



文章编号:1001-9081(2017)07-1921-05

DOI:10.11772/j.issn.1001-9081.2017.07.1921

车联网轨迹隐私保护研究进展

张春花¹, 瞿海娟^{2*}, 薛小平¹, 张芳¹, 陈康强¹, 冯丽娟¹

(1. 同济大学 电子与信息工程学院, 上海 201804; 2. 江苏理工学院 计算机工程学院, 江苏 常州 213001)

(*通信作者电子邮箱 zhuan@qq.com)

摘要:轨迹隐私保护对车联网(IoV)的发展至关重要,归纳和分析现有研究方法有重要意义。车联网轨迹隐私保护思想有轨迹模糊、假名更换和轨迹加密等3类,实现方法分别有基于用户真实轨迹的方法和基于哑元轨迹的方法、基于混合区域的方法和基于路径混淆的方法、基于私密信息检索(PIR)协议的方法和基于空间转换的方法。首先,介绍和归纳了研究背景和常见攻击等车联网轨迹隐私保护关键问题;然后,从方法思想、科学问题、方法演进等方面详细综述了现有车联网轨迹隐私保护方法,并阐述了需深入研究的难题;在此基础上,总结了代表性方案的隐私保护度、抗攻击性、复杂度等性能指标;最后展望了车联网轨迹隐私保护的未来研究方向。

关键词:车联网;轨迹隐私;隐私保护

中图分类号: TP309; TP393.083 **文献标志码:**A

Research progress in Internet of vehicles trajectory privacy protection

ZHANG Chunhua¹, ZANG Haijuan^{2*}, XUE Xiaoping¹, ZHANG Fang¹, CHEN Kangqiang¹, FENG Lijuan¹

(1. College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China;

2. College of Computer Engineering, Jiangsu University of Technology, Changzhou Jiangsu 213001, China)

Abstract: Trajectory privacy protection is critical to the development of Internet of Vehicles (IoV), which makes it important to summarize and analyze existing research methods. Existing IoV trajectory privacy protection methods can be divided into three categories: trajectory obfuscation, pseudonym change and trajectory encryption. Trajectory obfuscation can be achieved based on users' real trajectory or dummy trajectory. Pseudonym change can be achieved based on mix-zone or path confusion. Trajectory encryption can be achieved based on Private Information Retrieval (PIR) protocol or spatial transformation. Firstly, the research background and common attacks were introduced and summarized in this paper. Secondly, existing IoV trajectory privacy protection methods were surveyed from the aspects of methodology, scientific problem and method evolution. The problems need to be further studied also were elaborated. Furthermore, the performances of representative schemes were summarized, such as privacy protection, attack resistance and complexity. Finally, the future research directions of IoV trajectory privacy protection was prospected.

Key words: Internet of Vehicles (IoV); trajectory privacy; privacy protection

0 引言

车联网(Internet of Vehicles, IoV)是由车辆自组织网络(Vehicular Ad-Hoc Network, VANET)和移动互联网组成的开放异构网络,支持交通安全、交通效率和信息娱乐等服务^[1]。车辆的位置信息是车联网正常运作的基础。通常车辆的位置即是车载用户所在的位置,若不受保护,则用户会受到与时间和空间相关的推理攻击,导致用户的社会角色、生活习惯等敏感隐私信息泄露,甚至威胁用户的人身和财产安全。

轨迹是具有时空关联的位置信息,存在于连续更新位置的应用,如多数安全应用、交通效率应用及连续空间查询等。轨迹隐私保护是位置隐私保护的重要范畴,受到国内外学者的关注,并已提出了许多有效的方法,包括混合区域、哑元轨迹、空间转换等。然而,车联网的高度移动可预测性、社会性、

网络连通度不确定性、短暂性通信等特性^[2],使轨迹隐私保护极具挑战,仍存在亟待突破的研究难题。

1 车联网轨迹隐私保护关键问题

1.1 车联网轨迹隐私保护的难点

车联网中,车辆轨迹实质上反映了车辆及驾乘人员的行为,是车辆及驾乘人员隐私的重要内容。这种轨迹通常是由车辆连续地更新位置形成的,如主动安全应用要求车辆周期性地广播包含位置、速度等信息的信标消息。

轨迹隐私若不受保护,非法人员通过分析轨迹可获取驾乘人员的兴趣爱好、家庭住址、社会关系等隐私信息,则轨迹隐私保护无论对车辆或是对驾乘人员都十分重要。

车联网具有高动态性、高度移动可预测性和社会性等特性,导致车联网轨迹隐私保护研究非常复杂。具体地,车辆高

收稿日期:2017-01-24;修回日期:2017-03-23。

基金项目:“十二五”国家科技支撑计划项目(2015BAG13B01);江苏省前瞻性联合研究项目(BY2014038-03)。

作者简介:张春花(1989—),女,山东莒县人,博士研究生,主要研究方向:信息安全、隐私保护;瞿海娟(1965—),女,江苏常州人,副教授,博士,主要研究方向:网络与信息安全;薛小平(1963—),男,上海人,教授,主要研究方向:可信计算、信息安全;张芳(1971—),女,上海人,讲师,博士,主要研究方向:可信计算;陈康强(1992—),男,浙江金华人,硕士研究生,主要研究方向:VANET隐私与安全;冯丽娟(1994—),女,四川雅安人,硕士研究生,主要研究方向:VANET安全与隐私。



速移动,网络割裂频繁发生;车辆的移动受限于道路网络;交通管理部门为不同类型的车辆划分车道并规定不同车道的最高和最低限速;车辆的移动速度和方向受邻居车辆和交通状况的制约;车辆是由人驾驶的,车辆的移动规律与人的移动规律相符,如基于最短路径移动。

1.2 常见攻击类型

车联网是开放性网络,容易遭受各种隐私攻击,常见攻击类型有:基于移动预测(Mobile Forecast, MF)的攻击、基于查询关联(Query Association, QA)的攻击和基于车辆分布概率(Vehicle Distribution Probability, VDP)的攻击。

基于移动预测的攻击是指攻击者利用路网拓扑结构、最大运动速度、交通状况、路段转移概率等知识,预测并关联用户的位置,从而构造出车辆的移动轨迹。

基于查询关联的攻击是指攻击者利用查询内容间的相关性,识别出发起查询的用户,继而连续地追踪用户。

基于车辆分布概率的攻击是指攻击者利用车辆在道路上的分布概率,结合匿名算法,推断车辆所在的路段。

车联网轨迹隐私保护研究应围绕常见攻击展开,否则攻击者会通过推理获得轨迹隐私信息。

2 车联网轨迹隐私保护方法

现有轨迹隐私保护方法的核心策略有轨迹模糊、假名更换和轨迹加密等3种。根据实现策略的途径/机制,轨迹隐私保护方法可分别细分为:基于真实用户轨迹的方法^[3-4]和基于哑元轨迹的方法^[5-7];基于混合区域的方法^[8-10]和基于路径混淆的方法^[11-12];基于私密信息检索(Private Information Retrieval, PIR)协议的方法^[13-14]和基于空间转换的方法^[15-16]。

2.1 基于轨迹模糊的轨迹隐私保护方法

轨迹模糊模型通过连续匿名,使攻击者无法将单一用户轨迹从某轨迹集合中精确地识别出来。如何构造有效抵抗攻击的轨迹集合(称为匿名轨迹集)是此类模型的关键问题,通常利用真实用户轨迹或哑元轨迹实现匿名。集合的基数称为匿名度,一般记为k。

2.1.1 基于真实用户轨迹的方法

基于真实用户轨迹的方法是用户在请求基于位置的服务(Location-Based Service, LBS)时,每次向服务器提交多个服务请求用户的真实位置。这些位置所在的空间区域称为匿名区域,通常采用路段集的形式。

轨迹隐私保护方法的抗攻击能力与路网拓扑和用户分布状况密切相关。由于车辆的情境感知能力有限,现有工作普遍采用集中式架构^[3-4]。

为实现快速匿名,文献[3]基于用户密度、历史轨迹和路网拓扑,构建了路网层次结构;轨迹k-匿名要求构造的所有匿名区域至少有k个相同的用户^[17],为此通常将移动趋势、速度差异、目的地信息等因素作为构造匿名集的条件^[3-4]。

显然,集中式架构存在单点故障和性能瓶颈等安全隐患^[18]。如何支持用户的优先查询请求仍是开放性问题。

2.1.2 基于哑元轨迹的方法

哑元轨迹即虚拟轨迹,此类方法是在用户每次更新位置时,产生新的虚拟用户位置(即哑元位置),连续的哑元位置

构成哑元轨迹。

哑元轨迹的合理性决定方法的有效性^[19]。考虑到用户在固定时间内移动的距离是受限的,文献[5]从当前哑元位置的附近区域选择下一哑元位置。文献[6]以集中式的架构实现了文献[5]提出的算法,通过利用所有用户的活动,优化了系统行为和性能。除了可达性,文献[7]考虑了道路网络限制和用户运动模式(如用户运动一段时间后会停留一段时间)。

哑元轨迹方法能够获得一定的轨迹隐私保护,但如何产生与真实轨迹不可区分的哑元轨迹是一个复杂的问题,还需要进一步的研究。

2.2 基于假名更换的轨迹隐私保护方法

假名是隐藏了用户真实身份的身份标识,但若用户长期使用一个假名,则将被攻击者连续追踪,泄露轨迹隐私,故需更换假名。实现假名更换的机制有混合区域和路径混淆。

2.2.1 基于混合区域的方法

基于混合区域的方法是协调多个用户在特定的空间区域同步更换假名,使攻击者无法确定新假名和旧假名的映射关系,以保护用户的完整轨迹。图1是典型的混合区域模型,用户{a,b,c}进入混合区域,并停止所有通信,离开混合区域时,使用新假名{r,s,t}发送数据包^[20]。攻击者不能确定{a,b,c}和{r,s,t}之间的关联,则用户的完整轨迹得到了保护。

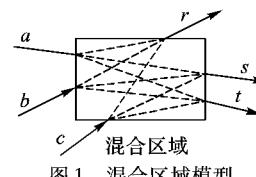


图1 混合区域模型

Fig. 1 Mix-zone model

直观上,车辆密度越高,攻击者越不能确定新假名和旧假名的映射关系,因而研究者提出在十字路口、大型商场的免费停车场等社会热点区域部署混合区域^[8]。

但基于社会热点区域的方案缺乏灵活性,且攻击者会针对某混合区域采取攻击手段,因而研究人员提出了动态混合区域模型^[21-22],由用户根据邻居车辆密度情况,通过协作构造混合区域。此类方法的有效性依赖于同步更换假名的用户数量。在假名机制中引入信誉机制可激励用户参与假名更换^[9],通过同步多个混合区域可摆脱对车辆密度的依赖,增强更换假名的灵活性^[10]。

假名更换会影响安全应用的性能,为解决此问题,一方面可选择车辆并线、变道、低速行驶等作为假名更换的时机^[23-24],另一方面可利用加密技术保持用户间的通信^[8,25]。

在抗攻击性研究方面,文献[26]形式化分析了直接将理论的矩形混合区域应用于路网的弱点,主张通过仔细考虑区域的几何学、用户的统计行为、用户移动模式的空间限制、位置暴露的时间和空间分辨率等多种因素,构建有效的混合区域,并提出了构建抗攻击能力更强的非矩形混合区域的方法;文献[27]讨论了基于辅助信息的真实身份揭露和轨迹追踪攻击,建议通过使用多个混合区域抵抗基于辅助信息的推理攻击,提出了将部署多个混合区域的问题转化为成本约束优化问题的数学模型,并考虑了交通密度的影响,提出了两个启发式算法以战略性地选择混合区域位置,从而降低了用户轨



迹的隐私威胁;文献[28]描述和分析了基于查询关联的攻击对匿名性的影响,提出了延迟容忍的混合区域框架。

总体来讲,设计适用于车联网的混合区域需充分考虑灵活性、对安全应用性能的影响和抗攻击的能力,这是仍具有挑战性的问题。

2.2.2 基于路径混淆的方法

基于路径混淆的方法是在至少有两个用户的物理位置邻近时,通过用户间的交互,在用户真实位置上添加噪声使他们的路径出现交叉点,并更换假名,以增加攻击者追踪用户的难度^[11]。

位置数据噪声必然会影响服务质量,为此,文献[11]定义了期望距离误差和平均位置错误,分别用于量化攻击者准确估计用户位置的能力和用户获得的服务质量,从而将路径交叉问题公式化为约束非线性优化问题,实现在满足给定的服务质量需求时,最大化位置隐私保护强度。

文献[12]提出了集中式的路径混淆方法,由可信匿名器根据历史数据预测用户的移动,并使每个新预测的路径与其他用户的路径相交。攻击者只能看到一系列交叉的路径,很难准确地追踪用户。

以上工作未探讨基于用户移动模型和家庭住址信息等知识的移动预测攻击。整体上,路径混淆机制的隐私保护能力不如混合区域机制。

2.3 基于轨迹加密的轨迹隐私保护方法

轨迹加密模型利用密码学加密用户的真实位置,使其对服务器及其他实体完全不可见,从而保护轨迹隐私,实现技术有 PIR 协议^[29]和空间转换。

2.3.1 基于 PIR 协议的方法

PIR 协议是数据库检索领域的密码学原语,目标是实现数据库服务器在不知道用户提交的查询信息的情况下,仍然能够完成查询,因此,若将 PIR 协议应用于 LBS,能够获得攻击者对用户的查询信息一无所知的强隐私保护。

基于 PIR 协议的方法处理 LBS 查询服务的流程是:移动客户端依照 PIR 协议加密包含位置数据的查询信息,集成了 PIR 服务端的 LBS 服务器在不知道用户的位置数据的情况下检索数据库,并返回查询结果。

PIR 协议支持的数据访问模式是从一个二值数据库上查询某一个二进制位或块,通常需要针对特定的空间查询方式设计 LBS 服务器端的数据库和索引结构,并进行性能优化。

已有的基于 PIR 协议的轨迹隐私保护研究工作主要包括最短路径计算^[13,30]和最近邻查询^[14,31–32]。

1) 基于 PIR 协议的最短路径计算。

最短路径计算是车联网中常用的查询之一,需要用户提供始发地和目的地信息。若这些信息不受保护,攻击者很容易推断出用户的社会活动等敏感信息。

文献[13]首次将 PIR 协议应用于最短路径计算,基于提出的具有最低空间代价和可管理查询处理代价等特征的简略索引机制,实现了性能合理的强隐私保护,但时间和空间消耗仍明显高于不受保护的查询处理。

文献[30]提出了压缩下一跳路由矩阵的新方法,结合对称 PIR 协议,得到了完全隐私的高效城市街道实时导航协议。

2) 基于 PIR 协议的最近邻查询。

文献[31]最先将 PIR 协议的理论工作应用于近似最近邻查询和精确最近邻查询,实现了抗关联攻击的可证明的强隐私保证。近似最近邻查询方案包含离线阶段和响应查询阶段。离线阶段:LBS 服务器生成所有兴趣点(Point Of Interest, POI)的 kd (k -dimensional)-树索引,并将空间划分成多个区域。响应查询阶段:LBS 服务器将划分的区域发送给用户;查询用户使用 PIR 协议将自己所在的区域发送给 LBS 服务器;LBS 服务器在不知道查询用户所在区域的情况下,完成查询处理,将得到的加密查询结果返回给查询用户;查询用户解密 LBS 服务器返回的查询结果,得到最近邻 POI。通过利用 Voronoi 图划分空间区域,实现了精确最近邻查询。

AHG(Aggregate Hilbert Grid)^[32]是基于安全硬件辅助的 PIR 协议的 K 最近邻(K Nearest Neighbor, KNN)查询方法。AHG 将一个 KNN 查询分解成一系列的数据库块检索。每个数据块检索由安全硬件 PIR 执行,以防止 LBS 服务器识别出数据块,并且,所有查询遵循一个混淆块访问模式的通用查询规划,实现了查询不可区分的强隐私保护。

文献[14]提出的基于安全硬件辅助的 PIR 协议的隐私保护 KNN 查询方法,考虑了道路网络因素,通过为任意 K 设计固定的查询计划,以提供强隐私保护。

在连续查询中,用户需要执行多次 PIR 访问才能获得查询结果,而不同的位置对应的查询结果或 PIR 访问次数存在差异。例如,不同的起点或终点,计算得到的最短路径包含的边数不同,那么查询结果的大小或查询处理过程中数据访问的次数就不同,因此,应避免攻击者利用这些信息推断出用户的轨迹隐私。

虽然基于 PIR 协议的隐私保护研究成果已取得了合理的检索时间,但仍然比不受保护的磁盘读取慢很多。另外,基于 PIR 协议的隐私保护方法要求客户端和 LBS 服务器支持 PIR 协议,可能产生客户端和 LBS 服务器负担不起的高计算与通信开销,并且 PIR 构件具有限制条件,如支持的文件规模是有限的。

2.3.2 基于空间转换的方法

基于空间转换的方法使用空间填充曲线将 2-D 的空间数据和查询用户的位置数据转换到 1-D 空间。LBS 服务器存储转换的空间数据,并根据转换的查询用户的位置数据在转换的空间数据库中完成查询处理。由于转换过程是单向的,LBS 服务器不能根据 1-D 的位置数据得到 2-D 的位置数据,则轨迹隐私受到了保护。

空间转换方法在最近邻查询的位置隐私保护中得到应用,可行的方法应满足:空间转换函数具有单向函数的特性,使空间转换是计算安全的,以防止转换后的数据被不可信实体恶意使用;保持原始空间数据的邻近性,以保证查询结果的准确性;在转换的空间数据库中执行查询的效率要能满足用户的需求。

Hilbert 曲线具有很好的距离保持特性和聚类特性,且在计算上,不知道曲线参数(包括曲线的起始点、曲线方向、曲线结束和曲线缩放因子)的实体不能通过组合参数发现正确的曲线,因此,Hilbert 曲线是空间转换的有效工具。

通常在 2-D 空间中邻近的点在 Hilbert 曲线上仍然是邻近的,但由于遗漏边的性质,也会出现离得远的情况;另外,由于 Hilbert 曲线是对原始空间的降维,导致用户在转换空间的



最近邻数量少于在原始空间的最近邻数量。基于双 Hilbert 曲线的查询解析技术^[33]可减少遗漏边和降维对查询精度的影响,但仍不能返回精准的最近邻。

基于标准 Hilbert 曲线的空间转换仍保持了兴趣点的分布特征,即相同或相近 Hilbert 值的数量与未转换空间中兴趣点的密度正相关,则增加了隐私泄露的风险。

为抵抗基于兴趣点分布知识的攻击,文献[15]提出了联合加密哈希函数与双 Hilbert 曲线的隐私保护机制,实现了更加严格的隐私保护;文献[16]提出了根据空间区域内兴趣点分布密度而自动调整曲线参数的自适应 Hilbert 曲线(Adaptive Hilbert Curve, AHC)。基于 AHC 的空间转换方法,也避免了使用标准 Hilbert 曲线转换空间时需要多次调整曲线参数,且可支持数据拥有者对空间区域的自定义授权。

但在道路网络环境下,兴趣点是沿道路分布的,用户的行驶状态(方向和轨迹)受限于道路网络,则利用 Hilbert 曲线转换兴趣点和查询点对象的方法很难保持原始道路网空间中对象之间的邻近关系。如图 2 所示,查询用户 u_1 的 Hilbert 值为 1,兴趣点 p_1 和 p_2 的 Hilbert 值分别为 5 和 12,在转换空间中, u_1 和 p_1 更近,但实际上 u_1 和 p_2 更近,因此有待进一步研究如

表 1 车联网轨迹隐私保护方案比较
Tab. 1 Comparison of trajectory privacy protection schemes in vehicular network

代表性工作	类别	方法	体系结构	隐私保护度	抗攻击性			服务质量	复杂度
					MF 攻击	QAI 攻击	VDP 攻击		
文献[3]	轨迹模糊	基于真实用户轨迹的方法	集中式	高;取决于匿名集的大小和用户分布	✓	✓	✓	准确查询	时间复杂度 $O(k)$, k 是匿名度
文献[6]		基于哑元轨迹的方法	集中式	高;取决于匿名集的大小、用户分布和合理性	✓	✓	✓	准确查询	时间复杂度 $O(mk)$, m 是位置更新数, k 是匿名度
文献[10]	假名更换	基于混合区域的方法	分布式	高;取决于混合区域的用户数和群签名的安全性	✓	✗	✓	准确查询	时间复杂度 $O(k)$, k 是混合区域的用户数
文献[11]		基于路径混淆的方法	分布式	低;与假名更换次数及同步更换假名的用户数相关	✗	✗	✓	近似查询	时间复杂度 $O(kn^3)$, k 为匿名度, n 为假名更换次数
文献[13]	轨迹加密	基于 PIR 协议的方法	分布式	高;取决于 PIR 协议的安全性	✓	✓	✓	准确查询	计算复杂度 $O(n)$, n 是数据集大小
文献[16]		基于空间转换的方法	分布式	高;取决于转换函数的安全性	✓	✓	✓	近似查询	计算复杂度 $O(\log_4 n)$, n 是兴趣点数量

由表 1 可知,整体上,基于加密思想的 PIR 协议和空间转换方法的隐私保护强度高,但复杂度高,而其他轨迹隐私保护方法较好地平衡了隐私保护度、服务质量与复杂度。在实际应用中,应综合考虑轨迹隐私保护方法的特性、应用场景的特征和用户的隐私需求,以选择合适的轨迹隐私保护方法。

4 研究展望

尽管学术界已提出了许多有效的车联网轨迹隐私保护方法,但车联网是一个复杂的信息网络,对车联网的认知还在不断深入,车联网轨迹隐私保护研究仍存在挑战:

1) 基于车辆移动的社会性特征和规律的轨迹隐私保护方法研究。

由于车辆是由人控制的,因此车辆的移动不是随机的,而是与驾驶员/乘客的行车习惯和社会关系等有关,具有车辆停留、最短路径驾驶、趋向社会热点、场景多样化等社会性特性和规律。而传统的轨迹隐私保护方法未充分考虑这些特征,在鲁棒性方面存在脆弱性,例如,若攻击者拥有分辨哑轨迹和

何获取准确的查询结果。

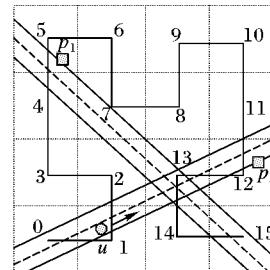


图 2 Hilbert 曲线填充路网空间
Fig. 2 Hilbert curve filling road network space

3 车联网轨迹隐私保护方法总结

轨迹隐私保护是车联网研究领域的一项重要内容,本文综述了学者针对不同的应用场景和系统目标而提出的基于真实用户轨迹的方法、基于哑元轨迹的方法、基于混合区域的方法、基于路径混淆的方法、基于 PIR 协议的方法和基于空间转换的方法等 6 类方法。表 1 总结了代表性工作在体系结构、隐私保护度、抗攻击性、服务质量与复杂度等方面的特征。

用户真实轨迹的知识,则会削弱方法的隐私保护能力,因此基于车辆移动的社会性特征和规律的车联网轨迹隐私保护方法研究极具意义。

2) 对背景知识不敏感的车联网轨迹隐私保护方法研究。

由于车辆的移动具有高度可预测性,则攻击者极可能利用路网拓扑图、交通状况等背景知识推断用户的位置,进而持续追踪用户。目前考虑位置推断攻击的车联网轨迹隐私保护方法都是基于对攻击者拥有的背景知识的假设,那么当攻击者拥有新的背景知识时,隐私保护方法可能变得无效,因此需深入探索对背景知识不敏感的车联网轨迹隐私保护方法。

3) 车联网轨迹隐私保护方法度量机制研究。

目前,在车联网轨迹隐私保护方法评估方面缺少系统化的动态度量机制,一方面尽管研究者提出了一些度量指标,但这些指标往往是针对特定的隐私保护方法、攻击模型或隐私威胁等,没有统一的量化标准,另一方面车联网上下文环境(如用户密度和道路拓扑)具有动态性,静态的单一度量指标不能客观地刻画隐私保护方法的性能。



车联网轨迹隐私保护方法度量机制对于车联网轨迹隐私保护方法的发展有重要作用。依据度量机制评估隐私保护方法的性能,一方面能够比较不同隐私保护方法的性能,为特定的场景和应用选择合适的隐私保护方法,另一方面能够为分析和确定影响轨迹隐私保护性能的关键因素提供参考,为隐私保护方法的改进提供指导性建议。

5 结语

轨迹隐私保护研究对于车联网的落地至关重要,但车联网的节点高速移动、短暂停性通信、节点移动高度可预测、社会性等特性,使得传统的轨迹隐私保护方法不适用于车联网。为此,本文在介绍车联网轨迹隐私保护的关键问题的基础上,从方法思想、科学问题、方法演进等方面详细分类综述了现有主要研究成果,并总结了具有代表性的车联网轨迹隐私保护方案的特点,最后展望了未来的研究方向。

参考文献 (References)

- [1] 陈宇峰,向郑涛,董亚波,等.车联网建模和统计性质分析及其路由策略综述[J].计算机应用,2015,35(12):3321–3324.(CHEN Y F, XIANG Z T, DONG Y B, et al. Review of modeling, statistical properties analysis and routing strategies optimization in Internet of vehicles [J]. Journal of Computer Applications, 2015, 35(12): 3321 – 3324.)
- [2] LU R. Security and privacy preservation in vehicular social networks [D]. Waterloo: University of Waterloo, 2012: 18 – 28.
- [3] WANG Y, XIA Y, HOU J, et al. A fast privacy-preserving framework for continuous location-based queries in road networks [J]. Journal of Network and Computer Applications, 2015, 53(7): 57 – 73.
- [4] SONG D, PARK K. A privacy-preserving location-based system for continuous spatial queries [J/OL]. Mobile Information Systems, 2016, 2016: 1 – 9 [2016-09-25]. <http://dx.doi.org/10.1155/2016/6182769>.
- [5] KIDO H, YANAGISAWA Y, SATOH T. An anonymous communication technique using dummies for location-based services [C]// Proceeding of the 21st International Conference on Data Engineering Workshops. Piscataway, NJ: IEEE, 2005: 88 – 97.
- [6] TRAN M T, ECHIZEN I, DUONG A D. Binomial-mix-based location anonymizer system with global dummy generation to preserve user location privacy in location-based services [C]// Proceedings of the 2010 International Conference on Availability, Reliability, and Security. Piscataway, NJ: IEEE, 2010: 580 – 585.
- [7] HARA T, SUZUKI A, IWATA M, et al. Dummy-based user location anonymization under real-world constraints [J]. IEEE Access, 2016, 4: 673 – 687.
- [8] LU R, LIN X, LIUAN T H, et al. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs [J]. IEEE Transactions on Vehicular Technology, 2012, 61(1): 86 – 96.
- [9] YING B, MAKRAKIS D. Reputation-based pseudonym change for location privacy in vehicular networks [C]// Proceedings of the 2015 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2015: 7041 – 7046.
- [10] YU R, KANG J, HUANG X, et al. MixGroup: accumulative pseudonym exchanging for location privacy preservation in vehicular social networks [J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 93 – 105.
- [11] HOH B, GRUTESER M. Protecting location privacy through path confusion [C]// Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. Piscataway, NJ: IEEE, 2005: 194 – 205.
- [12] MEYEROWITZ J, ROY CHOWDHURY R. Hiding stars with fireworks: location privacy through camouflage [C]// Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2009: 345 – 356.
- [13] MOURATIDIS K, YIU M L. Shortest path computation with no information leakage [J]. Proceedings of the VLDB Endowment, 2012, 5(8): 692 – 703.
- [14] WANG L, MA R, MENG X. Evaluating k nearest neighbor query on road networks with no information leakage [C]// WISE 2015: Proceedings of the 16th International Conference on Web Information Systems Engineering. Berlin: Springer, 2015: 508 – 521.
- [15] KHOSHGOZARAN A, SHIRANI-MEHR H, SHAHABI C. Blind evaluation of location based queries using space transformation to preserve location privacy [J]. GeoInformatica, 2013, 17(4): 599 – 634.
- [16] 田丰,桂小林,张学军,等.基于兴趣点分布的外包空间数据隐私保护方法[J].计算机学报,2014,37(1):123 – 138.(TIAN F, GUI X L, ZHANG X J, et al. Privacy-preserving approach for outsourced spatial data based on POI distribution [J]. Chinese Journal of Computers, 2014, 37(1): 123 – 138.)
- [17] 周长利,马春光,杨松涛.路网环境下保护 LBS 位置隐私的连续 KNN 查询方法[J].计算机研究与发展,2015,52(11):2628 – 2644.(ZHOU C L, MA C G, YANG S T. Location privacy-preserving method for LBS continuous KNN query in road networks [J]. Journal of Computer Research and Development, 2015, 52(11): 2628 – 2644.)
- [18] PENG T, LIU Q, WANG G. Enhanced location privacy preserving scheme in location-based services [J]. IEEE Systems Journal, 2014, 11(1): 219 – 230.
- [19] KATO R, IWATA M, HARA T, et al. User location anonymization method for wide distribution of dummies [C]// Proceedings of the 2013 International Conference on Database and Expert Systems Applications. Berlin: Springer, 2013: 259 – 273.
- [20] ATAEI M, KRAY C. Ephemerality is the new black: a novel perspective on location data management and location privacy in LBS [M]// Progress in Location-Based Services 2016. Berlin: Springer, 2017: 357 – 373.
- [21] SONG J H, WONG V W S, LEUNG V C M. Wireless location privacy protection in vehicular Ad-Hoc networks [J]. Mobile Networks and Applications, 2010, 15(1): 160 – 171.
- [22] HUANG L, MATSUURA K, YAMANE H, et al. Enhancing wireless location privacy using silent period [C]// Proceedings of the 2005 Wireless Communications and Networking Conference. Piscataway, NJ: IEEE, 2005: 1187 – 1192.
- [23] SAMPIGETHAYA K, LI M, HUANG L, et al. AMOEBA: robust location privacy scheme for VANET [J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8): 1569 – 1589.
- [24] BUTTYÁN L, HOLCZER T, WEIMERSKIRCH A, et al. SLOW: a practical pseudonym changing scheme for location privacy in VANETs [C]// Proceedings of the 2009 Vehicular Networking Conference. Piscataway, NJ: IEEE, 2009: 1 – 8.

(下转第 1942 页)



- ence and Technology, 2011: 88 – 104.)
- [4] 王若愚. 基于 SIFT 的数字水印算法研究 [D]. 武汉: 华中科技大学, 2011: 8 – 42. (WANG R Y. Research on digital watermarking algorithm based on SIFT [D]. Wuhan: Huazhong University of Science and Technology, 2011: 8 – 42.)
- [5] 张金利, 李敏, 何玉杰. 基于 SIFT 特征点和交比值的水印图像抗攻击算法 [J]. 通信学报, 2014, 35(11): 170 – 181. (ZHANG J L, LI M, HE Y J. Image watermarking algorithm against attacks based on SIFT feature point and cross-ratio value [J]. Journal on Communications, 2014, 35(11): 170 – 181.)
- [6] 高虎明, 李凯捷, 王英娟. 基于 SIFT 抗几何攻击的数字水印算法 [J]. 计算机应用, 2013, 33(3): 748 – 751. (GAO H M, LI K J, WANG Y J. Digital watermarking algorithm of anti-geometric attacks based on SIFT [J]. Journal of Computer Applications, 2013, 33(3): 748 – 751.)
- [7] 罗海军. 基于图像特征的抗几何攻击水印研究 [D]. 长沙: 湖南大学, 2011: 30 – 41. (LUO H J. Research on digital watermarking against geometric attacks based on image features [D]. Changsha: Hunan University, 2011: 30 – 41.)
- [8] SHUKLA D, SHARMA M. Video watermarking using dyadic filter and discrete wavelet transform [C]// WiSPNET 2016: Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking. Piscataway, NJ: IEEE, 2016: 1647 – 1650.
- [9] SHI Y J, QI M, YI Y, et al. Object based dual watermarking for video authentication [J]. Optik—International Journal for Light and Electron Optics, 2013, 124(19): 3827 – 3834.
- [10] 段加姣. 变换域双水印算法研究 [D]. 哈尔滨: 哈尔滨工业大学, 2015: 29 – 34. (DUAN J J. Research of the dual watermarking algorithm in transform domain [D]. Harbin: Harbin Institute of Technology, 2015: 29 – 34.)
- [11] 李智, 陈孝威. 基于内容自适应小波域鲁棒公开数字水印算法 [J]. 计算机应用, 2005, 25(9): 2148 – 2150. (LI Z, CHEN X W. Content-based adaptive robust public watermarking algorithm [J]. Journal of Computer Applications, 2005, 25(9): 2148 – 2150.)
- [12] 李智, 陈孝威. 基于熵模型的高透明性自适应视频水印算法 [J]. 软件学报, 2010, 21(7): 1692 – 1703. (LI Z, CHEN X W. Adaptively imperceptible video watermarking algorithm using entropy model [J]. Journal of Software, 2010, 21(7): 1692 – 1703.)
- [13] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91 – 110.

This work is partially supported by the National Natural Science Foundation of China (61462013, 61661010), Graduate Innovation Funds of Guizhou University (Research Engineering 2017079).

CHEN Shuqin, born in 1993, M. S. candidate. Her research interests include multimedia, information hiding, intelligent computing.

LI Zhi, born in 1977, Ph. D., associate professor. Her research interests include multimedia, information hiding, intelligent computing.

CHENG Xinyu, born in 1978, M. S. candidate, associate professor. His research interests include artificial intelligence, graphics and image.

GAO Qi, born in 1992, M. S. candidate. His research interests include multimedia, information hiding, virtual reality.

(上接第 1925 页)

- [25] SCHEUER F, FUCHS K P, FEDERRATH H. A safety-preserving mix zone for VANETs [M]// Trust, Privacy and Security in Digital Business. Berlin: Springer, 2011: 37 – 48.
- [26] PALANISAMY B, LIU L. MobiMix: protecting location privacy with mix-zones over road networks [C]// Proceedings of the 2011 International Conference on Data Engineering. Piscataway, NJ: IEEE, 2011: 494 – 505.
- [27] LIU X, ZHAO H, PAN M, et al. Traffic-aware multiple mix zone placement for protecting location privacy [C]// Proceedings of the 31st Annual IEEE International Conference on Computer Communications. Piscataway, NJ: IEEE, 2012: 972 – 980.
- [28] PALANISAMY B, LIU L, LEE K, et al. Anonymizing continuous queries with delay-tolerant mix-zones over road networks [J]. Distributed and Parallel Databases, 2014, 32(1): 91 – 118.
- [29] CHOR B, KUSHLEVITZ E, GOLDREICH O, et al. Private information retrieval [J]. Journal of the ACM, 1998, 45(6): 965 – 981.
- [30] WU D J, ZIMMERMAN J, PLANUL J, et al. Privacy-preserving shortest path computation [EB/OL]. (2016-01-10) [2017-01-25]. <http://arxiv.org/abs/1601.02281>.
- [31] GHINITA G, KALNIS P, KHOSHGOZARAN A, et al. Private queries in location based services: anonymizers are not necessary [C]// Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2008: 121 – 132.
- [32] PAPADOPOULOS S, BAKIRAS S, PAPADIAS D. Nearest neighbor search with strong location privacy [J]. Proceedings of the VLDB Endowment, 2010, 3(1/2): 619 – 629.
- [33] KHOSHGOZARAN A, SHAHABI C. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy [C]// Proceedings of the 2007 International Symposium on Spatial and Temporal Databases. Berlin: Springer, 2007: 239 – 257.

This work is partially supported by the National Key Technology R&D Program during the Twelfth Five-year Plan Period (2015BAG13B01), the Prospective Joint Research Project of Jiangsu Province (BY2014038-03).

ZHANG Chunhua, born 1989, Ph. D. candidate. Her research interests include information security, privacy protection.

ZANG Haijuan, born in 1965, Ph. D., associate professor. Her research interests include network and information security.

XUE Xiaoping, born in 1963, Ph. D., professor. His research interests include trusted computing, information security.

ZHANG Fang, born in 1971, Ph. D., lecturer. Her research interests include trusted computing.

CHEN Kangqiang, born in 1992, M. S. candidate. His research interests include VANET privacy and security.

FENG Lijuan, born in 1994, M. S. candidate. Her research interests include VANET security and privacy.