行预处理以提高度量准确性。此外,不同的概率分布可能会产生相同的熵值,亦会对度量准确性产生影响。基于失真的隐私度量方法主要依赖于全局敏感度 Δf 和隐私预算 ϵ 来衡量隐私保护强度。隐私预算 ϵ 越小,添加的噪声越多,隐私保护强度越高,隐私泄露程度越低。隐私预算 ϵ 可以直观反映保护水平,而且计算简便、效率高,在度量相互独立的数据时无需考虑攻击者的背景知识,减少了计算开销。由于差分隐私通常对每个特征应用独立的噪声,在处理高度相关的特征时可能无法捕捉到其间的复杂关系,此时可适当结合其他隐私度量方法。

Table 2 Summary comparison of privacy measurement methods

表2 隐私度量方法总结性比较

隐私度量方法	度量指标	主要优点	主要缺点
基于匿名的方法	匿名集大小、匿名成功率	实现简单	应用范围受限
基于不确定性的方法	信息熵、互信息	通用性高且效率高,可结合攻击者以及背景知识进行度量	度量结果易受异常值、错误数据的影响
基于失真的方法	差分隐私	原理简单且准确性高,无需量化攻击者的背景知识	难以准确反映高度相关的数据的隐私保护强度

表3从各类度量指标的影响因素及其优缺点等方面进一步分析了近年来的相关工作。

表4总结了近年来车联网隐私度量的研究方案,有助于研究者了解在特定情境下应该优先考虑哪种隐私度量方法,从而提高隐私保护技术的可行性和实用性。

4 车联网隐私度量的未来研究方向

面向车联网隐私度量的研究目前仍面临诸多挑战。通过分析现有工作,本文认为未来研究将主要集中于隐私度量的过程、效果以及方法3个方面。

4.1 隐私度量过程

当前的隐私保护方法在提高隐私保护强度的同时往往需要牺牲数据可用性,降低了车联网数据共享的服务质量。为找到合适的平衡点,可以借助博弈论模型等来分析用户的实际需求,在给定的最大数据可用性损失和计算开销条件下提供最佳隐私保护。

4.2 隐私度量效果

虽然现有隐私度量方法可以衡量不同隐私保护技术的强度,但缺少对其粒度的研究。一方面,现有位置语义度量方法较为粗糙且数量不多,评估指标较少;另一方面,由于处于同一区域内的车辆查询内容具有信息相关性,在实际应用中,查询内容可能会泄露用户的隐私数据。因此,如何构造出更细粒度的语义隐私度量方法以及根据不同车辆之间的信任度来度量查询内容的隐私泄露程度是一个具有挑战性的问题。

4.3 隐私度量方法

车联网数据不仅包括基础的车辆信息,而且包括行驶轨迹、驾驶行为、交通流量、道路状态等丰富的数据类型,需要采用不同的隐私保护技术进行处理。不同类型的车联网隐私保护技术具有各自的特性,其度量方法也存在差异。为提升度量效率与准确性,可构建一套标准化车联网隐私度量模型,旨在精简需观测的特征数量,从而实现各类车联网隐私保护技术的有效度量。此外,还可以将多种隐私度量方法结合起来,优势互补,扩展其适用范围。

Table 3 Comparative analysis of various related works
表 3 各类相关工作比较分析

度量指标	影响因素	优点	缺点
匿名集大小	车辆数量 ^[45, 60]	车辆数量变化可以动态调整匿名集的大小,使得在不同情况下都能实现一定程度的隐私保护	在车辆数量较少的地区,匿名集大小可能较小,导致隐私保护效果不佳
	移动模式 ^[48]	在不同的移动模式下,用户可能会表现出不同的行为特征,这可以帮助减少不同行为之间的关联性	如果用户的移动模式未能被正确识别或分类,可能导致匿名集大小不合适
	假名数量 ^[49, 62]	匿名集中假名的多样性可以减少攻击者获取用户真实身份的机会,有效保护用户隐私	生成和维护多个假名可能需要额外的计算和存储资源,可能会影响系统的性能
	通信范围 ^[63]	可以根据交通流量动态调整通信范围,灵活变化匿名集的规模	容易出现网络拥堵、资源消耗等问题
匿名成功率	匿名区域大小 ^[46]	可以根据不同区域(如住宅区、商业区等)的特点,灵活调整匿名策略,以优化隐私保护	匿名区域并非均匀分布,不同区域的隐私保护级别差异可能导致某些车辆在驶入低保护区域时迅速失去隐私
	车辆数量 ^[67]	车辆数量越多,使得单个车辆被识别或定位的难度增加,从而提高了整体的隐私保护水平	尽管车辆数量多有助于提升匿名成功率,但也可能吸引更多恶意的攻击者,增加系统受到攻击的风险
位置熵	车辆位置 ^[47]	在进行位置熵分析时,只需关心位置的频率分布和变化规律,可以减少对敏感位置信息的依赖	用户的位置信息可能随时间变化,位置熵只反映特定时间段内的情况
	历史查询概率 ^[68, 73]	根据不同位置的历史查询概率,系统可以优先分配资源到隐私保护要求较高的位置	用户的行为模式可能随时间变化,基于历史数据的静态分析可能无法及时响应这些变化
匿名集合熵	车辆数量 ^[74]	在车辆数量较多的情况下,攻击者难以通过统计分析或其他方法识别出特定的车辆	面临着车辆分布不均及动态变化等问题
语义多样性熵	查询的语义类型 ^[75, 77]	查询的语义类型多样化时,攻击者难以从单一的查询中推断出用户的具体意图	依赖语义分析模型的准确性,如果模型无法正确理解或分类语义类型,则可能导致隐私泄露
假名熵	假名年龄 ^[78]	定期更新和替换使用时间较长的假名,有助于降低车辆信息泄露的风险,增强整体系统的安全性	假名的年龄可能被攻击者利用,通过分析假名的使用模式来推断用户行为
	外部信息可获得性 ^[79]	通过监测外部信息的获取途径,可以设计更复杂的假名生成机制,以抵御潜在的信息收集攻击	攻击者如果能够获取关于可获得性的信息,也可能针对性地选择攻击策略,从而降低假名熵的效果
数据熵	概率密度函数 ^[50, 82]	在机器学习中,数据熵常用作特征选择、模型评估等过程中的标准,有助于优化决策和提高模型性能	概率密度函数可能对数据中的异常值敏感,这可能导致熵的计算受到干扰,从而影响最终的分析结果
互信息	随机变量间的相关性 ^[84-86]	互信息捕捉高阶关系,这使得它在许多复杂系统中表现良好	车辆轨迹数据不足或存在异常值时,互信息的估计可能会不稳定或者不准确,从而影响分析结果的可靠性
差分隐私	Δf 和 ϵ ^[92]	ϵ 允许用户根据特定应用场景的需求来调整隐私保护级别	在多个查询中,每个查询都消耗一定的 ϵ ,如果未能合理控制总的 ϵ 值,可能导致整体隐私保护不足

Table 4 Research plan for privacy measurement of Internet of Vehicles
表 4 车联网隐私度量研究方案

隐私度量方法	度量指标	隐私分类	针对的技术	针对的攻击	应用场景
基于匿名	匿名集大小 ^[45]	位置/身份隐私	k -匿名	位置同质攻击	车辆隐私保护
	匿名成功率 ^[46]	位置/身份隐私	k -匿名	区域攻击	车辆隐私保护
	匿名集大小 ^[49]	位置/身份隐私	假名	共谋攻击	车辆通信
	匿名集大小 ^[63]	数据隐私	k -匿名	内部攻击	车辆通信
	匿名成功率 ^[67]	位置隐私	k -匿名	位置连接攻击	车辆隐私保护
	位置熵 ^[47]	位置隐私	k -匿名	背景知识攻击	车辆隐私保护
	匿名集合熵 ^[48]	位置/身份隐私	假名	窃听攻击	车辆隐私保护
	数据熵 ^[50]	数据隐私	联邦学习、区块链	单点/中毒攻击	车辆数据共享
	匿名集合熵 ^[74]	位置隐私	假名	窃听攻击	车辆通信
	语义多样性熵 ^[75]	位置隐私	k -匿名	共谋/推理攻击	车辆隐私保护
基于不确定性	语义多样性熵 ^[77]	轨迹隐私	k -匿名、缓存	位置关联攻击	车辆隐私保护
	假名熵 ^[78]	位置隐私	假名	跟踪攻击	车辆更换假名
	假名熵 ^[79]	轨迹隐私	轨迹隐私保护技术	恶意车辆攻击	车联网轨迹隐私保护
	语义多样性熵 ^[80]	语义隐私	k -匿名	语义攻击	相关位置语义隐私保护
	平均匿名集、匿名集合熵、归一化熵 ^[81]	轨迹隐私	混淆技术、静默期	语义/链接攻击	云驱动的车联网
	信息熵 ^[82]	数据隐私	机器学习	拒绝服务攻击	车联网数据共享
	互信息 ^[85]	轨迹隐私	轨迹隐私保护技术	推理攻击	原始轨迹与发布轨迹间的隐私泄露
基于失真	互信息、有向信息 ^[86]	轨迹/语义隐私	语义感知技术	语义攻击	在线位置轨迹数据共享
	差分隐私 ^[91]	位置/轨迹隐私	k -匿名、差分隐私	概率攻击	连续位置查询
	差分隐私 ^[92]	轨迹隐私	隐私累积	背景知识攻击	轨迹隐私保护中的隐私预算与服务质量问题

5 结语

本文在充分调查与分析相关研究的基础上对基于车联网的隐私度量方法进行系统梳理,并对不同类型的隐私度量方法进行综述,深入分析基于匿名、不确定性和失真的隐私度量方法的基本思想与实现原理,总结了3种隐私度量方法的评估指标及主要优缺点,为相关领域研究提供了参考与借鉴。车联网隐私度量方法的研究前景广阔,但也面临着诸多挑战。通过在隐私度量粒度精细化、标准化推进、多种方法组合优化、与新兴技术融合以及用户体验平衡等方面开展深入研究,有望为车联网隐私保护提供更加有效、可靠的技术支持,推动车联网行业的健康、可持续发展。

参考文献:

- [1] HILDEBRAND B, TABASSUM S, KONATHAM B, et al. A comprehensive review on blockchains for Internet of Vehicles: challenges and directions[J]. Computer Science Review, 2023, 48(5): 100547–100559.
- [2] RANI P, SHARMA R. Intelligent transportation system for Internet of Vehicles based vehicular networks for smart cities[J]. Computers and Electrical Engineering, 2023, 105(7): 108543–108555.
- [3] XU X Y, YU H Y, CUI Z Y, et al. Privacy security measurement methods in the Internet of Vehicles environment [J]. Journal of Tongji University (Natural Science Edition), 2022, 50(12): 1693–1702.
徐小雅, 于海洋, 崔志勇, 等. 车联网环境下的隐私安全度量方法[J]. 同济大学学报(自然科学版), 2022, 50(12): 1693–1702.
- [4] ZHOU Q, ZENG Z, WANG K, et al. Privacy protection scheme for the Internet of Vehicles based on collaborative services [J]. IEEE Internet of Things Journal, 2023, 10(15): 13342–13353.
- [5] LIU J, PENG C, SUN R, et al. CPAHP: conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV [J]. IEEE Transactions on Vehicular Technology, 2023, 72(7): 8929–8940.
- [6] QI Z, CHEN W. Location privacy protection of IoV based on blockchain and k-anonymity technology [C]//Proceedings of the 2023 6th International Conference on Electronics Technology, 2023: 15–21.
- [7] ATAUBA V M. A study on preserving privacy of Internet of Vehicles (IOV) data in cloud infrastructure using homomorphic encryption [D]. Dublin: National College of Ireland, 2022.
- [8] AMAN M N, JAVAID U, SIKDAR B. A privacy-preserving and scalable authentication protocol for the Internet of Vehicles [J]. IEEE Internet of Things Journal, 2020, 8(2): 1123–1139.
- [9] XING L, HUANG Y, GAO J, et al. Location entropy-based privacy protection algorithm for social Internet of Vehicles [J]. Wireless Personal Communications, 2023, 130(4): 3009–3025.
- [10] ZHOU Y, TAN H, IROSHAN K C A A. A secure authentication and key agreement scheme with dynamic management for vehicular networks [J]. Connection Science, 2023, 35(1): 217–228.
- [11] BAJRACHARYA C. Performance evaluation for secure communications in mobile Internet of Vehicles with joint reactive jamming and eavesdropping attacks [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(11): 22563–22570.
- [12] XU J, LI M, HE Z, et al. Security and privacy protection communication protocol for Internet of Vehicles in smart cities [J]. Computers and Electrical Engineering, 2023, 10(5): 108–129.
- [13] RASHID K, SAEED Y, ALI A, et al. An adaptive real-time malicious node detection framework using machine learning in vehicular Ad-Hoc networks (VANETs) [J]. Sensors, 2023, 23(5): 2594–2610.
- [14] SEDAR R, KALALAS C, ALONSO-ZARATE J, et al. Multi-domain denial-of-service attacks in Internet-of-Vehicles: vulnerability insights and detection performance [C]//Proceedings of the 2022 IEEE 8th International Conference on Network Softwarization (NetSoft), 2022: 438–443.
- [15] KOSMANOS D, PAPPAS A, MAGLARAS L, et al. A novel intrusion detection system against spoofing attacks in connected electric vehicles [J]. Array, 2020, 5(2): 100–112.
- [16] PARAMESWARATH R P, ABHISHEK N V, SIKDAR B. PREVENT: a mechanism for preventing message tampering attacks in electric vehicle networks [C]//Proceedings of the 2023 IEEE 97th Vehicular Technology Conference, 2023: 1–5.
- [17] KUMARI I, SINGH P K, GOWTHAM S N, et al. RFPM: a RSU-aided framework for pseudonym management to preserve location privacy in IoV [J]. Security and Privacy, 2024, 7(1): 78–89.
- [18] MEMON I, SHAIKH R A, SHAIKH H. Dynamic pseudonyms trust-based model to protect attack scenario for Internet of Vehicle ad-hoc networks [J]. Multimedia Tools and Applications, 2024, 83(5): 13395–13426.
- [19] ZHANG W, GUO Z, HAN G, et al. DPSP: a dynamic pseudonym swap program based location privacy protection algorithm for Internet of Vehicles [J]. IEEE Transactions on Network Science and Engineering, 2024, 11(5): 4525–4535.
- [20] WANG H, ZHANG F, SHEN Z, et al. Blockchain-based IVPPA scheme for pseudonym privacy protection in Internet of Vehicles [EB/OL]. <https://bit.nkust.edu.tw/~jni/2024/vol9/s2/41.JNI-S-2023-05-022.pdf>.
- [21] MA W, YU Y, WANG Y, et al. A pseudonym exchange-based traceable location privacy protection scheme for IoV [C]//Proceedings of the 2023 International Conference on Networking and Network Applications, 2023: 287–292.
- [22] BENAROUS L, BITAM S, MELLOUK A. CSLPPS: concerted silence-based location privacy preserving scheme for Internet of Vehicles [J]. IEEE Transactions on Vehicular Technology, 2021, 70(7): 7153–7160.
- [23] CUI J, CHEN X F, ZHANG J, et al. A location privacy protection scheme based on bus caching in the Internet of Vehicles [J]. Journal of Communications, 2021, 42(7): 150–161.
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.
- [24] LIU Y D, MA Y L, DU Y B, et al. A certificate-free anonymous authentication key agreement protocol in the Internet of Vehicles [J]. Information Network Security, 2024, 24(7): 983–992.
刘一丹, 马永柳, 杜宜宾, 等. 一种车联网中的无证书匿名认证密钥协商协议[J]. 信息网络安全, 2024, 24(7): 983–992.
- [25] XING D D, CAO S Z, ZHAO X, et al. A multi-receiver anonymous sign-encryption scheme in the Internet of Vehicles environment [J]. Computer Engineering, 2024, 6(2): 1–13.
邢丹丹, 曹素珍, 赵晓, 等. 车联网环境下多接收者匿名签密方案[J]. 计算机工程, 2024, 6(2): 1–13.
- [26] WANG B, LIU J, DAI L. K-anonymity-based privacy-preserving and efficient location-based services for Internet of Vehicles withstand Viterbi attack [C]//Proceedings of the International Conference on Image, Vision and Intelligent Systems, 2022: 1016–1028.
- [27] XIE P, HAN X M, FENG T, et al. A method of constructing arc edge anonymous area based on LBS privacy protection in the Internet of Vehicles [J]. International Journal of Network Security, 2020, 22(2):

- 275–282.
- [28] LI H, XUE X, LI Z, et al. Location privacy protection scheme for LBS in IoT [J]. *Wireless Communications and Mobile Computing*, 2021, 18(3): 1–18.
- [29] WU W Q, ZHAO Y X, WANG Q, et al. A trajectory data secure storage and publishing method that satisfies differential privacy [J]. *Computer Research and Development*, 2021, 58(11): 2430–2443.
吴万青, 赵永新, 王巧, 等. 一种满足差分隐私的轨迹数据安全存储和发布方法[J]. *计算机研究与发展*, 2021, 58(11): 2430–2443.
- [30] CHEN R, CHEN X, ZHAO J. Private and utility enhanced intrusion detection based on attack behavior analysis with local differential privacy on IoV [J]. *Computer Networks*, 2024, 12(6): 110560–110571.
- [31] KONG X, LU L, XIONG K. Privacy-preserving estimation of electric vehicle charging behavior: a federated learning approach based on differential privacy [J]. *Internet of Things*, 2024, 11(5): 101344–101355.
- [32] BATOOL H, ANJUM A, KHAN A, et al. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy [J]. *Information Sciences*, 2024, 12(5): 119717–119728.
- [33] KWON D, SON S, PARK K, et al. A secure authentication scheme with local differential privacy in edge intelligence-enabled VANET [J]. *Mathematics*, 2024, 12(15): 2383–2395.
- [34] XU C, WU H, LIU H, et al. Blockchain-oriented privacy protection of sensitive data in the Internet of Vehicles [J]. *IEEE Transactions on Intelligent Vehicles*, 2022, 8(2): 1057–1067.
- [35] HUSSAIN S, TAHIR S, MASOOD A, et al. Blockchain-enabled secure communication framework for enhancing trust and access control in the Internet of Vehicles (IoV) [J]. *IEEE Access*, 2024, 12(8): 110992–111006.
- [36] EHSAN I, KHALID M I, HELFERT M, et al. Chain links on wheels: a security scheme for IoV connectivity through blockchain integration [C]// *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 2024: 1–8.
- [37] MEN H L, CAO L, ZHENG G L, et al. LBS privacy protection scheme based on sparse user environment in the Internet of Vehicles [J]. *Computer Applications Research*, 2024, 6(2): 1–10.
门红蕾, 曹利, 郑国莉, 等. 车联网基于稀疏用户环境的LBS隐私保护方案[J]. *计算机应用研究*, 2024, 6(2): 1–10.
- [38] MANH B D, NGUYEN C H, HOANG D T, et al. Homomorphic encryption-enabled federated learning for privacy-preserving intrusion detection in resource-constrained IoV networks [DB/OL]. <https://arxiv.org/pdf/2407.18503>.
- [39] MO Z, GAO Z, ZHAO C, et al. FedDQ: a communication-efficient federated learning approach for Internet of Vehicles [J]. *Journal of Systems Architecture*, 2022, 131(6): 102690–102705.
- [40] CHEN T, BAI X, ZHAO J, et al. ShieldTSE: a privacy-enhanced split federated learning framework for traffic state estimation in IoV [J]. *IEEE Internet of Things Journal*, 2024, 11(22): 37324–37339.
- [41] XU Z, ZHANG R, LIANG W, et al. A privacy-preserving data aggregation protocol for Internet of Vehicles with federated learning [J]. *IEEE Transactions on Intelligent Vehicles*, 2024, 10(3): 1–11.
- [42] KAN C, WU H, XING L, et al. Cooperative caching strategy based mobile vehicle social-aware in Internet of Vehicles [J]. *Transactions on Emerging Telecommunications Technologies*, 2023, 34(7): 4792–4805.
- [43] ZHANG J R, WANG Q G, HUANG Y H, et al. A location privacy enhancement method against inference attacks in the Internet of Vehicles [J]. *Modern Electronic Technology*, 2024, 47(14): 182–186.
张金瑞, 王庆国, 黄元浩, 等. 抵抗推理攻击的车联网位置隐私增强方法[J]. *现代电子技术*, 2024, 47(14): 182–186.
- [44] SHEN Z, WANG Y, WANG H, et al. Privacy-protecting predictive cache method based on blockchain and machine learning in Internet of Vehicles [J]. *Vehicular Communications*, 2024, 47(5): 100771–100782.
- [45] WU L, WEI X, MENG L, et al. Privacy-preserving location-based traffic density monitoring [J]. *Connection Science*, 2022, 34(1): 874–894.
- [46] XIE P, XIAO T, FAN H J. An algorithm of the privacy security protection based on location service in the Internet of Vehicles [J]. *International Journal of Network Security*, 2019, 21(4): 556–565.
- [47] XING L, JIA X, GAO J, et al. A location privacy protection algorithm based on double k-anonymity in the social Internet of Vehicles [J]. *IEEE Communications Letters*, 2021, 25(10): 3199–3203.
- [48] BABAGHAYOU M, CHAIB N, LAGRAA N, et al. A safety-aware location privacy-preserving IoV scheme with road congestion-estimation in mobile edge computing [J]. *Sensors*, 2023, 23(1): 531–544.
- [49] BAO S, CAO Y, LEI A, et al. Pseudonym management through blockchain: cost-efficient privacy preservation on intelligent transportation systems [J]. *IEEE Access*, 2019, 7(2): 80390–80403.
- [50] JIANG W, CHEN M, TAO J. Federated learning with blockchain for privacy-preserving data sharing in Internet of Vehicles [J]. *China Communications*, 2023, 20(3): 69–85.
- [51] XU C, DING Y Y, LUO L, et al. Personalized location privacy protection based on location services in the Internet of Vehicles [J]. *Journal of Software*, 2022, 33(2): 699–716.
徐川, 丁颖祎, 罗丽, 等. 车联网中基于位置服务的个性化位置隐私保护[J]. *软件学报*, 2022, 33(2): 699–716.
- [52] CHEN J M, WANG L, XIAO Y F, et al. A metric method for query privacy under k-anonymity mechanism [J]. *Journal of University of Science and Technology of China*, 2018, 48(6): 512–518.
陈家明, 王丽, 肖亚飞, 等. k-匿名机制下查询隐私的一种度量方法[J]. *中国科学技术大学学报*, 2018, 48(6): 512–518.
- [53] WANG H B, LIU H W, WANG Z L. Research on privacy metric methods based on information theory [J]. *Information Technology and Informatization*, 2023(9): 4–10.
王鸿波, 刘华伟, 王子龙. 基于信息论的隐私度量方法研究[J]. *信息技术与信息化*, 2023(9): 4–10.
- [54] CHAUM D. The dining cryptographers problem: unconditional sender and recipient untraceability [J]. *Journal of Cryptology*, 1988, 1: 65–75.
- [55] SWEENEY L. k-anonymity: a model for protecting privacy [J]. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 2002, 10(5): 557–570.
- [56] WANG B, GUO Y, LI H, et al. K-anonymity based location privacy protection method for location-based services in Internet of Thing [J]. *Concurrency and Computation: Practice and Experience*, 2021, 5(2): 231–242.
- [57] ZHANG Y B, ZHANG Q Y, YAN Y, et al. A k-anonymous location privacy protection method of polygon based on density distribution [J]. *International Journal of Network Security*, 2021, 23(1): 57–66.
- [58] PARMAR D, RAO U P. Privacy-preserving enhanced dummy-generation technique for location-based services [J]. *Concurrency and Computation: Practice and Experience*, 2023, 35(2): 18–32.
- [59] ZHAO P, LIU W, ZHANG G, et al. Preserving privacy in Wi-Fi localization with plausible dummy locations [J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(10): 11909–11925.
- [60] HUANG J, QIAN Y, HU R Q. A privacy-preserving scheme for location-based services in the Internet of Vehicles [J]. *Journal of Communi-*

- cations and Information Networks, 2021, 6(4): 385–395.
- [61] HOH B, GRUTESER M, XIONG H, et al. Preserving privacy in GPS traces via uncertainty-aware path cloaking[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007: 161–171.
- [62] ARTAIL H, ABBANI N. A pseudonym management system to achieve anonymity in vehicular ad-hoc networks [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 13(1): 106–119.
- [63] NITSCHKE M, ROTH C, HOYER C, et al. Harmonic group mix: a framework for anonymous and authenticated broadcast messages in vehicle-to-vehicle environments[C]//Proceedings of the Information Systems Security and Privacy: 6th International Conference, 2022: 178–200.
- [64] TU Z, ZHAO K, XU F, et al. Protecting trajectory from semantic attack considering k-anonymity, l-diversity, and t-closeness [J]. IEEE Transactions on Network and Service Management, 2019, 16(1): 264–278.
- [65] BENNATI S, KOVACEVIC A. Modelling imperfect knowledge via location semantics for realistic privacy risks estimation in trajectory data [J]. Scientific Reports, 2022, 12(1): 246–257.
- [66] KUANG L, WANG Y, ZHENG X, et al. Using location semantics to realize personalized road network location privacy protection [J]. EURASIP Journal on Wireless Communications and Networking, 2020(1): 1–16.
- [67] ZHENG Y, LUO J, ZHONG T. Service recommendation middleware based on location privacy protection in VANET [J]. IEEE Access, 2020, 8(5): 12768–12783.
- [68] WANG J, WANG C R, MA J F, et al. A fake location selection algorithm based on location semantics and query probability [J]. Journal of Communications, 2020, 41(3): 53–61.
王洁, 王春茹, 马建峰, 等. 基于位置语义和查询概率的假位置选择算法[J]. 通信学报, 2020, 41(3): 53–61.
- [69] YANG X, GAO L, LI Y, et al. A semantic-based dual location privacy-preserving approach [J]. IEICE Transactions on Information and Systems, 2022, 105(5): 982–995.
- [70] WAN S, LI F H, NIU B, et al. Research progress on location privacy protection technologies [J]. Journal of Communications, 2016, 37(12): 124–141.
万盛, 李风华, 牛犇, 等. 位置隐私保护技术研究进展[J]. 通信学报, 2016, 37(12): 124–141.
- [71] HOU L, YAO N, LU Z, et al. Tracking based mix-zone location privacy evaluation in VANET [J]. IEEE Transactions on Vehicular Technology, 2021, 70(10): 10957–10969.
- [72] PENG C G, DING H F, ZHU Y J, et al. Information entropy model for privacy protection and its measurement method [J]. Journal of Software, 2016, 27(8): 1891–1903.
彭长根, 丁红发, 朱义杰, 等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报, 2016, 27(8): 1891–1903.
- [73] LIU J, JIANG X, ZHANG S, et al. FADBM: frequency-aware dummy-based method in long-term location privacy protection [C]//Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems, 2019: 384–391.
- [74] SAINI I, SAAD S, JAEKEL A. A comprehensive pseudonym changing scheme for improving location privacy in vehicular networks [J]. Internet of Things, 2022, 19(3): 16–31.
- [75] XU X, CHEN H, XIE L. A location privacy preservation method based on dummy locations in Internet of Vehicles [J]. Applied Sciences, 2021, 11(10): 4594–4606.
- [76] HUA J, LIU Y, SHEN Y, et al. A privacy-enhancing scheme against contextual knowledge-based attacks in location-based services [J]. Frontiers of Computer Science, 2020, 14(1): 1–4.
- [77] HUANG Q, XU X, CHEN H, et al. A vehicle trajectory privacy preservation method based on caching and dummy locations in the Internet of Vehicles [J]. Sensors, 2022, 22(12): 4423–4434.
- [78] ZHONG H, NI J, CUI J, et al. Personalized location privacy protection based on vehicle movement regularity in vehicular networks [J]. IEEE Systems Journal, 2021, 16(1): 755–766.
- [79] XIA Y, WU L, ZHENG X, et al. Data dissemination with trajectory privacy protection for 6G-oriented vehicular networks [J]. IEEE Internet of Things Journal, 2022, 9(21): 21469–21480.
- [80] YANG X, GAO L, WANG H, et al. A user-related semantic location privacy protection method in location-based service [C]//Proceedings of the 2021 IEEE 27th International Conference on Parallel and Distributed Systems, 2021: 691–698.
- [81] BENAROUS L, KADRI B. Obfuscation-based location privacy-preserving scheme in cloud-enabled Internet of Vehicles [J]. Peer-to-Peer Networking and Applications, 2022, 15(1): 461–472.
- [82] MUSTAFA M, BUTTAR A M, SAJJIA G S, et al. Multitask learning for security and privacy in IoV (Internet of Vehicles) [J]. Autonomous Vehicles, 2022, 11(5): 217–233.
- [83] ZHAO X, PENG J, LI Y, et al. A privacy-preserving computation offloading method based on privacy entropy in multi-access edge computation [C]//Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications, 2020: 1016–1021.
- [84] ZHANG Z, XU X, XIAO F. LGAN-DP: a novel differential private publication mechanism of trajectory data [J]. Future Generation Computer Systems, 2023, 14(3): 692–703.
- [85] ZHANG W, LI M, TANDON R, et al. Online location trace privacy: an information theoretic approach [J]. IEEE Transactions on Information Forensics and Security, 2019, 14(1): 235–247.
- [86] ZHENG Z, LI Z, JIANG H, et al. Semantic-aware privacy-preserving online location trajectory data sharing [J]. IEEE Transactions on Information Forensics and Security, 2022, 17(5): 2256–2271.
- [87] DWORK C. Differential privacy [C]//Proceedings of the Automata, Languages and Programming: 33rd International Colloquium, 2006: 1–12.
- [88] YE Q Q, MENG X F, ZHU M J, et al. A survey of local differential privacy [J]. Journal of Software, 2018, 29(7): 1981–2005.
叶青青, 孟小峰, 朱敏杰, 等. 本地化差分隐私研究综述[J]. 软件学报, 2018, 29(7): 1981–2005.
- [89] DUAN Y, LIU J, MING X, et al. Characterizing and optimizing differentially-private techniques for high-utility, privacy-preserving Internet-of-Vehicles [C]//Proceedings of the International Conference on Human-Computer Interaction, 2023: 31–50.
- [90] CHEN R, ACS G, CASTELLUCCIA C. Differentially private sequential data publication via variable-length n-grams [C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security, 2012: 638–649.
- [91] LIU Z, MIAO D, LI R, et al. Cache-based privacy protection scheme for continuous location query [J]. Entropy, 2023, 25(2): 201–215.
- [92] YE A Y, MENG L Y, ZHAO Z W, et al. A trajectory differential privacy protection mechanism based on prediction and sliding window [J]. Journal of Communications, 2020, 41(4): 123–133.
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.

(责任编辑:尹晨茹)