车联网隐私保护技术研究

李瑞琴[1], 胡晓雅[1], 张倨源[1], 王励成[1]

[1]北京邮电大学信息安全中心 网络与交换技术国家重点实验室 北京 中国 100876

摘要 随着汽车智能化、网联化程度的不断加深, 车辆、用户及第三方机构之间的数据共享日益成为刚需, 由车辆、用户、路边单元等通信实体之间构建的网络车联网应运而生, 而车联网的高移动性和网络拓扑多变性使其更容易遭受攻击, 进而导致严重的车联网用户隐私泄露问题。如何平衡数据共享和隐私保护之间的关系成为车联网产业发展所面临的一个关键挑战。近年来, 学术界针对车联网隐私保护问题进行了深入的研究, 并提出了一系列解决方案, 然而, 目前缺少对这些方案从隐私属性方面进行分析。为此, 本文首先从车联网的系统架构、通信场景及标准进行阐述。然后对车联网隐私保护的需求、攻击模型及隐私度量方法进行分析与总结。在此基础上从车联网身份隐私、匿名认证位置隐私和车联网位置服务隐私三个方面出发, 介绍了匿名认证、假名变更、同态加密、不经意传输等技术对保护车联网用户隐私起到的重要作用, 并讨论了方案的基本原理及代表性实现方法, 将方案的隐私性从不可链接性、假名性、匿名性、不可检测性、不可观察性几个方面进行了分析与总结。最后探讨了车联网隐私保护技术当前面临的挑战及进一步研究方向, 并提出了去中心化的车辆身份隐私技术以保护车辆身份隐私、自适应假名变更技术以支持匿名认证、满足个性化隐私需求的位置服务隐私保护技术, 以期望进一步推动车联网隐私保护技术研究的发展与应用。

关键词 隐私保护; 车联网; 匿名认证; 假名变更; 位置服务

中图法分类号 TP309.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.03.01

Research on Privacy Protection Technology of IoV

LI Ruiqin[1], HU Xiaoya[1], ZHANG Juyuan[1], WANG Licheng[1]

[1] Department of Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract With the deepening of vehicle intelligence and network connectivity, data sharing among vehicles, users, and third-party organizations have become an urgent need, and the Internet of Vehicles built by vehicles, users, roadside units, and other communication entities has emerged, while the high mobility and network topology variability of the Internet of Vehicles makes it more vulnerable to attacks, which leads to serious privacy leakage problems of the Internet of Vehicles users. How to balance the relationship between data sharing and privacy protection has become a key challenge for the development of the Internet of Vehicles industry. In recent years, academics have conducted in-depth research on the privacy protection of the Internet of Vehicles and proposed a series of solutions. However, there is a lack of analysis of these schemes in terms of privacy properties. For this reason, this paper first describes the system architecture, communication scenarios, and standards of the Internet of Vehicles. Then the requirements, attack models, and privacy metrics of the Internet of Vehicles privacy protection are analyzed and summarized. And on this basis, from three aspects of the Internet of Vehicles identity privacy, anonymous authentication location privacy and Internet of Vehicles location service privacy, we introduce the important role played by anonymous authentication, pseudonym change, homomorphic encryption, inadvertent transmission, and other techniques to protect the privacy of the Internet of Vehicles users. The basic principles and representative implementation methods of the scheme are also discussed, and the privacy of the scheme is analyzed and summarized in terms of unlinkability, pseudonymity, anonymity, undetectability, and unobservability. Finally, the current challenges and further research directions of the Internet of Vehicles privacy protection technology are discussed, and decentralized vehicle identity privacy technology to protect vehicle identity privacy, adaptive pseudonym change technology to support anonymous authentication, and location service privacy protection technology to meet personalized privacy needs are proposed in the hope of further promoting the development and application of Internet of Vehicles privacy protection technology research.

Key words privacy protection; internet of vehicles; anonymous authentication; pseudonym change; LBS

通讯作者: 王励成, 博士, 教授, Email: wanglc2012@126.com。

本课题得到了国家重点研发计划(No. 2018YFE0126000)、国家自然科学基金(No. 61972050)资助。

收稿日期: 2022-05-10; 修改日期: 2022-08-28; 定稿日期: 2023-11-01

1 前言

车联网以车内网、车际网和车载移动互联网为基础, 通过新一代的通信技术, 实现车内、车与车、车与路、车与人、车与服务平台之间全方位的网络连接, 实现交通的智能化管理, 以及交通信息服务的智能决策和车辆的智能化控制, 进而实现“人-车-路-云”合为一体的新生态, 是物联网技术在交通系统领域的典型应用。华为将车联网的发展过程分为三个阶段[1]: 1996—2015 年的车载信息服务阶段, 在该阶段中车辆具备基本的联网能力, 通过 2G/3G/4G 通信实现紧急救援、导航、信息娱乐等服务; 2015—2025 年的智能网联汽车阶段, 在该阶段中利用 C-V2X 和 LTE-V 通信使得车路开始协同, 提供单车自动驾驶、共享出行、人-车智能互联等服务; 2025 年之后车联网的发展将会进入智慧出行阶段, 在该阶段中利用 5G 和 NR-V2X 通信实现协同式智能交通、协同式自动驾驶、高级自动驾驶等服务。

目前, 汽车智能化与网联化的实现必须以大量的数据作为基础。以特斯拉为例, 特斯拉配备了多种摄像头、毫米波雷达、激光雷达、卫星定位等感知设备, 能采集车主个人信息、车辆环境信息、车辆行驶信息、车主手机信息等在内的 200 多项信息, 而国内智能汽车厂商采集的信息也有 170 多项。当前许多组织针对如何保障车联网隐私数据不被泄露开展了大量研究, 并提出了车联网隐私保护方案。针对近年来车联网隐私保护的学术研究和工业发展情况, 研究人员分别从匿名认证 [2-3]、信任管理[2]、位置轨迹隐私[4]、假名变更[5]等方面进行了总结归纳。从车联网系统需要满足的安全属性出发, 介绍了对应的攻击方法以及应对这些攻击设计的解决方案, 并对这些方案进行了分类。但是文献都是从车联网架构中某一部分内容进行分析, 没有从车联网的整体架构进行分析。文献[6]介绍了车联网各层之间的联系以及组成部分, 分析了车联网的性质、对每层架构使用的隐私保护策略进行了详细介绍及分类。但是, 在做分层架构之前没有对现有车联网标准中的分层架构做介绍, 并且没有阐述隐私需求以及隐私度量方法。本文从国内车联网标准划分的车联网层次架构出发, 根据隐私保护需求以及隐私度量方法对车联网隐私保护技术进行了总结归纳, 重点关注车联网在车辆身份隐私、匿名认证位置隐私、位置服务隐私三个方面的隐私保护技术。车辆身份隐私就是防止系统在实现身份认证的过程中, 泄露车辆的真实身份信息。匿名认证位置隐私就是防止攻击者使用位置跟踪技术获取车辆在任意时间段的任意位置。位置服务隐私保护方案需要保护的信息有用户位置隐私、用户查询隐私以及服务提供商的兴趣点(Point of interests, POIs)隐私。为了方便不同背景的读者, 本文先对车联网进行了简单的介绍, 然后对现有车联网隐私保护技术进行了整理分类, 最后对车联网的研究方向进行展望。

2 车联网概述

本节将首先介绍了车联网的系统模型, 然后描述了车联网中的通信场景以及实现车联网通信的底层技术及标准。最后介绍了车联网所具有的特性以及车联网相关的应用。

2.1 系统模型

如图 1 所示, 车联网系统主要包含以下几个组成部分: 车载单元(On board unit, OBU)、路边单元(Road side unit, RSU)、可信机构(Trusted authority, TA)、证书颁发机构(Certificate authority, CA)以及服务提供商(Service provider, SP)。每辆车的 OBU 与传感器相连, 以获得传感器产生的数据, 也可与其他车辆的 OBU 和附近的 RSU 进行速度、位置等信息交换[7]; RSU 之间相互连接, 具有转发消息的功能, 可以使车辆连接到互联网; TA 负责车辆的身份注册, 信任管理等, 而 CA 负责颁发证书; SP 则向用户提供各种服务。各组成部分的详细介绍如下:

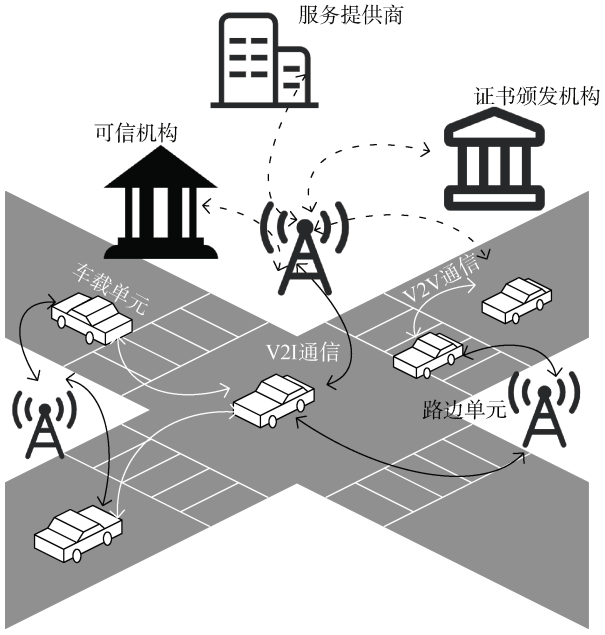

图 1 车联网系统模型

Figure 1 System model of Internet of Vehicles

(1) 车载单元: 每辆车都配备了 OBU 作为收发

器, 用于与其他车辆的 OBU 和 RSU 进行通信。OBU 由资源命令处理器、存储器、网络设备和传感器组成。全球定位系统、激光雷达、速度等传感器收集信息发送至 OBU, OBU 收到信息处理之后通过无线介质发送给相邻车辆或者 RSU。

(2) 路边单元: RSU 通常是指沿道路或专用位置(如十字路口、停车场)部署的固定基础设施, 具有数据运算、存储、转发等功能[8]。它主要采用专用短距离无线通信技术(Dedicated short range communication, DSRC)与 OBU 或其他 RSU 进行通信, 以扩大车联网的通信范围。

(3) 可信机构: TA 负责整个车联网的信任和安全管理, 包括验证车辆的真实性, 在车辆出现恶意行为(如广播虚假消息)的情况下将该车辆从可信列表中撤销[7]。因此, TA 需要具有较强的计算能力和足够的存储空间。

(4) 证书颁发机构: CA 是一个可信的第三方机构(Trusted third party, TTP), 它部署了基于公钥基础设施(Public key infrastructure, PKI)的假名认证系统, 为车联网提供具有安全性和隐私性的服务, 这些服务包括车辆注册、证书颁发、密钥对和假名集的提供、假名填充、凭证管理、行为不端检测、吊销证书等[9]。它和 TA 的主要区别是 TA 管理是针对车辆本身的管理, 而 CA 管理是针对车辆假名的管理。

(5) 服务提供商: 服务提供商通过基础设施向车辆用户提供服务, 这些服务包括位置服务、内容交付服务、互联网服务、智能交通系统(Intelligent transportation system, ITS)服务等。

2.2 通信场景及标准

车联网中的通信场景包含了车内通信、车云通信以及车与车、人、路基设施的通信。如图 2 所示, 车内通信是指将传感器、控制器、执行器等元件连接在一起, 使各元件之间进行数据交换, 适用于车内设备状态检测和车辆的运行控制, 最终建立起数字化的车辆内部系统。车云通信是指车载设备通过新一代的通信技术与云平台连接, 使云平台与车辆之间进行高效通信, 适用于导航、紧急救援和信息娱乐等场景。车与车通信是指车载终端无需通过基站转发, 彼此直接交换消息以实时获取周围车辆的车速、位置、行车情况等信息, 适用于自适应巡航、自动紧急刹车、盲区预警、前车防撞预警等场景。车与人通信是指行人或骑行者通过智能手机或笔记本与车辆进行通信, 适用于行人碰撞预警等场景。车与路通信是指车载设备与路基设施(如红绿灯、交通摄像头、路侧单元等)进行通信, 路基设施可以获取附近区域车辆的信息并发布各种实时信息, 适用于自动泊车、交通信号及标志牌识别、不停车收费、限速预警等场景。

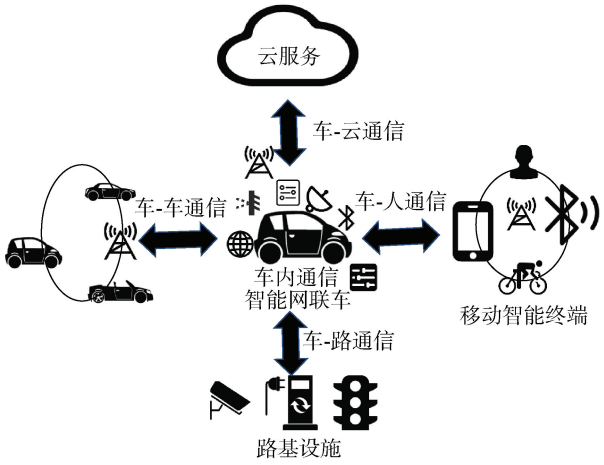

图 2 车联网通信场景

Figure 2 Communication scene of Internet of Vehicles

车联网依托新一代信息通信技术, 通过车辆与人、车辆与基础设施、车辆与云、车辆之间的信息交互, 形成汽车、电子、信息通信、道路运输等产业融合的产业格局, 为用户提供了安全、智能、高效的行车服务[10]。它对通信时延、可靠性和数据传输速率等方面有更高要求, 需要更先进的专用通信技术。目前主流的车联网通信技术标准主要有由美国、欧洲和日本自 20 世纪 90 年代开始研究开发的专用短距离无线通信技术 DSRC 和第三代合作伙伴计划(3rd generation partnership project, 3GPP)于 2015 年立项启动的基于蜂窝网络的车用无线通信技术(Cellular vehicle-to-everything, C-V2X)。

(1) 专用短距离无线通信技术: DSRC 也称 IEEE 802.11p 和 IEEE WAVE, 用作 V2V 和 V2I 的通信标准, 它是一种短距离通信协议, 支持多个需要低延迟和高数据速率的应用程序。它主要基于 IEEE 802.11p, IEEE 1609, SAE 三套标准, 包括了从物理层到应用层的操作以及跨层方面的安全保障和管理方法。IEEE 802.11p 是由 IEEE 标准组织修改了 802.11a 的物理层和 MAC 层使之成为汽车相关的 DSRC 物理标准。IEEE 1609 协议家族, 又称为 WAVE 协议定义了网络架构和流程, 它使用 WLAN 技术建立专用短程通信 DSRC 通道, 使车辆可以在中短程(通常为 300 m)范围内直接与其他实体通信[11], DSRC 系统网络架构如图 3 所示。此外, IEEE 还定义了车载移动通信网络(Vehicular ad hoc network, VANET)中的体系结构、通信模型、管理结构、安全性和物理访问从而构成了一个完整的协议栈, 如图 4 所示。

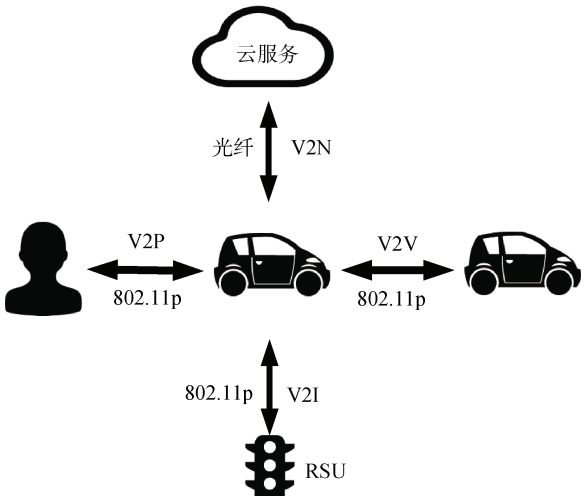

图 3 DSRC 系统网络架构

Figure 3 DSRC system network architecture

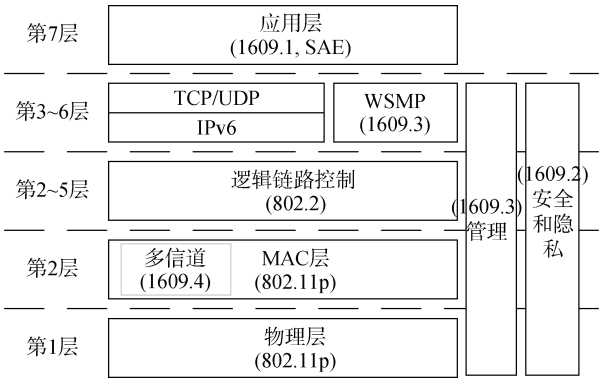

图 4 DSRC 协议栈

Figure 4 DSRC protocol stack

(2) 基于 LTE 的车联网无线通信技术: 基于 LTE 的车联网无线通信技术是基于 3GPP LTE-V/5G 底层通信和 CSAR 0053 应用标准的通信标准, 包含了 LTE-V2X 标准和 5G-V2X 标准, 是基于蜂窝网通信技术形成的车用无线通信技术, 所以又称 C-V2X 无线通信技术。我国工业和信息化部在《基于 LTE 的车联网无线通信技术 总体技术要求》中, 规定了基于 LTE 的车联网无线通信技术的总体业务要求、系统架构和基本功能需求, 将我国的车联网无线通信技术协议栈分为接入层、网络层和应用层。在《基于 LTE 的车联网无线通信技术 空中接口技术要求》中规定了车联网无线通信技术接入层相关技术要求, 其中定义了两种通信方式, 蜂窝式和直通式, 其中蜂窝式又称广域蜂窝式, 它提供了 Uu 接口, 即终端与基站之间的通信接口, 最终实现更大范围的可靠通信。直通式又称短程直通式, 它提供 PC5 接口, 目的是实现车、人、路之间的短距离通信。两种接口的共同作用可满足 V2X 业务的传输, 保证车辆的行驶安全; 在《基于 LTE 的车联网无线通信技术 网络层技术要求》中规定了车联网无线通信技术的网络层相关技术要求, 包括短消息协议、应用注册、业务管理以及业务公告等; 2016 年 CAICV 和 C-ITS 制定完成了中国第一个应用层规范《合作式智能运输系统车用通信系统应用层及应用数据交互标准》, 该标准规定了 5 个车-车、车-路等直接通信的消息定义和 ASN.1 编码文件, 包括: 基础安全消息、路侧安全消息、路侧消息、交通灯相位与时序消息和地图消息。随后, CCSA 和 C-ITS 在 C-V2X 标准体系下, 以上述标准为基础, 制定了《基于 LTE 的车联网无线通信技术 消息层技术要求》, 它包括了消息层数据集的架构以及具体的数据定义和编码方式等。此外, 我国工业和信息化部还发布了与车联网的相关标准, 具体如表 1 所示。对我国的车联网相关标准进行了进一步增强和完善, C-V2X 系统网络架构如图 5 所示, C-V2X 协议栈如图 6 所示。

表 1 车联网相关标准列表

Table 1 List of standards related to the Internet of Vehicles

标准分类	标准号	标准名称	标准组织
总体技术要求规范	YD/T 3400-2018	基于 LTE 的车联网无线通信技术 总体技术要求	CCSA/TC485
接入层协议	YD/T 3340-2018	基于 LTE 的车联网无线通信技术 空中接口技术要求	CCSA/TC485
	YD/T 3592-2019	基于 LTE 的车联网无线通信技术 基站设备技术要求	CCSA
	YD/T 3629-2020	基于 LTE 的车联网无线通信技术 基站设备测试方法	CCSA
	YD/T 3593-2019	基于 LTE 的车联网无线通信技术 核心网设备技术要求	CCSA
	YD/T 3847-2021	基于 LTE 的车联网无线通信技术 支持直连通信的路侧设备测试方法	CCSA
	YD/T 3848-2021	基于 LTE 的车联网无线通信技术 支持直连通信的车载终端设备测试方法	CCSA
网络层协议	YD/T 3707-2020	基于 LTE 的车联网无线通信技术 网络层技术要求	CCSA
	YD/T 3708-2020	基于 LTE 的车联网无线通信技术 网络层测试方法	CCSA
应用层协议	YD/T 3709-2020	基于 LTE 的车联网无线通信技术 消息层技术要求	CCSA
	YD/T 3710-2020	基于 LTE 的车联网无线通信技术 消息层测试方法	CCSA
	YD/T 4008-2022	基于 LTE 的车联网无线通信技术 应用标识分配及映射	CCSA

续表

标准分类	标准号	标准名称	标准组织
安全标准	YD/T 3594-2019	基于 LTE 的车联网通信安全技术要求	CCSA
	YD/T 3746-2020	车联网信息服务 用户个人信息保护要求	CCSA
	YD/T 3750-2020	车联网无线通信安全技术指南	CCSA
	YD/T 3751-2020	车联网信息服务 数据安全技术要求	CCSA
	YD/T 3752-2020	车联网信息服务平台安全防护技术要求	CCSA
	YD/T 3957-2021	基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求	CCSA/TC485

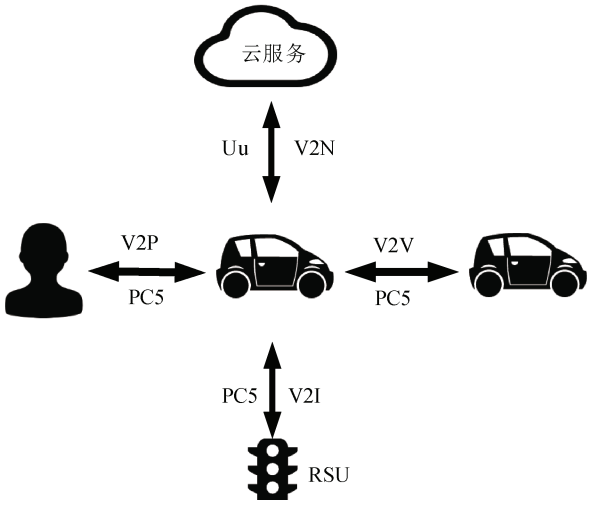

图 5 C-V2X 系统网络架构

Figure 5 C-V2X system network architecture

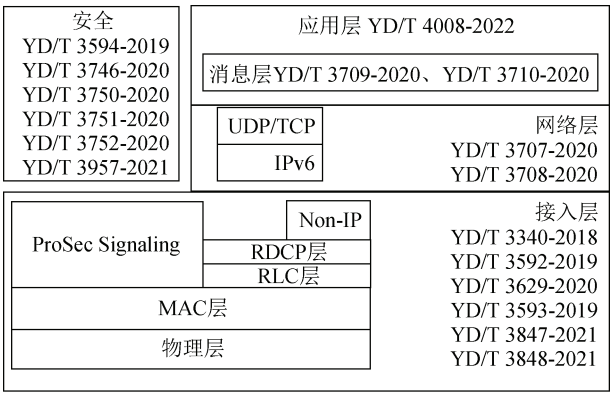

图 6 C-V2X 协议栈

Figure 6 C-V2X protocol stack

2.3 车联网的特性

在车联网中, 车辆作为移动通信设备和用户的载体, 以拓扑节点的形式组织移动网络拓扑, 它具有以下几个特性:

(1) 车辆节点的高移动性: 虽然车辆的移动会受到公路拓扑的限制, 但是由于车辆节点都是高速移动的, 导致车联网非常容易受到攻击且不易发现恶意节点, 在通信时间方面也会受到限制[2]。

(2) 信息传递的低时延性: 车联网中安全相关的应用允许的时延很小。因此, 车联网传递的信息必须在特定时间范围内到达车辆节点以便车辆节点能及时做出决策并采取相应对策。

(3) 网络密度的高动态性: 由于车辆节点的高速移动, 导致网络拓扑多变[2], 动态的网络拓扑、恶劣天气和车辆的高密度都会导致车辆节点频繁与网络断开连接, 导致网络密度在时间和空间上发生变化。

(4) 数据收集的全方位性: 要实现车辆的智能化、网联化, 需要车辆对车内外的信息进行分析, 帮助驾驶人员更安全舒适的出行。因此, 它需要车辆传感器收集的信息也更加多样化。

2.4 车联网的应用

车联网具有广阔的应用前景和商业价值, 车联网所能提供的主要应用可以归为两类:

(1) 安全应用: 安全应用依赖于车辆、道路以及其他交通参与要素的实时状态共享, 在充分利用 C-V2X 信息交互实现状态共享的基础上, 辅助驾驶员进行自主决策, 来提高驾驶安全以及道路通行效率[5]。如前方静止车辆告警、紧急电子刹车灯告警、碰撞预警、行人横穿预警等。

(2) 娱乐应用: 娱乐应用通过向司机或乘客提供天气、交通信息、最近的餐馆、加油站、酒店的位置及其价格等服务类信息, 来提高驾驶员和乘客的舒适度并提高交通效率[5], 如网络游戏、在线视频、数据下载、位置服务、本地电子支付等。

3 隐私保护需求与攻击模型

如果不能很好地保证用户的隐私, 用户对这个产品就不会产生信任, 那么该产品就无法进行推广使用。本节首先介绍了车联网的隐私保护需求, 然后根据不同划分方法对车联网中的敌手模型进行介绍。最后介绍了攻击车联网的常见攻击方法。

3.1 隐私保护需求

由于车辆与车主的出行位置、工作地点、行为偏好紧密联系, 车联网环境下用户隐私的泄露将会威胁到车主的财产甚至生命安全。在标准《基于 LTE

的车联网无线通信技术 安全证书管理系统技术要求》中提出车联网消息安全需求有机密性、完整性、身份认证、隐私保护。要有效保护车辆用户的隐私, 除了上述基本的安全需求外, 还需要满足隐私保护需求, 本文根据 Deng 等人[12]提出的 LINDDUN 模型的隐私分析方法, 结合车联网的实际情况, 本文提出在车联网场景下, 还需要满足以下隐私需求:

(1) 不可链接性: 在车联网身份认证中, 指攻击者无法链接真实身份与假名、假名与假名之间的关系; 在车联网位置服务中, 指攻击者无法链接用户与 POI 之间的关系[5]。

(2) 假名性: 指车联网各个实体之间进行数据交换所使用的身份标识不是其真实身份信息。目的是保护车联网实体的身份信息。

(3) 匿名性: 指系统可以隐藏身份与动作或信息之间的连接, 当消息被发送时, 该消息的发送者在其他潜在发送者集合内保持匿名[13]。对于身份隐私, 匿名性是指攻击者从假名集合里面判断用户的假名信息; 对于位置隐私, 攻击者无法从位置集合里面判断用户的真实位置; 对于位置服务, 匿名性指攻击者无法从查询内容集合里面找到真正的用户查询内容。

(4) 不可检测性和不可观察性: 不可检测性和不可链接性与匿名性之间的区别在于后者保护的是车联网实体与信息之间的关系, 而不可检测性还保护信息, 比如, 在车联网位置服务中, 若对传输的消息做了加密, 那就满足不可检测性, 若加密信息具有匿名性, 那就满足不可观察性。

(5) 内容有意识性: 用户会向服务提供商提供过多的信息, 这可能会导致其对个人信息的控制, 内容有意识性可以确保用户了解他们共享的数据是什么。即用户在访问相关服务之前, 系统应告知用户系统会采集的数据内容、数据用途、数据保护策略, 让用户选择同意。

(6) 隐私合规性: 服务提供商在收集车联网实体信息时, 应该要满足数据最小化以及最小泄露原则, 即用户在通信中泄露的信息应该保持在最小限度, 即不超过应用程序正常功能所需的信息; 车联网在采集数据时应当遵循数据最小化原则, 即只收集和保留为了达到合法商业目的所需的最少数据。

3.2 隐私攻击

近年来, 车联网安全事件频发, 且安全威胁逐步升级, 攻击者采用不正当手段对网络架构进行攻击, 恶意破坏系统的正常运行, 车联网的敌手模型可以分为以下几类[5]:

(1) 从攻击角度进行划分, 可以将其分为内部攻击和外部攻击。内部攻击者是车联网中经过身份验证的成员, 能够对网络进行多次严重攻击; 外部攻击者通常没有合法身份, 其通过伪装或窃听攻击网络。

(2) 从攻击方式进行划分, 可以将其分为主动攻击和被动攻击。主动攻击者可以更改删除消息或将生成的恶意数据注入网络从而影响网络的正常通信和操作; 被动攻击者一般不影响网络的正常通信, 通过监听或窃取消息获取车辆用户信息。

(3) 从攻击目的进行划分, 可以将其分为理性攻击和恶意攻击。理性攻击是指攻击者为自身利益发起攻击, 如散布错误道路信息误导其他车辆从而方便自身驾驶; 恶意攻击是指攻击者为影响交通系统整体正常运转发起攻击, 对网络进行大肆破坏。两者相比, 恶意攻击者的产生的风险更大, 而理性攻击者的行为更容易预测。

(4) 从监听能力进行划分, 可以分为全局攻击者和局部攻击者。全局攻击者有良好的监听设备, 可以实现对整个网络通信状况进行监听。因此, 它可以对网络数据进行流量分析、时间关联分析、位置关联分析等结合的攻击方式。而局部攻击者的监听设备有限, 通常只能对一定范围内的局部网络进行监听。因此, 它倾向于使用逐跳回溯追踪等攻击。

根据隐私需求, 将相关的攻击方法进行了总结归纳, 如表 2 所示。由于内容有意识性、隐私合规性是服务提供商遵循一定数据采集、数据使用等政策提供数据保护, 最终目的是防止用户数据被非授权的实体非法利用, 主要靠服务提供商是否遵循相关协议。因此, 表中没涉及相关的攻击方法。

表 2 隐私需求、威胁、攻击方法映射表

Table 2 Mapping table of privacy requirements, threats, and attack methods

隐私需求	隐私威胁	攻击方法
不可链接性	可链接性	背景知识攻击[85]、链接攻击[37]、合谋攻击[44]等
假名性/匿名性	可识别性	假冒攻击[40]、身份泄露攻击[38]、位置跟踪攻击[2]等
不可检测性/不可观察性	可探测性	移查询关联攻击[13-14]、查询跟踪攻击[70]等
内容有意识性	内容无意识性	/
隐私合规性	隐私不合规	/

4 隐私度量

Asuquo 等人[15]调研了许多隐私度量方法。本文主要关注车联网中隐私保护技术中的隐私度量方法。

(1) 匿名集大小(Anonymity set size, ASS): 匿名集大小是评估匿名级别的良好指标。在论文[15]中指出, 匿名集大小统计可能为目标车辆 u 的数量, $|AS_u|$ 表示为目标车辆可以混合的区域大小, $Priv_{ASS} \equiv |AS_u|$。匿名集大小的主要缺点是, 它只取决于系统中的车辆数量, 没有考虑背景知识、敌手观察系统中收集的信息或者匿名集中每个成员成为目标的可能性[16-17]。因此, 匿名集大小与其他度量方法(如归一化熵)结合使用可以提供更好的隐私保障[18]。

(2) 熵(Entropy): 由于匿名集大小不能很好的度量隐私水平。因此, 研究人员利用信息熵来度量匿名通信系统中的匿名性。在评估位置隐私的时候可以使用位置熵来量化指标, 熵值越大说明攻击者的确定性越低, 车辆的位置隐私性越高, $\mathrm{Priv}_{ENT} = H(X) = -\sum_{i=1}^{N} p_i \log_2\left(p_{(i)}\right)$, N 表示匿名集合中的节点数, $p_{(i)}$ 表示根据对手的估计 i 成为目标节点的概率。

(3) K-匿名(K-Anonymity): K-匿名在概念上类似于匿名集的大小, 当用户的确切位置扩展到掩蔽区域, 使得每个区域至少覆盖 K 个用户时, 就实现了位置 K-匿名性。在位置 K-匿名中, 用户的隐私通过使用当前位置而不是历史位置进行保护。位置掩蔽策略 CliqueDope[19]、HilbertDope[20]、Casper[21]都提供了位置 K-匿名性。

(4) 掩蔽粒度(Cloaking granularity): 位置 K-匿名性保护用户的身份(K 个用户中的一个), 但它不阻止用户信息的泄露。因此, Pan 等人 [22]提出利用掩蔽粒度来度量位置隐私, 在掩蔽粒度中, 掩蔽区域的面积必须大于用户指定的阈值, 掩蔽粒度可以防止用户信息被泄露, 但当用户位置被公开时, 无法阻止用户受到与身份相关的攻击。

(5) 敌手成功率(Adversary's success rate): 敌手成功率用于衡量攻击者成功跟踪目标用户的概率。但是由于敌手的目的可能会因为兴趣的不同而发生变化。因此, 这种方法只适用于知道敌手实际搜索内容的情况。成功的敌手可以破坏通信信道或识别消息发送者[15]。

(6) 最大追踪时间(Maximum tracking time, MTT): 在位置隐私方面, 对手的目标不仅是在单个时间点破坏车辆隐私, 而且还会随着时间的推移跟踪目标的位置。攻击者的追踪能力通过最大追踪时间来衡量, 最大追踪时间定义为目标 u 的匿名集大小保持为 1 的累计时间[23]。该指标往往会高估目标的隐私, 因为它假设当敌手完全确定匿名集大小为 1 时才算成功。然而, 在现实中, 目标车辆的匿名集合中有少量非目标车辆, 敌手仍能够继续追踪。

(7) 平均混淆时间(Mean time to confusion): 为了避免最大跟踪时间高估隐私水平, 平均混淆时间指的是敌手的不确定性保持在混淆阈值 τ 以下的时间[24]。使用熵 $H(X)$ 测量对手的不确定性, 随机变量 X 表示攻击者猜测匿名集中的车辆为目标车辆的预期概率。

(8) 混淆区域的准确性(Accuracy of obfuscated region, AOR): 在基于位置的服务中, 用户会向服务提供商发送某个确定的区域来获取本地服务。为了保护自己的位置隐私, 用户在请求某区域的本地服务之前, 可以将这个区域扩大到满足用户最小需求的区域 $r_{\min}$。混淆区域的准确性表示所提交的区域与服务提供商所在区域的相关性, 值为 0 表示最低相关性或最高隐私级别。可根据所用的传感技术 r_{opt} 和用户指定的最小 $r_{\min}$ 提供的最佳精度计算该度量[25], 即 $Priv_{\mathrm{AOR}} \equiv \frac{r_{\mathrm{opt}}^2}{r_{\min}^2}$。

(9) 地理不可区分性(Geo-Indistinguishabilit y): 地理不可区分性将差分隐私扩展到位置隐私场景, 弥补了差分隐私对位置隐私保护的空缺[26]。

(10) d-χ-$Privacy$: d-χ-$Privacy$ 用来构造适应位置隐私领域特点的弹性度量, 比如兴趣点密度可能会影响地理不可区分性所期望的隐私水平: 在兴趣点较少的农村地区, 则需要比城市地区更大的半径才能达到相同的隐私水平[27]。

(11) 假名变更统计: 这可能包括有关已更改假名的信息, 例如成功的假名变更总数、假名关联总数。

5 车联网中的隐私保护技术

在标准《基于 LTE 的车联网通信安全技术要求》中指出, 在 PC5 和 Uu 通信中, V2X 设备都需要支持基于证书的应用层安全机制, 为保护用户隐私, V2X 可以在应用层进行假名处理。在实现通信安全过程中需要满足不可链接性、假名性、匿名性 3 种隐私属性, 而车联网信息服务平台需要满足不可链接性、假名性、匿名性、不可检测性、不可观察性 5 个隐私属性。本章节将从车辆身份隐私、匿名认证位置隐私和位置服务隐私 3 个方面对已有的隐私保护技术进行介绍, 分析他们对隐私属性的满足情况。车联网与传统系统类似, 在通信过程中会对车辆节点进行身份认证, 区分合法车辆用户和非授权车辆用户。车联网中认证包括以下两个级别: ①车辆之间的认证用

于保证通信链路的安全性; ②车辆和 RSU 以及服务提供商之间的认证用于确保正确执行协议与服务。

5.1 车辆身份隐私

在车联网中, 匿名认证是保护用户身份隐私的有效手段, 根据匿名认证使用的密码技术将已有的匿名认证技术分为基于对称加密的方案、基于非对称加密的方案、基于身份的签名方案、基于无证书的签名方案、基于群签名的方案。

5.1.1 基于对称加密的方案

基于对称加密的方案使用消息验证码(Message authentication code, MAC)对通信消息进行验证, 即车辆使用共享密钥为每条消息生成 MAC, 匿名集合中的所有节点使用相同的密钥对消息附加的 MAC 进行验证。由于使用对称加密技术使得它具有较高的计算效率和较低的通信开销。

Lin 和 Zhang 等人[28-29]都使用了消息认证码 MAC 来验证数据包, 车辆使用对称密钥生成 MAC, RSU 对 MAC 进行验证并将消息的真实性传递给其他范围的车辆, 与基于 PKI 的 ECDSA 签名方案和基于群签名的方案相比, Zhang 等人[29]提出的通信开销更低, Lin 等人[28]提出的丢包率低。Chuang 等人[30]提出的信任扩展认证机制和 Umar 等人[31]提出的启用 PUF(Physically Unclonable Function)的基于身份的轻量级认证协议都利用基本加密操作(异或和哈希函数)来提高车联网的认证效率, Chuang 等人[30]利用扩展信任关系的概念来提高车联网认证过程中的性能。

5.1.2 基于非对称加密的方案

在车联网中, 每辆车都配备了用于匿名通信的公私钥对, 车辆使用私钥生成签名, 将该签名和相应的公钥证书附加到消息中。接收方使用发送方的公钥验证该消息, 整个过程不会暴露发送方的真实身份。

Schuab 等人[32]提出了一种不依赖于假名与真实身份映射的方案来实现问责, 该方案将身份信息嵌入到假名证书中, 使得每辆车携带其自身的身份信息, 具有可扩展性, 但存在假名证书撤销的问题。

5.1.3 基于身份的加密方案

为了设计更高效的车联网通信和存储方案, 研究人员利用基于身份的加密技术来设计身份认证方案。Sun 等人[33]提出了一个基于假名、门限签名和门限认证技术的方案来实现车联网安全系统的隐私保护。因为基于身份的加密系统没有使用证书, 所以该方案消耗的内存空间较少。Zhang 等人[34]基于身份的加密系统提出了一次性基于身份认证的非对称群密钥协议来安全地获取群密钥, 在该协议的基础上, 提出了一种 CMIX 协议来创建加密混合区(Cryptography mix-zone, CMIX), 使车联网具有抵抗恶意窃听的能力。CMIX 中的任何载体都可以是群密钥分发器, 而 RSU 无法读取群密钥。因此, 该方案不依赖于完全信任的第三方机构。

5.1.4 基于身份的签名方案

在车联网中, 车辆使用自身的身份信息作为公钥, 利用身份信息生成的私钥签名消息, 最后接收者使用车辆的身份信息验证签名。由于验证过程无需使用数字证书来认证签名者的身份和公钥。因此, 减少了密钥管理所产生的通信和管理问题。

为了降低通信和存储开销, Shim 等人[35]在计算 Diffie-Hellman 的假设下提出一种有效的车载网络条件隐私保护认证方案, 在该方案中, RSU 能够同时对接收到的大量消息进行验证。He 等人[36]提出一种有效的基于身份的车载网络条件隐私保护认证协议, Zhang 等人[37]提出了具有分层聚合和快速响应的隐私保护车辆通信认证协议, 上述两个协议通过使用不同的技术实现批量验证, 从而降低通信和存储开销。Li 等人[38]提出了一种基于条件隐私保护的车联网认证框架, 该框架利用公钥密码技术生成假名, 采用现有的 IBS 方案和 IBOOS 方案, 实现了 RSU 与车辆、车辆与车辆之间的匿名身份认证。

2017 年, Zhang 等人[39]引入了一种分布式聚合隐私保护认证技术, 该技术利用多个拥有 IBS 技术的可信机构, 使得车辆可以同时验证许多消息, 并且它们的签名可以被压缩成一个单独的签名, 这大大减少了车辆和数据收集机构所需的存储空间, 解决 IBS 产生的托管问题。2018 年, Zhang 等人[40]提出了一种隐私保护通信方案, 用于建立车辆云(Vehicle cloud, VC), 并在 VC 中进行数据广播。该方法利用一组位于车联网附近的车辆来开发一个安全、动态的 VC, 实现所有车辆资源集成和数据交换的安全性, VC 形成后任何云用户都可以安全地处理自己的数据。

5.1.5 基于无证书的签名方案

由于基于无证书的签名方案可以解决 IBS 中的托管问题, Horng 等人[41]提出了一种基于 CLSS 的 V2I 通信无证书聚合签名方案, 该方案同时拥有无证书密码体制和聚合签名的优点, 该方案在隐私和可追踪性之间保持平衡, 实现了匿名认证、消息完整性和不可链接性。Cui 等人[42]提出了一种基于椭圆曲线密码体制 ECC 的无证书聚合签名方案, 该方案提供了车联网中 V2I 之间的安全通信并且支持条件隐私保护。有条件隐私保护是通过将车辆广播的消息映

射到一个假身份来实现的。如果发生争议, 权威机构可以通过假身份检索真实身份。Li 等人[43]提出的条件隐私方案可以抵抗假冒攻击和篡改攻击, 并且具有不可链接性。由于使用双线性对和哈希函数的无证书认证方案需要的验证时间过长。因此, 设计了一种基于椭圆曲线密码体制的可证明安全高效的无证书短签名条件保护隐私认证方案, 与上述几个方案相比, 该方案在计算和通信方面具有更好的性能。

5.1.6 基于群签名的方案

在基于群签名的方案中, 允许有效的群管理员代表群成员对消息进行匿名签名, 只有群管理员有能力确定谁是实际发送者, 它能有效的保护用户隐私, 但其缺点是签名验证非常耗时, 这使得它不适用于车联网即时应用程序。

Guo 等人[44]提出了一种基于群签名技术的车载隐私保护通信框架, 该框架具有真实性、数据完整性、匿名性和可追究性。在此群签名方案中, 攻击者可以轻松找到发送消息的群组, 但无法跟踪消息的发送者。

Lin 等人[45]提出了一种基于群签名和身份签名技术的车联网条件隐私保护协议 GSIS。GSIS 一方面利用群签名提供匿名性和可跟踪性, 另一方面使用基于身份的签名进一步降低公钥证书管理的复杂性, 节省了带宽。2009 年, Zhang 等人[46]提出了一种分散的群认证协议来进行群管理, 每个 RSU 对其通信范围内的动态群以及进入群内能秘密发送 V2V 消息的车辆进行维护和管理。车辆产生的任何伪造消息都能被可信的权威机构追踪。由于大量 RSU 共享负载以维护系统, 当更多车辆加入 VANET 时, 车联网性能不会显著降低。为了减少撤销的开销, 2011 年, Sun 等人[47]在车联网系统中引入了分布式密钥管理系统, 在该系统中, 域被划分为多个小的子区域, 任何车辆都必须定期从管理车辆所在区域的区域管理员处更新其群密钥, 将授权限制在特定的区域和时间内。然而, 群签名的匿名性使恶意用户仍然有可能广播虚假消息。2011 年, Park 等人[48]提出了一种基于 RSU 的分布式密钥管理方法, 该方法仅用于车辆通信系统中的群广播服务, 它通过向 RSU 提供部分密钥管理功能以及更新 RSU 内的加密密钥, 减少了大量的密钥更新开销。2018 年, Islam 等人[49]提出了一种基于密码的条件隐私保护认证和群密钥生成协议, 用于在车联网中提供群密钥生成、用户离开、用户加入和密码更改。由于该协议不是基于双线性配对的, 所以它在计算和通信方面的开销较低。

Calandriello 等人[50]将群签名和假名结合起来, 在车联网中实现匿名认证。该方案缓解了假名生成的限制, 使得车辆可以自己动态生成短期匿名证书。但是, 一旦车辆被盗, 偷车的人可以在被发现之前的任意时间内生成有效的短期匿名证书。因此, 该方案潜在的危险会更大。Lu 等人[51]提出了一种密钥隔离假名自授权模型, 该模型可安全地按需生成多个短期匿名证书, 可减轻因车辆盗窃造成的危害。Lu 等人[52]还提出了一种结合了群签名和普通签名的匿名身份认证技术, 在认证流程中, 当合法车辆经过 RSU 时, RSU 将向车辆授权短期匿名证书。然后, 车辆可以使用普通签名技术对消息进行签名。在收到签名消息后, 任何人都可以通过检查匿名证书和消息签名来验证消息的真实性。当车辆对多条消息进行签名时, 验证者只需对证书执行一次群签名验证操作即可。因此, 它比 GSIS 更有效。

Zhang 等人[53]提出了一种基于位置服务的协议, 在该协议中 RSU 和 LBS 提供者都是基于身份的, 车辆只有一个成员密钥, 车辆使用成员密钥生成群签名, 这些签名可以在不侵犯车辆隐私的前提下被 LBS 提供商验证, 如果发现 LBS 请求是虚假的, KGC 可以确定车辆的身份。该方案有效地解决了车联网中提供 LBS 所固有的安全和条件隐私问题, 为服务提供商和车辆提供身份验证、完整性和不可否认性。但是存在通信成本高和不能抵抗位置跟踪攻击的问题。

由于车辆身份隐私没有涉及服务查询问题, 因此, 车辆身份隐私中不涉及不可检测性和不可观察性。从表 3 中可以看出, 所有方案都满足隐私属性不可链接性, 部分方案满足假名性、匿名性。对于假名性, 不满足的原因是使用真实身份去通信, 虽然真实身份在通信过程中满足匿名性, 但是受到的保护程度会比较低, 攻击者一旦找到了真实的用户名, 那将会造成严重后果; 对于匿名性, 当使用假名进行通信时, 可以保护车辆的真实身份, 但存在句法或者语法链接攻击[2]造成车辆位置与假名相关联, 因此提出假名变更策略来阻止此类攻击。根据本文的调查发现, 在车辆身份隐私方面, 每篇论文所关注的攻击方法都比较类似, 有主动攻击者, 也有被动攻击者。因此, 本文根据满足的隐私属性情况将隐私性分为了强、中、弱三个等级。

5.2 匿名认证位置隐私

匿名认证位置隐私是指在广播信标消息过程中使用假名的时候, 如果长期使用同一个假名, 会存在假名链接攻击, 针对该问题提出了许多假名变更策略, 它主要目的是确定车辆应在何时何地更改其

表 3　车辆身份隐私分析

Table 3　Vehicle identity privacy analysis

分类	文献	不可链接性	假名性	匿名性	隐私性	隐私度量方法
基于对称加密的方案	Lin 等人[28]方案	√	√	/	中	/
	Zhang 等人[29]方案	√	√	√	强	*K*-匿名
	Chuang 等人[30]方案	√	√	/	中	/
基于非对称加密的方案	Umar 等人[31]方案	√	/	√	中	/
	Schaub 等人[32]方案	√	/	√	中	/
基于身份加密的方案	Sun 等人[33]方案	√	/	√	中	/
	Zhang 等人[34]方案	√	√	√	强	假名变更统计
基于身份的签名方案	Shim 等人[35]方案	√	√	/	中	/
	He 等人[36]方案	√	√	/	中	/
	Zhang 等人[37]方案	√	√	/	中	假名变更统计
	Li 等人[38]方案	√	√	/	中	/
基于无证书的签名方案	Zhang 等人[39]方案	√	√	/	中	/
	Zhang 等人[40]方案	√	√	√	强	最大追踪时间
	Horng 等人[41]方案	√	√	/	中	/
	Cui 等人[42]方案	√	√	/	中	/
	Li 等人[43]方案	√	√	/	中	/
	Guo 等人[44]方案	√	√	√	强	/
	Lin 等人[45]方案	√	√	√	强	/
基于群签名的方案	Zhang 等人[46]方案	√	/	√	中	/
	Islam 等人[49]方案	√	/	/	弱	/
	Calandriello[50]方案	√	√	√	强	/
	Lu 等人[52]方案	√	√	√	强	/
	Zhang 等人[53]方案	√	√	√	强	/

假名, 以实现车辆之间的不可链接性, 保护车辆位置不被攻击者知道。本文将假名变更策略分为基于 Mix-Zone 的假名变更策略和基于 Mix-Context 的假名变更策略两类。

5.2.1　基于 Mix-Zone 的假名变更策略

在基于混合区的假名变更策略中, 车辆在预定义的道路区域(称为混合区)上更改假名。图 7 显示了安装在道路交叉口处的混合区。如果车辆从端口 1 进入该区域, 在混合区内更改其假名, 然后从端口 2、3、4 中的一个离开, 则攻击者无法将车辆与假名进行链接。

Freudiger 等人[54]提出了一个 CMIX 协议, 它是针对混合区域概念的首次实现。CMIX 区是安全信息被加密的道路区域, 作者建议将这些混合区域设置在十字路口, 车辆在 CMIX 区域内进行假名变更, 并使用由 RSU 分发的共享密钥来加密他们的安全信息, 该方案存在 RSU 之间密钥管理同步的问题。Lu 等人[51]提出在社交地点改变假名的策略, 该策略旨在最大限度的增加同时更改假名的次数, 为此, 作者将改变假名的正确时刻定义为许多车辆在同一时间和地点聚集(例如, 最近红绿灯的路口或购物中心附近的停车场), 作者建立了两个匿名集分析模型来分析位置隐私的级别, 最后实验结果表明, 该策略使得车辆达到了较好的隐私性, 但是它在车辆密度低的情况下不能很好地发挥作用。

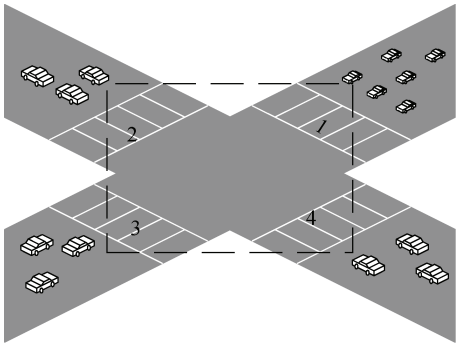

图 7　基于 Mix-Zone 的假名变更策略

Figure 7　Pseudonym change strategy based on Mix-Zone

5.2.2　基于 Mix-Context 的假名变更策略

与基于 Mix-Zone 的策略相比, 在基于混合上下文的策略中, 每辆车独立地决定何时何地更改其假名。它以用户为中心, 让用户控制其位置隐私。在车

联网中, 混合上下文定义为任何情况或机会帮助车辆通过假名变更机制增加其位置隐私保护级别。准确地说, 混合上下文被定义为在车辆之间同步更改假名的任何情况或机会。只有在找到混合上下文时, 车辆才会更改其假名。图 8 展示了基于混合上下文策略的一般状态图。车辆最初配备了一组假名, 每个假名使用的时间有限, 称为稳定时间。稳定时间大于某个阈值, 以免影响相关安全应用运行。稳定时间结束后, 车辆将状态变换为准备更改状态, 它初始化计时器并开始查找混合上下文, 如果找到混合上下文车辆将立即更改其假名。但是, 如果在系统设计的某个确定时间阈值后未找到混合上下文, 车辆将被迫更改其假名。

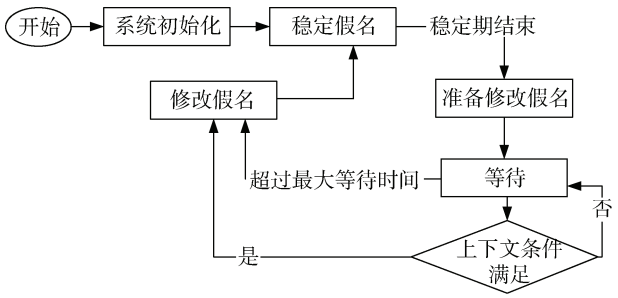

图 8 基于 Mix-Context 的假名变更策略
Figure 8 Pseudonym change strategy based on Mix-Context

Huang 等人[55]认为静默期的概念可以在时间(可变时间)或空间(固定位置)上使用。在采用最大跟踪时间隐私度量隐私级别后, 作者发现使用静默期可以很好地增强无线节点的隐私。Boualouache、Benarous 等人[56,58]都采用了静默期技术, 在静默期修改假名, 他们的区别在于决定进入静默期的触发机制不同。

Eckhoff等人[59]采用非重叠时隙假名池的解决方案; Yu 等人[60]将假名交换技术与群签名机制结合构造扩展匿名变化区域; Wang 等人[61]消除了跟踪器的干扰, 但存在严重依赖 RSU 的问题。

Song 等人[62]将车辆密度视为假名变化阈值的主要参数; Pan 等人[63]分析了合作假名变更方案的可行性, 提出了合作假名变更策略, 两个方案采用的混合上下文假名变更策略, 即在寻找 $K-1$ 辆具有相似特征的车辆时更改假名。

Wasef 和 Shen 等人[64]提出随机加密周期方案(Random encryption periods, REP)。当车辆想要变更假名的时候, 它会在相邻车辆的帮助下用共享密钥创建一个加密区域, 在 REP 期间, 安全消息使用共享密钥进行加密。因此, REP 也可以被视为一个动态的 CMIX 区域。与 CMIX 相比, 该策略减少了 RSU 的管理与维护, 但是当车辆密度较高的时候, 加密过程会降低车联网的性能。

Ying 等人[65]针对位置隐私问题引入动态混合区(Dynamic mix-zone for location privacy, DMLP)。DMLP 根据一些属性(如车辆的预测位置、隐私要求、道路交通统计、车辆行车记录)动态形成混合区, 该方案提供了较高的位置隐私级别, 然而当动态混合区的车辆密度过大时消息加密会导致巨大开销, 这会对车联网性能产生影响。基于 DMLP 策略, Ying 等人[66]提出自私车辆的位置隐私保护方案 MSPVLP, MSPVLP 通过增加声誉系统来激励车辆进行合作。每次车辆需要更新其假名时, 都会创建一个动态混合区, 并在执行假名更改后获得声誉积分。

Zidani 等人[67]提出了一种基于自适应信标的假名变更策略, 该策略允许车辆在很有可能迷惑敌手的情况下更改假名, 车辆设置了一个 Readyflag 的标志位, 以表明他们愿意在下一个时隙变更假名, 这样车辆就能够同步更改假名, 并使用自适应信标速率方法使得车辆可以改变两个连续信标之间的恒定时间, 从而抵御时间相关攻击。然而, 该策略在车辆密度稀疏下缺乏有效性。Kang 等人[68]为解决传统假名管理方式延迟大、成本高等问题, 提出了一种基于雾计算的网络匿名管理模型, 该方案将假名管理部署到车辆附近, 车辆根据上下文信息选择是否更改假名, 为车联网提供了安全的通信和隐私保护。因为方案是假名变更策略, 所以所列方案都具有假名性, 不可链接性, 位置信息都具备匿名性。本文根据文献能够抵抗的敌手模型, 将隐私性强弱分为弱、中、强。其中, 能够抵抗全局被动攻击者隐私性为弱, 能够抵抗全局被动攻击者以及内部攻击者隐私性为强, 能够抵抗全局主动攻击者隐私性为中, 详细内容如表 4 所示。

5.3 位置服务隐私

车联网作为一种新型的移动终端, 车辆能够实时接入互联网, 能够为用户提供基于位置的服务, 它可以回答用户兴趣点位置相关查询, 并利用交通信息为用户提供专门的服务。但是用户在使用这些服务的时候需要将自己的位置或者查询内容透露给位置服务提供商, 这样就会导致用户的兴趣爱好、生活习惯、家庭住址等信息泄露。因此, 保护用户的隐私是成功部署 LBS 应用的基本要求。目前, 已提出了许多隐私保护策略来增强用户的隐私, 主流的技术可以分为基于空间掩蔽的技术、基于加密的技术、基于差分隐私的技术、基于空间扭曲的技术。

表 4 匿名认证位置隐私分析

Table 4 Location privacy analysis of anonymous authentication

分类	文献	隐私性	隐私度量方法
基于 Mix-Zone 的假名变更策略	Lu 等人[51]方案	弱	匿名集大小
	Julien 等人[54]方案	弱	假名熵
	Huang 等人[55]方案	弱	最大追踪时间
	Boualouache 等人[56]方案	强	假名熵
	Wahid 等人[57]方案	中	假名熵
	Benarous 等人[58]方案	弱	敌手成功率
	Echhoff 等人[59]方案	中	敌手成功率
基于 Mix-Context 的假名变更策略	Yu 等人[60]方案	强	假名熵、敌手成功率
	Wang 等人[61]方案	弱	位置熵、敌手成功率
	Song 等人[62]方案	弱	敌手成功率
	Pan 等人[63]方案	弱	匿名集大小
	Wasef 等人[64]方案	弱	匿名集大小
	Ying 等人[65]方案	弱	假名熵
	Ying 等人[66]方案	弱	混合区域大小, *K*-匿名
	Zidani 等人[67]方案	强	平均混淆时间
	Kang 等人[68]方案	弱	假名熵

5.3.1 基于空间掩蔽的技术

空间掩蔽技术的主要思想是对 LBS 查询中的真实信息进行必要的干扰, 以此避免攻击者直接获取用户的真实信息。用户在请求 LBS 服务的时候使用的位置(查询内容)由 q 变为了一个掩蔽区域 Q。掩蔽区域的表示形式有两种, 一种是一个连续的区域, 另外一种是离散的区域[69]。基于空间掩蔽的技术包括以下几类:

(1) *K*-匿名: *K*-匿名的主要思想是通过包含查询位置(查询内容)q 和其他至少 *K*-1 个其他用户的位置(查询内容)来表示掩蔽区域[70]。Luo、Li 等人[71-72]利用区块链构建信任模型创建匿名掩蔽区域, 达到管理车辆间的可信性以及增加车联网可靠性的效果。Rajput 等人[73]提出一个基于 *K*-匿名的分布式方案, 在用户隐私和请求保密性保持不变的情况下, 该方案在 TA、LBS 和用户上的计算开销较低。Ying 等人[74]利用周围的用户位置来保护原始发件人的位置, 提出了三种社交感知位置隐私保护方案, 分别为 B-SLP、I-SLP 和 E-SLP, 其中 B-SLP 具有最高级别的隐私保护, 而 I-SLP 和 E-SLP 具有较小的掩蔽区域。

(2) 虚拟生成: 虚拟生成的主要思想是通过包含查询位置(查询内容)q 和由客户端生成虚拟位置(虚拟查询)来表示掩蔽区域[25,75]。Cui 等人[42]提出了一种利用虚拟位置和路线混淆来保护车辆位置隐私的方案, 车辆根据周围车辆的情况动态生成虚拟位置, 提供有关驾驶路线的误导信息, 从而实现位置隐私保护, 该方案使用匿名集合的熵和敌手跟踪成功率来衡量隐私保护级别, 结果表明该方案提供了较好的隐私级别, 也具有较好的安全性能。Wu 等人[76]通过计算历史位置服务请求的概率分布来生成位置匿名集, 从而防止虚拟位置被过滤。

(3) 混淆: 混淆的主要思想是通过包含查询位置(查询内容)q、其他用户位置(查询内容)和客户端生成的假位置(假查询)来表示掩蔽区域[25,75]。Ullah 等人[77]提出了一种多级位置隐私保护方案 MLPS 来混淆车辆位置, 为了混淆位置, 该方案分为三个级别, 每个级别都会在信息中增加混淆, 目的是隐藏车辆的真实位置坐标, 它不仅提供了位置隐私, 还具有匿名性、不可抵赖性、消息身份验证、完整性。Lim 等人[78]提出了一种相互混淆路径方法, 使车辆能够向 LBS 提供高度准确的实时位置更新, 同时防止 LBS 跟踪车辆。

5.3.2 基于加密的技术

加密的主要思想是对用户的 LBS 查询信息进行加密处理, 使其对服务器完全不可见, 即使攻击者获取了加密后的数据, 仍然无法解析出用户的真实数据。该方法以更高的计算复杂度为代价, 保证了强大的保密性。因此, 高计算和通信复杂度使得这些方法应用起来有些困难。它包括以下几类:

(1) 隐私信息检索: 隐私信息检索(Private information retrieval, PIR)是一种基于加密技术的位置隐私保护方案。PIR 方案建立在 PIR 协议之上, PIR 方案将数据库设定为一个二进制字符串 X, 表示为 $X=\{X_1,X_2,\cdots,X_N\}$。当用户想要查找字符串中的第

i 位数据 X_i 时, 会向服务器发送一个加密的查询请求 $q(i)$, 服务器通过对查询请求的分析匹配, 向客户端做出响应并返回一个查询结果 $r(X,q(i))$, 客户端对查询结果进行解密操作, 得到结果 X_i。Tan 等人[79]提出了一个基于计算信息检索的 VLBS 隐私保护框架。在道路网络的限制下, 该框架将可用的交通信息作为计算信息检索的背景知识降低计算成本。

(2) 不经意传输协议: 不经意传输(Oblivious transfer, OT)协议是 Rabin 在 1981 年提出的一种基础的多方安全计算协议。Liu 等人[80]提出了两个 LBS 隐私保护方案 *k*NN 和 T-*k*NN, 它采用 OT 协议和基于属性基加密的密文策略技术, 两个方案都能保护 LBS 服务提供商和车辆的隐私, 但 T-*k*NN 支持更细粒度的 LBS 查询。Yadav 等人[81]提出了基于位置的可链接服务方案, 作者将可链接自发匿名群签名方案与 OT 协议技术组合, 使得该方案具有服务器 POIs 隐私、用户查询隐私、用户位置隐私、抗量子、匿名性、用户身份认证、服务可链接性。Chim 等人[82]利用假名、不可区分凭证和 OT 技术提供隐私保护, 该方案假设所有基础设施单元不可信也能够保证用户隐私。

(3) 同态加密: 同态加密是指明文加密之后的密文进行代数运算, 计算后的结果解密与对应明文计算的结果相同。Youssef 等人[83]提出了基于同态加密的位置服务隐私保护方案, 利用同态加密保证数据的保密性和完整性。Farouk 等人[84]提出了用于查询隐私保护的全同态加密技术, 在该方案中, 它允许位置服务提供商在保护车辆查询和身份隐私的同时执行查询请求, 能够以安全有效的方式保护司机未来路线的隐私, 并且允许云服务提供商(Cloud server provider, CSP)对加密数据进行计算, 以检测到达期望目的的最短路径。

(4) 空间变换: 空间变换的主要思想是利用单向变换的能力将所有对象和查询的空间映射到另一个空间, 并在变换后的空间中进行空间查询。Liu 等人[85]采用 Hilbert 曲线将区域划分为原子区域, 并使用 SSW 加密算法判断空间数据与查询范围的关系, 在保证数据隐私和查询隐私的前提下实现精确的范围查询。Aloufi 等人[86]使用空间填充曲线对 GPS 坐标进行地理哈希以保持位置的降维。

5.3.3 基于差分隐私的技术

差分隐私(Differential privacy, DP)是由 Dwork 等人[87]在 2006 年提出的一种新的隐私安全定义, McSherry 等人[88]将 Netflix 奖中比较领先的算法通过添加噪声设计具有差分隐私性质的推荐系统。通过实验, 领先的几个算法都能够通过调整实现差分隐私的性质。推荐系统主要是分为两个阶段, 第一个阶段是在差分隐私保障下的聚合/学习阶段, 第二个阶段是个人兴趣推荐阶段。通过实验证明具有差分隐私性质的推荐系统是可行的, 并且对推荐的准确性不会造成重大影响。

Andr'es 等人[26]利用差分隐私的定义, 提出了在位置系统中隐私保护的形式化定义地理不可区分性, 并通过在用户位置中添加受控随机噪声来实现 Geo-Indistinguishability 的机制。Jiang 等人[89]首先采用专门设计的差分隐私建立注入噪声与隐私保护之间的关系, 构建数据驱动的隐私保护模型, 然后结合递归神经网络和多爬山算法添加细粒度噪声。该方法提供可量化的位置隐私保护, 同时保证了预测结果的实用性。徐川等人[90]为解决用户在不同位置隐私保护需求的差异性问题提出了一种满足用户个性化隐私需求的一种基于差分隐私的个性化位置隐私保护方案。

5.3.4 基于空间扭曲的技术

Yiu 等人[69]首次提出了空间扭曲技术, 其主要思想是当用户发送位置服务请求时, 客户端随机指定一个锚点, 将该锚点作为用户的位置数据发送给服务器, 服务器以该锚点为中心, 不断扩大搜索范围, 搜索其周围的兴趣点, 直至包含用户的真实位置。如图 9 所示, anchor 表示锚点, user 表示用户真实节点, supply space 表示服务器按照锚点搜索的兴趣点集合, demand space 表示用户真实需要的兴趣点集合。在方案开始时, demand space 设置为域空间, supply space 为空; 当服务器不断地以 anchor 为中心向四周搜索兴趣点时, supply space 会扩大; 直到 supply space 完全包含了 demand space 时, 停止搜索, 服务器将 demand space 中的兴趣点返回给客户端。

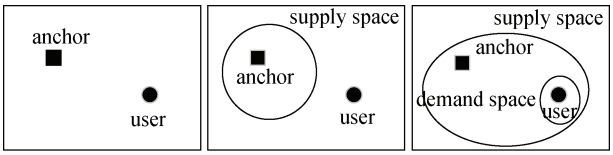

图 9 SpaceTwist 方案时序图

Figure 9 SpaceTwist scheme timing diagram

马春光等人[91]提出了基于 Voronoi 图预划分的 LBS 位置隐私保护方法, 该方法结合了 *K*-匿名和空间扭曲技术, 在查询过程中用户以固定锚点代替真实位置, 向位置服务器逐步获取兴趣点候选集并计算出想要的结果。与 SpaceTwist[69]相比, 该方案具有明显的查询时间优势。针对 SpaceTwist 算法只适用于欧式空间且不能实现 *K*-匿名的问题, 刘振鹏等

人[92]提出了一种基于 SpaceTwist 的 *K*-匿名增量近邻查询算法, 它根据路网环境, 将用户查询内容生成 *K*-匿名区, 结合 POIs 的分布, 选择最优的锚点位置, 最后进行增量近邻查询。

根据表 5 的位置服务隐私分析, 可以看出, 在车联网位置服务当中, 对于不可观察性, 只要满足匿名性和不可检测性, 就会满足不可观察性, Wu、Yadav 等人[76,81]提出的方案在满足了匿名性和不可检测性的情况下, 还是不满足不可观察性, 原因在于满足匿名性的是位置, 而满足不可检测性的是查询内容。根据隐私属性的满足情况, 对隐私性的强弱做了一个总结。

表 5 位置服务隐私分析

Table 5 Location service privacy analysis

分类	文献	不可链接性	假名性	匿名性	不可检测性	不可观察性	隐私性	隐私度量
基于空间掩蔽的技术	Wang 等人[70]方案	√	√	√	/	/	中	*K*-匿名
	Luo 等人[71]方案	√	√	√	/	/	中	*K*-匿名
	Li 等人[72]方案	√	√	√	/	/	中	*K*-匿名
	Rajput 等人[73]方案	√	√	√	√	√	强	/
	Ying 等人[74]方案	√	/	√	/	/	弱	熵
	Wu 等人[76]方案	√	/	√	√	/	弱	*K*-匿名
	Ullah 等人[77]方案	√	√	√	/	/	中	匿名集大小、位置熵
	Lim 等人[78]方案	√	/	√	/	/	弱	最大跟踪时间、位置熵、敌手成功率
基于加密的技术	Tan 等人[79]方案	√	/	/	/	/	肉	/
	Liu 等人[80]方案	√	/	/	√	/	弱	/
	Yadav 等人[81]方案	√	√	√	√	√	强	/
	Chim 等人[82]方案	√	√	/	√	/	中	/
	Youssef 等人[83]方案	√	/	/	√	/	弱	/
	Farouk 等人[84]方案	√	/	/	√	/	弱	/
	Liu 等人[85]方案	√	/	√	√	√	强	/
	Aloufi 等人[86]方案	√	/	√	√	√	强	/
基于差分隐私的技术	徐川等人[90]方案	√	/	√	√	√	强	地理不可区分性
基于空间扭曲的技术	马春光等人[91]方案	√	/	√	/	/	弱	*K*-匿名
	刘振鹏等人[92]方案	√	/	√	/	/	弱	*K*-匿名

6 讨论

本文从车联网中的身份隐私、匿名认证位置隐私以及位置服务隐私三个方面讨论了车联网中的隐私保护技术。身份隐私即车辆在广播信标信息的时候, 如果使用真实身份进行信息发送, 那么将会泄露个人身份隐私, 造成一定的危害。因此, 发送信标信息的时候需要使用匿名身份, 保护身份隐私常用的技术有基于对称加密的技术、基于非对称加密的技术、基于身份加密的技术、基于身份签名的技术、基于无证书签名的技术、基于群签名的技术。使用匿名身份定期广播信标信息会面临链接攻击, 攻击者可以建立匿名与车辆之间的关系, 从而知道车辆何时会出现什么位置。因此, 需要及时更换假名, 以保护车辆位置隐私, 即匿名认证位置隐私, 匿名认证位置隐私一般使用的技术有基于 Mix-Zone 的技术、基于 Mix-Context 的技术。随着全球定位设备技术的发展, 驾驶员或者车辆使用基于位置的服务开始发展起来, 而驾驶员或者车辆在请求位置服务时, 不希望服务提供商或者非授权者知道自己的位置。因此, 需要保护用户的位置隐私, 它使用的技术包括基于空间掩蔽的技术, 如 *K*-匿名、虚拟生成(Dummies)、混淆(Obfuscation)等, 基于加密的技术, 如 PIR、同态加密等技术, 基于差分隐私的技术、基于空间扭曲的技术。从目前的针对车联网隐私保护技术的研究现状来看, 在理论基础和实现技术等许多方面尚有待深入研究。同时, 随着新业务的不断推陈出新, 车联网隐私保护也必将面临更多的挑战, 本文提出了以下几个车联网隐私保护技术研究方向。

6.1 去中心化的车辆身份隐私技术

通过本文的调查发现, 为保护身份隐私, 大部分都是基于已有的一些密码技术做一些改进, 从而达到假名性, 但是这些密码技术本身存在一些问题, 比如基于对称密码体制的方案存在密钥分发繁杂、

花费代价高的缺点, 而基于非对称密码体制具有计算代价高的缺点。除此之外, 还有密钥管理、证书撤销等问题, 而基于无证书签名的匿名认证技术具有无证书管理、系统轻量、通信开销低等优点, 区块链具有高安全性、不可篡改性等优点, 将基于无证书签名的方案与区块链结合, 研究出更加适用于车联网高效率匿名身份认证方案是目前的一个研究方向。

6.2 自适应的假名变更技术

通过对匿名认证位置隐私方面的调查发现, 基于Mix-Context的假名变更策略由车辆自己决定何时更改假名, 与基于 Mix-Zone 的假名变更策略只能在固定位置更改假名相比, 前者的灵活性更高, 但它存在过分依赖 RSU; 车辆密度较高的时候由于频繁的假名变更, 会降低车联网的性能; 假名管理的方式存在延迟大、成本高等问题。未来的研究方向可以针对不同车辆密度稀疏场景, 研究出自适应的基于 Mix-Context 假名变更技术。

6.3 个性化的位置服务隐私保护技术

在基于空间掩蔽技术的研究中, 基于虚拟和混淆的技术优点在于易于实现, 在服务质量和隐私水平之间有较好的平衡, 但是由于在发送请求的过程中会加入其他数据, 使得请求中的位置数据失真, 并且也会受到数据特征推测攻击; 基于 K-匿名技术的优点在于能降低用户隐私泄露的风险, 隐私保护程度可以由用户根据需求自己定义, 算法移植性强, 缺点在于未考虑攻击者拥有的背景知识, 会受到重放攻击。基于加密的技术隐私保护效果较好、服务质量较高, 但是由于加密后的密文信息长度普遍比明文长度大很多, 并且中间会涉及加密解密的过程, 导致通信与计算开销大、部署复杂等问题。基于差分隐私的技术以数学理论为支撑, 对隐私保护进行了严格的数学定义, 其优点在于不受攻击者具有的背景知识影响和不受具体某条数据变化的影响, 隐私保护效果好, 缺点在于合理分配隐私预算 ε 困难, 位置数据有失真。基于空间扭曲的技术优点在于没有使用第三方服务器, 降低了数据泄露的风险, 它的缺点在于选择锚点困难, 查询结果不准确。由于不同的用户对隐私需求也不同, 用户更希望有个性化的隐私保护策略, 因此, 可以将现有隐私保护技术的优点与个性化隐私需求结合, 提出基于车联网的个性化位置服务隐私保护方案。

7 总结

随着车联网的兴起, 车联网隐私保护问题受到了学术界、政府部门、消费者和产业界的多方关注。本文对车联网现有隐私保护技术进行阐述和分析, 介绍了目前主要的隐私保护技术, 并对各个技术进行了相应的分类及分析。最后, 结合车联网隐私保护的研究现状, 指出了该领域在未来的研究方向。

参考文献

[1] Huawei. C-V2X white paper for cooperative Intelligent Transport System[R/OL]. [2022-05-06]. https://www.bj-xinghe.com/wp-content/uploads/2021/04/%E5%8D%8E%E4%B8%BA-%E8%BD%A6%E8%B7%AF%E4%B8%80%E4%BD%93%E5%8C%96%E6%99%BA%E8%83%BD%E7%BD%91%E8%81%94%E4%BD%93%E7%B3%BB-C-V2X%E7%99%BD%E7%9A%AE%E4%B9%A6%EF%BC%88%E7%89%A9%E8%81%94%E7%BD%91%EF%BC%89.pdf.
(华为. 车路一体化智能网联体系 C-V2X 白皮书[R/OL]. [2022-05-06].https://www.bj-xinghe.com/wp-content/uploads/2021/04/华为-车路一体化智能网体系-C-V2X 白皮书(物联网).pdf.)

[2] Lu Z J, Qu G, Liu Z L. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2019, 20(2): 760-776.

[3] Sheikh M S, Liang J, Wang W S. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)[J]. *Sensors*, 2019, 19(16): 3589.

[4] Zhang Q Y, Zhang X, Li W J, et al. Overview of Location Trajectory Privacy Protection Technology Based on LBS System[J]. *Application Research of Computers*, 2020, 37(12): 3534-3544.
(张青云, 张兴, 李万杰, 等. 基于 LBS 系统的位置轨迹隐私保护技术综述[J]. *计算机应用研究*, 2020, 37(12): 3534-3544.)

[5] Babaghayou M, Labraoui N, Abba Ari A A, et al. Pseudonym Change-Based Privacy-Preserving Schemes in Vehicular Ad-Hoc Networks: A Survey[J]. *Journal of Information Security and Applications*, 2020, 55: 102618.

[6] Deng Y K, Zhang L, Li J. Overview of Research on Privacy Protection of Internet of Vehicles[J]. *Application Research of Computers*, 2022, 39(10): 2891-2906.
(邓雨康, 张磊, 李晶. 车联网隐私保护研究综述[J]. *计算机应用研究*, 2022, 39(10): 2891-2906.)

[7] Azees M, Vijayakumar P, Jegatha Deborah L. Comprehensive survey on security services in vehicular ad‐hoc networks[J]. *IET Intelligent Transport Systems*, 2016, 10(6): 379-388.

[8] Al-Sultan S, Al-Doori M M, Al-Bayatti A H, et al. A Comprehensive Survey on Vehicular Ad Hoc Network[J]. *Journal of Network and Computer Applications*, 2014, 37: 380-392.

[9] Singh P K, Agarwal A, Nakum G, et al. MPFSLP: Masqueraded Probabilistic Flooding for Source-Location Privacy in VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(10): 11383-11393.

[10] Standardization Administration of the People's Republic of China. National IoV Industry Standard System Construction Guide[R/OL]. [2022-05-06].https://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c6223806/part/6223840.pdf.
(国家标准化管理委员会. 国家车联网产业标准体系建设指南[R/OL].[2022-05-06].https://www.miit.gov.cn/n1146295/n165285

8/n1652930/n3757016/c6223806/part/6223840.pdf.)

[11] Boualouache A, Senouci S M, Moussaoui S. A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(1): 770-790.

[12] Deng M N, Wuyts K, Scandariato R, et al. A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements[J]. *Requirements Engineering*, 2011, 16(1): 3-32.

[13] Liu Y B, Chang G H, Li T. Analysis on key technologies of vehicle networking security[M]. Beijing: Science Press, 2019: 114.
(刘宴兵, 常光辉, 李暾. 车联网安全关键技术解析[M]. 北京: 科学出版社, 2019: 114.)

[14] Zhang C H, Zang H J, Xue X P, et al. Research Progress in Internet of Vehicles Trajectory Privacy Protection[J]. *Journal of Computer Applications*, 2017, 37(7): 1921-1925, 1942.
(张春花, 臧海娟, 薛小平, 等. 车联网轨迹隐私保护研究进展[J]. *计算机应用*, 2017, 37(7): 1921-1925, 1942.)

[15] Wagner I, Eckhoff D. Technical Privacy Metrics: A Systematic Survey[J]. *ACM Computing Surveys*, 51(3)Article No. 57,

[16] Diaz C, Seys S, Claessens J, et al. Towards measuring anonymity[C]. *International Workshop on Privacy Enhancing Technologies*, 2002: 54-68.

[17] Serjantov A, Danezis G. Towards an Information Theoretic Metric for Anonymity[C]. *The 2nd international conference on Privacy enhancing technologies*, 2002: 41-53.

[18] Steinbrecher S, Köpsell S. Modelling unlinkability[C]. *International Workshop on Privacy Enhancing Technologies*, 2003: 32-47.

[19] Gedik B, Liu L. Location Privacy in Mobile Systems: A Personalized Anonymization Model[C]. *25th IEEE International Conference on Distributed Computing Systems*, 2005: 620-629.

[20] Kalnis P, Ghinita G, Mouratidis K, et al. Preventing Location-Based Identity Inference in Anonymous Spatial Queries[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2007, 19: 1719-1733.

[21] Mokbel M F, Chow C Y, Aref W G. The new casper: Query processing for location services without compromising privacy[C]. *International Conference on Very Large Data Bases*, 2006, 6: 763-774.

[22] Pan X, Xu J L, Meng X F. Protecting Location Privacy Against Location-Dependent Attacks in Mobile Services[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2012, 24(8): 1506-1519.

[23] Sampigethaya K, Huang L, Li M, et al. CARAVAN: Providing location privacy for VANET. Technical report. Washington Univ Seattle Dept of Electrical Engineering, 2005.

[24] Hoh B, Gruteser M, Xiong H, et al. Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking[C]. *The 14th ACM conference on Computer and communications security*, 2007: 161-171.

[25] Ardagna C A, Cremonini M, Damiani E, et al. Location Privacy Protection through Obfuscation-Based Techniques[C]. *The 21st annual IFIP WG 11.3 working conference on Data and applications security*, 2007: 47-60.

[26] Andrés M E, Bordenabe N E, Chatzikokolakis K, et al. Geo-Indistinguishability: Differential Privacy for Location-Based Systems[C]. *The 2013 ACM SIGSAC conference on Computer & communications security*, 2013: 901-914.

[27] Chatzikokolakis K, Palamidessi C, Stronati M. Constructing Elastic Distinguishability Metrics for Location Privacy[J]. *Proceedings on Privacy Enhancing Technologies*, 2015, 2015(2): 156-170.

[28] Lin X D, Sun X T, Wang X Y, et al. TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(12): 4987-4998.

[29] Zhang C X, Lin X D, Lu R X, et al. An Efficient Message Authentication Scheme for Vehicular Communications[J]. *IEEE Transactions on Vehicular Technology*, 2008, 57(6): 3357-3368.

[30] Chuang M C, Lee J F. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks[C]. *2011 International Conference on Consumer Electronics*, *Communications and Networks*, 2011: 1758-1761.

[31] Umar M, Islam S H, Mahmood K, et al. Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(11): 12158-12167.

[32] Schaub F, Kargl F, Ma Z D, et al. V-Tokens for Conditional Pseudonymity in VANETs[C]. *2010 IEEE Wireless Communication and Networking Conference*, 2010: 1-6.

[33] Sun J Y, Zhang C, Zhang Y C, et al. An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2010, 21(9): 1227-1239.

[34] Zhang L. OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(12): 2998-3010.

[35] Shim K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. *IEEE transactions on vehicular technology*, 2012, 61(4): 1874-1883.

[36] 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.

[37] Zhang L, Hu C Y, Wu Q H, et al. Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response[J]. *IEEE Transactions on Computers*, 2016, 65(8): 2562-2574.

[38] Li J, Lu H, Guizani M. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(4): 938-948.

[39] Zhang L, Wu Q H, Domingo-Ferrer J, et al. Distributed Aggregate Privacy-Preserving Authentication in VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(3): 516-526.

[40] Zhang L, Meng X Y, Choo K K R, et al. Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud[J]. *IEEE Transactions on Dependable and Secure Comput-*

ing, 2020, 17(3): 634-647.

[41] Horng S J, Tzeng S F, Huang P H, et al. An Efficient Certificateless Aggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks[J]. *Information Sciences*, 2015, 317: 48-66.

[42] Cui J, Zhang J, Zhong H, et al. An Efficient Certificateless Aggregate Signature without Pairings for Vehicular Ad Hoc Networks[J]. *Information Sciences*, 2018, 451/452: 1-15.

[43] Li J L, Ji Y S, Choo K K R, et al. CL-CPPA: Certificate-less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles[J]. *IEEE Internet of Things Journal*, 2019, 6(6): 10332-10343.

[44] Guo J H, Baugh J P, Wang S Q. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework[C]. *2007 Mobile Networking for Vehicular Environments*, 2007: 103-108.

[45] Lin X D, Sun X T, Ho P H, et al. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications[J]. *IEEE Transactions on Vehicular Technology*, 2007, 56(6): 3442-3456.

[46] Zhang L, Wu Q H, Solanas A, et al. A Scalable Robust Authentication Protocol for Secure Vehicular Communications[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(4): 1606-1617.

[47] Sun Y, Feng Z, Hu Q, et al. An efficient distributed key management scheme for group‐signature based anonymous authentication in VANET[J]. *Security and Communication Networks*, 2012, 5(1): 79-86.

[48] Park M H, Gwon G P, Seo S W, et al. RSU-Based Distributed Key Management (RDKM) for Secure Vehicular Multicast Communications[J]. *IEEE Journal on Selected Areas in Communications*, 2011, 29(3): 644-658.

[49] Islam S H, Obaidat M S, Vijayakumar P, et al. A Robust and Efficient Password-Based Conditional Privacy Preserving Authentication and Group-Key Agreement Protocol for VANETs[J]. *Future Generation Computer Systems*, 2018, 84: 216-227.

[50] Calandriello G, Papadimitratos P, Hubaux J P, et al. Efficient and Robust Pseudonymous Authentication in VANET[C]. *The fourth ACM international workshop on Vehicular ad hoc networks*, 2007: 19-28.

[51] Lu R X, Lin X D, Luan 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.

[52] Lu R, Lin X, Zhu H, et al. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications[C]. *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008: 1229-1237.

[53] Zhang L, Wu Q H, Qin B, et al. Practical Secure and Privacy-Preserving Scheme for Value-Added Applications in VANETs[J]. *Computer Communications*, 2015, 71: 50-60.

[54] Freudiger J, Raya M, Félegyházi M, et al. Mix-Zones for Location Privacy in Vehicular Networks[J]. *Proceedings of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems*, 2007.

[55] Huang L P, Matsuura K, Yamane H, et al. Enhancing Wireless Location Privacy Using Silent Period[C]. *IEEE Wireless Communications and Networking Conference*, 2005: 1187-1192.

[56] Boualouache A, Moussaoui S. TAPCS: Traffic-Aware Pseudonym Changing Strategy for VANETs[J]. *Peer-to-Peer Networking and Applications*, 2017, 10(4): 1008-1020.

[57] Wahid A, Yasmeen H, Ali Shah M, et al. Holistic Approach for Coupling Privacy with Safety in VANETs[J]. *Computer Networks*, 2019, 148: 214-230.

[58] 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.

[59] Eckhoff D, Sommer C. Readjusting the Privacy Goals in Vehicular Ad-Hoc Networks: A Safety-Preserving Solution Using Non-Overlapping Time-Slotted Pseudonym Pools[J]. *Computer Communications*, 2018, 122: 118-128.

[60] Yu R, Kang J W, Huang X M, et al. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks[J]. *IEEE Transactions on Dependable and Secure Computing*, 2016, 13(1): 93-105.

[61] Wang S B, Yao N M, Gong N, et al. A Trigger-Based Pseudonym Exchange Scheme for Location Privacy Preserving in VANETs[J]. *Peer-to-Peer Networking and Applications*, 2018, 11(3): 548-560.

[62] 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.

[63] Pan Y Y, Li J Q. Cooperative Pseudonym Change Scheme Based on the Number of Neighbors in VANETs[J]. *Journal of Network and Computer Applications*, 2013, 36(6): 1599-1609.

[64] Wasef A, Xuemin. REP: Location Privacy for VANETs Using Random Encryption Periods[J]. *Mobile Networks and Applications*, 2010, 15(1): 172-185.

[65] Ying B D, Makrakis D, Mouftah H T. Dynamic Mix-Zone for Location Privacy in Vehicular Networks[J]. *IEEE Communications Letters*, 2013, 17(8): 1524-1527.

[66] Ying B D, Makrakis D, Hou Z Z. Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks[J]. *IEEE Transactions on Vehicular Technology*, 2015, 64(12): 5631-5641.

[67] Zidani F, Semchedine F, Ayaida M. Estimation of Neighbors Position Privacy Scheme with an Adaptive Beaconing Approach for Location Privacy in VANETs[J]. *Computers & Electrical Engineering*, 2018, 71: 359-371.

[68] Kang J W, Yu R, Huang X M, et al. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2018, 19(8): 2627-2637.

[69] Yiu M L, Jensen C S, Huang X G, et al. SpaceTwist: Managing the Trade-Offs among Location Privacy, Query Performance, and Query Accuracy in Mobile Services[C]. *2008 IEEE 24th International Conference on Data Engineering*, 2008: 366-375.

[70] 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: 57-73.

[71] Luo B, Li X H, Weng J, et al. Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET[J]. *IEEE Transac-*

tions on Vehicular Technology, 2020, 69(2): 2034-2048.

[72] Li B H, Liang R C, Zhu D, et al. Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 22(6): 3765-3775.

[73] Rajput U, Ansari A, Zai S, et al. Privacy Preserving Location based Services Through K-Anonymized Vehicular Social Network[J]. *Quaid-E-Awam University Research Journal of Engineering, Science & Technology Nawabshah*, 2020, 18(2): 163-168.

[74] Ying B D, Nayak A. A Distributed Social-Aware Location Protection Method in Untrusted Vehicular Social Networks[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(6): 6114-6124.

[75] Duckham M, Kulik L. Simulation of Obfuscation and Negotiation for Location Privacy[C]. *The 2005 international conference on Spatial Information Theory*, 2005: 31-48.

[76] Wu L, Wei X, Meng L Z, et al. Privacy-Preserving Location-Based Traffic Density Monitoring[J]. *Connection Science*, 2021, 34: 874-894.

[77] Ullah I, Shah M A, Khan A, et al. Privacy‐preserving multilevel obfuscation scheme for vehicular network[J]. *Transactions on Emerging Telecommunications Technologies*, 2021, 32(2): e4204.

[78] Lim J, Yu H, Kim K, et al. Preserving Location Privacy of Connected Vehicles with Highly Accurate Location Updates[J]. *IEEE Communications Letters*, 2017, 21(3): 540-543.

[79] Tan Z, Wang C, Zhou M C, et al. Private Information Retrieval in Vehicular Location-Based Services[C]. *2018 IEEE 4th World Forum on Internet of Things*, 2018: 56-61.

[80] Liu S S, Liu A, Yan Z, et al. Efficient LBS Queries with Mutual Privacy Preservation in IoV[J]. *Vehicular Communications*, 2019, 16: 62-71.

[81] Yadav V K, Verma S, Venkatesan S. Linkable Privacy-Preserving Scheme for Location-Based Services[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(7): 7998-8012.

[82] Chim T W, Yiu S M, Hui L C K, et al. OPQ: OT-Based Private Querying in VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2011, 12(4): 1413-1422.

[83] Youssef G, Mouhcine G, Zouhair G, et al. Privacy Preserving Scheme for Location-Based Services[J]. *Journal of Information Security*, 2012, 3(2): 105-112.

[84] Farouk F, Alkady Y, Rizk R. Efficient Privacy-Preserving Scheme for Location Based Services in VANET System[J]. *IEEE Access*, 2020, 8: 60101-60116.

[85] Liu Z M, Wu L, Meng W Z, et al. Accurate Range Query with Privacy Preservation for Outsourced Location-Based Service in IoT[J]. *IEEE Internet of Things Journal*, 2021, 8(18): 14322-14337.

[86] Aloufi A, Hu P Z, Liu H, et al. Universal Location Referencing and Homomorphic Evaluation of Geospatial Query[J]. *Computers & Security*, 2021, 102: 102137.

[87] Dwork C. Differential privacy: A survey of results[C]. *International conference on theory and applications of models of computation*, 2008: 1-19.

[88] McSherry F, Mironov I. Differentially Private Recommender Systems: Building Privacy into the Netflix Prize Contenders[C]. *The 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009: 627-636.

[89] Jiang H B, Wang M Y, Zhao P, et al. A Utility-Aware General Framework with Quantifiable Privacy Preservation for Destination Prediction in LBSS[J]. *IEEE/ACM Transactions on Networking*, 2021, 29(5): 2228-2241.

[90] Xu C, Ding Y Y, Luo L, et al. Personalized Location Privacy Protection for Location-Based Services in Vehicular Networks[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.)

[91] Ma C G, Zhou C L, Yang S T, et al. Location Privacy-Preserving Method in LBS Based on Voronoi Division[J]. *Journal on Communications*, 2015, 36(5): 5-16.
(马春光, 周长利, 杨松涛, 等. 基于Voronoi图预划分的LBS位置隐私保护方法[J]. *通信学报*, 2015, 36(5): 5-16.)

[92] Liu Z P, Zhao X, Dong Y W, et al. Improved SpaceTwist Privacy Protection Method Based on Anchor Optimization Algorithm[J]. *Journal on Communications*, 2017, 38(S1): 32-38.
(刘振鹏, 赵璇, 董亚伟, 等. 结合锚点优选算法改进的SpaceTwist隐私保护方法[J]. *通信学报*, 2017, 38(S1): 32-38.)

李瑞琴 于 2020 年在西南科技大学信息安全专业获得学士学位。现在北京邮电大学电子信息专业攻读硕士学位。研究领域为车联网安全与隐私保护、安全多方计算。研究兴趣包括: 车联网安全与隐私保护、安全多方计算。Email: liruiqin2022@126.com

胡晓雅 于 2020 年在北京邮电大学计算机技术专业获得硕士学位。现在北京邮电大学网络空间安全专业攻读博士学位。研究领域为区块链安全与隐私保护、车联网数据隐私保护。研究兴趣包括: 区块链安全与隐私保护、车联网安全与隐私保护。Email: huxiaoya@bupt.edu.cn

张倨源 于 2019 年在山东大学信息安全专业获得学士学位。现在北京邮电大学网络空间安全专业攻读硕士学位。研究领域为密码学、车联网数据隐私保护。研究兴趣包括: 密码学、车联网安全与隐私保护。Email: zhangjuyuan2020@163.com

王励成 于 2007 年在上海交通大学计算机软件与理论专业获得博士学位。现任北京邮电大学教授。研究领域为密码学、区块链、量子计算。研究兴趣包括: 密码学、区块链、量子计算、未来互联网架构。Email: wanglc2012@126.com