第六代移动通信车联网中的位置隐私威胁与保护：全面综述

Baihe Ma、Xu Wang、Xiaojie Lin、Yanna Jiang、Zhe Wang、Caijun Sun*、Guangsheng Yu、Suirui Zhu，Ying He，*IEEE*高级会员、Wei Ni，*IEEE*会士和Ren Ping Liu，*IEEE*高级会员 *E*

摘要—**位置隐私对于车联网至关重要，因为驾驶员轨迹和个人信息可能被泄露，使对手能够发起数据攻击和物理攻击，威胁驾驶员的安全和人身保障。本综述全面回顾了不同的定位技术，包括感知基础设施定位、光学视觉定位和基于蜂窝无线电的定位等广泛使用的技术，并指出了尚未得到充分解决的位置隐私问题。我们将位置隐私保护机制（LPPM）分为用户侧、服务器端和用户—服务器接口侧，并评估其有效性。我们的分析表明，尽管用户—服务器接口侧的位置隐私保护机制对于车联网至关重要，但在现有文献中却未得到充分关注。此外，我们还研究了现有车联网位置隐私保护机制中平衡数据效用与隐私保护的方法，并强调了未来上层位置隐私攻击、无线技术和网络融合所带来的新兴挑战。通过阐明定位技术与位置隐私之间的关系，并评估不同位置隐私保护机制的有效性，本综述有助于指导未来车联网位置隐私保护机制的发展。**

索引词—**位置隐私、车联网、第五代移动通信、第六代移动通信、定位、跟踪攻击。**

I. 引言

车联网是第五代移动通信和第六代移动通信等移动系统发展的重要组成部分，在提供可靠的实时信息、提升驾驶安全和效率方面发挥着关键作用。多年来，人们开发了种类繁多的基于位置的服务，以改进这些网络的功能。这些服务用途广泛，包括导航、天气更新、场所定位器、社交媒体交互和群智感知 [1]。借助这些基于位置的服务，驾驶员可以获取交通状况、天气预报以及前往目的地的最高效路线等关键信息。然而，享受这一便利也意味着需要与基于位置的服务平台共享位置数据，这可能会使用户面临隐私风险 [2]。随着车联网在第五代移动通信和第六代移动通信环境中不断发展，如何平衡在确保强大隐私保护的同时发挥基于位置的服务的优势，仍然是一项亟待解决的重要挑战。

B. Ma (0000-0003-4167-2797)、X. Wang (0000-0001-9439-6437)、X. Lin (0000-0002-0133-4737)、Y. Jiang (0000-0002-8176-6264)、G. Yu (0000-0002-6111-1607)、Y. He (0000-0003-1603-9375) 和 R. P. Liu (0000-0001- 7001-6305) 隶属于澳大利亚悉尼科技大学全球大数据技术中心，澳大利亚悉尼，2007（电子邮箱：Baihe.Ma@uts.edu.au；Xu.Wang@uts.edu.au；Xiaojie.Lin@uts.edu.au；Yanna.Jiang@uts.edu.au；Guangsheng.Yu@uts.edu.au Ying.He@uts.edu.au；RenPing.Liu@uts.edu.au）。C. Sun (0000-0003-1529-3179) 隶属于中国杭州之江实验室（电子邮箱：sun.cj@zhejianglab.com）。S. Zhu 隶属于澳大利亚新南威尔士州新南威尔士大学，邮编 2033（电子邮箱：suirui.zhu@student.unsw.edu.au）；W. Ni (0000-0003-0780-4637) 隶属于澳大利亚联邦科学与工业研究组织 Data61，澳大利亚悉尼，邮编 2122（电子邮箱：Wei.Ni@data61.csiro.au）。

A. 未来车联网概述

5G/6G车联网的架构旨在促进无缝数据交换，同时支持多种通信环境，包括地面、水下、空中和太空 [3]。这些网络中的车辆经常共享数据以访问基于位置的服务，这对实时运行至关重要。通过融入边缘计算，网络能够在更靠近终端设备的位置执行计算任务，从而降低延迟和网络负载。图1展示了这些车联网的架构，说明了各种通信模式和组件的集成。该架构的核心组件包括实体、车联网通信（V2X）和基于位置的服务，具体如下：

- **实体：**在车联网中，实体包括基础设施和车辆。传感器、基站（BS）和充电站等基础设施组件充当接入点，为车辆提供服务。车辆包括普通车辆、自动驾驶车辆和无人驾驶飞行器（UAV），它们与其他车辆及基础设施进行交互，以访问基于位置的服务（LBS）。
- **V2X通信：** V2X通信使车辆能够与各种实体交换位置数据，以使用基于位置的服务。这种通信包括车到基础设施（V2I）、车到网络（V2N）、车到车（V2V）、车到行人（V2P）以及车到设备（V2D）通信。
- **基于位置的服务：** 基于位置的服务会收集并存储车辆传输的位置数据，以提供各种服务，包括实时导航和交通管理。

5G/6G赋能的车联网具有互联数十亿台设备的能力，使设备到设备（D2D）通信能够在异构环境中无缝进行。这些网络有望显著提升通信能力，实现更高的数据传输速率、更低的延迟和更强的可扩展性。因此，必须考虑这些特性对车联网中位置隐私保护的影响，因为这些网络在实时高速环境中带来了维护安全的新挑战。

- **高数据速率：** 据预测，支持5G/6G的车载网络的数据速率将比当前网络快数百至数千倍

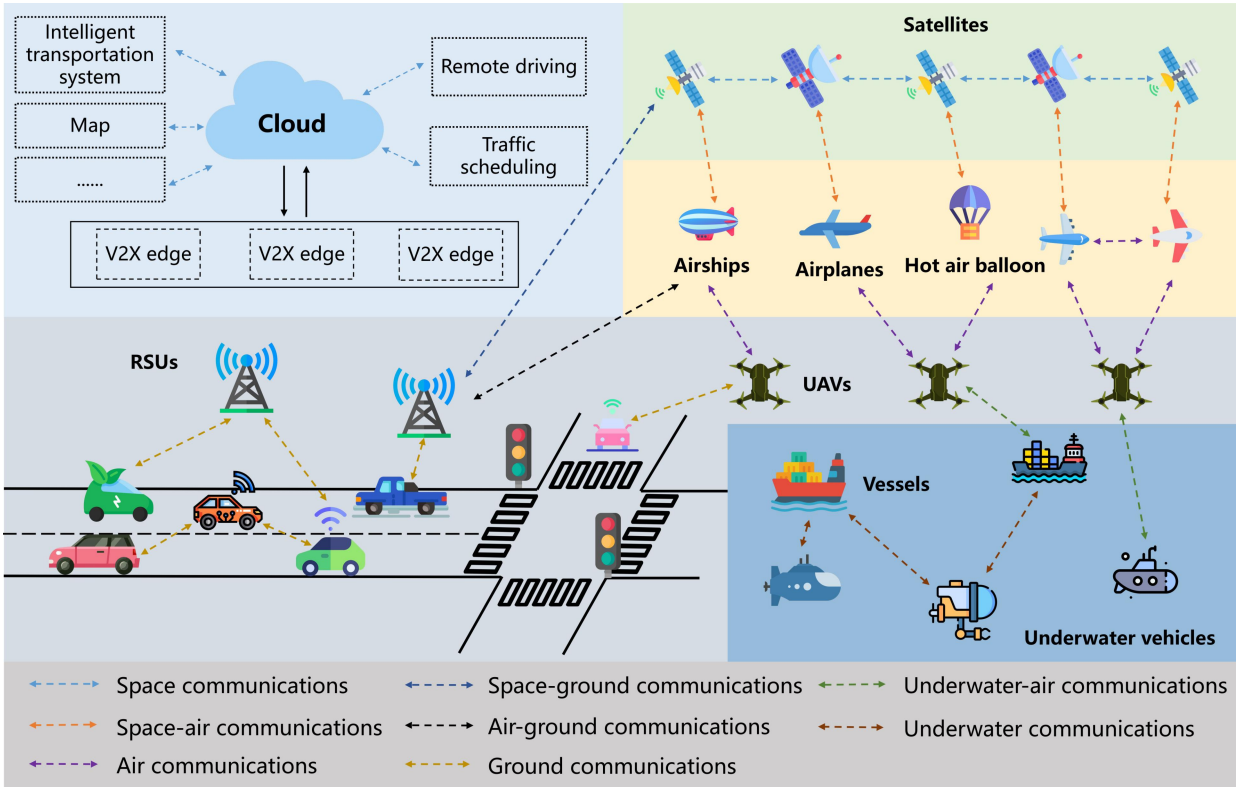

图1. 5G/6G赋能的车联网。通过数据共享，车联网能够从先进技术中获益。采用第五代移动通信（5G）网络的车联网能够提高通信容量、降低通信时延，并改善车联网的连通性。提出了基于人工智能（AI）的下一代（6G）网络，以实现未来网络的智能化。采用人工智能赋能的6G技术的车联网能够在三维环境（例如太空、空中、地面和水下）中提供异构结构。

[4]。采用设备到设备通信、大规模多输入多输出（MIMO）和毫米波等技术，以实现这些高数据速率 [5]。然而，数据速率的提升要求位置隐私保护机制具备较低的计算开销，以便高效处理位置数据。

- **超低延迟：** 5G/6G网络旨在将延迟降低至毫秒级或微秒级，并利用设备到设备通信、软件定义网络（SDN）和云无线接入网（C-RAN）等技术 [6]。确保位置隐私得到保护，同时不显著增加延迟，对于这些系统的正常运行至关重要。

- **高可扩展性：** 凭借支持海量节点（如车辆和其他设备）的能力，启用 5G/6G 的网络依靠网络功能虚拟化实现有效扩展 [7]。尽管可扩展性有助于通过协作增强位置隐私，但在如此庞大且分布式的网络中，检测恶意节点变得越来越困难。

为实现灵活性、安全性和低运营成本，5G/6G赋能的车联网可以采用各种网络管理技术 [3]。这些技术有助于优化网络性能，同时确保有效处理现代车载系统的复杂通信需求。

- **软件定义网络：** 软件定义网络可将网络控制与数据管理解耦，从而更高效、灵活地管理车联网。通过分层架构，控制层负责管理控制器，数据层负责数据转发和协议处理，软件定义网络能够为软件定义网络支持的车辆路径规划等应用提供跨平台且经济高效的解决方案。与机器学习相结合后，软件定义网络还能实现跨多项任务的联邦资源分配。例如，Gao 等人 [8]提出了一种结合软件定义网络与多路径技术的架构，以增强高移动性车联网中的数据传输；Sadreddini 等人 [9]则开发了一种基于软件定义网络的路由协议，可减少链路故障并提高吞吐量。

- 网络功能虚拟化（*NFV*）：NFV可将网络功能虚拟化，从而无需依赖传统的基于硬件的网络架构 [10]。电信服务提供商（TSP）可借此淘汰物理中间盒，简化网络运营并提升服务质量。尽管NFV网络面临挑战，尤其是在资源分配方面，但随着第五代移动通信和第六代移动通信网络的发展，这些问题有望得到解决，从而实现更高效的

先进车联网中的资源管理 [11]

- .**网络切片：**网络切片能够在共享基础设施上创建多个虚拟子网络，以满足车联网中不同的服务质量（QoS）要求。借助软件定义网络（SDN）和网络功能虚拟化（NFV），切片可对自动驾驶、信息娱乐系统和紧急通信等服务进行独立管理和资源分配 [10], [12]。随着第六代移动通信网络的发展，网络切片对于管理多样化的流量需求至关重要，例如超可靠低延迟通信（URLLC）和海量机器类通信（mMTC）。这使得V2X通信能够优化资源利用，并根据实时数据、交通状况和车辆密度动态调整切片，从而提升未来车载应用的效率、安全性和成本效益。

B. 位置数据与位置隐私问题

有效管理位置数据对于确保车联网中的安全和效率至关重要。随着V2V通信和摄像头等先进通信与感知技术的集成，持续产生大量实时位置数据。这些数据在车辆、基础设施和行人之间共享，具有流量大、相关性高、动态变化且敏感程度各异等特点 [13]。正确分析和利用这些位置数据，对于优化交通管理、提升道路安全以及支持智能交通系统至关重要：

- **海量数据：**车联网中基于位置的服务生成的位置数据流量极大，带来了严峻的隐私挑战。每辆车都会持续产生实时位置更新数据流，如果管理不当，可能导致隐私风险。未经授权访问此类数据，可能会暴露有关驾驶员习惯或日常活动的敏感信息 [14]。为降低这些风险，需要采用高级加密技术和数据匿名化方法，确保仅共享必要数据，同时保护个体身份。

- **高度相关性：**车联网中的位置数据具有高度相关性，这意味着即使少量数据也可能揭示大量信息。例如，关联多个位置点可能使观察者重建驾驶员的路线或识别其常去地点。在这种情况下保护隐私，需要采用稳健的聚合和混淆技术。可以运用差分隐私等隐私保护分析方法，在不损害个体驾驶员隐私的前提下提取有助于交通管理的实用洞见 [15]。

- **动态拓扑：** 车联网不断变化的特性，以及车辆移动时位置的持续变动，使隐私保护更加复杂。位置数据的持续更新使实时追踪车辆成为可能，从而构成重大的隐私威胁。应对此问题的有效策略包括使用频繁更换的假名和安全通信信道，以防止窃听 [16]。此外，还可设置位置隐私区域，根据区域敏感程度实施数据匿名化或限制措施，从而进一步保护实时位置数据。

- **重要性不均：**并非所有位置数据都具有相同程度的敏感性 [15]。例如，驾驶员的家庭住址或工作地址，远比涉及停车场等公共场所的数据敏感。有效的隐私保护必须考虑这种重要性差异，采用上下文感知隐私策略。此类策略会根据位置的敏感程度动态调整保护级别，并通过基于同意或多级隐私控制等选择性共享机制，确保敏感程度更高的信息得到更严格的保护。

- **驾驶员安全：**在车联网中共享位置数据，主要目的是提升驾驶员安全，但必须谨慎平衡隐私问题。实时数据共享对于应急响应、导航和碰撞避免等服务至关重要，但同时也会带来隐私风险。因此，应将安全多方计算和区块链等隐私增强技术纳入数据共享协议，以确保只有经过授权的实体才能访问数据。这样既能确保数据完整性，又不会损害隐私，从而增强信任并促进基于位置的服务得到更广泛的应用 [17]。

1) 车联网中的隐私风险： 在车联网的基于位置的服务中共享位置数据会带来重大的隐私风险 [15]。虽然基于位置的服务依赖实时位置数据来有效运行，但不可信的服务提供商和潜在对手会对这些信息的隐私和安全构成重大威胁 [13]。对手可以利用基于位置的服务服务器中的漏洞，通过窃听截获数据，或与不可信的服务器合谋，以获取未经授权的访问权限，访问位置数据 [15]。这些隐私泄露使对手能够分析和滥用共享数据，凸显了车联网亟需强有力的隐私保护机制。

- **驾驶员私人信息的暴露：** 对手可以利用车联网中传输的位置数据，推断敏感的个人详情，例如驾驶员的家庭住址、宗教信仰、政治观点、职业和工作地点 [18]。例如，频繁前往宗教机构或政治办公室，可能会暴露驾驶员的私人信仰和政治归属。定期前往特定地址，也可能泄露家庭或工作地点等个人信息，进而用于对个人或群体进行画像。这些画像可能被用于身份盗窃、歧视或定向骚扰。此外，对手还可以利用这些画像实施个性化攻击、扰乱特定群体的活动，甚至破坏整个车联网系统。此类未经授权访问私人信息的行为会削弱用户对基于位置的服务和车联网的信任，可能降低用户参与度，并损害这些服务的功能。

- **物理攻击：**位置隐私遭到侵犯可能导致现实中的人身威胁，例如跟踪骚扰、入室盗窃，甚至伤害驾驶员 [19]。例如，如果对手

得知驾驶员不在家，可能会以其财产为目标实施入室盗窃。此外，攻击者可能操纵导航系统，将驾驶员误导至易受攻击的区域，从而增加其受伤害的风险。一个典型的例子是欺骗导航数据，制造虚假的交通拥堵，或将驾驶员重新引导至危险地点[1]。如果缺乏充分的隐私保护，位置数据就会成为策划物理攻击的有力工具。

- **其他车辆隐私信息的暴露：**在车联网中共享位置数据不仅会危及个体驾驶员的隐私，还可能损害道路上其他车辆的隐私。对手可以分析共享数据，追踪其他车辆的轨迹并预测其移动情况，其中包括敏感车辆或应急车辆 [20]。例如，通过研究相遇记录和移动模式，对手可能预测车队路线、应急车辆行驶路线，甚至知名人士的行踪，从而可能危及个人隐私和公共安全。追踪或预测关键车辆行踪的能力，对个人和集体安全都构成了重大风险。

*2）5G/6G*车联网中的位置隐私挑战：车联网（VN）的快速发展给现有的位置隐私保护机制带来了重大挑战。随着车联网日益先进，其架构也愈发复杂，导致不同网络层之间交换的数据量不断增加。这种复杂性的提升为对手利用安全漏洞创造了新的机会，尤其是通过复杂的跨层攻击。传统的位置隐私保护机制通常针对单个网络层内的威胁而设计，已不足以应对这些新兴威胁。以下是亟待解决的主要挑战：

- **复杂网络架构：**现代车联网跨越多个层级运行，包括物理层、网络层和应用层。这种多层结构加剧了对手同时利用不同层级漏洞的可能性。**跨层攻击：**对手可以通过结合来自不同层级的信息实施跨层攻击，从而实现更准确、更有效的位置跟踪。旨在保护单一层级的传统位置隐私保护机制无法应对这类协调性的多层威胁。**传统位置隐私保护机制的无效性：**当前的位置隐私保护机制尚无法处理跨层攻击的复杂性。这些机制往往无法提供全面保护，使车联网暴露于跨越多个层级的协调性攻击所导致的隐私泄露之中。**间谍软件与位置跟踪：**类似 Pegasus 的间谍软件工具可以访问历史接触数据。当与实时拦截的信息相结合时，对手能够实现高度精确的车辆跟踪，绕过现有的位置隐私保护机制 [21]。
- **V2X通信中的数据交换日益增加：**The 5G/6G车联网中V2X通信的日益普及，使车辆、基础设施及其他实体之间的数据共享更加频繁且广泛，从而增加了位置隐私泄露的风险。
- **需要多层隐私保护：**为应对5G/6G车联网中不断涌现的威胁，位置隐私保护机制必须不断演进，以提供强健的多层隐私保护。这包括集成高级加密、上下文感知隐私控制以及实时跨层异常检测系统。
- **动态适应不断演变的威胁：**未来的位置隐私保护机制必须能够在高度动态的车载环境中，动态适应实时威胁。这些机制应有效抵御新型跨层攻击，确保在日益复杂的网络场景中实现隐私保护。

C. 贡献

本综述探讨了定位技术及相关应用对位置隐私的影响。具体而言，现有研究尚未充分考虑不同网络层的定位技术以及相关应用对现有位置隐私保护机制构成的威胁，例如 [22], [24]–[28]。如表I所示，现有研究仅关注5G/6G车联网中的位置隐私保护机制。然而，位置隐私与数据效用之间的平衡对位置隐私保护机制的设计至关重要，但迄今为止在文献中一直被忽视，例如 [22]–[29], ，相关详细比较见表I。

鉴于此，我们回顾了最新的定位与跟踪方法及其对车联网中位置隐私构成的潜在威胁。我们还对车联网中现有的位置隐私保护机制进行了深入调查，并从通信和定位需求方面总结了这些机制在应对定位与跟踪技术时的局限性。

With a f关注 he locati隐私i隐私的f vehicul车联网 k

因此，本综述的主要贡献如下。1. 我们分析了不同第五代移动通信/第六代移动通信定位与跟踪范式下，用户侧、服务器端及用户-服务器接口中的现有位置隐私保护机制，并考虑了多源数据和跨层漏洞。2. 我们发现了一项新的挑战：对手可以利用来自不同层的多种跟踪数据，规避对车辆位置隐私的保护。随着基于位置的应用和社交网络平台不断普及，这种威胁日益可能发生，且后果严重。我们详细考察了对手可能如何利用多个数据源，以及如何利用上层和下层定位技术来侵害车辆的位置隐私。3. 我们还发现，位置隐私的理论研究与实际应用之间存在显著差距。为此，我们分析了近期文献和基于位置的应用。造成这一差距的主要原因是不同层的数据可靠性各不相同：实际应用倾向于使用下层数据，而理论方法通常依赖于

[1] https://simonweckert.com/googlemapshacks.html

表I COMPARISON 相关工作的。

参考文献	定位	现有的位置隐私保护机制				其中的位置隐私保护机制未来车载网络[4]		平衡[5]	
		用户侧[1]	服务器端[2]	用户-服务器-接口[3]	局限性				
[22]			✓						
[23]		✓	✓		✓				
[24]			✓		✓				
[25]		✓	✓	✓	✓				
[26]	✓				✓	✓			
[27]		✓	✓	✓		✓			
[28]	✓								
[29]		✓	✓						
[30]		✓	✓		✓			✓	
[31]		✓	✓		✓				
[32]					✓	✓			
[33]					✓	✓			
[34]				✓	✓				
[35]	✓	✓	✓		✓				
[36]	✓	✓	✓	✓	✓			✓	
[37]	✓	✓	✓	✓	✓				
本文	✓ (90)	✓	✓	✓	✓	✓	(28)	✓	(80)

[1] 用户侧：传递并离开、证书、安全计算和数据扰动；[2]服务器端：统计披露控制、同态加密、隐私信息检索和可搜索加密；[3]用户-服务器-接口：安全通信和可信方；[4]车载网络：车联网；[5] 平衡：位置隐私与数据效用之间的平衡。

上层数据。要弥合这一差距，需要采取整体性方法，考虑不同层和数据源之间的数据整合与保护。

4.我们重点指出轨迹数据中时间信息与空间信息之间关系所引发的挑战。轨迹中的时间信息使得能够结合来自不同层面和来源的数据，这可能导致精确跟踪并重建位置信息，从而侵犯位置隐私。我们的分析强调，需要采取稳健的隐私保护策略，同时保护具体位置信息和时间信息。

本文其余部分安排如下。我们在第二节将本文与现有综述进行比较，并评估它们的贡献。第三节列出现有跟踪技术、威胁和位置隐私要求。第四节阐述现有位置隐私保护机制，以及位置隐私与数据效用之间的平衡；随后，第五节讨论未来的位置隐私挑战。第六节总结本文。本文结构如图2所示，所用缩略语和简称列于表 II。

II. 现有综述与差距分析

本文考察了近期研究，尤其是过去五年间发表于 IEEE 和 ACM 的研究，重点关注车联网中位置隐私保护机制（LPPMs）的发展。我们的分析聚焦于定位技术，并探讨保护位置隐私与维持数据效用之间的权衡。本节将我们的工作与 2018 年至 2024 年间发表的先前文献综述 [22]–[37],进行比较，以评估它们的贡献。如表 I 所示，比较聚焦于四个关键方面：定位技术、现有的位置隐私保护机制、车联网中未来的位置隐私保护机制，以及位置隐私保护与数据效用之间的平衡。

本文根据车联网的发展回顾定位技术，并从位置隐私的角度探讨定位技术。Wang 等人 [28]介绍了适用于第五代移动通信和 6G 网络的未来定位技术及其应用。/ Hussain等人 [26]讨论了基于第五代移动通信车联网架构的定位方法及其面临的攻击。

本文根据位置隐私保护机制的部署阶段，并考虑定位技术带来的威胁 [38]，将现有位置隐私保护机制划分为用户侧、服务器端和用户-服务器接口位置隐私保护机制。用户侧位置隐私保护机制使驾驶员能够在将数据发送至基于位置的服务之前对其进行处理，而服务器端位置隐私保护机制则处理数据集中汇总的位置数据。用户-服务器接口位置隐私保护机制利用可信第三方和安全通信，确保位置数据在传输过程中安全。我们全面比较了各类别的相关研究。已发表的综述 [22], [23], [29], [30] 主要关注当前车联网中现有的用户侧和服务器端位置隐私保护机制。

Lu 等人 [22]阐述了当前车联网中基于统计披露控制的位置隐私保护机制，例如匿名性，但未讨论其他技术。类似地， [24]的作者关注统计披露控制中假名变更方法，并比较了不同基于假名的位置隐私保护机制的开销。Sheikh等人 [29]比较了不同对手条件下的用户侧和服务器端位置隐私保护机制，例如证书、安全计算和统计披露控制，并阐述了这些机制的优势与局限。作者列出了现有车联网中对手带来的风险下的位置隐私问题和潜在应用。然而，该研究并未讨论未来车联网中的位置隐私保护机制。

通过考虑相同的场景，Ali 等人 [23] 将位置隐私保护机制（LPPMs）分为基于假名的、基于群组的、混合的、基于匿名的和基于密码学的。作者重新-

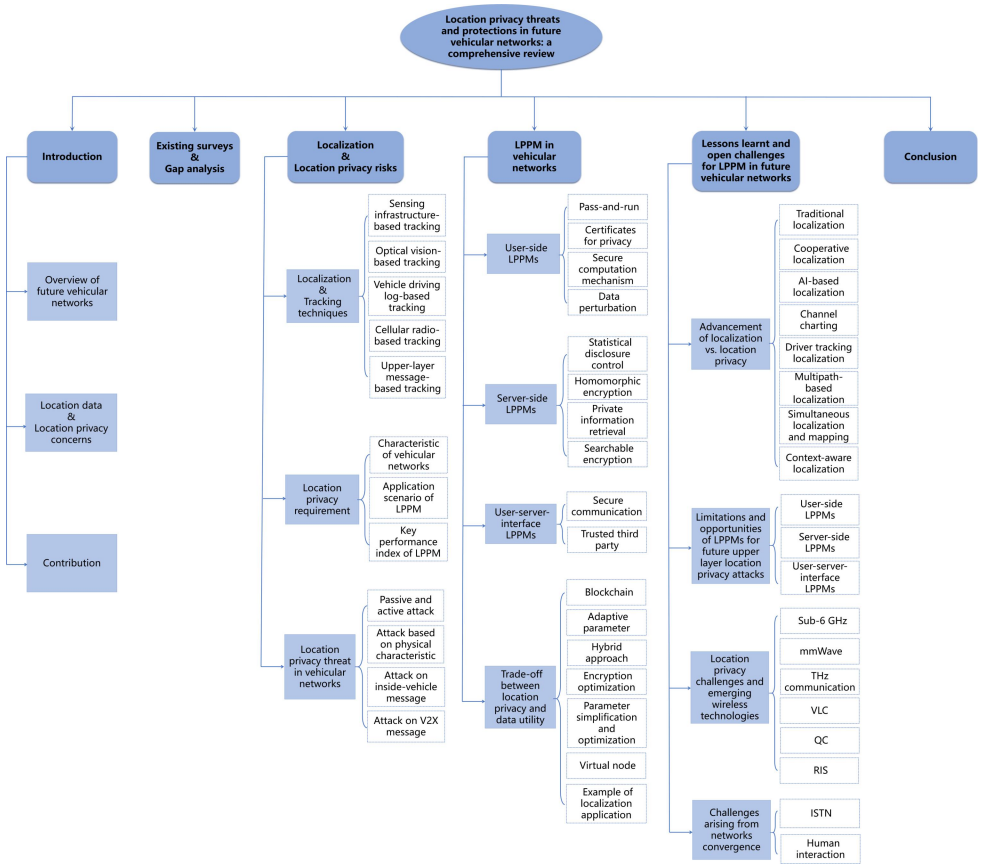

图2。本文的组织结构。第一节：本文的引言；第二节：现有综述与差距分析；第三节：现有跟踪技术、威胁和位置隐私要求；第四节：现有位置隐私保护机制以及位置隐私与数据效用之间的平衡；第五节：未来的位置隐私挑战。

考察了位置隐私要求、攻击以及各类位置隐私保护机制的效率。作者还比较了各类位置隐私保护机制抵御不同攻击的能力，但未能充分考虑用户-服务器接口位置隐私保护机制。在同一研究主题下，Mundhe等人 [31]概述了当前的车联网，并总结了现有的用户侧和服务器侧位置隐私保护机制。作者评估了当前车联网中现有位置隐私保护机制的优势与局限性，尤其关注基于密码学的位置隐私保护机制。Talat等人 [25] 比较了各类位置隐私保护机制的位置隐私保护能力。作者总结指出，在特定情况下，每种位置隐私保护机制都能提供比其他同类机制更高的位置隐私保护能力。研究 [30]聚焦于基于位置的服务的应用，讨论了用户侧和服务器侧位置隐私保护机制，并对其性能进行了定性分析。

本文从车联网的定位需求和未来通信技术角度，评估现有位置隐私保护机制的优势与局限性。

相比之下，Ali等人 [23]，[39] 和Mundhe等人 [31]根据各自的方法，讨论了现有用户端和服务器端位置隐私保护机制的优缺点。Jiang 等人 [30]指出，现有位置隐私保护机制难以满足不同基于位置的服务的需求。Boual等人 [24] 评估了现有车联网中采用语法关联和语义关联的基于匿名的位置隐私保护机制，即服务器端位置隐私保护机制。Talat等人 [25] 考察了更多类型的攻击和位置隐私保护机制，比较了现有车联网中各类位置隐私保护机制在多种攻击下的表现，包括信息/服务拒绝、信息隐私泄露、伪装攻击和数据篡改。Hussain等人 [26],Dibaei 等人 [32]，Boualouache 等人 [33]，和Haddaji 等人 [34] 指出了第五代移动通信车联网中现有位置隐私保护机制面临的潜在挑战。Belal等人 [35]探讨了将联邦学习集成到车联网中以增强位置隐私保护机制，而Rasheed等人 [36] 则系统地研究了侧重于】【。

表 II 缩写UMMARY

缩写	定义
2D	二维
3D	三维
5G	第五代移动通信（5G）网络
6G	人工智能（AI）赋能的下一代
AI	人工智能
AP	接入点
AVI	自动车辆识别
BS	基站
CAN	控制器局域网
CSI	信道状态信息
D2D	设备到设备
ECU	电子控制单元
FHE	全同态加密
Geo-I	地理不可区分性
GNSS	全球导航卫星系统
GPA	全局被动对手
GPS	全球定位系统
HE	同态加密
ID	标识
LBSs	基于位置的服务
LED	发光二极管
LPA	局部被动对手
位置隐私保护机制	位置隐私保护机制
MAC	介质访问控制
MIMO	多输入多输出
毫米波	毫米波
NFV	网络功能虚拟化
OBD	车载诊断
OBU	车载单元
PHE	部分同态加密
PIR	隐私信息检索
QC	量子通信
QoS	服务质量
RFID	射频识别
RIS	可重构智能表面
RSU	路侧单元
SDC	统计披露控制
SDN	软件定义网络
SE	可搜索加密
SHE	轻度同态加密
SLAM	同步定位与制图
THz	太赫兹
TPMS	胎压监测系统
TTP	可信第三方
UE	用户设备
VN	车联网
V2D	车到设备
V2I	车到基础设施
V2N	车到网络
V2P	车到行人
V2V	车到车
V2X	车对万物通信
VLC	可见光通信

位置隐私与查询隐私之间的权衡。Mianji 等人[37]回顾了多智能体强化学习在车联网隐私与安全方面的作用。基于所列威胁，作者讨论了现有位置隐私保护机制的性能。

本文还从第五代移动通信和第六代移动通信车联网未来通信需求的角度，探讨现有位置隐私保护机制在未来车联网中的潜在发展及跨层挑战。Hussain 等人 [26]研究了支持第五代移动通信的车联网中的当前隐私问题及解决方案。作者提出了一种支持 5G 应用的支持第五代移动通信的车联网架构，并开发了潜在的基于机器学习的位置隐私保护机制。Lu 等人 [27]考察了 5G 车联网架构中的位置隐私问题。他们分析了现有的单层攻击，并探讨了 5G车联网中位置隐私保护机制未来的发展方向。Dibaei 等人 [32] 结合未来车联网中的技术，指出了现有位置隐私保护机制的局限性，并据此提出了结合区块链和机器学习的未来位置隐私保护机制潜在发展方向。Boualouache 等人 [33]综述了现有的服务器侧位置隐私保护机制，这些机制通过检测未来第五代移动通信及后续车联网中的不当行为来保护位置隐私。作者提出了人工智能赋能的位置隐私保护机制在未来车联网中的潜在发展方向。Haddaji 等人 [34] 总结了人工智能赋能的车联网中的位置隐私问题。作者涵盖了未来车联网中的隐私与安全问题，并讨论了未来框架内基于人工智能的解决方案。

本文还通过理论和实践案例进一步阐明了位置隐私与数据效用之间的权衡，这对位置隐私保护机制的设计至关重要。在所比较的综述中，只有 Jiang 等人 [30] 讨论了平衡位置隐私与数据效用的方法。他们根据现有位置隐私保护机制中不同位置隐私保护机制的方法论，阐述了这种权衡。本文则从定位需求和车联网未来通信技术的角度，探讨了理论与实践中的权衡。

A. 关键要点

通过对现有研究的综合分析，针对车联网中位置隐私保护机制的开发与应用，我们得出了以下几项关键见解：

- 首先，尽管用户侧和服务器侧位置隐私保护机制已取得显著进展，但如何将二者整合到无缝的用户—服务器接口机制中仍存在空白。这种碎片化特征削弱了应对整体隐私与安全问题的能力，尤其是在复杂的车联网环境中。

- 其次，目前大多数研究侧重于探讨现有网络架构所涉及的需求与挑战，却忽视了新兴第五代移动通信和第六代移动通信技术及其先进攻击向量所引入的跨层威胁。换言之，在不久的将来，应重点开展相关研究，推动基于不断演进的技术构建自适应且可扩展的位置隐私保护机制。

- 第三，尽管许多人将位置隐私与数据效用之间的平衡视为重要权衡之一，但这一问题尚未得到充分研究。关于此类问题的大多数讨论都停留在理论层面，实际验证不足。它们均采用临时指标，而这些指标可能并不适用于不同的应用场景，也未必具有相关性。

III. 定位与位置隐私风险

本节从位置隐私的角度总结了各种车载网络场景中现有的跟踪技术，如表III所示。接下来，我们

概述定位的关键需求，介绍常见的对手模型，并讨论目前影响车联网的潜在隐私威胁。通过考察定位技术带来的威胁，我们介绍了文献中已有充分记载的对手。

A. 定位与跟踪技术

近几十年来，人们开发了各种跟踪技术，以提升高精度基于位置的服务和防盗系统的功能。这些技术提供实时监控和导航功能，对于路线优化、应急响应和被盗车辆追回等应用至关重要 [57]。然而，尽管这些技术具有诸多益处，同样的跟踪方法也可能被对手利用，从而危及驾驶员的位置隐私。

先进的跟踪方法，例如全球导航卫星系统（GNSS）欺骗、蜂窝三角定位以及对车载传感器数据的利用，使对手能够准确推断驾驶员的实时位置、日常路线和习惯模式。滥用这些技术会带来重大的隐私风险，使恶意行为者能够实施监视、定向攻击或身份盗窃。为应对这些威胁，人们开发了多种位置隐私保护机制。这些机制利用数据匿名化 [16], 混淆 [15], 假名化 [58], 和密码协议 [59] 等技术，对车联网中交换的精确位置信息进行隐藏或扰乱。然而，随着现代车联网变得更加动态且互联，跨层攻击等新的安全漏洞不断出现，从而降低了传统位置隐私保护机制的有效性。因此，越来越需要更加稳健且自适应的位置隐私保护机制，在平衡合法基于位置的服务和车载应用对数据准确性与效用的需求的同时，针对先进的跟踪威胁提供全面的隐私保护。

车联网中的跟踪技术可分为五大类：基于感知基础设施、基于光学视觉、基于车辆驾驶日志、基于蜂窝无线电以及基于上层消息的跟踪。虽然大多数位置位置隐私保护机制（LPPM）侧重于缓解基于上层消息的跟踪所带来的威胁，例如防范利用共享车联网数据包的攻击，但往往忽视了基于车辆驾驶日志的跟踪所造成的风险。这种跟踪方式利用车载系统直接记录的数据（如事件数据记录器（EDR）或远程信息处理系统），重建车辆的路线、速度模式和停车位置，从而在无需拦截外部数据的情况下暴露敏感信息。

车联网面临着重大的隐私挑战，这是由于先进跟踪技术的出现，而当前的位置隐私保护机制尚未具备应对这些技术的能力。尤其是基于感知基础设施、基于光学视觉以及基于蜂窝网络无线电的跟踪方法，对位置隐私构成了严重风险。例如，配备传感器和摄像头的路侧单元能够实时捕获并分析车辆位置，而基于光学视觉的系统利用监控摄像头和计算机视觉算法，可以在大范围内跟踪车辆区域。同样，基于蜂窝无线电的跟踪利用移动网络信号，以高精度对车辆位置进行三角定位。由于这些方法不依赖上层车载通信，因此很难通过传统的位置隐私保护机制检测或缓解。车辆广泛暴露于这些基于基础设施的跟踪技术之下，凸显了现有隐私保护中的一个关键缺口，也表明亟需创新策略来应对日益普遍的这些威胁。

1）近距离检测：基于传感器的跟踪技术利用车辆的物理特征，通过感应线圈和磁传感器等设备检测这些特征，从而监测车辆轨迹。这些方法主要用于改善交通管理和安全；然而，若被对手利用，也会对位置隐私构成重大风险。通过这些传感器收集的数据可能被滥用，以持续跟踪特定车辆，使驾驶员面临隐私泄露、定向监控以及潜在的人身威胁。

- **磁传感器：**磁传感器可检测经过车辆造成的地球磁场变化，从而确定车辆的三维位置和二维朝向。这些传感器不仅用于识别车辆是否存在，还能分析行程时间，甚至通过绘制磁扰动图谱来识别车辆。这类跟踪方法（包括 Feng 等人 [60], 提出的局部磁扰动模型）提供了经济且环保的解决方案。然而，这些方法也会带来隐私风险，因为它们能够根据磁特征唯一识别车辆。对手可能利用这些系统追踪移动模式或预测未来位置，尤其是在结合多个传感器的数据时。Su 等人 [61] 通过使用相邻传感器数据和图优化技术，解决了假阳性和检测错误等问题；但若被恶意利用，这些方法也可能提高跟踪精度，生成更准确的移动画像，从而加剧隐私风险。

- **感应线圈：**感应线圈检测器广泛应用于交通管理系统，可收集车辆速度、流量和尺寸数据。尽管这些系统对于实时交通监测至关重要，但事实证明，它们在各个区域都能有效运行，车辆排队建模方面的进展也进一步提升了其效用 [62]。然而，由于它们靠近车辆，且经常安装在关键交通节点，一旦遭到入侵，也可能成为隐私侵犯的目标。Gheorghiu 等人 [63] 指出，尽管这些检测器容易因交通或道路施工而受损，带来维护挑战，但这也造成了安全漏洞，对手可能利用这些漏洞截获未受保护的数据。若有人不当访问感应线圈数据，恶意行为者便可能长期跟踪特定车辆，暴露有关驾驶员日常规律、常去地点和出行模式的敏感信息。这些信息可能被用于恶意目的，包括跟踪骚扰或策划犯罪活动。

- **标签与信号读取器：** 利用自动车辆识别（AVI）系统、射频

表 III EXISTING LOCALIZATION 技术。

技术	描述	主要特征	优势	挑战
磁传感器	捕捉车辆磁场 扰动 [40]	三维位置和二维 朝向检测 [40]	经济实惠、环保	速度分辨率限制； 易受外部场影响
感应线圈 检测器	采集车辆交通 数据 [41]	集成于道路中； 测量速度、流量、 尺寸 [41]	经验证的效用	维护；环境 影响
标签与信号 读者	使用自动车辆识别 , RFID, Wi-Fi/blacktooth MAC 信号 [42]–[45]	通过车辆定位进行分分彩 信号分析 [42]–[45]	利用住宅 Wi-Fi 进行 跟踪	隐私风险；射频识别 必要性
光学视觉	利用.....定位车辆 摄像头数据 [46]	在多种环境中具有高精度 环境 [47]	先进的机器学习/人工智能跟踪	依赖视觉； 高计算负载
ISAC	类似雷达的蜂窝网络信号 用于检测 [48]	被动检测； 双用途信号 [48]	创新型定位 方法	隐私；未经授权 的跟踪风险
基于车辆的 传感器	访问车辆控制 单位数据 [49], [50]	来自各种数据 传感器 [51]	传感器数据融合	数据泄露风险；传感器 依赖
基于移动设备的 传感器	使用移动设备中的全球定位系统进行 跟踪	侧信道攻击 协助	增强外部 定位	隐私问题；数据 对传输的依赖
车载 服务	提升驾驶 体验 [3]	生成地理位置数据	对现代 车辆至关重要 [3]	隐私与安全 担忧
ToA	通过信号定位车辆 时间时延	与车辆一起使用 锚点 [52]	位置误差缩减 估计 [53]	传输计划； 环境因素
TDoA	利用时间差异在 多个信号到达娱乐主管 接收器来定位射频 来源 [54]	增强型三维定位 精度 [55]	在各种场景中的 鲁棒性	受同步限制 需求、信号干扰， 以及计算需求
RSS	基于 sig- 信号强度衰减	近场跟踪 [56]	精确近场 定位 [56]	环境影响；高 衰减
无线电 指纹	识别独特的 ra- 二极管波签名 [56]	硬件特定信号 分析 [56]	接收信号强度数据库创建 分析	隐私问题； 硬件限制
DoA	根据以下信息进行三角定位： 信号角度 [52]	精确的二维定位	准确定位 [52]	大型天线阵列；信号 处理复杂度

频率识别（RFID）标签以及 Wi-Fi/蓝牙媒体访问控制（MAC）信号的技术对车辆定位至关重要，但若被对手利用，也会带来严重的隐私风险 [42], [45]。家庭 Wi-Fi 网络的普及又为这些风险增添了新的层面。当车辆穿过城市环境时，可能会被众多广播其 MAC 地址的住宅 Wi-Fi 设备检测到。广泛的连通性使对手能够利用密集分布的 Wi-Fi 设备网络，准确追踪车辆的位置。通过监测 MAC 地址广播的序列和时间，他们可以重建车辆的路线，识别常去地点，并预测未来的行驶轨迹，从而损害驾驶员的隐私。

近场通信（NFC）设备（如 RFID标签）在密集部署时也会带来跟踪风险。Liu 等人 [64]展示了 RFID读写器如何通过分析反向散射信号相位来确定标签的位置。虽然这种方法在定位方面非常有效，但也可能被恶意用于跟踪车辆经过路线上的多个 RFID读写器时的行踪。结合视频监控或 GPS数据等其他数据源后，基于 RFID 的跟踪能够提供更加详细的车辆移动信息，从而加剧隐私威胁。

由于这些唯一标识符会持续广播，与 MAC 地址跟踪相关的隐私风险尤其令人担忧。Spiess [65]指出，对手如何利用 MAC 地址广播来长期跟踪车辆，从而实施未经授权的监视，并可能导致定向攻击或胁迫行为。Liu 等人 [66]进一步阐述了使用 Wi-Fi MAC时隙跟踪车辆时存在的安全漏洞。通过观察广播的时间和顺序，对手无需直接访问车载系统，便能有效定位和监控车辆。虽然有些方法建议采用

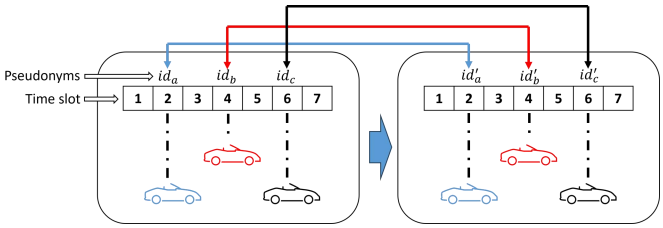

图 3. 基于 MAC 层上下文数据的跟踪攻击示例 [66]。

假名变更计划以中断持续跟踪，但对手仍可汇总数据，并运用复杂的模式识别技术适应这些变化。尽管这些定位技术在交通管理、收费和车队监控等应用中具有显著优势，但一旦被滥用，也会对位置隐私构成重大风险。借助自动车辆识别、射频识别和 Wi-Fi/蓝牙 MAC 数据进行持续、高精度跟踪的可能性，意味着亟须采用更强有力的隐私保护协议、加强监管，并实施技术保障措施，以防止未经授权的数据收集和滥用。此外，开发先进的匿名化方法和加密通信协议，对于缓解日益严重的位置隐私威胁至关重要。

- **光学视觉：** 基于光学视觉的定位系统依靠摄像机捕获的几何帧数据，即使在纹理较少或能见度较低的环境中，也能准确确定车辆位置 [46]。尽管这些系统对于交通管理和监视非常有效，但当被滥用时，其持续跟踪车辆的能力会带来严重的隐私风险。通过利用先进的机器学习（ML）和人工智能（AI）技术，这些系统可以提取车辆外观特征（如颜色和纹理），并将这些数据与语义信息相结合，从而提高跟踪精度 [47]。

  这种能力使对手能够跨多个摄像机网络跟踪车辆，或根据车辆的显著特征推断其身份。例如，Yang 等人 [67] 开发了一种协同感知系统，该系统利用度量学习，将外观数据与交通网络连接相结合，以重新识别车辆，从而实现高精度跟踪。如果被恶意利用，此类系统可能实现持续监控，使对手能够在较长距离或复杂环境中监视目标车辆，进而严重损害位置隐私。

2）蜂窝感知与跟踪： 为了在车联网中实现有效的跟踪与定位，将紧凑型全向传感器阵列与波束成形技术相结合具有显著优势，因为这种方式能够同时捕获来自多个方向的信号，从而提高定位精度 [68]。然而，全向天线面临着诸多挑战，例如信号在长距离传输过程中会发生损耗，这限制了其在需要较长通信距离的应用中的效用。为了克服这些挑战，研究人员采用了定向高增益天线，将信号能量集中在特定方向，从而提高了……

信噪比（SNR），并支持更可靠的远距离通信。

除了天线设计方面的进步外，人们还开发了信号处理方法来提升车辆定位能力。例如，Burghal 等人 [69]提出了一种定位方法，该方法利用来自多天线收发器的信道状态信息（CSI），并结合前馈神经网络。这项技术减少了可训练参数的数量，从而无需大量计算资源即可实现高效、精准的定位。

毫米波（mmWave）通信进一步提升了车辆定位能力，相控阵的电控波束指向性可实现精准测向 [70]。配备毫米波天线的基站可以采用多种测向算法，通过交叉方位定位实现高精度的车辆三角定位。基于蜂窝无线电的跟踪技术，例如到达时间差（TDoA）和接收信号强度指示（RSSI），也利用蜂窝网络广泛部署的基础设施来辅助定位。这些方法在城市和农村环境中都非常有效，凭借蜂窝网络的广泛覆盖，能够提供稳健的定位能力。

- **到达时间（ToA）：** 基于到达时间（ToA）的定位技术通过测量从车辆传输到多个锚点的信号时延来确定车辆位置。虽然这些方法能够有效确定车辆位置，但若被对手利用，便会带来显著的隐私风险。通过分析 ToA 测量值并求解基于时延的非线性方程，对手可以估算车辆的精确位置；如果他们事先了解车辆的传输计划，这种情况尤其如此。借助多个参考点，对手便可利用这些信息进行三角定位，从而跟踪车辆的移动。

  然而，基于 ToA 的定位精度可能受到多种因素影响，例如距离测量误差和锚点部署不理想。此外，如果对传输计划作出错误假设，也可能导致定位不准确。Rao 等人 [53] 针对这一问题提出了一种最小化估计误差的方法，该方法利用误差大小与距离之间的相关性，将误差限制在可接受的阈值范围内。尽管有所改进，基于 ToA 的跟踪仍然构成隐私威胁，因为它所需的硬件成本相对较低，且在中等距离内能够抵御信号衰减，因此对手也容易获取。

  此外，由于基于到达时间（ToA）的定位依赖于对传输时序的了解，任何此类信息的泄露都可能导致持续且高度准确的跟踪，严重损害驾驶员隐私。为应对这些风险，必须实施相应对策，包括采用安全的传输协议以及对传输时序进行动态随机化，以防止恶意行为者滥用基于 ToA 的定位。

- **到达时间差：** 到达时间差是一种通过使用三个或更多个同步的射频（RF）信号源来确定其位置的有效方法。

同步接收器捕获同相/正交（I/Q）数据，并分析信号到达这些接收器的时间差。通过各接收器推算出的距离曲线的交点，可以精确确定信号源的位置。虽然到达时间差在定位方面具有很高的准确性，但如果被对手利用，也会带来重大的隐私风险；对手可以借此在未经同意的情况下追踪车辆或其他目标。

在 Sinha 等人的一项研究中，作者探讨了三维定位的局限性，以及天线特性对其精度的影响。通过部署配备单个或多个偶极天线的多个射频传感器，他们提取了到达时间（ToA）和到达时间差（TDoA）信息，并通过考虑视距（LoS）和非视距（NLoS）场景中不同的信号辐射模式，提高了定位精度。尽管这些进展增强了三维定位的鲁棒性和精度，但也增加了对手滥用该技术的可能性。恶意行为者可以利用这些技术，通过捕获射频辐射并利用到达时间差计算位置，跟踪车辆甚至无人机（UAV），即便是在复杂的城市环境中也能做到。

利用到达时间差技术跟踪车辆的能力，对位置隐私构成了严重威胁，因为这使对手能够以极少的基础设施在大范围区域内实施秘密监视。此外，通过合并来自多个接收器的数据，攻击者可以减少信号遮挡或反射造成的误差，从而增强跟踪能力。此类滥用可能导致未经授权的监控、通信拦截，以及车辆或个人遭到潜在的定向攻击。这些风险凸显了采取先进对策的迫切性，例如安全通信协议、动态跳频和信号加密，以防范这些隐私威胁。

- **到达方向（DoA）：** 基于 DoA 的跟踪通过分析多个天线接收信号的角度来确定车辆的二维位置。这项技术在存在多条信号路径的环境中特别有用，因为反射可能会降低定位精度。通过分离并利用入射信号的角度，DoA 方法可以有效滤除这些反射，从而实现更精确的定位，尤其是在复杂的城市地区。Xu 等人 [71] 通过采用大规模均匀线性阵列（ULA）而非传统的小规模天线阵列，改进了这一方法。这项改进提升了高维环境中的空间分辨率和信号接收能力。该研究还通过应用线性变换来减少信号干扰，从而应对天线之间的互耦干扰。此外，托普利兹校正和相位变换技术纠正了相位误差，提高了精度。所提出的方法结合信噪比数据和信号角度，实现了可靠、高精度的 DoA 跟踪。

尽管取得了这些进展，但若被滥用，基于到达方向（DoA）的跟踪会带来重大的隐私风险。先进的 DoA 系统使对手能够部署大规模天线阵列，捕获由车辆发出的信号中的角度数据，从而以极高的精度跟踪其行驶轨迹，即使是在人口稠密的城市地区也是如此。DoA 跟踪中使用的先进校正技术，会削弱信号混淆和假名变更等传统隐私保护措施对防止未经授权跟踪的效果。这种能力可能会严重危害敏感场景中的安全和人身安全，例如监控执法部门或军用车辆，这凸显了采取强有力的对策以防范此类隐私威胁的必要性。

- **接收信号强度（RSS）：** 基于 RSS 的跟踪依靠测量路径损耗、衰落和阴影效应等因素造成的信号强度衰减，来估计车辆或目标的位置。由于方法简单且信号强度数据易于获取，它被广泛用于无线网络中的定位。然而，对手可以利用此方法跟踪车辆，而无需复杂的基础设施。Huang 等人 [72]针对近场区域中基于 RSS 的跟踪所面临的挑战提出了解决方案；在这些区域，障碍物往往会降低定位精度。他们提出了一种在节点之间创建虚拟视距（LOS）路径的方法。他们优化了方位角和相位参数，以最大化 RSS，从而提高精度并降低计算需求。

尽管这一进展提升了复杂条件下的定位能力，但也带来了显著的隐私风险。攻击者可能采用类似技术，即使存在信号遮挡或多径干扰，也能跟踪车辆。通过模拟虚拟视距（LOS）路径并微调 RSS 参数，攻击者能够绕过信号干扰或假名变更等常见隐私保护措施。这将使攻击者能够持续、隐蔽地跟踪车辆，进而可能导致未经授权的监视、定向攻击或胁迫性监控，从而加剧隐私漏洞。

- **无线电指纹：** 基站发出的无线电波具有独特特征，这些特征称为“无线电指纹”，可被系统性地收集起来，建立用于跟踪车辆的 RSS 信息数据库。攻击者可以利用与每辆车通信硬件相关联的独特射频指纹，准确跟踪车辆。Chen 等人 [73]在车联网中常用的 IEEE 802.11p 协议下，利用专用短程通信（DSRC）对此进行了演示。通过分析物理层帧中的前导码字段特征，他们提取出了各车辆硬件独有的射频指纹。

这些射频指纹由硬件组件固有差异产生，使对手能够将先前记录的指纹与集中式数据库进行关联，从而持续监控车辆。这种方法可以绕过较高通信层中的假名变更或加密等隐私保护机制。利用射频指纹识别和跟踪车辆会带来重大的隐私风险，使未经授权的监视以及跟踪骚扰、车辆劫持或数据泄露等潜在定向攻击成为可能。在车辆

发送未加密或未受保护的信号时，便容易遭受被动窃听和数据收集。为降低这些风险，必须开发先进的对策，例如射频指纹随机化技术、安全通信协议和硬件级保护。这些策略有助于隐藏或修改车载通信系统发出的独特标识符，从而加强位置隐私，并防范复杂的跟踪技术。

- **集成感知与通信（ISAC）：** ISAC 是车联网中的一项先进技术，它利用蜂窝无线电信号将通信与被动车辆检测相结合。ISAC 的工作方式类似于雷达，利用现有基站基础设施分析反射信号，从而检测和跟踪车辆，无需车辆主动发射无线电信号。这种方法能够持续监测车辆；汇总多个基站的数据后，还可以准确重建车辆轨迹。

尽管 ISAC 在交通管理和安全方面具有显著优势，但也会带来隐私问题。由于车辆不会主动传输信号，驾驶员难以察觉正在受到监控，对手可能会利用其被动跟踪能力进行秘密监视。恶意实体可以整合来自不同基站的数据，绘制大范围内车辆的实时移动情况，进而揭示驾驶模式、常去地点和个人行为等敏感信息。这种程度的跟踪会严重威胁位置隐私，削弱加密和假名变更等依赖主动传输的传统隐私保护机制。

为减轻 ISAC 的滥用，必须制定隐私保护措施。这些措施可包括数据匿名化技术、安全数据共享协议和监管框架，以确保 ISAC 数据仅用于合法目的，防止未经授权的跟踪或监视。

3) 车内感知与跟踪：车辆技术的快速发展显著增加了车内通信系统的复杂性，并带来了新的隐私挑战。控制器局域网（CAN）等系统广泛用于管理和记录车辆数据，如近期研究所指出的，它们如今会跟踪多种参数，包括速度、发动机状态和传感器活动 [74]。智能手机和笔记本电脑等移动设备作为额外感知平台的使用日益普遍，进一步扩大了车辆内所收集数据的范围和细节。这种扩展加剧了隐私风险，因为敏感信息可能通过数据恢复、模式分析和轨迹匹配技术遭到暴露。

- **车内数据收集：** 连接至控制器局域网的车载诊断（OBD）读取器对于访问车辆电子控制单元（ECU）的详细数据至关重要，可提供发动机性能、速度和传感器输出等参数的相关信息。为增强安全性，制造商将控制器局域网划分为多个子网络，旨在降低与通过单一传感器进行跟踪相关的风险。然而，面对通过多个车载诊断读取器聚合数据的高级定位攻击，这种防御措施仍然不足。对手可以整合来自各种来源的信息，包括惯性测量单元（IMU）、航向、压力和速度传感器，从而准确绘制车辆的轨迹和行为 [51]。

这种能力对位置隐私构成了重大威胁，使恶意行为者能够追踪并重建车辆的移动轨迹，即使是在GPS信号较弱或不可用的区域也是如此。此外，结合此类数据流，对手能够预测未来路线、分析驾驶模式并识别常去地点，从而实现定向监控或画像分析。通过整合来自多个传感器的数据所达到的精度，削弱了CAN子网络所提供的隐私优势，因此有必要采取更强有力的隐私保护措施来应对这些风险。

- **胎压监测系统（TPMS）：** TPMS是集成在车辆无线网络基础设施中的一项关键安全功能，旨在监测并报告轮胎气压。然而，由于该系统使用唯一可识别传感器，且其通信协议容易遭受逆向工程攻击，因此也带来了显著的隐私风险。每个TPMS传感器都会广播一个独特的标识符，以便将气压变化告知车辆中央系统。这些广播频繁发生，且驾驶员并不知情，配备被动跟踪能力的路侧单元（RSU）或其他对抗设备可以截获这些广播。通过捕获这些TPMS数据包，对手可以利用这些唯一标识符，长期跟踪特定车辆，并重建其路线和驾驶模式 [75]。

TPMS 使秘密监视成为可能，因为 TPMS 数据的持续传输使攻击者能够在不引人注意的情况下收集位置信息。此外，TPMS 协议缺乏加密机制，且容易受到逆向工程攻击，使对手能够轻易解码数据，进一步加剧了对位置隐私的威胁。在车辆经过多个路侧单元（RSU）的人口密集型城市地区，对手可能会整理出车辆移动的详细记录，从而识别其常规路线、目的地和行为模式。这种程度的跟踪会带来严重风险，包括未经授权的监视、定向跟踪骚扰，以及车辆盗窃或劫持等潜在犯罪活动。解决这些安全漏洞需要采取强有力的安全措施，例如对 TPMS 数据采用加密通信协议、使用匿名化技术隐藏传感器标识符，以及建立监管框架，以防止未经授权的数据拦截和滥用。

- **移动终端：** 配备全球定位系统和其他传感器的手机被广泛使用，大幅增加了侧信道攻击的风险；这类攻击能够推断行驶轨迹并危害位置隐私。戴姆勒克莱斯勒的Tegaron等系统将先进的导航功能与向集中控制中心的数据传输相结合，充分体现了车载系统容易遭受外部定位攻击和安全漏洞。通过将车辆数据传输至控制中心，Tegaron等系统

会暴露敏感信息，对手可能截获这些信息，并利用它们暗中监视车辆移动。此外，已知对手会利用移动传感器数据（包括加速度计、陀螺仪和磁力计）准确追踪车辆移动。Guha 等人 [76]的研究表明，即使不直接使用全球定位系统输入，加速度计和陀螺仪的测量值也能够检测并分析车辆动力学，从而重建精确的行驶路线。攻击者能够被动收集广泛普及的移动设备所产生的传感器数据，进而推断车辆的速度、方向和移动模式。若将这些数据与外部数据库（如包含道路网络数据的数据库）结合，攻击者便能揭示敏感位置、常去目的地和驾驶习惯，进而实施未经授权的监视、画像分析，并可能以个人或资产为目标。

- **车载服务与应用：**为增强自动驾驶功能并提高乘客舒适度，车载服务与应用迅速扩展，这大大增加了保护车辆数据隐私的难度。这些系统如今已成为现代车辆运行不可或缺的一部分，它们持续收集并传输大量数据，包括车辆状态（如速度、制动情况和发动机性能）的详细信息、地理位置，以及用户与车辆界面的交互信息 [3]。

此类数据收集对于优化车辆性能、提供实时交通更新以及支持高级驾驶辅助系统（ADAS）至关重要，但也带来了诸多隐私风险。对手可以利用这些系统中的安全漏洞，通过入侵联网应用或拦截传输至外部服务器的数据，未经授权地访问敏感数据流。导航系统依赖频繁的位置更新，因此尤其容易受到攻击，这使恶意行为者能够跟踪车辆、重建路线，并识别常去目的地或行为模式。

旨在提供个性化服务的应用（如信息娱乐系统、预测性维护或路线优化）通常需要持续与云平台共享数据，从而增加数据泄露或未经授权的数据聚合风险。滥用这些数据可能导致未经授权的画像分析、定向广告、跟踪骚扰，甚至劫车或车辆盗窃等更严重的威胁。这些服务产生的大量数据凸显了严格落实数据管理实践的必要性，包括采用稳健的加密、安全的认证协议和严格的访问控制，以保护智能交通系统中的用户隐私。

4）基于上层消息的跟踪：基于上层消息的跟踪对车联网中的位置隐私构成了重大风险，尤其是通过拦截车联网通信或直接攻击参与基于位置的服务的实体。如图4所示，基于位置的服务系统由三个主要组件构成：用户（驾驶员及其设备）、服务器（基于位置的服务服务器和位置隐私服务器）以及网络（Wi-Fi、蜂窝网络和互联网）。每个组件都容易受到

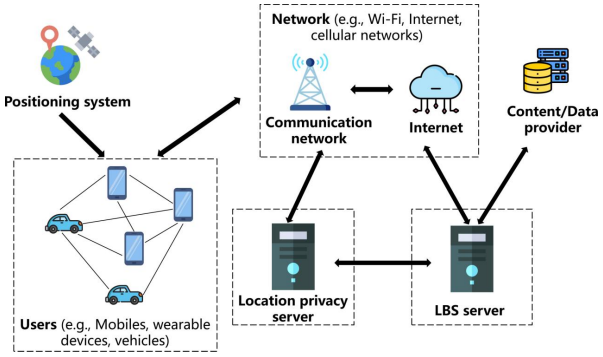

图4. 基于位置的服务系统模型。基于位置的服务由驾驶员、服务器和网络组成。驾驶员通过接入点（例如基站和路侧单元）访问车联网。随后，基于位置的服务服务器会响应驾驶员的查询。所有这三个组件都可能受到对手的威胁。

利用可能会让恶意行为者访问敏感位置数据并损害隐私。

对手可以窃听车联网通信，以追踪车辆的实时位置，或攻击处理或存储位置数据的服务器。人们日益依赖基于位置的服务进行导航、交通管理和获取个性化服务，而这些服务都需要持续交换位置信息，这加剧了上述风险。因此，保护这些组件对于维护网联车辆网络中的用户隐私至关重要。

- **用户组件：** 驾驶员、车辆及其相关设备（如手机和可穿戴设备）可能因数据拦截而面临隐私威胁。车辆中的设备经常通过接入点（包括基站和路侧单元）与外部网络通信。如果对手设法窃听这些通信，就可能直接从设备获取敏感位置数据，泄露实时位置、路线历史记录或常去目的地。

- **服务器组件：**基于位置的服务和位置隐私服务器负责处理位置查询，并管理用户与服务提供商之间的数据交换。这些服务器是对手的主要攻击目标，因为攻破它们可能会让攻击者访问聚合数据，包括用户的位置和移动模式。例如，针对基于位置的服务服务器的攻击可能使对手得以拦截查询、长期追踪用户，或修改位置数据以误导或追踪个人。
- **网络组件：**用户与服务器之间通过 Wi-Fi、蜂窝网络和互联网等信道进行通信，而这些信道容易受到网络窃听。对手可能在传输过程中拦截数据包，从而危及位置数据的机密性和完整性。例如，中间人（MitM）攻击可用于捕获或篡改通过网络发送的消息，进而向未授权方泄露敏感位置信息。

利用上层基于消息的跟踪技术的对手，大致可分为主动攻击者和被动攻击者。利用上层基于消息的跟踪技术的对手

可以大致分为主动攻击者和被动攻击者 [77]。主动对手会通过注入伪造数据、发起欺骗攻击，以及克隆或捕获合法驾驶员以向网络中插入虚假消息，主动干扰网络通信。相比之下，被动对手专注于监控和分析数据流量，通过拦截通信流来推断驾驶员的位置、路线和日常行程，而不会直接干扰或篡改通信流。鉴于被动对手行事隐蔽，且对隐私的影响可能更广泛，当前的位置隐私保护机制优先防御此类对手。主动对手会通过注入伪造数据、发起欺骗攻击，以及克隆或捕获合法驾驶员以向网络中插入虚假消息，主动干扰网络通信。相比之下，被动对手专注于监控和分析数据流量，通过拦截通信流来推断驾驶员的位置、路线和日常行程，而不会直接干扰或篡改通信流。鉴于被动对手行事隐蔽，且对隐私的影响可能更广泛，当前的位置隐私保护机制优先防御此类对手。

在车联网中，被动对手会对位置隐私构成重大威胁。根据监控能力的范围，这类对手分为两种：全局被动对手（GPA）和局部被动对手（LPA），如图 5 所示。全局被动对手是能力最强的被动攻击者，监视范围极广。他们能够截获整个网络中的数据传输，并利用对道路基础设施的全面了解、对授权系统的合法访问权限，或应用中的安全漏洞。他们可以在数小时乃至数年的较长时间内收集和分析数据，从而重建车辆移动的详细模式。由于其访问范围广、监控时间长，全局被动对手在许多隐私保护框架中被视为最危险的对手模型 [78]。然而，部署大规模全局被动对手通常受到高昂基础设施维护成本的限制。相比之下，局部被动对手的活动范围较小，通常只在局部区域内开展监控，所需资源也较少。尽管监控范围有限，局部被动对手仍会带来相当大的隐私风险，尤其是在针对特定车辆或地理区域时。他们能够在有限范围内收集详细的位置数据，造成与全局被动对手同样的隐私泄露，只是目标更加集中。

如图 6 所示，位置攻击通常包括四个主要步骤：数据收集、分析、推断和暴露。首先，对手通过窃听、数据拦截或系统入侵等方法获取位置数据。随后，他们利用上下文关联、概率论、机器学习等先进技术，或借助（虚假）同伴用户场景分析这些数据，以推断车辆的位置。最后一步是暴露驾驶员身份、离散化轨迹点和连续移动路径，对手可将这些信息用于各种恶意目的，包括未经授权的监视、用户画像或定向攻击。

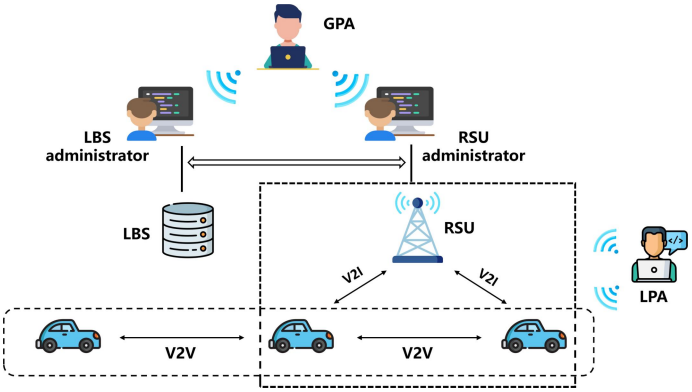

图 5. 用于车辆位置隐私保护的 GPA 和 LPA。GPA 掌握完整的道路信息，因此能够窃听网络中传输的数据；而 LPA 只能使用有限设备，在较小范围内进行窃听。

车联网中基于上层消息的跟踪所面临的关键问题是容易受到各种可能危及隐私的网络攻击。网络对手利用数据传输中的漏洞，采用先进的大数据挖掘技术，从较低层收集并聚合信息。这些信息包括邻近检测、交易日志、停车位置和 Wi-Fi 信号数据等来源，所有这些信息都可以结合起来，形成车辆移动的详细画像。当攻击者拦截并挖掘这些聚合数据时，他们能够准确重建车辆轨迹，并推断敏感的位置信息，从而带来严重的隐私威胁。

为应对 5G/6G 车联网中日益受到关注的位置隐私问题，人们开发了各种位置隐私保护机制，专门用于保护位置和轨迹相关数据，防止基于上层消息的跟踪。这些机制旨在模糊消息与特定用户或位置之间的可关联性，使对手难以准确跟踪车辆。为增加对手实施攻击的难度，人们采用了上下文关联混淆、概率性数据修改、基于机器学习的异常检测，以及生成难以区分的虚假用户画像等方法。这些技术尤其能有效缓解身份推断、分段轨迹暴露以及连续行驶路径重构所带来的风险 [79]。如第四节所述，这些策略对于保护上层数据层中的用户隐私至关重要，也进一步彰显了它们在防范日益复杂的位置隐私威胁方面的作用。

B. 位置隐私要求

研究人员对车联网中的位置隐私有多种定义 [80]，[81]。本文将位置隐私定义为信息隐私的一个子集，侧重于保护位置数据，使驾驶员能够控制其数据何时、以何种内容以及通过何种方式共享。这一定义强调需要建立可靠的机制，确保在车联网中共享的数据不会危及驾驶员的安全，也不会使其面临潜在威胁。车联网的核心隐私要求

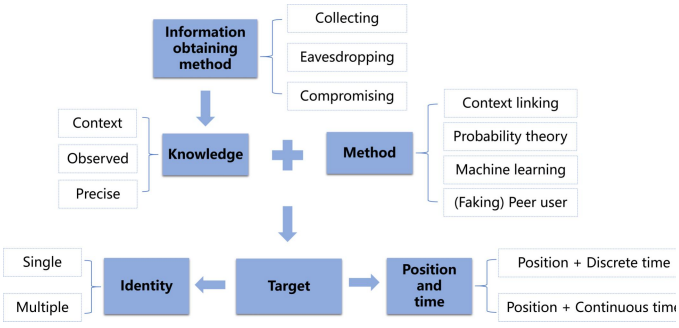

图6. 位置攻击与对手概览。对手可以通过收集、窃听和攻破车辆信息来获取驾驶员的位置信息。通过分析所获取的数据，对手可以利用这些信息了解驾驶员。

可分为四个关键类别：机密性、匿名性、不可链接性和上下文不可观测性 [82]。

- **机密性：**机密性是位置隐私的基石，可确保车辆与外部服务（例如基于位置的服务）之间交换的数据保持安全，不会被未经授权的实体访问 [83]。这通过采用稳健的加密协议来保护传输中的数据，从而防止对手窃听或拦截数据。若缺乏强有力的机密性保护措施，敏感位置数据可能会暴露，导致严重的隐私泄露，例如实时跟踪、驾驶员行为画像分析，或数据被恶意用于跟踪骚扰或盗窃。例如，对手可能会拦截车辆发送至基于位置的服务服务器的位置查询，从而获知车辆当前位置和路线信息。**匿名性：**匿名性对于保护车联网中车辆的身份至关重要，可确保即使位置数据遭到拦截，也无法识别具体车辆或驾驶员 [84]。通常通过假名化实现这一点：车辆使用频繁更换的临时标识符，以防对手长期跟踪或进行画像分析。在车辆频繁与路侧单元或其他车辆通信的环境中，匿名性尤为重要；若缺乏匿名性，攻击者便能将位置数据与特定车辆或驾驶员关联起来，进而发动定向攻击或造成严重的隐私泄露。**不可链接性：**不可链接性确保对手或未经授权的实体无法将位置数据与车辆身份关联起来，即使数据遭到拦截也是如此 [85]。这项保护对于防止纵向跟踪至关重要，因为攻击者可能会随着时间推移不断收集数据，从而推断车辆的路线、出行模式或常去目的地。为保持不可链接性，人们采用了多种技术，例如随机化标识符、延迟传输时间或使用混合区域。在这些区域中，车辆会在受控环境下更换标识符，从而有效切断任何可追踪性联系并增强隐私。**上下文不可观测性：**上下文不可观测性对于确保同一车辆连续的数据传输不会暴露可能损害隐私的模式至关重要 [86]。这项保护可防范推断攻击，即对手分析数据发布中的重复行为

以推断车辆的移动情况和日常规律。例如，如果车辆持续传输位置更新，显示其频繁前往特定地点（如家或工作地点）的模式，对手便可能将这些数据片段结合起来，描绘出车辆的完整日程。为此，通常会采用混淆技术（通过更改数据来掩盖实际模式）或差分隐私（通过添加统计噪声）等方法，以防止得出准确推断。

机密性确保未授权方无法访问车辆通信数据，从而保护内容不被窃听者获取；匿名性则隐藏数据中车辆的标识符，防止其与特定驾驶员关联。不可链接性进一步防止对手将不同数据与同一车辆联系起来，从而难以随时间追踪移动模式。上下文不可观测性确保连续的数据发布彼此不相关，防止对手通过重复观察推断轨迹或行为。

1）车联网的特征：车联网具有区别于其他通信环境的鲜明特征，例如不受限制的传输功率、更强的计算能力以及可预测的移动模式。这些因素给位置隐私保护带来了独特挑战。车联网的特征大致可分为三个方面：拓扑特征、节点特征和传输特征，如图7所示。了解这些特征对于设计有效的位置隐私保护机制至关重要，从而应对车联网固有的特定威胁和安全漏洞。

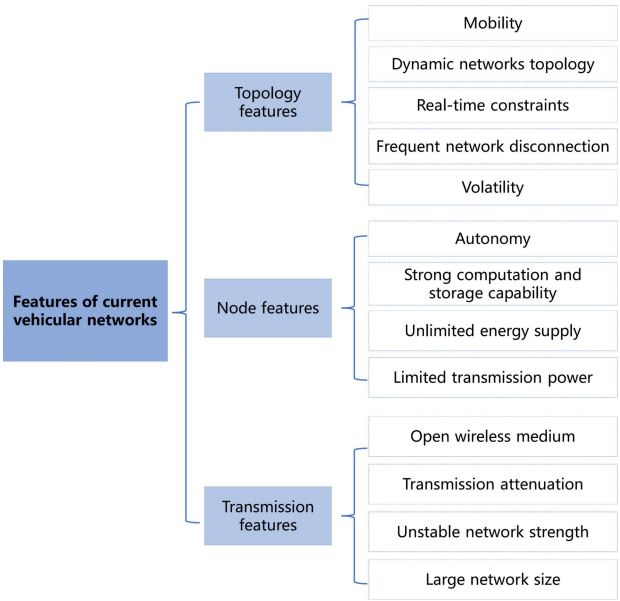

图7。车联网的特征。拓扑特征、节点特征和传输特征使车联网与其他场景存在显著差异。

拓扑特征：车联网具有独特的拓扑特征，会对位置隐私产生重大影响，

包括高移动性、动态网络拓扑、实时约束、频繁断连和连接波动性。

- **移动性：**车联网中的车辆通常以较高速度行驶，这给通过传统的位置隐私保护机制（如基于握手的身份验证技术）维护位置隐私带来了重大挑战。这些方法需要车辆与网络节点之间进行多次消息交换以建立安全通信；而在高速场景下，可用于此类交换的时间有限，因此这些方法并不实际 [87]。

  车辆经常更换网络接入点，例如从一个基站或路侧单元移动到另一个，因此位置隐私保护机制必须采用先进的移动性管理技术，以确保在不同网络区段之间实现无缝切换，同时保护位置隐私。高速移动还会造成短暂的通信窗口，对手可能利用这些窗口截获位置数据，尤其是在数据未及时加密或未充分混淆的情况下。因此，有必要开发快速、高效的隐私协议，即使网络拓扑和连接点快速且频繁变化，也能提供可靠保护。这些协议必须尽量降低延迟并减少数据交换的开销，以防对手获取有意义的信息，同时确保位置数据经过匿名化处理，且在连续通信中不可链接。此外，还应将动态假名变更和上下文感知隐私策略等自适应技术集成到位置隐私保护机制中，以应对对手试图将截获的数据片段与特定车辆关联起来的行为，从而提升高移动性车联网环境中的整体隐私保护水平。

- **动态网络拓扑：**车联网的动态网络拓扑——其特点是车辆密度、速度和移动模式变化导致网络频繁且难以预测地变化——对位置隐私保护机制的有效性构成了重大挑战。

  在车辆密度较高的环境中，例如城市中心区，假名交换等协作式位置隐私保护机制可能非常有效，因为有大量车辆可供交换假名，从而破坏对手跟踪的连续性。然而，在郊区或农村地区等车辆密度较低的区域，车辆数量有限，减少了此类交换的机会，因而削弱了这些机制保障隐私的能力。这种可变性要求开发自适应位置隐私保护机制，使其能够根据网络拓扑和车辆密度的变化动态调整，确保即使在稀疏交通条件下，隐私保护仍然稳健。例如，在低密度场景中，位置隐私保护机制可能需要纳入虚假消息生成、机会式信标广播或基于基础设施的假名化（例如通过路侧单元）等额外措施，以弥补车辆交互不足。此外，网络拓扑的快速变化，例如车辆进入和离开通信范围，要求位置隐私保护机制采用快速重新认证和实时决策过程，以在不影响关键车载通信及时性的前提下维护隐私。

- **实时约束：**车联网的特点是需要快速、低延迟通信，以确保及时传递关键信息，例如碰撞警报、道路危险通知或紧急制动信号，这些信息对驾驶员安全和交通管理至关重要 [88]。

  然而，在满足这些实时约束的同时维护位置隐私是一项重大挑战。加密、假名变更和消息验证等隐私保护机制不可避免地会增加计算开销和通信延迟，从而减慢时效性数据的传输。例如，对用于身份认证和保护消息所必需的加密签名进行生成和验证，可能会造成延迟，超出安全关键型应用可接受的阈值。此外，为增强不可链接性而频繁变更假名，可能会导致丢包，或因重新认证流程而增加传输延迟。因此，必须谨慎设计位置隐私保护机制，以尽可能减少这些延迟，并优先确保安全消息及时送达，同时保护位置数据免遭窃听和未经授权的访问。这需要采用轻量级加密算法、优化数据包结构，并采用自适应隐私策略，根据具体情境动态调整隐私保护级别，例如传输数据的紧迫性、当前网络条件以及涉及的潜在隐私风险。平衡这些相互竞争的需求，对于确保车联网兼顾安全与隐私至关重要，可防止对手利用实时数据交换推断车辆位置或追踪驾驶员行为。

- **频繁网络断连：**高速移动、地形和天气等环境因素或网络拥塞所导致的车联网频繁断连，对维持有效的位置隐私构成了重大挑战 [89]。这些中断会导致连通性不可靠，使持续、实时的隐私保护难以实施。位置隐私保护机制必须具备足够的韧性，即使网络连接丢失或性能下降，也能保护敏感位置数据。数据缓存策略和容延网络协议等解决方案，对于防止断连期间的数据暴露至关重要。此外，去中心化的位置隐私保护机制无需依赖中央服务器，即可在车辆内部或车辆集群中进行本地位置隐私管理，从而增强系统的鲁棒性。本地数据聚合和间歇性加密等技术能够在偶发的数据交换过程中保障数据安全，对于降低频繁断连带来的隐私风险至关重要。这些方法对于防御利用断连期间网络安全漏洞发起的攻击至关重要，例如窃取残留数据，或在连接恢复后重放截获的数据。这确保了车联网在不利网络条件下的位置数据隐私。

- **连接波动性：**车联网中连接固有的波动性表现为车辆之间随机且短暂的交互，这给使用基于密码的身份认证等传统长时效机制来维护位置隐私带来了重大挑战 [90]。在这种高度动态的环境中，车辆频繁进入彼此的通信范围，又不断离开彼此的通信范围，导致频繁断连，从而中断维持传统身份验证方法所必需的持续通信会话。

这种不可预测性使得在较长时间内建立并维护安全信道变得困难，从而产生对手可能利用来拦截、分析或操纵位置数据的安全漏洞。因此，车联网中的位置隐私保护机制必须设计为能够在这些条件下有效运行，采用轻量级、快速的身份验证流程以及不依赖持久连接的去中心化隐私策略。例如，位置隐私保护机制可以使用频繁变化的临时标识符，或广播难以与特定车辆关联的假名，从而确保即使连接不断波动，位置数据仍然无法被跟踪。此外，隐私保护机制还可以采用机会通信协议，利用车辆之间的短暂接触快速交换隐私保护信息，缩小对手利用网络波动性进行跟踪的机会窗口。通过最大限度地减少对持续通信链路的依赖，这些自适应隐私解决方案能够针对车联网中瞬时连接固有的独特隐私风险提供稳健保护。

节点特征：传输特性，例如有限的传输功率、开放式无线介质、传输衰减、不稳定的网络能力以及大型网络规模，对于理解位置隐私挑战同样至关重要。

- **自主性：**车联网中的车辆表现出显著的自主性，能够以极少依赖集中式控制的方式独立发送、路由和接收数据 [91]。这种去中心化特性既是维护位置隐私的一项优势，也带来了挑战。一方面，缺乏集中式监管降低了遭受单点故障或集中式攻击的风险，否则这些问题可能会暴露网络中所有车辆的位置数据。另一方面，这种自主性要求开发稳健的分布式位置隐私保护机制，使其能够在去中心化环境中有效运行。这些机制必须确保各个车辆在与其他车辆通信和协作时能够管理自身隐私。例如，去中心化的位置隐私保护机制必须能够在没有中央服务器持续支持的情况下保护位置数据，通常会采用假名变更、本地数据加密和协作式数据混淆等策略。然而，如何在大型动态网络中协调这些隐私措施是一项挑战，因为每辆车都必须根据本地情况自主决定何时以及如何实施隐私保护。此外，

缺乏集中式控制可能会使检测和缓解复杂攻击变得困难，例如恶意实体实施的协同窃听或数据聚合攻击。因此，尽管自主性提升了车联网的灵活性和可扩展性，但也需要先进的位置隐私保护机制，以便动态适应这些环境的去中心化特性和快速变化，从而保护位置隐私。

- **强大的计算与存储能力：**车辆强大的计算与存储能力，为高级位置隐私保护机制提供了独特机会，使其能够利用复杂算法和大型数据集来实现稳健的隐私保护 [92]。这些能力可用于实施复杂的密码协议、用于异常检测的机器学习模型，以及区块链等分布式账本技术，从而确保位置数据的完整性和机密性。例如，车辆可以采用联邦学习方法协同训练隐私保护模型，而无需共享原始数据，从而降低敏感信息泄露的风险。然而，这些计算资源也使车辆成为对手的诱人目标。

攻击者可能会利用车辆强大的车载系统发起复杂的攻击，例如部署恶意软件以收集位置数据、执行数据挖掘技术以分析存储的信息，或应用机器学习算法从拦截的通信中推断模式。在本地处理大量数据的能力增加了对手入侵车载系统以访问和操纵数据、达到恶意目的的风险。计算能力的这种双刃剑特性要求开发位置隐私保护机制，不仅要利用车辆的计算资源来增强隐私保护，还要纳入强大的安全措施，以防止这些资源遭到对手利用。因此，要实现车联网中的位置隐私，需要在先进算法与确保车辆计算环境的安全性和完整性之间取得平衡。

- **能源供应充足：**车辆电池提供的大量能源资源为车联网带来了显著优势，因为这使得部署能耗较高的位置隐私保护机制（LPPMs）不再受到通常的功耗限制 [93]。这使得能够采用更复杂的隐私保护措施，例如先进的加密算法、实时数据混淆以及频繁的假名变更，从而显著增强位置隐私保护。然而，尽管现代车辆的能源供应实际上近乎无限，仍然需要确保隐私保护机制在效率方面得到优化。

过度使用计算资源可能会影响其他关键的车辆功能，例如导航、碰撞规避系统或 V2X 网络中的实时通信。此外，对手可能通过发起拒绝服务（DoS）攻击，利用消耗大量计算能力的位置隐私保护机制，迫使系统过度使用其资源，从而可能导致隐私泄露或系统故障。因此，尽管无限的能源供应能够实现更强大的隐

私保护，这些机制仍必须在安全性与计算资源的高效分配之间取得平衡，以维持整体系统性能，并确保持续防范位置隐私威胁。

通信与网络：与位置隐私相关的车联网传输特征包括开放式无线介质、传输衰减、不稳定的网络强度以及庞大的网络规模。

- **传输功率有限：**在车联网中，通信协议和无线环境所决定的传输功率固有限制，会显著影响隐私保护机制的适用范围和有效性 [94]。由于这些限制，车辆的通信范围有限，这给实施依赖车辆间协作的位置隐私保护机制带来了挑战，例如假名交换或协作混淆。

通信范围受限意味着车辆只能在短时间内与附近的车辆互动，因此难以执行需要多辆车持续互动的复杂隐私协议。这一限制在车辆稀少的地区尤其成问题，例如乡村道路或高速公路，因为可参与隐私保护交换的车辆较少，从而增加了位置数据暴露的风险。此外，通信范围有限还会妨碍去中心化隐私方案的有效性；这类方案依赖广泛的网络覆盖，将位置数据混淆分散到多个节点。因此，位置隐私保护机制必须通过纳入自适应技术来考虑这些功率和范围限制，例如根据车辆密度动态调整传输功率，或采用结合短距离与远距离通信技术的混合通信模型，以便在不同的车载环境中维持稳健的隐私保护。

- **开放式无线介质：**在车联网中使用开放式无线介质会带来固有的安全挑战，尤其是位置隐私方面。无线电波的开放特性使无线通信更容易被截获——窃听等行为因此变得更加容易，对车辆与基础设施之间传输的敏感位置数据的机密性构成严重威胁 [95]。

为了应对这些安全漏洞，位置隐私保护机制（LPPMs）必须整合强大的安全措施。高级加密技术，例如端到端加密，可确保数据对于拦截传输内容的未授权方而言始终无法解密。此外，数据混淆方法可以改变正在传输的位置数据的精度或真实性，通过增加潜在对手有效利用截获数据的难度，进一步提升安全性。在车联网中实施这些策略对于维护位置隐私至关重要，因为这些策略能够通过保护数据免受常见无线攻击的侵害，降低开放传输介质所带来的风险，从而维护敏感信息的完整性和机密性。

在这些高度动态环境中共享的信息。

- **传输衰减：**在车联网中，由衍射、反射、散射和折射等环境因素引起的传输衰减，会对位置隐私造成重大风险。这些物理层漏洞可能降低信号质量，导致位置数据意外泄露，即使采用加密技术保护更高层的通信也无法避免。例如，当信号被建筑物或车辆反射时，对手可能通过分析变化后的信号路径或信号强度波动，推断车辆的位置。在这种情况下，传统加密方法可能不足以防范基于位置的攻击，因为它们关注的是数据内容，而非传输特性。

有效的位置隐私保护机制必须通过融入先进的信号处理技术来减轻衰减的影响，从而应对这些物理层挑战。这可以包括多径校正、自适应调制和纠错码等技术，以确保信号失真不会向对手泄露可利用的车辆位置信息。此外，混淆传输模式并动态调整信号参数，也能进一步防止对手根据信号行为重建车辆轨迹，从而在物理因素干扰信号完整性的环境中保护位置隐私。

- **网络能力不稳定：**车联网的通信和计算能力变化很大，并且受实时交通状况影响，这会直接影响位置隐私保护机制的有效性 [96]。在交通拥堵等高密度交通场景中，众多车辆彼此接近，可以增强网络强度，形成通信可用性高的稳健车联网。这种环境有利于采用协作式位置隐私保护机制，例如假名交换，即车辆频繁更换标识符以防止长期跟踪。然而，在车辆较少、拥堵程度较低的场景中，例如农村或郊区，网络会变得更加稀疏，车辆之间的协作机会随之减少，这会显著削弱这些机制所提供的隐私保护。

对手可以利用这些网络不稳定时期，通过关注标识符变更之间的间隔来跟踪车辆，尤其是在假名交换不太频繁的低密度区域。因此，LPPMs 必须适应网络变化，通过整合动态假名更新、本地协- 作，或不完全依赖车辆密度或网络强度的替代隐私策略等机制，确保在高密度和低密度交通状况下都能提供强有力的隐私保护。这种适应性对于维持一致的位置隐私至关重要，无论车载环境的通信能力如何波动。

- **大型网络规模：**车联网通常覆盖广阔的地理区域，包括人口密集的城市环境和绵延广大的高速公路系统，这给维护位置隐私带来了重大挑战，

因为这些网络规模庞大，位置隐私保护机制的部署更加复杂：这些机制必须在广泛的网络覆盖与局部通信区域的限制之间实现有效平衡。在城市地区，车辆密度较高，车辆与基础设施（例如路侧单元）之间能够频繁交互，这有助于采用假名交换或协作式数据混淆等增强隐私的技术。然而，在乡村公路等人口较少的地区，可参与协作式位置隐私保护机制的车辆较少，因此更难通过协作方式混淆位置数据。

大型网络规模增加了对手长期跟踪车辆的风险。对手可以利用通信稀疏区域，在不受干扰的情况下监控更长距离内的车辆移动。因此，有必要开发自适应位置隐私保护机制，使其能够根据网络密度的变化动态调整，从而无论通信环境如何，都能持续提供位置隐私保护。此外，车辆在不同网络区域之间移动时，隐私保护机制必须能够在人口密集区和稀疏区之间无缝切换，同时不损害位置隐私，这就需要先进的移动性管理和安全切换协议。

2）车载通信技术：作为两种得到广泛研究的车载通信技术，专用短程通信（DSRC）V2X 和蜂窝车联网（C-V2X）具有不同的运行架构，各自对位置隐私和安全有着独特的影响。

- **DSRC V2X：**DSRC V2X 采用去中心化的点对点通信模型，使车辆能够彼此直接交换信息，并与路侧基础设施通信，而无需依赖集中式控制系统。这种去中心化架构有利于实现低延迟通信，这对于碰撞避免和交通协调等实时应用至关重要，尤其是在蜂窝基础设施有限的环境中，例如乡村或偏远地区 [97]。

这种点对点模式也给位置隐私带来了重大挑战。由于没有集中式权威机构监督安全，DSRC 通信更容易受到窃听和数据注入攻击。对手可以截获车辆之间或车辆与路侧单元之间交换的消息，从而获取敏感位置数据并跟踪车辆。由于缺乏健全的集中式安全协议，DSRC 网络往往默认不采用加密或假名化，这使攻击者更容易追踪特定车辆、分析驾驶员特征，或根据移动模式推断其身份。这会使车辆面临长期跟踪风险，对手可以监控车辆的路线、常去目的地和行为模式，从而损害驾驶员的隐私与安全。为应对这些安全漏洞，DSRC 网络应采用动态假名变更、端到端加密和定期重新认证等先进安全机制。这些措施有助于防止未经授权的跟踪，并降低身份推断攻击的风险，从而增强去中心化车载环境中的位置隐私。

- **蜂窝车联网：**蜂窝车联网采用集中式通信架构，利用通常由服务提供商管理的现有蜂窝基础设施。这种集中式结构能更有效地控制通信，从而实施更严格的安全措施，例如先进的加密协议、稳健的数据保护机制和安全的身份认证流程，这些措施对于保护位置隐私至关重要 [98]。

与去中心化模型不同，蜂窝车联网能够更有效地管理隐私保护技术，包括通过位置模糊化隐藏车辆的精确坐标，以及通过假名化频繁更换车辆标识符以防止长期跟踪。还可以集中实施安全密钥管理系统，确保只有经授权的实体才能访问敏感位置数据。然而，蜂窝车联网依赖蜂窝基础设施，因此存在一些局限，尤其是在蜂窝网络覆盖较弱或无法覆盖的偏远地区或欠发达地区。在此类情况下，车辆可能难以与网络保持稳定通信；如果无法实时采取保护措施，便可能面临隐私泄露风险。

尽管存在这些局限，蜂窝车联网固有的集中式控制使服务提供商能够比专用短程通信等去中心化模型更有效地检测并缓解未经授权的跟踪企图或数据拦截。网络运营商可以监控可疑活动、及时采取对策，并根据需要调整安全协议，因此蜂窝车联网通常能更好地保护位置隐私。然而，其整体有效性取决于蜂窝网络覆盖的质量和范围。这一能力凸显了蜂窝车联网提供更强位置隐私保护的潜力，尤其是在蜂窝基础设施完善的城市地区；但在连接较弱的地区，它仍然容易受到威胁。

3）位置隐私保护机制的应用场景：在车联网中，位置隐私保护机制应用于位置数据生命周期的各个阶段，以确保从数据收集到数据发布的整个过程中隐私都得到保护。如图8所示，保护机制可分为两个主要阶段：收集阶段（在线）和发布阶段（离线）。每个阶段会根据数据的敏感程度和应用的隐私要求采用不同的位置隐私保护机制 [99]。

- **收集阶段（在线保护）：**在收集阶段，应用实时或批处理位置隐私保护机制，确保位置数据从车辆传输至基于位置的服务服务器的过程中保持安全。在实时保护中，位置隐私得到保护。与此同时，数据会发送至对时间敏感的基于位置的服务，例如交通管理系统、紧急服务或导航系统，这些系统需要即时且持续的更新。实时位置隐私保护机制必须在加密或匿名化数据以防止对手跟踪车辆位置的同时，确保低延迟。

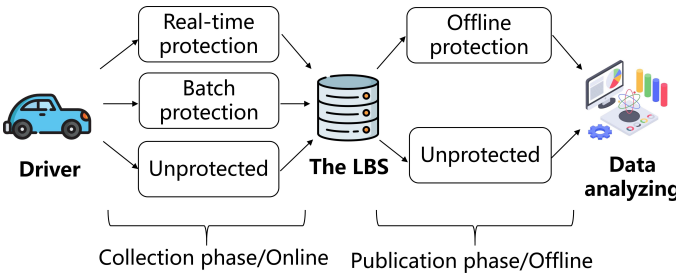

图 8. 使用位置隐私保护机制保护位置隐私的情形。位置隐私保护机制可用于两个阶段，即收集阶段和发布阶段，以满足不同的隐私要求。

实时。动态假名化、实时加密和空间隐匿等技术通常用于保护传输过程中的驾驶员位置数据。这些方法可以降低数据被对手截获的风险，并确保驾驶员的位置不会泄露，即使是在与时间敏感型基于位置的服务通信时也是如此。

另一方面，批量保护用于对时间不太敏感的基于位置的服务，在将多名驾驶员的位置数据发送到服务器之前，先对其进行聚合。由于汇集了多个来源的数据，这种方法能提供更强的隐私保障，也让对手更难追踪特定个体。对于需要收集大量位置数据以进行统计分析、交通规划或路线优化，且无需即时实时数据的应用，批量位置隐私保护机制尤为适用。在这些情况下，可采用数据聚合、k-匿名性或同态加密等技术，确保即使数据遭到拦截，也无法与个体驾驶员关联。批量处理方法既能保护每位驾驶员的隐私，又能维持聚合数据的效用。

- **发布阶段（离线保护）：**当位置数据到达基于位置的服务服务器后，可能会经过处理，并最终出于各种分析目的而发布，例如城市规划、交通模式分析或学术研究。在发布阶段，位置数据不再与实时服务相关联，因此在向公众或第三方实体共享之前，会采用离线位置隐私保护机制来保护整个数据集 [100]。离线位置隐私保护机制侧重于防止已发布数据集中的个人被重新识别，因为对手可能会通过交叉引用外部数据源，试图将匿名化的位置轨迹关联回特定车辆或驾驶员。

离线位置隐私保护机制采用差分隐私等技术，通过向数据集添加统计噪声来防止精确的重新识别；或采用轨迹混淆，调整数据集以降低隐私泄露风险，同时保持其用于分析的整体效用。这些方法对于需要出于研究或商业目的发布大型数据集的场景尤为重要，例如包含长期车辆轨迹的数据集。若缺乏强有力的离线保护，对手便可能利用复杂的数据挖掘技术推断出驾驶员的敏感信息，例如他们的常去目的地、出行习惯，甚至家庭住址，从而对位置隐私构成重大风险。

位置隐私保护机制的有效性在于其平衡隐私与数据效用的能力。虽然目标是确保位置数据保持私密且无法被未授权方访问，但位置隐私保护机制还必须确保数据仍可用于其预期目的，无论是导航、交通管理还是城市规划 [15]。实时位置隐私保护机制优先考虑低延迟和安全性，以确保驾驶员能够获得准确且及时的信息，同时不损害隐私；而离线位置隐私保护机制则侧重于在分析过程中保护数据，因为此时重新识别风险更高。这种双重方法确保了在车联网中位置数据的整个生命周期内都能维护隐私。位置隐私保护机制通过应对数据处理各阶段存在的安全漏洞，在保护车联网中驾驶员的位置隐私方面发挥着至关重要的作用。在收集阶段，实时和批量位置隐私保护机制确保敏感位置数据免受拦截或未经授权的访问，而离线位置隐私保护机制则保护已发布数据集的完整性，防止对手对匿名化数据实施旨在重新识别个人的事后攻击。这种多层次的隐私保护方法对于车联网至关重要，因为车辆的持续移动以及敏感位置数据在开放无线信道中的传输，使对手很容易追踪、监控或损害驾驶员的隐私。

4）位置隐私保护机制的关键性能指标：位置隐私保护机制根据若干关键性能指标进行评估，这些指标反映了其在平衡隐私保护、可用性和系统效率方面的有效性。这些指标——隐私、数据效用和效率——为比较不同的位置隐私保护机制提供了全面的框架，尤其适用于车联网中的位置隐私。理解并优化这些指标，对于开发能够保护敏感位置数据、同时又不会显著损害基于位置的服务的性能或功能的位置隐私保护机制至关重要 [1], [101]。

- **隐私：**隐私指标用于衡量位置隐私保护机制（LPPM）保护驾驶员位置数据免受对手攻击的程度。在车联网中，对手可能通过窃听、数据挖掘或针对匿名化数据的重新识别攻击，推断车辆的位置、身份或出行模式 [19]。稳健的位置隐私保护机制应确保敏感位置数据不被未授权方获取，即使存在复杂的攻击也是如此。这可以通过加密、动态假名化、空间隐匿或差分隐私等技术实现；这些技术旨在隐藏车辆的真实位置，同时仍能与基于位置的服务（LBS）进行通信。然而，设计有效的位置隐私保护机制的难点在于车联网具有动态特性。车辆频繁进出通信区域，对手可以利用这些转换跟踪车辆随时间的移动，因此位置隐私保护机制必须持续保护数据，使其在不同网络环境和交互过程中均得到保护。因此，隐私指标是衡量

位置隐私保护机制在适应这些场景、抵御各种隐私威胁方面表现如何的一项关键指标。

- **数据效用：**在保护隐私至关重要的同时，位置隐私保护机制还必须维持较高水平的数据效用，以确保基于位置的服务的功能。数据效用是指基于位置的服务所使用的位置数据的准确性、完整性和及时性，而这反过来会影响导航、交通管理和应急响应等服务的质量 [101]。隐私与数据效用本质上是相互冲突的指标——更强的隐私保护通常会导致数据效用降低，因为更激进的匿名化或加密方法会掩盖基于位置的服务所需的有价值信息。例如，采用高等级的空间隐匿来保护位置数据，可能导致导航路线不够准确或交通警报延迟，从而降低基于位置的服务对驾驶员的有效性。在极端情况下，当位置数据被完全匿名化或混淆时，基于位置的服务可能变得无法使用，其效用也会完全丧失。位置隐私保护机制面临的挑战是在隐私与效用之间取得平衡，在不降低服务质量的情况下提供充分保护。选择性混淆、上下文感知隐私控制，以及根据服务敏感性调整隐私级别等技术，可以帮助位置隐私保护机制管理这种权衡，确保驾驶员在保护其位置隐私的同时，仍能获得准确、及时的信息。

- **效率：**效率指标评估实施位置隐私保护机制所涉及的计算和存储开销，这对于车联网等资源受限环境尤为重要 [102]。效率通过计算时间、存储需求、可扩展性和容错能力来衡量。由于车联网需要实时处理数据，以确保车辆的安全与协调，因此位置隐私保护机制必须以最小时延运行，避免干扰车辆与基于位置的服务之间的通信。较高的计算开销可能导致延迟问题，降低碰撞规避系统或紧急通知等时间关键型应用的响应能力。此外，需要大量存储空间来保存加密密钥、假名管理信息或轨迹数据的位置隐私保护机制，可能会给车辆的车载系统带来负担，而这些系统的内存和处理能力可能有限。因此，高效的位置隐私保护机制必须经过精心设计，以尽量降低这些开销，确保其能够适应大量车辆和通信事件，同时不降低系统性能。这一点在大型城市地区或高速公路网络中尤为重要，因为车辆密度可能会发生显著变化，要求位置隐私保护机制根据可用网络资源动态调整。轻量级加密算法、去中心化处理和高效的密钥管理等技术有助于提升位置隐私保护机制的效率，使其更适合在现实世界的车联网中部署。

在车联网中设计位置隐私保护机制时，如何在隐私、数据效用和效率之间实现最佳平衡，是一项核心挑战。在许多情况下，提高某一指标可能会对其他指标产生负面影响 [15]。例如，通过采用更强的加密来增强隐私保护，可能会因位置信息精度降低而损害数据效用，也可能增加计算开销，从而降低系统效率。反过来，如果通过尽量减少混淆或加密来优先保障数据效用，位置数据就可能容易受到攻击。开发有效的位置隐私保护机制，关键在于找到一种平衡：既能将隐私保护在令人满意的水平，又不会显著损害系统的可用性或性能。这种平衡可能因具体应用或情境而异：对于紧急服务等对时效性要求较高的基于位置的服务，位置隐私保护机制可能会优先考虑数据效用和效率；而对于路线规划或停车辅助等非关键应用，则可能更注重加强隐私保护。此外，用户可控的隐私设置可以让驾驶员根据自身需求或顾虑，选择隐私与效用之间的理想平衡。

C. 车联网中的位置隐私威胁

车联网具有动态、开放的通信环境，因此越来越容易受到各种位置隐私威胁的影响。这些攻击针对敏感位置数据，旨在通过跟踪驾驶员的行动、推断其身份，或分析其长期行为来侵犯驾驶员的隐私。一种最简单却不切实际的车辆跟踪方法，是在车辆上非法安装全球导航卫星系统（GNSS） [103]。虽然这能让对手获取实时位置数据，但由于必须在每辆目标车辆上实际安装 GNSS 设备，因此并不适用于大规模监视。因此，对手通常会采用更复杂的数字攻击，利用车联网无线通信系统固有的弱点发动攻击。

1）被动攻击与主动攻击：车联网中的位置隐私攻击可以建模为多目标跟踪（MTT）问题：对手收集传感器定期检测到的一组含噪测量值或观测结果，以推断出对驾驶员位置或轨迹最准确的估计。通过这些技术，对手可以系统地降低车辆位置的不确定性，从而实现长期精准跟踪。此类位置隐私攻击通常分为被动攻击和主动攻击，两者都给车联网安全带来独特的风险与挑战。

被动攻击是指对手悄无声息地监控和分析车联网中的数据流量，以推断位置信息。这类攻击具有隐蔽性，因为它们不会直接干扰车辆之间的通信或破坏网络服务，因此难以被检测到。被动攻击者的目标是利用网络固有的安全漏洞，尽可能收集与位置相关的数据。以下是车联网中常见的被动攻击类型 [104]:

- **无线窃听攻击：**车联网开放且去中心化的特性，加上无线通信协议的使用，使其极易遭受无线窃听攻击。在此类攻击中，

对手可以通过共享的无线媒介，截获车辆之间或车辆与路侧单元之间交换的通信信号。鉴于车联网旨在通过广播信息来促进道路安全和导航，传输的数据大多未加密或保护不足，导致实时位置、导航请求和出行路线等敏感信息暴露于未经授权的截获之下。窃听使对手能够编制车辆的详细移动画像，进而追踪驾驶员的日常活动规律、识别常去目的地（例如家或工作地点），并可能发起更具针对性的攻击。

在车辆经常于公共场所进行通信的情境中，无线窃听所带来的隐私风险会进一步加剧，使对手更容易设置监听设备或部署被动监控设备。此外，对手还可以利用先进的分析技术，将捕获的数据与其他信息来源相关联，从而重建完整的车辆轨迹或推断出身份，即使原始数据已匿名化。

- **回溯攻击：**在回溯攻击中，对手利用三角定位技术，通过测量部署在不同位置的多根天线所接收到的信号强度、方向或到达时间差（TDoA），计算车辆的精确位置 [105]。通过使用至少两根经过策略性部署的天线，对手可以捕获并分析通信信号，例如来自车联网通信系统的信号，从而高精度地估算车辆位置。这种跟踪方式在高密度城市环境中尤为有效，因为无线基础设施的广泛部署，以及信号反射、折射和多径传播的普遍存在，实际上能够提高三角定位的精度。

多径传播通常被视为无线通信中的一项挑战，但可能为对手提供额外的数据点，以优化其估计结果，尤其是在对手采用先进的信号处理技术时。三角测量方法对位置隐私构成重大威胁，因为它不需要直接访问车辆的通信系统，也不需要车辆本身的任何配合，因此难以被检测或缓解。此外，该攻击的被动性质使对手能够在不引起怀疑的情况下，沿较长距离持续跟踪车辆，从而进行长期画像分析、路线预测，并可能暴露家庭住址、工作场所或常去地点等敏感目的地。

- **流量分析攻击：**在流量分析攻击中，对手会利用车联网中的数据流模式，通过监控通信流量和频率来推断车辆的位置和移动情况。基站、网络枢纽等核心节点在车联网中发挥着关键作用，负责处理车辆与基于位置的服务之间的大量数据流量 [106]。这些节点负责促进通信，因此成为对手收集位置相关信息的主要目标。

通过分析这些核心节点的进出流量，对手可以识别高优先级车辆，例如急救人员车辆或商业配送卡车，因为它们会产生频率更高或流量更大的数据交换。与普通车辆相比，这些车辆的高流量使对手能够追踪其移动情况或推断其位置。此外，流量的时空相关性可以揭示某些模式，例如频繁前往特定区域，从而让对手能够预测未来的移动情况或识别惯常目的地。这会对位置隐私构成重大风险，因为对手可能利用这些信息进行长期监控、画像分析或定向攻击。

- **数据包分析攻击：**即使车联网采用加密来保障安全通信，仍容易受到复杂的数据包分析攻击。这类攻击利用的是与传输数据包相关的元数据，而非加密载荷本身。攻击者会捕获并分析各种数据包特征，例如时间戳、数据包大小、传输间隔和数据包频率，以推断敏感的位置信息 [107]。例如，通过监测同一标识符的数据包在不同地理位置出现时是否具有一致的时间戳相关性，攻击者可以描绘出车辆的轨迹，从而危及其位置隐私。

在车辆经过不同检查点或路侧单元时反复传输相似数据包的场景中，这一点尤其令人担忧。即使数据包时序或大小仅有细微变化（通常由车辆速度变化或拥堵造成），也可能为对手提供足够的信息，以推断实时移动情况并预测未来路线。在高密度城市环境中，这种攻击会更加有效，因为攻击者可以利用多个观测点进行三角定位，并进一步优化轨迹估计。

- **回溯攻击：**对手利用大量存储空间和计算能力，归档并分析大量有关车辆移动的历史数据，随后将这些数据与新捕获的位置数据进行关联，以追踪车辆的当前位置并预测其未来轨迹。通过维护一个全面的移动模式数据库，对手能够构建驾驶员的详细行为画像，从而识别日常通勤、频繁访问特定位置以及偏好的路线等规律。这种对驾驶员行为习惯的精细洞察显著增加了隐私侵犯的风险，因为对手能够以很高的精度确定家庭和工作地址等敏感位置。

回溯攻击的预测特性使对手能够预判潜在的未来位置，从而实施更具侵扰性的监控措施，例如定向跟踪或实体跟踪。对手利用时间数据进行模式识别的能力进一步加剧了这一威胁的严重性，使驾驶员难以通过假名变更或加密等传统隐私保护技术来隐藏自己随时间变化的行踪。

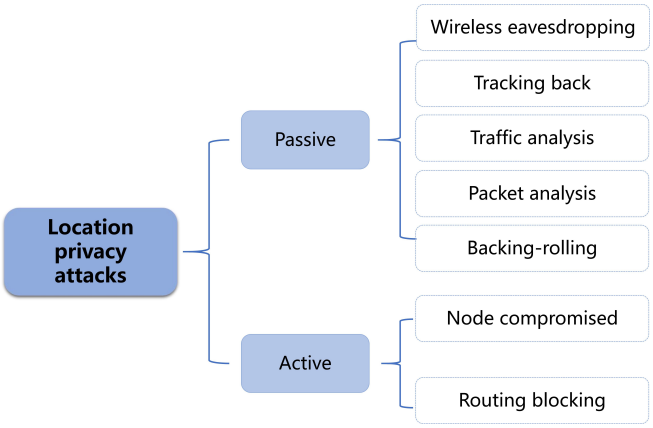

图 9. 主要隐私攻击。针对位置隐私的攻击可分为被动攻击和主动攻击。被动攻击旨在监控和分析数据流量，而主动攻击则会干扰车联网。

与被动攻击不同，主动攻击会直接干扰车联网，例如中断通信信道、注入虚假数据，或冒充合法节点来欺骗车辆或路侧单元。与被动攻击相比，这类攻击更具攻击性，但也更容易被检测到。主动攻击者可以操纵网络来收集位置数据，或阻止车辆维护自身隐私，从而严重损害位置隐私。以下是车联网中常见的主动攻击类型 [104]:

- **节点攻陷攻击：** 节点攻陷攻击通过损害合法网络组件（如路侧单元和车载单元（OBU））的信任和完整性，对车联网中的位置隐私构成严重威胁 [108]。当对手控制这些节点后，便可截获、操纵并分析车辆与网络之间传输的数据。这使攻击者能够从捕获的数据包中提取敏感位置信息，并绘制网络拓扑图，其中包括常用路线和关键网络节点。此类攻击的影响不止于数据泄露，还可能导致长期的隐私侵犯，并进一步利用遭攻陷的网络组件。

  遭攻陷的节点可能成为发起更高级攻击的关键入口，例如节点克隆：对手复制合法的节点身份，以创建具有欺骗性的通信路径。这可能误导车辆与这些克隆节点共享敏感信息，从而实现实时跟踪，甚至操纵导航指令，将车辆引向脆弱或危险的地点。此外，遭攻陷的节点还可能通过扰乱假名变更等隐私策略，削弱位置隐私保护机制的有效性，而这些策略依赖于网络基础设施的可信度。因此，利用遭攻陷的节点对维护车联网中的位置隐私构成了重大挑战。

- **路由阻断攻击：** 路由阻断攻击会扰乱数据传输的正常流程，严重威胁车联网中的位置隐私，并危及位置信息 [109]。在此类攻击中，对手会选择性地拦截或阻断特定通信路由上的数据包，尤其是目标车辆用于与路侧单元或其他车辆通信的路由。通过阻断这些路由，对手可以迫使目标车辆通过安全性较低或已遭入侵的节点重新路由通信，从而监视这些替代路径。这使攻击者能够追踪通信的来源和目的地，并可能泄露车辆的位置和移动模式。此外，此类干扰会造成数据传输时延，在通信模式中形成间断，对手可利用这些间断推断车辆的位置。车联网的动态特性进一步加剧了这一问题：车辆不断加入和离开网络，因此难以建立安全可靠的通信路由。对手迫使车辆改走其他路线的能力，不仅会增加数据拦截和未经授权的访问风险，还会带来实施更复杂攻击的机会，例如位置欺骗，即向网络注入虚假的位置数据，误导车辆和路侧单元。

2）基于物理特征的攻击：基于物理特征的攻击对车联网中的位置隐私构成了重大威胁，因为这类攻击利用车辆固有的可识别性，通过车辆的形状、颜色、车牌及其他显著特征进行识别（如图 10[2]，所示）。自动车牌识别（ANPR）系统等先进跟踪技术，使对手能够系统地监控并记录车辆在多个位置之间的移动轨迹 [110]。

一旦在某个位置识别出车辆的物理特征，对手就可以利用这些信息建立该车辆轨迹的时空画像。随着车辆在更多位置被观测到，轨迹估计的准确性也会提高，从而降低对手的估计误差，并增强其预测车辆未来移动情况的能力。这种持续监控不仅会损害驾驶员的实时位置隐私，还会使长期跟踪、画像分析和行为分析成为可能。这些数据还可被进一步用于后续更具侵入性的攻击，包括身份推断，甚至定向监控。如果路侧摄像头和收费站等多个传感器联网，形成全面的监控网络，使对手能够全面掌握车辆的移动情况，那么风险将会进一步加剧。

3）针对车内消息的攻击：车内通信系统（如电子控制单元（ECU）、胎压监测系统（TPMS）和遥控无钥匙进入（RKE）技术）在现代车辆中发挥着至关重要的作用，可控制各种功能并提升驾驶员安全。然而，由于容易遭受未经授权的访问和数据泄露，这些系统也对位置隐私构成重大风险。对手可以利用这些漏洞获取敏感的位置相关数据。例如，

[2]图中的车辆归作者所有

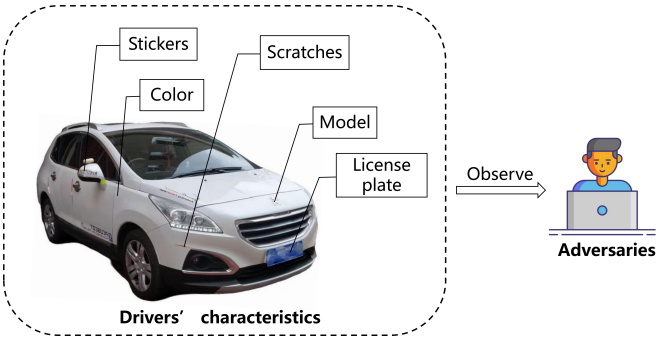

图 10. 可用于跟踪车辆的可识别特征。对手可以通过贴纸、颜色、车型、划痕和车牌等外观特征跟踪车辆。基于光学视觉的跟踪几乎无法防范。

攻击者将非法的车载诊断（OBD）读取器连接到 OBD 端口，便可检索车辆网络中存储的实时信息，包括车速、加速度、转向角，甚至全球定位系统（GPS）坐标 [108]。这些数据结合起来后，可能会暴露精确的位置轨迹和驾驶模式。

车辆网络内的无线数据传输进一步加剧了这些隐私风险。例如，胎压监测系统通常会广播未加密的数据，其中包括车辆独有的传感器标识符。这些数据可在最远 40 米的距离被截获，使对手无需直接接触车辆本身，就能跟踪车辆的移动。同样，远程无钥匙进入系统会通过短距离广播发送唯一标识符以解锁车门；如果这些标识符被捕获，不仅会危及车辆安全，还可能成为数字指纹，用于追踪车辆的位置 [111]。

4）对 V2X 消息的攻击：V2X通信是现代智能交通系统的基石，能够促进车辆与基础设施之间实时交换信息，从而提升道路安全和交通效率。然而，持续广播位置敏感信息会造成严重的隐私漏洞。协作感知消息（CAM）和去中心化环境通知消息（DENM）等关键 V2X 消息类型包含详细的车辆状态数据，包括精确时间戳、地理坐标和速度信息 [112]。这些消息对于碰撞避免和危险预警等安全关键型应用至关重要，但为了降低延迟并确保警报及时送达，它们以明文形式传输。不幸的是，由于缺乏加密，恶意实体很容易截获并分析这些广播，从而重构车辆的实时轨迹，并识别其移动中的潜在模式。

附加在 CAM 和 DENM 消息上的数字签名旨在用于身份认证和完整性验证，但攻击者可以利用这些签名精准定位车辆，并对其进行长期跟踪。这一问题因这些消息具有较高的时间分辨率而加剧：它们以 1 至 10Hz 的频率广播，持续提供粒度极细的位置数据。此外，

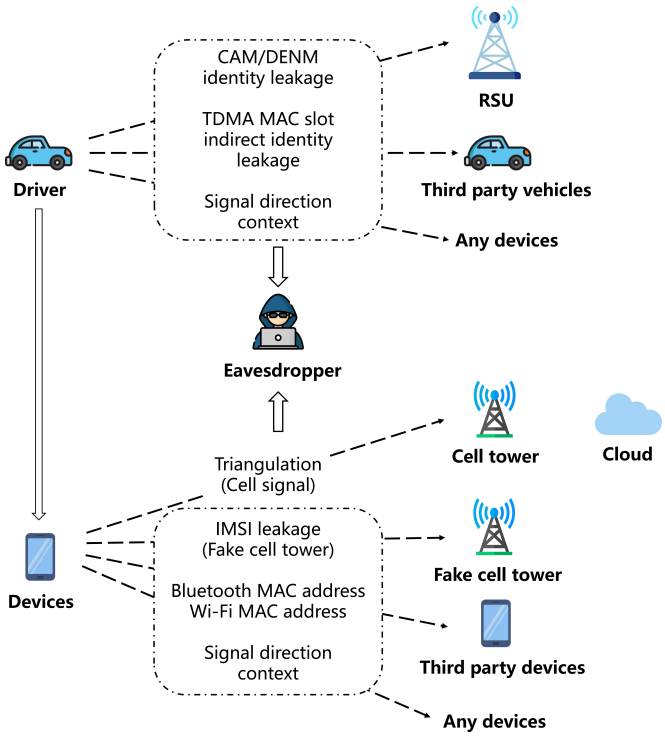

图 11. V2X 和车内通信威胁。由于车辆会定期广播数据，对手可以通过窃听 V2X 通信信道获取数据。对手还可以利用车内通信轻易跟踪车辆。

MAC 层协议中的安全漏洞也会进一步损害隐私，例如采用时分多址（TDMA）的协议。TDMA 为每辆车分配唯一的时隙，实际上起到了数字标识符的作用。对手可以利用这些信息监控时隙分配情况，并跟踪车辆在网络中的移动轨迹 [113]。

除了这些直接的 V2X 威胁外，车辆外围设备也可能危及位置隐私。例如，可以利用附近的蜂窝塔对驾驶员手机发出的电信信号进行三角定位，使对手能够确定车辆的大致位置。采用多个蜂窝塔数据的先进定位技术可以实现高精度跟踪。此外，每台移动设备独有的国际移动用户识别码（IMSI）可能会被 IMSI 捕捉器截获，只要驾驶员的手机仍处于 [27] 范围内，就可以持续跟踪车辆。同样，车辆内的蓝牙设备（包括用于车载娱乐和驾驶辅助的设备）经常会广播包含其 MAC 地址的广播数据包。对手可以监控这些广播，以推断车辆的位置和移动轨迹 [114]。

对手无需获取传输数据的内容即可追踪车辆。如图 9 和图 10 所示，信号方向上下文足以使对手在无线传感器网络 [115] 中实施回溯攻击。对手还可以根据在车联网中接收到的协同感知消息推断位置和速度变化。

D. 关键要点

对5G/6G车联网中位置隐私威胁和保护机制的分析，揭示了该领域现状及其面临挑战的若干关键见解。

车联网由于其开放的通信环境、高移动性以及对持续数据交换的依赖，本质上容易受到攻击。这使其面临多种对抗技术的威胁，包括被动窃听、主动攻击和物理层漏洞利用。即使是先进的隐私保护机制，例如假名变更或加密，也难以提供全面保护，因为对手能够利用元数据、信号特征或跨层漏洞。高密度城市环境中的挑战尤为突出，因为对手可以轻易关联来自多个来源的数据；而在农村地区，有限的网络密度则会削弱协作式隐私策略的效果。

隐私、效用与效率之间的相互制约，是设计位置隐私保护机制时面临的一项根本挑战。较高的隐私保护水平往往会降低基于位置的服务的效用，而过度的资源需求则会损害实时功能。要确保位置隐私保护机制既能保护位置数据，又能满足车载应用的运行要求（例如碰撞避免或应急响应），关键在于实现这种平衡。这凸显了设计位置隐私保护机制的重要性：它们必须能够无缝融入车联网动态且资源受限的环境。

The key ob服　i务　f thi分　i节包括　follows:

- **不断演变的威胁态势：**对手正变得愈发老练，采用元数据相关性分析和物理层攻击等先进技术，绕过传统隐私防护。因此，位置隐私保护机制需要应对来自多个攻击向量的威胁。
- **网络固有挑战：**高移动性、动态拓扑和不断变化的车辆密度，在车联网中造成了独特的脆弱性。这些特征使静态隐私保护机制的实施更加复杂，凸显了对自适应、情境敏感型解决方案的需求。
- **隐私与效用平衡：**在维护位置隐私与保留基于位置的服务效用之间固有的矛盾仍然是一个核心挑战。解决方案必须确保隐私保护不会损害关键车载应用的准确性、及时性或功能性。

IV. 车联网中的位置隐私保护机制

本节将现有的位置隐私保护机制分为三类进行评估，并讨论各类别的局限性，如表 IV 所示。这些机制分为用户侧、服务器端和用户-服务器接口位置隐私保护机制。用户侧位置隐私保护机制在收集阶段处理位置数据，而服务器端位置隐私保护机制则在发布数据时保护位置隐私。用户-服务器接口位置隐私保护机制借助可信第三方和安全通信来实现位置隐私保护。我们还从定位和通信需求的角度总结位置隐私保护机制的局限性，并从理论和实践两个方面回顾平衡位置隐私与数据效用的方法。理论方法包括区块链、自适应参数、混合、加密、元素简化和虚拟节点。我们以现实世界中的车载追踪技术（即 COVID-19 追踪应用）为例，讨论实践中如何平衡位置隐私与服务质量。

A. 用户侧位置隐私保护机制

用户侧位置隐私保护机制旨在收集阶段保护驾驶员的位置隐私。常见的用户侧位置隐私保护机制包括传递并运行、证书、安全计算和数据扰动。现有用户侧位置隐私保护机制的比较见表 V。

1) 传递并运行：传递并运行策略是一种保护隐私的技术，旨在利用车辆固有的移动性来增强车联网中的位置隐私。车辆不会直接向基于位置的服务传输敏感位置数据，而是通过中间车辆转发信息，从而减少数据的直接暴露。该方法最初由 Dunbar 等人提出 [116]，旨在应用于容延网络，使车辆能够根据网络条件和隐私要求，动态决定是将消息传递给附近的车辆，还是直接上传至基于位置的服务。

基于这一概念，Lu 等人 [117] 提出了一种轻量级的传递并运行方法，该方法采用了与车辆移动性和传输延迟约束相适应的数据扰动技术。该方法采用两种自适应策略：贪心策略，即车辆通过选择最近的中继车辆来优先降低时延；以及随机策略，即随机选择一辆中继车辆以最大限度地保护隐私。非对称加密进一步保护了中继传输过程中消息的完整性和机密性。尽管取得了这些进展，该方法仍会产生显著的传输延迟，尤其是在稀疏车联网或高移动性条件下，此时找到合适中继车辆的可能性较低。这种延迟可能会妨碍实时应用，并限制传递并运行策略在需要及时交付数据的场景中的有效性，因此有必要在隐私保护与通信效率之间取得平衡。

2）隐私证书：证书，即保护隐私的基于属性的凭证，对于维护车联网中的位置隐私至关重要。这些密码学机制使驾驶员能够进行身份验证，并证明其拥有某些属性，而无需向基于位置的服务披露不必要的个人信息。这些证书具有灵活性，可以仅选择性披露满足基于位置的服务预定义谓词所需的信息，从而降低过度共享敏感数据（如实时位置）所带来的风险 [139]–[142]。基于证书的系统通常依赖于可塑签名的稳健性，允许对特定消息部分进行受控修改，以防止披露特定属性，包括位置。

表 IV AN OVERVIEW 现有位置隐私保护机制s。

类别	技术	描述	优点	局限性
用户侧 位置隐私 保护机制	传递并运行	通过以下方式传输位置数据 其他车辆	传输延迟 打破.....的关联 位置信息	高通信 复杂度
	隐私 证书	身份认证	同时提供位置 隐私和身份认证	高计算量和 存储消耗
	安全 计算	直接操作加密数据	操作灵活，且 不会泄露隐私 data	高计算量和 传输时延
	数据扰动	使用伪造位置应用基于位置的服务 数据而非实际 版本	考虑先验分布 知识的 对手，且不会 需要可信第三方	低数据效用
服务器端 位置隐私 保护机制	统计 披露内容 控制	匿名化或混淆数据于 数据集	保持通用的 的统计特征 数据集	需要可信第三方
	同态 加密	直接操作加密数据 在服务器端	该操作可以 灵活执行，且无需 解密数据	计算开销高 且 传输延迟
	隐私 信息 检索	隐藏请求的项目	驾驶员可以申请 基于位置的服务，而无需披露 他们的要求	高计算 开销
	可搜索 加密	隐藏.....中的明文关键词 搜索。	可与 其他方法	准确度低
用户-服务器- 接口 位置隐私 保护机制	安全 通信	使用传统协议或 端到端加密服务	技术已 在过去几十年中发展起来的	存在一些 局限性 传统协议
	可信第三方 方	引入可信第三方以 辅助通信	高效率	这是一个理想的环境。

- **基于属性的签名（ABS）：** Shahandashti 等人 [118] 提出了基于属性的签名概念，使驾驶员能够使用特定属性对消息进行签名，而无需披露个人标识符。这些签名依赖于属性值，该值可以表示为二进制位字符串，也可以基于复杂的数据结构，从而支持车联网中的选择性披露。基于属性的签名能够对共享的信息进行细粒度控制，使用户可以隐藏身份或位置等敏感数据；然而，该系统的有效性取决于维持强大的匿名性。

  El Kaafarani 等人 [120]通过强调签名既不应泄露驾驶员身份，也不应允许对手通过识别属性模式推断位置，从而正式提出了这一要求。这对于保护位置隐私至关重要，因为即使是看似无害的属性，如果随时间关联起来，也可能被利用来追踪驾驶员的移动。然而，基于属性的签名的一个局限在于，它可能容易受到高级关联攻击的影响，对手会交叉比对多个数据点或属性来推断位置。为了解决这一问题，Kaaniche 等人 [121] 提出了一种改进的基于属性的签名模型，采用具体的数学构造和随机预言机模型，显著增强位置隐私和身份隐私。尽管这一改进强化了隐私保障，但生成和验证签名所涉及的计算复杂度仍令人担忧，尤其是在车联网这类高速移动环境中，实时通信至关重要。尽管存在这些局限，基于属性的签名仍是平衡位置隐私需求与车载通信中共享数据效用的有力工具，可为隐私保护提供灵活且可扩展的解决方案。

- **群签名：** 群签名提供了一种强有力的机制，通过允许群组成员（例如驾驶员）代表群组匿名签署消息，而不暴露其身份，从而保护位置隐私。这确保消息在被验证为来自合法成员的同时，签名者的真实身份仍然保密，这对于保护车联网中的驾驶员位置隐私至关重要。

  郑等人提出的可链接群签名 [122] 等增强方案增加了审计和追踪等功能，并通过引入盲签名和陷门承诺等先进密码学技术，提升了该框架的安全性。这使主管部门能够进行审计

表 V COMPREHENSIVE OVERVIEW OF USER-SIDE 位置隐私保护机制S IN VEHICULAR NETWORKS

LPPM Type	机制描述	Key 参考文献	主要优点	显著缺点
Pass 和 Run	将车联网视为 容延网络，路由 通过其他车辆发送消息	[116]	破坏时空相关性	通信中的高复杂性 和传输
		[117]	破坏时空相关性； 个性化保护	
属性- 基于 签名	对消息进行精细粒度签名 对识别的控制 信息。	[118]	精细化控制； 个性化保护	签名可能会揭示驾驶员 高存储消耗 高计算开销
		[119], [120]	匿名性基于属性的签名	
		[121]	匿名性基于属性的签名； 低计算开销	高存储消耗
群组 签名	群组成员共同地 匿名身份验证 通过群签名	[122]	可追踪群签名； 提高通信效率并 安全	签名生成时间长，且 验证时间
		[59]	签名长度短； 签名生成时间短，且 验证时间	双线性对密码学 对于车载单元和路侧单元而言过于复杂
		[123]	使用椭圆曲线密码系统； 降低计算复杂度	忽略车辆在 身份认证中的协作
		[124]	实现无条件隐私保护，采用的是 匿名环签名	身份认证时延
		[125]	在签名中引入路侧单元； 降低身份认证延迟	高带宽资源开销 在传输中
		[126]	无证书签名； 传输中的低带宽资源开销 传输； 低存储消耗	车辆的参与影响 隐私保护较少
可净化 签名	半可信的传感器在 获得授权后，可以修改一条 已签名消息	[127]	首先开发可净化签名	日志信息可能暴露 敏感数据
		[128]	隐藏经过身份验证的标识； 匿名化的日志信息	忽略了对先验知识的 车辆
盲 签名	消息内容被隐藏 在签名之前	[129]	使用零知识来改进 盲签名的安全性	双线性对密码学 对车载单元和路侧单元而言复杂
安全 计算 tion	一种安全外包方案 利用多个对象进行计算 keys	[130]	身份认证和 通信开销较低； 避免重复且无用的 加密的基于位置服务消息	无需密钥协商和相互 身份认证
Data 扰动	发送前扰动位置 将其发送给基于位置的服务 服务器	[131]	使用虚假位置实现 *k*-匿名性	忽略时空相关性
		[132]	结合本地差分隐私 和匿名性	
		[133]	首先改进 Geo-I	
		[134]	考虑时空相关性	计算开销高
		[135]	平衡边缘 计算	
		[136]	个性化保护	忽略短距离的位置 偏移
		[137]	为位置敏感应用提供高数据效用 LBS	隐私成本高
		[138]	使用长期标识符以减少 计算和存储消耗	由于跟踪窗口较长，安全性 较低
		[58]	首先使用差分隐私辅助假名交换	忽略.....的不可重复性 假名

或追踪可疑活动，同时不损害普遍的匿名性。正如 Hakeem 等人所探索的那样，采用双线性对密码学可缩小签名的大小，并提高跨多个区域的消息验证效率。 [59], 然而，正如 Wu 等人指出的，双线性对密码学对车载单元和路侧单元而言计算开销可能很大， [123],这会限制此类系统在实时车载环境中的可扩展性和实用性。为解决这一问题，建议采用椭圆曲线密码学来降低计算复杂度，使群签名更适合资源有限的设备。Mundhe 等人提出的环签名通过让消息经由经过验证的合法车辆传递，提供无条件隐私保护，并通过确保群组内的匿名性进一步增强位置隐私。 [124], 此外，在基于环签名的位置隐私保护机制中，采用假名并允许路侧单元协助生成签名，可显著缩短身份认证延迟，提升实时效率。尽管如此，这也带来了权衡，包括签名管理开销增加，以及撤销方面可能面临的挑战；一旦密钥或假名遭到泄露，就需要及时使其失效。

- **可净化签名：**Ateniese 等人 [127], 提出的可净化签名允许获得授权的半可信方或“审查者”修改已签名消息的特定部分，而无需与原始签名者交互。当需要在与第三方共享数据之前隐藏或更改敏感数据（例如驾驶员身份或位置）时，这一功能尤其有用。例如，Pa mies 等人 [128] 展示了如何将日志匿名性与可净化签名相结合，在将信息从本地节点传输到远程存储服务器时保护身份和位置数据。通过允许选择性修改，可净化签名有助于维护隐私，同时确保消息的完整性。然而，这种方法存在局限，尤其是在信任方面：半可信审查者可能会滥用权力，修改超出必要范围的信息，甚至引入恶意修改。此外，验证已修改签名以及控制消息中哪些部分可以修改所需的计算复杂度会增加开销，进而可能影响车联网的可扩展性和效率。可净化签名支持灵活的数据共享，因此能带来显著的隐私保护优势；在需要动态数据净化以保护位置隐私、同时又不损害消息真实性的场景中，这一点尤为重要。

- **盲签名：**盲签名提供了一种强大的隐私保护机制，对于保护车联网中的位置隐私尤为重要。在盲签名方案中，消息内容在签名之前会被隐藏或“盲化”，这意味着签名者——通常是可信实体——无法看到实际的消息内容，而其中可能包含敏感位置数据。将消息作者与签名者分离，确保即使消息经过身份认证，签名者仍然不知道其具体内容，从而为驾驶员提供强有力的匿名性。Sun 等人 [129] 在雾计算众包感知架构中改进了这一方法，通过部分盲签名认证保护驾驶员的身份和位置隐私。借助零知识验证，系统确保签名者能够验证请求的真实性，却无法获知驾驶员位置的任何信息，从而进一步增强安全性和隐私保护。在这一理念的基础上，近期的盲签名方案发展引入了融合公开元数据的变体 [143]。这些方案使发行方能够将匿名令牌与特定元数据关联起来，同时不损害用户不可关联性，谷歌 VPN 服务的实际部署便证明了这一点。这种方法在增强盲签名在特定应用中的效用的同时，保留了传统盲签名的隐私性和可扩展性。

盲签名面临着若干局限性。其中一个关键问题是计算开销增加，尤其是在资源受限的车载环境中，实时响应至关重要。此外，尽管零知识证明增强了隐私保护，但也增加了验证过程的复杂性，可能导致高流量场景下的身份认证速度下降。此外，如果管理不当，盲签名方案对可信第三方的依赖可能引入潜在的安全漏洞或单点故障。对强 RSA 模数的依赖，以及将密码哈希函数视为随机预言机的假设，进一步限制了这些方案的灵活性，这可能给需要模块化适应性的环境带来挑战。

总而言之，尽管基于签名的方法（如基于属性的签名、群签名和盲签名）在保护车联网中的位置隐私方面具有显著优势，但也存在局限性。主要挑战之一在于证书管理过程会带来大量计算和存储开销。证书管理，尤其是在大规模动态车联网中，需要持续进行更新、撤销和验证，所有这些操作都会给车载单元和路侧单元的计算资源带来压力。在实时处理大量数据时，这一问题尤为突出，因为证书验证延迟可能导致碰撞规避系统等关键应用出现延迟。此外，为确保持续隐私而维护多个假名或密码密钥，也会增加存储需求，从而提高资源受限环境中效率低下的风险。双线性配对、椭圆曲线密码学和零知识证明等操作的复杂性进一步加剧了这些问题，使实时处理面临挑战。尽管存在这些问题，基于签名的方法对于增强位置隐私仍至关重要，因为它们能够在不泄露敏感信息的情况下验证消息。未来，轻量级密码技术和去中心化证书管理协议的发展，有望在维持车联网强隐私保护的同时，减轻计算负担。采用无证书密码学或聚合签名等更具可扩展性的方法，或可】【。

还提供了在安全、隐私和效率之间取得平衡的潜在解决方案。

3）安全计算机制：安全计算机制在保护位置隐私方面发挥着关键作用，使系统能够处理敏感位置数据，而无需直接向包括基于位置的服务在内的第三方披露这些数据。这些技术最初由姚氏协议于 1982 年基于百万富翁问题形式化 [144], ，允许多方在保护各自输入隐私的同时，共同计算输入对应的函数。在车联网中，安全计算可确保驾驶员使用基于位置的服务时，不会暴露其精确的位置数据。通过处理加密位置信息，安全计算机制使基于位置的服务提供商能够提供路线优化或交通警报等服务，而无需获取原始数据，从而保护驾驶员的隐私。

Zhuo 等人 [130] 通过提出一种多密钥安全外包计算方案拓展了这一概念，该方案无需基于位置的服务服务器与驾驶员直接交互，即可增强位置隐私。其方法通过在身份验证前删除冗余或无法使用的加密消息，最大限度地减少不必要的通信开销。这对于维持基于位置的服务应用的服务质量至关重要，因为过长的通信延迟会降低用户体验。该多密钥方案利用同态加密，可直接对加密数据进行计算，因此只需解密最终输出，例如导航指令或交通警报。此模型显著提升了隐私保护水平和效率，减轻了驾驶员设备的计算负担，并确保基于位置的服务无法推断敏感的位置详情。

虽然安全计算机制能够提供强有力的隐私保障，但其计算开销通常较大，尤其是在处理需要实时响应的复杂车载应用时。相关密码操作（如同态加密和安全多方计算）可能会引入延迟，这在紧急车辆路径规划或碰撞规避系统等对时间敏感的场景中或许无法接受。此外，安全计算方案假设所有参与实体都遵守协议，因此容易受到对手攻击；对手可能试图扰乱计算过程或篡改加密输入。未来的工作可着力优化这些密码协议，以降低延迟和计算复杂度，使安全计算更适用于实时车载应用。

4）数据扰动：作为基于混淆的位置隐私保护机制的一个分支，数据扰动技术通过在将实际位置信息传输至基于位置的服务之前对其进行扭曲，在保护驾驶员位置隐私方面发挥着关键作用 [15]。这些技术可应用于用户侧，即驾驶员在传输之前操纵其数据；也可应用于服务器端。在用户端数据扰动中，驾驶员无需信任外部实体，因为他们可以控制对其位置信息的混淆。这种对集中式信任模型的独立性降低了基于位置的服务服务器发生潜在数据泄露所带来的风险，从而增强了隐私保护。用户侧扰动面临的挑战在于平衡隐私保护与cuntegn以及数据效用——确保位置数据对基于位置的服务仍然有用，同时提供可靠的隐私保护。

- **基于虚拟位置的方法：**基于虚假数据的方法通过在真实位置旁生成多个伪造位置（虚拟位置），提供了一种简单而有效的位置隐私保护方案，使对手难以辨别真实位置。这些方法无需可信第三方或密钥共享机制参与，因此驾驶员可以完全掌控自己的位置数据。Niu 等人 [131] 改进了这一技术，提出了一种利用k匿名性的位置选择算法：真实位置隐藏在至少k 个其他虚拟位置之中，从而增加潜在攻击者的不确定性。该方法根据匿名熵选择虚拟位置，通过确保虚拟位置不易被区分来最大限度地保护隐私。在此基础上，Tadakaluru 和 Qin [145] 提出了一种基于Voronoi图的语义均衡虚假位置生成框架，可生成兼顾空间相似性和语义相似性的虚假位置。该方法通过确保虚假位置在语义上均衡且在地理位置上分散，有效抵御了时间约束攻击；这类攻击是传统虚拟位置方法的常见局限。然而，该框架会增加额外的计算开销，可能因此不适用于实时应用。

基于虚假数据的方法的一个显著局限是容易受到时空相关性攻击，尤其是在连续位置服务请求中。随着时间推移，对手可以分析时间可达性、方向相似性等模式，过滤掉虚假位置，从而逐渐暴露真实位置 [134]。为解决这一问题，Liu 等人提出了过滤策略，通过确保虚假位置随时间呈现逼真的行为来提升隐私保护，例如使其轨迹或行程时间与真实位置相似。尽管这些策略增强了隐私保护，但也增加了计算时延，可能会妨碍车联网中的实时应用。尽管如此，其存储成本仍在可接受范围内，因此，对于实时响应不那么重要、而隐私问题至关重要的应用而言，基于虚假数据的方法是一个实用的选择。总而言之，虽然基于虚假数据的方法以相对低成本、去中心化的方式保护位置隐私，但在高频数据环境中，时空相关性会降低其有效性，因此该方法存在局限。

- **本地差分隐私（LDP）：**差分隐私可以限制对手获取的知识，但可能会降低基于位置的服务的质量。从基于位置的服务提供商的角度来看，如果获得较高的精度，应用便能提供高质量的服务；但大多数基于位置的服务可以接受并非完全准确的位置数据。差分隐私可定义如下 [146],

定义 *1*（差分隐私（*DP*））：当且仅当对于任意一对数据x_i 和x_j，机制满足 ε-DP，

我们有

$$\frac{\Pr[\mathsf{M}(x_i) \rightarrow y]}{\Pr[\mathsf{M}(x_j) \rightarrow y]} \leq e^{\varepsilon}, \quad (1)$$

其中，y 是该机制的输出。 ε 取决于数据集的敏感度。通常， ε 是一个较小的正数。

LDP 是传统差分隐私的一种分布式变体，允许驾驶员在将位置信息发送至服务器之前对其进行扰动。Erlingsson 等人 [132]通过结合差分隐私与匿名性，增强了隐私保护，以实现本地差分隐私的高隐私保护能力。作者指出，如果该方法在客户端采用 LDP，并在服务器端采用洗牌策略，则无需添加任何显著的噪声即可实现位置隐私安全。然而，作者忽略了道路网络中的时空相关性。

- **地理不可区分性（Geo-I）：** Geo-I 最初由 Andre´s [133] 提出。Geo-I 允许驾驶员在给定的模糊半径 r 和隐私预算 E 下享受Er-差分隐私，其定义如下。

定义 *2*（*Geo-I*）：当且仅当对于任意两个位置 x_i 和 x_j，满足以下条件时，该机制满足 ε-Geo-I

$$\frac{\Pr[\mathsf{M}(x_i) \rightarrow y]}{\Pr[\mathsf{M}(x_j) \rightarrow y]} \leq e^{\varepsilon d(x_i, x_j)}, \quad (2)$$

其中，y 是该机制的输出，$d(x_i, x_j)$ 表示x_i 和 x_j之间的距离。

基于 Geo-I，Zhou 等人 [135]设计了一种在边缘计算中平衡效用与隐私的框架。该框架包括两部分：保护隐私的位置服务使用方法和基于隐私的服务调整。作者添加二维高斯噪声来偏移实际位置。尽管作者考虑了隐私与服务质量之间的平衡，该框架仍可能导致较高的计算开销。基于对可信服务的背景知识，Li 等人 [147]采用相关概率和相关转移概率来实现 Geo-I。所提出的方法可以为不同需求提供不同级别的隐私保护。位置偏移决定了隐私保护级别。当驾驶员的位置偏移小于阈值时，该偏移无效。尽管该方法可以提供不同级别的保护，但它忽略了道路状况。如果出现交通拥堵，且驾驶员频繁使用基于位置的服务，那么对手可以据此获取驾驶状态的模糊位置将始终不变。Li 等人 [137] 提出了一种改进的 Geo-I 定义，称为扰动隐藏，以确保扰动后的位置有效。扰动隐藏方法将道路网络地图转换为网格，并将可接受的位置用作候选集。此外，该方法采用动态规划确定检索区域，以提供准确的基于位置的服务。作者采用动态规划方法，为驾驶员确定最短的检索半径。扰动隐藏方法的局限性这种方法的缺点是，可能会导致隐私受限区域的隐私成本较高。

- **假名：** 假名被用作临时由证书颁发机构生成并分发的匿名证书。基于假名的位置隐私保护机制旨在确保通信中驾驶员身份与假名之间的不可链接性 [148]。Wang 等人 [138]将假名视为长期标识符，以降低计算和存储开销。作者设计了假名交换请求触发机制，以协助证书颁发机构更换假名。车辆在满足触发条件时更换假名。该方法存在一个局限：假名长期使用可能会为对手提供更长的跟踪窗口。假名不可区分性最早在 [58]中提出，旨在确保假名交换过程中的严格不可链接性。假名交换过程满足差分隐私。即使两辆车的驾驶状态相似，对手也无法在交换后关联这些假名。假名不可区分性方法只需较少的假名即可实现较高的交换完成概率。该方法的局限在于作者忽略了假名交换中的冲突。基于假名的位置隐私保护机制有两个弱点。其一，这类机制必须管理车辆的假名，导致较高的计算和存储开销。其二，这类机制无法确保在跟踪攻击中实现不可链接性。

5）用户侧位置隐私保护机制总结：本部分概述了用户侧位置隐私保护机制，展示了如何结合基于签名的方法和数据扰动方法，为位置隐私提供额外保护。

基于属性的签名的主要特点是，车辆能够使用指定属性选择性地对消息进行签名，同时不会泄露个人标识符；借助这一能力，车辆可以证明自己属于某个授权群组（例如紧急服务），而无需透露其身份。基于属性的签名所实现的细粒度特性，使其非常适用于需要验证某些属性、同时又需要保护敏感信息的场景。基于属性的签名能够提供个性化隐私保护和灵活性：服务可以根据需求选择性地披露某项属性，并通过在消息认证过程中仅在必要时减少数据暴露来增强隐私。然而，基于属性的签名的计算和验证开销仍然是一个重大挑战，尤其对于资源受限的车载设备而言。此外，某些属性的重复使用可能暴露行为模式，使系统容易受到关联攻击。

群签名使车辆能够代表群组以匿名方式对消息进行签名。验证者可以验证消息的合法性，而无需追踪发送者身份，同时保留可追踪性，以便审计违规车辆。群签名方案具有很强的匿名性，非常适合在动态车联网中实现隐私保护认证。然而，计算复杂度较高的签名生成与验证不利于实时性能。此外，在大规模

环境中，管理群组成员资格和撤销已泄露的密钥也面临重大可扩展性挑战。

盲签名使车辆能够在不向签名者透露消息内容的情况下验证消息；因此，它们能在通信中为位置和敏感内容提供强有力的隐私保护。事实上，盲签名具有很强的匿名性和内容隐私保护能力，尤其是在与其他隐私保护技术结合使用时；但它们依赖可信的第三方实体，这可能带来安全漏洞。此外，盲签名方案的计算开销较高，可能导致验证时延，因此不适用于时间要求严格的车联网。

数据扰动技术通过在信息传输前对其进行模糊处理来维护位置隐私，例如向数据中添加噪声或生成虚假位置。差分隐私也能进一步提供保障，为用户提供形式化的隐私保证。这些方法计算轻量、成本低，因此适用于用户侧设备。由此，这些方法能够主动抵御对抗性跟踪，有效地为位置信息引入不确定性。然而，过多的噪声会降低数据效用，导致基于位置的服务结果不准确；与此同时，扰动方法仍容易受到时空相关性攻击的影响，这类攻击会利用随时间变化的位置模式。

安全计算允许车辆在不解密的情况下处理加密位置数据，通过安全地外包计算，在轨迹分析或路线优化等操作中维护机密性。这样可以有效确保数据机密性，因此非常适合加密交通分析或路线查询等隐私保护型外包任务。然而，安全计算会增加显著的计算开销，影响实时性能，而复杂的密钥管理流程会降低可扩展性，尤其是在涉及车辆参与的高度动态环境中。

通过发挥各自的互补优势，可以构建一个多层框架，以应对车联网用户侧位置隐私保护机制中匿名性、完整性和计算效率方面的挑战。

- **基于属性的签名和群签名**可以协同工作，在细粒度隐私控制与匿名群级身份认证之间实现平衡。基于属性的签名允许车辆利用属性选择性地对消息进行签名，而无需泄露个人标识符；与此同时，群签名确保消息来源在群组内保持匿名。例如，驾驶员可以使用基于属性的签名来证明其凭证（如“授权用户”或“应急车辆”），而无需披露其身份；群签名则确保车辆的存在无法被追踪。然而，这两种方法都会带来计算开销和验证时延。为解决这一问题，可以采用椭圆曲线密码学来减小签名大小并缩短验证时间，从而使这种组合能够实际应用于资源受限的车载设备。
- **盲签名结合数据扰动**可有效确保内容和位置的匿名性。盲签名使驾驶员能够在不向签名者泄露消息内容的情况下对消息进行签名，从而在身份认证过程中提供强有力的隐私保护。为了进一步隐藏位置数据，可在将数据发送至基于位置的服务之前，采用基于差分隐私的扰动技术添加受控噪声或虚假位置。这种双层方法可确保消息和车辆位置都受到保护。其中一项挑战是盲签名的计算复杂度，尤其是在实时环境中。通过整合多重签名聚合技术，可以缓解这一问题；该技术允许同时验证多条消息，在不损害隐私的情况下降低开销。
- **与群签名相结合的安全计算**为维护数据机密性并实现安全消息认证提供了可靠的解决方案。群签名可在车辆签署消息时保障其匿名性，而安全计算则确保能够处理加密数据，而不泄露明文位置。例如，车辆可以将轨迹分析外包给安全计算方案，使基于位置的服务能够处理基于位置的查询，而无需访问原始数据。安全计算中的密钥管理局限性可通过去中心化无证书密码协议加以解决；此类协议可简化密钥分发与验证，提高系统可扩展性，并减少对中心化机构的依赖。

将这些方法整合到混合框架中，可以形成多方面的解决方案，从而增强隐私、降低通信开销并确保实时性能。实施这种混合方法的关键挑战在于管理计算复杂度并确保可扩展性。可采用边缘计算，将签名验证和数据扰动等计算任务卸载到附近的边缘服务器，以降低延迟并实现实时性能。此外，使用无证书密码方案可以简化证书管理，减少存储开销并简化撤销流程。

B. 服务器端位置隐私保护机制

通过采用服务器端位置隐私保护机制，服务提供商必须对其客户端托管的数据 [149] 执行额外的处理。服务提供商可以通过数据库匿名化、移除可识别痕迹或加密数据内容来实现这一目标。近期服务器侧位置隐私保护机制的比较如表 VI 所示。

1) 统计披露控制（*SDC*）：统计披露控制机制主要用于保护统计数据库中的数据，同时兼顾数据效用与驾驶员位置隐私。通常，统计披露控制机制的输出能够确保数据库不会泄露与特定驾驶员相关的信息。数据库匿名化和差分隐私是统计披露控制机制中最常用的两种技术。

- ***k*-匿名性：** *k*-匿名位置隐私保护机制通过确保驾驶员的数据与至少k 1 辆其他车辆的数据无法区分，从而保护驾驶员的位置，并增加对手的不确定性。这种方法迫使对手在多个潜在位置之间进行猜测，有效增大其估计误差，从而增强位置隐私。通常根据k 辆车辆的

表 VI COMPREHENSIVE OVERVIEW OF SERVER-SIDE 位置隐私保护机制S IN VEHICULAR NETWORKS

LPPM Type	机制描述	Key 参考文献	主要优势	显著缺点
SDC	输出保证 不披露驾驶员特定的 数据库中的信息	[150]	存储消耗低; 计算开销低; 不需要可信第三方	无身份认证和密钥协商 协议
		[151]	考虑历史信任信息	
		[152]	使用固定收发器以降低 交通状况的影响	需要专用硬件
		[153]	允许车辆传输加密的 静默区域中的信息	需要可信第三方; 计算开销高
		[154]	扩展了支持 请求限制属性的匿名认证	隐私保护可能遭到破坏 通过身份披露
		[155]	经济高效的匿名性	需要一个可信第三方
		[156]	低通信开销	忽略先验知识。
		[157]	考虑数据相关性; 减少所需的噪声	压缩数据可能会泄露 原始数据
		[158]	提高位置数据 发布的效率	忽视时空相关性
		[159]	采用私有对偶分解 技术; 提升调度性能; 高可扩展性	仅为.....提供隐私保护 调度过程
HE	通过直接分析密文 并镜像对应的 在.....上执行的操作 明文执行的 操作	[160]	避免频率调度过程中发生 隐私泄露	所考虑的半可信雾计算节点 节点并不可靠
		[161]	降低加密的开销 传感器数据	高传输时延
		[162]	允许一组乘客共享 总行驶距离最短的车辆 距离	计算开销高; 传输延迟高
		[163]	避免关联不同 同一车辆的假名	
		[164]	低计算开销	忽略对手的知识
		[2]	将加密位置数据外包给 云服务器以获取准确的 安全地获取基于位置的服务查询结果	基于位置的服务提供商的数据是 与该机制高度耦合
PIR	允许驾驶员请求数据 项而不披露所请求的 具体数据项	[165]	降低计算成本	隐私保护可能遭到破坏 通过较长的跟踪窗口
SE	使驾驶员能够安全地 保留明文关键词，同时 在基于位置的服务中进行 搜索	[166]	搜索结果的准确率高	计算开销高

最大熵原理来选取车辆，该原理会选择历史请求模式相似的车辆，以最大限度地提高匿名性。*k*-匿名位置隐私保护机制既可在集中式模型中实现，也可在分布式模型中实现。集中式*k*-匿名性需要可信位置模糊服务器来聚合和匿名化位置数据，这会引发对服务器可信度以及潜在单点故障的担忧。相比之下，分布式*k*-匿名方法依赖参与者之间的协作，无需中央机构，但会增加协调方面的复杂性。

近期的进展包括 Li 等人提出的基于区块链的分布式*k*匿名模型 [150],。该模型利用区块链技术记录并验证经过哈希处理的安全信标消息，从而降低存储消耗和处理时间。这种去中心化方法还能确保位置数据不被篡改，从而提高数据完整性，且无需可信第三方。类似地，Luo 等人 [151] 通过引入信任管理系统改进了该方法；该系统根据历史

交互记录计算车辆的信任等级，并将其记录在区块链中，进一步增强了该方法的可靠性。此外，Liu 等人 [167] 提出了一种用于分布式k匿名隐私保护的位置可用性度量方法，以解决恶意协作用户提供伪造位置的问题。该方法根据历史数据（包括访问时间、距离和频率）评估所接收位置的可用性，并成功过滤伪造位置，确保匿名隐藏区域有效。尽管该方法效果显著，但它依赖准确的历史数据，而且额外的计算开销可能会限制其在某些场景下的实时适用性。

k-匿名方法存在一定的局限性。例如，这些方法容易受到时空关联攻击的影响，对手可以将多个查询随时间关联起来，从而筛除虚假位置或匿名化位置。此外，在低密度交通区域，维持足够数量的附近车辆以确保k-匿名性可能颇具挑战性，从而降低其有效性。尽管如此，k-匿名性仍能提供显著的隐私保护优势，尤其是在高流量场景中，大量车辆构成的庞大集合能够增强匿名性，而区块链的集成则进一步强化了信任与完整性，无需依赖中心化实体 [168]。

- **混合区域：**混合区域方法允许驾驶员在指定区域（称为混合区域）内更换假名，以增强位置隐私。在这些区域中，车辆的进出点相互脱钩，使试图追踪车辆的对手难以确定其身份 [169]。驾驶员按一种顺序进入区域，却以不同的顺序离开，因此对手更难将旧假名与新假名关联起来。这种方法能够有效干扰位置追踪，尤其是在车辆众多的高密度城市环境中。然而，混合区域存在显著局限，尤其难以抵御时序与转换攻击。对手可以关联车辆进出混合区域的时间，从而重新识别假名，降低混合区域保护位置隐私的效果。此外，连续查询关联攻击也构成了另一项挑战：对手可以根据基于位置的服务请求、交通状况或时间限制的模式，将旧假名与新假名关联起来。根据已知的等待时间和观察到的车辆行为，可以排除假名之间的某些对应关系。

为解决这些问题，Amro [152]提出了一种混合区域方法，利用充当虚拟车辆的固定收发器参与假名交换过程，从而弥补低流量区域中实体车辆不足的问题。尽管这一创新减轻了交通状况的影响，但也引入了潜在的安全漏洞，因为获取收发器假名的对手可能会破坏交换过程。此外，对额外基础设施的依赖增加了系统的复杂性和潜在攻击面。另一项改进是基于群组的动态混合区域方法，该方法允许车辆在静默区域交换加密信息，同时考虑假名过期时间和车辆个性化需求等因素。这种动态方法增强了灵活性和隐私，尤其适用于资源受限区域。

尽管取得了这些进展，混合区域仍然面临与时序相关的安全漏洞，并且需要经过精心设计，以确保强大的假名不可链接性，同时保持较低的计算开销和基础设施开销。

- **其他基于匿名性的LPPM：**Meng等人 [154] 提出了一种方法，通过加入请求限制功能来扩展导航服务中的匿名认证，从而有效保护位置、路线和身份隐私。该方法可确保持续的基于位置的服务查询不会暴露驾驶员的实时移动情况，进而在多个会话中保持不可链接性和机密性。然而，尽管该方法在防范身份关联攻击方面表现出色，但由于请求限制机制带来的开销，它可能会增加实时应用的延迟。

Zhu等人 [155]提出了匿名智能停车与支付（ASAP）方法，该方法结合使用模糊化技术、哈希和加密，以匿名化驾驶员的位置，为智能停车服务提供支持。ASAP能够有效隐藏实际位置，但依赖模糊区域可能会降低服务精度，尤其是在需要精确导航或停车时。

Singh 等人 [156]提出了源位置隐私伪装概率泛洪（MPFSLP）方法，该方法通过使用概率泛洪确保不可追踪性。车辆不会生成虚假数据包，而是重新发送先前传输过的消息，从而增加对抗性跟踪的难度。MPFSLP 的主要优点在于能够降低通信成本，同时保持消息完整性和身份认证。然而，与许多基于匿名性的方案一样，该方法面临时空相关性方面的挑战，因为对手可能能够推断出随时间变化的模式。此外，由于消息传输中可能存在冗余，概率泛洪可能会降低大型网络的效率。

- **一般差分隐私：** 在车联网中，可在服务器端应用差分隐私，在基于位置的服务（LBS）或其他实体使用位置信息之前对其进行匿名化。Soheila等人 [157]提出了一种差分隐私数据流（DPDS）系统，用于聚合来自车联网的数据；该系统通过组长汇总并发送各组车辆的位置数据，从而减少隐私保护所需的噪声量。虽然这种聚合减少了噪声，但其主要局限在于压缩数据的大小与原始数据相近，因此可能无法显著节省存储空间或带宽。此外，在交通监控或事故预防等实时应用中，聚合和压缩引入的时延可能会影响系统性能。Miao等人 [158] 进一步通过引入噪声四叉树和基于希尔伯特曲线的方法来增强差分隐私，该方法可高效组织空间数据，以改进位置数据发布。然而，该方法的局限在于仅关注二维空间，无法充分捕捉现实车载环境的复杂性；现实环境涉及更多动态且多维的数据，例如海拔。

或对时效性要求较高的路由信息。

- **联合差分隐私：**联合差分隐私扩展了传统差分隐私，确保隐私保障适用于群体而非仅适用于单个实体。这在车联网中尤为实用，因为共享乘车或集体数据报告等协同行为十分常见。通过限制单个驾驶员的操纵能力，联合差分隐私降低了对手从虚假报告或异常值中推断敏感信息的风险。在网约车服务中，联合差分隐私通过增加对手从聚合数据中识别个体驾驶员或乘客的难度，提供了更强的保护。

Han等人 [159] 利用这一概念提出了一种调度协议，在网约车系统中平衡位置隐私与运营效率。该方法采用私有对偶分解和驾驶员聚类，在保护隐私的同时尽量减少行驶里程。通过对驾驶员和车辆进行分组，隐藏个体路线和偏好，系统在优化乘车分配的同时保护位置数据。此外，私有乘车分配协议确保在整个调度过程中保护有关乘车请求和驾驶员位置的敏感信息。然而，尽管联合差分隐私提供了强有力的隐私保障，也可能带来效率方面的挑战。平衡隐私与效用的需求——尤其是在拼车等时效性要求较高的场景中——可能导致计算开销增加和决策延迟，在处理大规模车联网时尤为明显。此外，尽管联合差分隐私降低了个体的操纵能力，但仍可能受到多方串通的威胁：对手可能协同工作，从共享报告中推断位置数据。

2）同态加密：同态加密（HE）是一种强大的密码学技术，可直接对加密数据进行计算，而无需解密。这一特性对于保护车联网中的位置隐私尤其重要，因为它可以确保敏感位置数据在整个传输、存储和计算过程中始终保持加密状态。同态加密方案将密文上的运算映射为明文上的相应运算，从而确保处理加密数据后得到的结果，与使用原始未加密数据进行处理所得的结果一致。这一能力在基于位置的服务等场景中尤为实用：驾驶员可能需要提交位置信息，以获取交通信息更新或导航辅助等实时服务，同时又希望向服务提供商隐瞒自己的实际位置。

HE 最常见的定义如下。

定义*3*：令和 Cp分别为明文与密文集合。如果且仅当对于任意给定的加密密钥 k 以及任意一对数据 x_i 和 x_j，以下关系成立时，加密机制满足同态性：$\forall x_i, x_j$

$$\mathsf{M}(x_i \,0_{\mathscr{O}}\, x_j) \leftarrow \mathsf{M}(x_i)\, 0_{\subset}\, \mathsf{M}(x_j), \qquad (3)$$

对于某些算子 $\mathscr{O}$，其属于 和 $\subset$，其属于 C，其中 表示左侧可以直接由右侧计算得出。

HE 方案可分为全同态加密和部分同态加密，如下所示。

- **部分同态加密（PHE）：**部分同态加密（PHE）是最早且最简单的同态加密形式之一，支持同态加法或乘法，但不能同时支持两者 [170]。因此，PHE 特别适用于无需解密即可对加密数据进行的特定有限计算。在位置隐私方面，Yucel 等人 [160] 将 PHE 用于保护充电站调度场景中的驾驶员位置数据。频繁的调度请求会暴露实时位置数据，给驾驶员带来隐私风险。通过使用 PHE 隐藏驾驶员的位置信息，系统可确保在调度操作期间不会泄露敏感位置数据，使驾驶员能够动态加入和离开充电站网络，同时维护隐私。整个过程中数据始终保持加密状态，这意味着仅对加密数据执行必要的计算（例如确定调度时段），实际位置信息则始终得到保护。

PHE 的局限性源于其功能受限——它只能执行同态加法或同态乘法中的一种，而无法同时执行两者。这限制了其在更复杂场景中的适用性，例如车联网中的路线优化或多步骤位置查询，这些场景在处理过程中需要同时执行这两种运算。此外，尽管与全同态加密（FHE）相比，PHE 的计算效率更高、更加轻量，但其简单性使其在动态实时应用中的通用性较低。PHE 的优势在于其效率，因此，对于那些仅需针对特定且定义明确的任务提供隐私保护、同时计算开销极低的应用而言，它是一种可行的选择。尽管存在局限性，PHE 仍然是充电站调度等场景中的一种实用解决方案，在这些场景中，即使采用功能有限但有效的加密方式，也能在不引入显著时延或资源消耗的情况下提供可靠的隐私保护。

- **轻度同态加密 (SHE)：**SHE 方案通过允许对加密数据进行有限次数的同态加法和乘法，在隐私保护与计算效率之间实现平衡。因此，SHE 非常适用于隐私至关重要、但数据处理需求并不十分繁重的车联网。例如，Subramaniyaswamy 等人 [161]提出了一种基于整数的轻度同态加密方案，通过优化传感器之间的数据传输间隔，降低了加密开销，从而提升了轻度同态加密算法的效率。在网约车服务场景中，Yu 等人 [162] 将 SHE 应用于计算共享车辆中多位乘客的总行驶距离。通过使用密文打包，他们确保能够计算加密后的距离总和，而不泄露乘客的实际位置

，从而保护位置隐私。
虽然 SHE 在安全性和性能之间取得了良好的平衡，但仍存在局限性。SHE 支持的运算次数有限，因此不太适合复杂或长期运行的计算；在这些计算中，加密方案可能会失效或效率低下。此外，与其他同态加密方案一样，相较于传统加密方法，SHE 仍会产生较高的计算成本，这使得在车联网中实现实时应用面临挑战。尽管存在这些不足，SHE 在拼车或传感器数据聚合等场景中仍很有价值，因为这些场景的计算范围适中，且必须保护位置隐私，同时无需大量计算资源。

- **全同态加密（FHE）：** FHE 为保护车辆网络中的位置隐私提供了强大的解决方案，它能够在无需解密的情况下对加密数据执行无限次操作。这使 FHE 非常适用于基于位置的服务等应用，在这些应用中，敏感位置数据需要持续处理，同时确保隐私。FHE 的一项主要优势在于，它允许车辆对加密位置数据执行复杂计算，例如路线优化或交通管理，从而保护驾驶员免受位置跟踪。

Perma等人 [163] 通过结合全同态加密与假名加密，解决了假名关联这一难题，确保即使使用多个假名，位置数据仍然保持不可链接。在车载雾云计算等实时应用中，Mohammed等人 [164] 利用全同态加密实现了安全且具有成本效益的计算，同时满足移动性约束和截止期限。类似地，Farouk等人 [2] 证明了全同态加密在城市移动性仿真和基于位置的服务查询中的可行性，确保加密位置数据能够在云端得到安全处理。然而，尽管全同态加密具有强大的隐私保障能力，但其计算消耗高、效率低，难以应用于实时大规模车联网。加密和解密过程需要大量计算资源，导致时延增加和开销增大，这在需要快速响应的动态车载环境中尤为突出。因此，尽管全同态加密能够提供可靠的位置隐私保护，但其实际部署仍受到显著性能缺陷的限制。未来若能进一步优化全同态加密的计算效率并降低开销，将有望使其更适用于实时车载应用。

3）隐私信息检索：隐私信息检索（PIR）是一种密码学技术，允许驾驶员从数据库（例如基于位置的服务）查询特定数据项，而无需向服务提供商透露请求的是哪一项数据。该机制在保护位置隐私方面十分有益，因为它能防止基于位置的服务服务器将查询与驾驶员的实时位置或个人数据关联起来。通过支持在不披露信息的情况下进行查询，PIR 可确保即使基于位置的服务服务器遭到入侵，对手也无法根据所请求的数据确定驾驶员的位置

然而，传统的私有信息检索协议会带来显著的计算开销，因此难以应用于车联网等实时应用。计算和通信成本高昂，往往源于处理大量加密数据的需求，这会导致效率低下，尤其是在速度和响应能力至关重要的动态环境中。

为解决这些问题，Tan 等人 [165]提出了一种优化的 PIR 方法，该方法利用道路网络的先验知识来降低计算成本。通过将交通信息（例如交通模式和道路拓扑）整合到 PIR 过程中，系统可以缩小数据查询范围，减少每次检索所需的计算量。这在不牺牲隐私保护的前提下提高了 PIR 的效率，显著增强了其在车联网中的实用性。然而，尽管这种优化降低了计算负担，却也使系统依赖准确且最新的交通数据，这可能限制其在交通状况快速变化时的适用性。此外，虽然 PIR 能确保数据请求保持私密，却无法防止随时间发生的时空相关性攻击；对手可能会根据重复查询推断驾驶员的位置。

4) 可搜索加密（*SE*）：可搜索加密是一种服务器端隐私增强技术，允许驾驶员加密其搜索查询（例如，基于位置的关键词），同时支持在基于位置的服务中高效搜索，而不会泄露查询的明文。在车联网中，当驾驶员搜索加油站或餐厅等附近服务时，这种机制对于保护其隐私至关重要，因为查询可能会泄露敏感位置数据。可搜索加密方案通常会加密关键词，并允许服务器在不解密的情况下处理搜索查询，从而确保敏感信息对服务提供商不可见。此外，可通过集成群签名、布谷鸟过滤器、Pederson 承诺、智能合约和代理重加密等额外工具来增强可搜索加密方案，从而提高搜索精度、效率和安全性。例如，将公钥加密与可搜索加密结合，用户便可在保持强安全保障的同时搜索加密数据。

然而，传统可搜索加密方案在处理几何范围搜索时面临挑战，而这对于依赖空间数据的基于位置的服务至关重要。大多数可搜索加密方案在搜索指定几何区域内的位置时，都会返回错误或不精确的结果，因为它们难以处理点与点之间的空间关系。为解决这一问题，Chen 等人 [166] 开发了一种基于公钥系统的新型可搜索加密方法，支持任意几何区域搜索，且具有 100

尽管取得了这些进展，可搜索加密方案，尤其是支持复杂几何搜索的方案，可能会在实时应用中带来计算开销和延迟，因为搜索过程需要对加密查询和数据进行密码运算。此外，要兼顾搜索效率与隐私并非易事，尤其是在需要快速实时响应的大规模车联网中。

5）服务器端位置隐私保护机制总结：本部分详细回顾了服务器端位置隐私保护机制，这些机制通过在服务器层面进行匿名化、加密或选择性数据管理来增强位置隐私。尽管服务器端位置隐私保护机制通常能够提供强有力的隐私保障，但通过审慎整合互补方法，可以进一步克服其各自的一些局限，提升其在车联网中的可扩展性、效率和实用性。

统计披露控制机制（SDC），包括*k*匿名和混合区域技术，旨在保护统计数据库中的位置数据。*k*匿名可确保驾驶员的位置无法与附近一组车辆的位置区分开来，从而有效提高对手不确定性。近期创新，例如基于区块链的分布式*k*匿名，减少了对可信第三方的依赖，并增强了数据完整性。然而，*k*匿名容易受到时空相关性攻击，在低密度交通区域的效果也较差。另一方面，混合区域方法允许在指定区域内变更假名，从而阻断位置跟踪。虚拟收发器等改进方案可弥补交通稀疏的问题，但也会带来安全风险和基础设施复杂性。为增强这些技术，可结合区块链实现去中心化信任，并采用基于群组的假名交换，以便在动态交通状况下兼顾安全漏洞防护与可扩展性。

同态加密通过支持对加密数据进行运算而无需解密，为服务器端位置隐私提供了强有力的解决方案。部分同态加密可为特定任务提供轻量级加密，例如充电站调度；而 SHE 在计算效率与隐私之间实现平衡，适用于中等规模的数据处理，例如网约车应用。全同态加密支持对加密数据进行无限次运算，能够为路线优化或基于位置的服务查询等复杂计算提供强有力的隐私保护。然而，全同态加密存在显著的计算开销和延迟，限制了其实时适用性。为解决这一问题，可采用结合部分同态加密/SHE 的混合加密方案处理简单运算，并将计算密集型的全同态加密任务交由边缘服务器处理，从而在不牺牲隐私保障的前提下优化性能。

PIR 使驾驶员能够查询基于位置的信息，而无需向服务器透露目标对象。近年来的技术将道路网络知识融入 PIR 流程，显著降低了计算成本，从而使 PIR 能够应用于实际车辆场景。然而，鉴于随着时间推移反复发起的查询会暴露驾驶员的位置，PIR 仍易受到基于时空相关性的某些攻击。因此，通过虚假查询机制或查询混淆技术增强 PIR，可以在保持查询效率的同时进一步干扰对抗性跟踪。

可搜索加密使驾驶员能够在基于位置的服务上执行加密关键词搜索，而不会泄露查询内容。最近，有研究提出了基于几何范围搜索的可搜索加密增强方案，可确保对任意空间区域的搜索准确性达到 100%，克服了传统可搜索加密方案固有的局限性。然而，由于涉及复杂的密码运算，可搜索加密会产生计算延迟。索引技术和代理重加密可用于优化搜索效率与隐私之间的权衡，从而在大规模车联网中实现快速实时响应。

为了解决各自的局限并发挥互补优势，可以按如下方式将服务器端位置隐私保护机制集成到混合隐私保护框架中：

- **基于 HE 的 SDC：**SDC 方法（如*k*-匿名性）会在存储前对位置数据进行匿名化处理，而 HE 则确保所有计算均在加密数据上安全进行。这种组合在存储和处理过程中保护位置数据，防止对抗性推断攻击。通过整合 HE，SDC 中的安全漏洞（如易受时空相关性攻击）得以缓解，因为即使统计匿名性失效，加密数据仍无法被访问。
- **隐私信息检索和同态加密：**隐私信息检索允许驾驶员在不泄露所请求内容的情况下私密地查询数据，而同态加密可确保对这些查询的计算以加密形式进行。这种集成在不影响基于位置的服务功能的前提下，为位置查询提供端到端隐私保护。将计算密集型任务卸载到边缘服务器，可显著降低隐私信息检索的开销；与此同时，同态加密可确保整个查询过程中数据的机密性。**可搜索加密与统计披露控制：**可搜索加密支持在使用统计披露控制方法（如混合区域或*k*-匿名）创建的匿名化数据库中进行安全、高效的加密搜索。这种组合在保护隐私的同时，确保空间数据检索准确。对匿名化数据进行预处理并为加密搜索查询建立索引，可减少可搜索加密的计算时延，即使在大规模系统中也能实现快速、高效的查找。

通过将这些方法策略性地结合为一个混合框架，可以在存储、查询和计算阶段保护敏感数据。未来研究应着重优化同态加密的计算效率、提升隐私信息检索和可搜索加密的可扩展性，并利用边缘计算确保实时性能。这些进展将有助于构建稳健且保护隐私的基础设施，在安全性、效用和运营效率之间取得平衡。

C. 用户-服务器接口位置隐私保护机制

用户-服务器接口位置隐私保护机制着重保护驾驶员与基于位置的服务（基于位置的服务）之间的通信信道，通过保护数据交换过程来维护位置信息的机密性和完整性。这些机制依赖于信道侧技术，以确保安全通信并建立对第三方的信任。虽然它们能够有效防范窃听和篡改，但在可扩展性和对信任的依赖方面仍存在局限。

1) 安全通信： 安全通信可分类如下。

- **加密通信协议：**加密通信协议，例如传输层安全协议（TLS）和安全外壳协议（SSH），通过加密数据，在保护车联网中的位置隐私方面发挥着至关重要的作用。

在驾驶员和基于位置的服务之间交换。这些协议利用公钥密码学建立安全信道，防止对手在传输过程中截获敏感位置数据。TLS 和 SSH 可确保即使通信受到监视，传输的数据在没有相应解密密钥的情况下仍无法被解读，从而为防范普遍存在的通信监视提供有力保护。

传统加密协议存在局限性。例如，SSH 需要定期进行用户验证，这会增加计算开销，并可能耗尽驾驶员设备的资源，尤其是在需要频繁更新位置的实时应用中 [171]。此外，加密过程本身会引入延迟，可能影响对时效性要求较高的车载应用的性能。尽管存在这些缺点，加密通信协议仍然是保护车联网数据安全的基石，因为它们能有效降低数据传输过程中发生位置数据泄露的风险。挑战在于如何针对高速、实时的车载环境优化这些协议，同时不削弱它们所提供的强大隐私保障。

- **端到端加密服务：**端到端加密（E2EE）服务通过确保只有预期接收者才能解密终端用户之间传输的数据，提供强大的隐私保护，使攻击者或中介无法在传输过程中获取敏感的位置数据 [172]。在车联网环境中，E2EE 是保护位置隐私的有力工具，尤其适用于车辆需要直接交换数据的场景，例如协同驾驶、交通协调或拼车。E2EE 的主要优势在于无需信任中介或第三方服务提供商，从而最大限度地降低数据泄露和未经授权访问的风险。

然而，尽管 E2EE 能有效保护传输中的数据，但由于密钥管理和可扩展性方面的挑战，它在当前车联网中很少使用。在庞大、分布式的车辆网络中动态管理加密密钥十分复杂，而且在维持强加密的同时，确保实时车载应用实现低延迟通信也会消耗大量资源。此外，E2EE 本身无法防范端点漏洞，这意味着如果对手获得发送方或接收方设备的访问权限，加密数据仍可能遭到泄露。尽管存在这些局限，随着车联网不断发展并融入第五代移动通信和第六代移动通信技术，E2EE 预计将在确保车辆与基础设施之间实现安全、私密的通信方面发挥更大作用，尤其是在自动驾驶或安全交通管理等需要高度保障数据完整性和隐私的任务中。

2）可信第三方（*TTP*）：TTP 技术在车联网中充当中介，通过对驾驶员的数据进行匿名化和假名化来保护驾驶员位置隐私。TTP 的主要目标是防止对手将驾驶员的真实身份与其位置数据关联起来，从而保护敏感信息。TTP 通过签发临时假名或管理加密通信，帮助驾驶员与基于位置的服务进行交互，同时不暴露其位置或身份。然而，依赖 TTP 会带来若干挑战。恶意实体，尤其是在协同攻击中，可能拥有足够的资源和能力攻破 TTP，或通过积累的假名数据追踪驾驶员，从而损害隐私 [173]。

此外，TTP 还构成单点故障：一旦遭到入侵，大量敏感信息就可能泄露。因此，近期研究提倡采用无需中心化可信第三方的隐私保护方法。例如，采用区块链的去中心化系统通过在多方之间分散信任，提供了一种替代方案，从而减少对单一实体的依赖 [174], [175]。这些去中心化方法增强了隐私和韧性，但也带来了新的挑战，例如更高的计算成本、延迟和存储需求，这些因素可能会限制其在资源受限环境中的可扩展性。

D. 位置隐私与数据效用之间的平衡

位置隐私与数据效用之间的平衡在车联网中至关重要，因为必须兼顾这两个目标，才能确保系统的有效性。位置隐私对于保护驾驶员免受潜在的跟踪、画像分析或恶意攻击至关重要，这些威胁可能源于敏感位置数据的滥用。然而，基于位置的服务的数据效用取决于实时位置信息的准确性和可用性，以提供导航、交通信息更新和个性化推荐等服务。过度保护隐私，例如采用过度的数据扰动或混淆，可能会降低这些服务的质量，使其效果变差，甚至无法使用。相反，隐私保护不足会使用户面临重大风险，削弱其对基于位置的服务的信任，并导致其不愿共享数据。

这种平衡使用户能够从基于位置的服务中受益，同时确信其位置数据得到了充分保护。此外，未能实现这种平衡可能导致用户参与度下降，并使服务提供商和用户双方的价值受损。因此，必须设计隐私保护技术，在最大限度降低隐私风险的同时优化数据效用，并根据不同应用和用户偏好的具体需求调整保护级别。

许多位置隐私保护机制专注于位置隐私与数据效用之间的平衡，如表 VII 所示。实现位置隐私与数据效用之间平衡的主要方法有六种，具体如下。

1）区块链：区块链技术通过实现去中心化数据存储和信任管理，无需中央机构即可为车联网中的分布式管理提供强有力的解决方案。这对位置隐私保护机制尤其有益，因为区块链能够让车辆安全地获取必要信息，同时保护匿名性和位置隐私。例如，Luo 等人 [151] 利用区块链存储基于狄利克雷分布的历史信任数据，使车辆能够匿名地与其他车辆协作。通过这种方式，他们减少了通信延迟，同时

表 VII EXISTING 位置隐私保护机制S IN 位置隐私与数据效用之间的平衡。

方法	技术	位置隐私保护机制类别	论文
区块链	分布式管理	k-匿名性	[150], [151], [176]
		其他	[17], [177]–[183]
自适应参数	调优参数	传递并运行	[117]
		基于属性的签名	[118], [121]
		Geo-I	[15], [135], [137], [147]
		假名	[58]
		其他匿名性	[155]
		一般差分隐私	[157], [158]
		SHE	[161]
		FHE	[164]
混合	结合多种方法	群签名	[122], [124]
		可净化签名	[128]
		基于虚假数据	[131]
		LDP	[132]
		联合差分隐私	[159]
		SE	[166]
加密优化	降低计算开销和 通信开销	群签名	[123]
		盲签名	[129]
		安全计算	[130]
		混合区域	[153]
		PHE	[160]
		FHE	[163]
参数简化 和优化	简化流程	群签名	[59], [126]
		盲签名	[129]
		基于虚假数据	[134]
		假名	[138]
		其他匿名性	[156]
		FHE	[2]
		隐私信息检索	[165]
虚拟节点	引入合作者	群签名	[125]
		假名	[138]
		k-匿名性	[152]
		TTP	[174], [175], [184], [185]

维持安全可信的环境。类似地，Li 等人 [150]提出连通性和平均距离这两个关键指标，用于衡量基于区块链的k-匿名框架中数据效用与隐私之间的平衡。

区块链技术通过提供无需可信第三方的去中心化解决方案 [186]，已成为在车联网中实现位置隐私与数据效用平衡的有力工具。Malik 等人 [17]开发了一种基于区块链的身份认证与撤销方法，降低了计算与通信开销，从而提高了隐私保护机制的效率。类似地，Wang 等人 [180]将盲签名与区块链相结合，设计了一种高效的身份认证方案，利用区块链存储车辆公钥，并将其与计算出的用于安全验证的默克尔根值。Tang 等人 [181]将群签名和其他密码学工具整合到基于区块链的停车场共享隐私保护可搜索加密方案中，扩展了这一概念，在隐私保护与服务准确性之间取得平衡。此外，Chaudhary 等人 [176] 和 Liang 等人 [182] 使用区块链解决k-匿名的局限性，后者还引入了模糊区域，以更好地保护位置数据。Wang 等人 [183] 通过基于区块链的路侧单元（RSU）增强了信任管理，而 Lu 等人 [177] 则利用区块链存在与缺席证明保护位置隐私，避免身份泄露。这些方案展示了区块链在确保可信度、减少语义攻击、关联攻击和数据挖掘攻击造成的脆弱性的同时，保障位置数据安全并维持数据效用的能力。然而，

实现最佳平衡仍至关重要，因为过度依赖隐私保护机制会降低车载网络中实时服务的有效性。

他们的方法表明，区块链能够通过提高安全信标消息交换的效率，优化位置隐私与数据效用之间的平衡。基于区块链的系统不仅能确保车辆的实时数据保持私密，还能缩短数据处理时间，确保通信及时，同时不损害隐私[187]。总而言之，区块链能够增强隐私和效率，但必须谨慎调整，以避免降低数据依赖型应用的性能。

2）自适应参数：基于自适应参数的位置隐私保护机制通过根据驾驶员的具体要求和系统的上下文需求调整隐私参数，动态平衡位置隐私与数据效用。这种适应性可减少不必要的资源消耗，并最大限度地降低数据效用损失，而这往往是静态隐私保护方法面临的挑战。例如，Lu 等人 [117] 量化位置隐私和“完美隐私”，帮助车辆通过其他车辆转发数据，同时确保基于位置的服务（基于位置的服务）的效率和准确性。同样，Shahandashti 等人 [118] 和 Kaaniche 等人 [121] 允许车辆根据预定义属性仅披露必要的数据，在保障隐私的同时不损害效用。此外，Ma 等人 [15], 、Zhou 等人 [135],和 Li 等人 [147] 提出了位置隐私保护机制，使车辆能够根据隐私保护和效用需求调整隐私设置，从而提升隐私保护效果和服务质量。Li 等人 [58]进一步优化了这一方案，使车辆能够根据驾驶状况更换假名，在提升隐私保护的同时维持实时数据的效用。差分隐私等技术也会通过控制噪声水平来平衡隐私保护与检索准确性，Ghane 等人 [157]和 Miao等人 [158] 对此进行了演示。此外，边缘计算和加密技术可减少时延与资源消耗，确保实时应用保持高效 [161], [164]。自适应参数的主要优势在于能够灵活满足隐私与效用需求，为车联网中保护敏感位置数据并提供准确、高效服务这一固有的平衡难题提供切实可行的解决方案。

3）混合方法：LPPM 中的混合方法结合多种方法，以同时优化隐私保护和系统效率。这些方法融合不同技术的优势，克服各自的局限，从而实现更加均衡的解决方案。例如，Zheng 等人 [122] 和 Mundhe等人 [125] 将群签名与假名相结合，在降低计算开销的同时确保安全的身份验证。通过使用假名，可以缩短签名长度，从而减少计算时间和资源消耗。同样，Pamies 等人 [128]采用日志匿名化与可净化签名相结合的混合方法，进一步降低隐私风险，确保位置数据等敏感信息得到保护在数据传输过程中。此外，Niu 等人 [131] 通过使用虚假位置增强k-匿名性，并考虑有关车辆的侧信息，以提高匿名性的稳健性；而 Erlingsson 等人 [132] 在用户侧使用差分隐私来模糊位置信号，防止对手将假名关联起来。Tong 等人 [159] 将联合差分隐私与空间索引和分布式优化相结合，在保护位置数据的同时优化计算效率。同样，Chen 等人 [166] 将 SE 与计算隐私信息检索相结合，在维护道路网络中的位置隐私的同时降低计算负担。这些混合方法为位置隐私与数据效用之间的基本平衡提供了更细致的解决方案，能够根据具体情境进行调整，在不影响基于位置的服务质量或及时性的情况下提供稳健的隐私保护。

4) 加密优化：车联网中的加密优化旨在减少传统加密方法所带来的通信和计算开销，同时保护位置隐私并保持数据效用。双线性对密码学等先进密码学技术通常会产生较高的计算成本和时延，从而降低基于位置的服务的性能。为解决这一问题，Wu 等人 [123] 转向采用更高效的密码方案，例如椭圆曲线密码系统。与双线性对相比，该系统能够减轻消息签名和验证的计算负担。此外，Sun 等人 [129]结合了基于加密的方法，包括零知识证明和同态加密，以提升网络响应速度，同时确保强有力的隐私保护。Zhou 等人 [130]采用互不串通的服务器，避免了车辆与基于位置的服务服务器之间不必要的加密数据交换，从而进一步降低延迟、提升实用性，且不损害安全性。Li 等人 [153] 提出在混合区内传输加密数据，以降低假名管理的存储成本，在增强隐私的同时确保数据效用不受影响。Yucel 等人 [160] 将同态加密纳入双染色最近邻分配中，以保护位置隐私，并实现较低的资源消耗和快速收敛。正如 Prema 等人 [163], 所指出的，全同态加密虽然能提供稳健的隐私保护，但可能造成显著的通信开销；他们通过将全同态加密与假名结合来控制消息频率，从而缓解这一问题。如何在强有力的位置隐私保护与保持较高数据效用之间取得恰当平衡，同时尽量减少时延，仍然是一项挑战：过于复杂的加密方案会降低服务器响应速度，而过于简化的方法则可能损害隐私。通过优化加密技术，可以在不过度牺牲车联网服务效率和效用的前提下保护位置隐私。

5) 参数简化与优化：当位置隐私保护机制能够简化流程时，可以显著降低时延。例如，免证书位置隐私保护机制可以消除证书身份认证时延和证书存储消耗。Hakeem 等人 [59] 实现了

利用双线性配对密码学和短签名，通过一条消息和短签名完成对大规模基站多个区域的身份认证。作者显著缩短了签名生成和验证时间。Mei 等人 [126] 采用具有完全聚合技术的无证书聚合签名方案，以减少资源消耗。在计算Diffie-Hellman假设下考虑随机预言机，实现了隐私保护与数据效用之间的平衡。Sun 等人 [129]优化了基于雾计算-公交的车辆群智感知框架，切断了身份与位置数据之间的关联。作者简化了数据上报、信誉管理和奖励发放中的数据处理流程，从而提高效率。

Liu 等人 [134]关注位置数据的时间可达性、方向相似性以及入度/出度。其开发的时空相关性感知位置隐私保护机制简化了相邻位置集合，以实现个性化的位置隐私保护。Wang 等人 [138] 通过引入基于触发器的结构，避免频繁更换假名，从而提升假名的数据效用。Singh 等人 [156]使用位置和速度而非车辆身份，简化了所需的车辆特征。作者允许每辆车发送其他车辆的数据，并将其伪装成自己的位置数据，在不损害数据效用的情况下，显著降低了基于假名的位置隐私保护机制的可追踪性。Farouk 等人 [2] 将位置数据托管在云服务器上，以避免车辆与多个实体共享位置数据。车辆只需与云服务器共享数据，即可低时延地获取基于位置的服务。Tan 等人 [165]利用道路网络的先验知识，降低预处理和通信过程中计算隐私信息检索的开销。

6) 虚拟节点： 位置隐私保护机制在平衡位置隐私与数据效用方面发挥着关键作用，尤其是对于k-匿名性这类需要特定数量相邻车辆才能提供强隐私保障的方法。在实体车辆稀少的场景中，位置隐私保护机制可以生成虚拟节点，作为真实车辆的占位符，使系统在不损害数据准确性或效用 [125]的前提下，达到所需的匿名性阈值。这些轻量级虚拟节点占用的存储空间有限，因此能够在维持系统性能的同时，高效地增强隐私保护。例如，Wang 等人 [138] 采用触发器等虚拟设备来辅助假名变更，从而提升基于假名的位置隐私保护机制中的隐私保护。同样，Zhu 等人 [155] 在道路网络中引入固定混合区域，虚拟节点可在其中帮助防止对手关联假名，确保即使在低流量区域也能持续保护位置隐私。通过创建虚拟实体，这些方案降低了对实际车辆密度的依赖，使位置隐私保护机制能够保持较强的隐私保护能力，同时不降低实时服务所需的数据效用。然而，虚拟节点的有效性取决于确保其不会过度扭曲底层数据，因为过度使用可能导致基于位置的服务不准确。

总之，现有试图平衡位置隐私与数据效用的方法，无法满足未来第五代移动通信/第六代移动通信赋能的车联网的需求。例如，基于 Geo-I 的位置隐私保护机制会向位置数据中注入受控噪声，导致数据不准确，因此需要额外的数据优化。这会降低第五代移动通信/第六代移动通信网络中的大数据处理效率；即便经过微调，数据效用仍会显著下降，因此这些方法并不适用于第五代移动通信/第六代移动通信服务提供商 [216]。同样，基于虚拟节点的方法也难以平衡隐私与效用。未来的第五代移动通信/第六代移动通信网络将配备大量传感器，用于实时环境监测，因此虚拟节点将不再必要。这进一步凸显了对更先进隐私保护解决方案的需求，以确保在高密度传感器丰富环境中兼顾隐私保护与数据效用。

7) 定位应用示例：利用车联网和基于蓝牙的近距离检测的 COVID-19 追踪应用，体现了平衡位置隐私与数据效用这一复杂挑战。在大流行病期间，这些系统通过从车辆和智能手机收集大量位置数据，在监测病毒传播和确保遵守健康指南方面发挥了重要作用 [217], [218]。虽然这些数据对于公共卫生工作至关重要，但也引发了严重的隐私问题。通过整合 GPS数据、驾驶日志和基于蓝牙的接触，此类应用可能会披露个体驾驶员及附近其他人员的敏感位置详情，从而增加轨迹重建和身份推断的风险。

车联网的更广泛背景进一步加剧了隐私保护的复杂性。来自联网车辆、智能设备和社交网络等各种来源的位置数据日益丰富，为大数据挖掘提供了丰富的环境。这也带来了重新识别攻击的风险：对手可能重建个人的出行轨迹并推断其个人信息，从而危及位置隐私。此外，车联网容易受到网络安全威胁，因而可能遭受利用这些数据的恶意攻击；当这些数据与大流行病期间的公共卫生监测等更广泛的应用相关联时，风险尤为突出。

与位置隐私和数据效用之间的理论平衡不同，实际应用更关注数据效用。在抗击 COVID-19 的过程中收集和交换位置数据，是车载追踪的一个典型示例。现有的疫情防控应用可分为集中式管理和去中心化管理。在集中式管理的情况下，政府或机构会监控确诊病例的医疗信息。只有出现新的患者时，政府或机构才会公开该患者的轨迹。在去中心化管理的情况下，位置数据由驾驶员管理。只有驾驶员感染后，其轨迹才会向主管部门公开。严格管理此类信息可以帮助世界免受病毒侵害，但患者的位置隐私会因此暴露。表 VIII 展示了相关应用的优势

表 VIII BALANCE 位置隐私与数据效用之间的权衡：实践中的-VEHICLE 跟踪： COVID-19 应用。

架构	应用	所需信息	局限性
集中式	COVIDSafe（澳大利亚） [188]	接触信息	驾驶员的个人信息，例如身份信息、电话号码和电子邮件。 频繁记录的接触信息会暴露驾驶员的轨迹。 可以从报告的地理信息中推断出私人信息。 地理信息会向公众披露，用于疫情防控
	E-Tabib（阿塞拜疆） [189]		
	BeAware Bahrain（巴林） [190]		
	新冠追踪器孟加拉国（孟加拉国） [191]		
	台湾社交距离（中国） [192]		
	TousAntiCovid（法国） [193]		
	病毒雷达（匈牙利） [194]		
	Rakning C-19（冰岛） [195]		
	Smittestopp（挪威） [196]		
	BlueTrace（新加坡） [197]		
	支付宝（中国） [198]	地理信息	
	微信（中国） [199]		
	LeaveHomeSafe（中国） [200]		
去中心化	Stopp Corona（奥地利） [201]	接触信息	恶意攻击者可以推断患者轨迹并通过创建匹配轨迹与标识符多个账户并记录多条路线。 地理信息被公开披露，用于疫情防控
	Stop COVID-19（克罗地亚） [202]		
	eRousˇka（捷克） [203]		
	Smittestop（丹麦） [204]		
	Koronavilkku（芬兰） [205]		
	Corona-Warn-App（德国） [206]		
	Apturi Covid（拉脱维亚） [207]		
	Radar COVID（西班牙） [208]		
	SwissCovid（瑞士） [209]		
	NHS COVID-19（英国） [210]		
	DP-3T（欧洲） [211]		
	PACT（美国） [212]		
	Private Kit: Safe Path（美国） [213]	地理信息	
	韩国系统 [214]		
	HaMagen（以色列） [215]		

和局限性。在表 VIII 中，现有的 COVID-19 应用程序分为集中式应用程序和去中心化应用程序。

集中式应用程序（例如，TraceTogether（新加坡） [219]，COVIDSafe（澳大利亚） [188],和 BlueTrace（新加坡） [197]）记录的是加密的接触记录，而非位置信息。只有主管部门才能解密接触记录。如果驾驶员感染，主管部门可以获取该驾驶员的身份信息。其他驾驶员可以通过接触记录查询自己的感染风险。然而，患者身份和轨迹会暴露给主管部门，从而增加位置隐私泄露的风险。如果其他驾驶员串通推断目标对象，应用的隐私保护能力就会降低。

DP-3T（欧洲） [211] 和 PACT（美国） [212] 是去中心化应用程序的两个示例。这两个应用程序创建周期性密钥，以生成多个临时标识符。临时标识符会作为信标消息在区域内广播。这两个应用程序会将接收到的信标消息与额外信息一同存储。这些应用程序根据主管部门提供的信息匹配临时标识符。然而，恶意攻击者可以通过创建多个账户并记录多条路线，推断患者轨迹，并将轨迹与标识符进行匹配。Private Kit: Safe Path（美国） [213] 和韩国系统 [214]是其他类型的 COVID-19 应用程序。它们会定期根据全球定位系统（韩国

韩国系统记录了详细的个人信息。如果驾驶员感染，他们可以向主管部门报告自己的轨迹。主管部门可以选择向公众公开的信息。为疫情防控，这些轨迹会向公众公开。然而，由于所有人都可以查看这些轨迹，这些应用无法提供预期的位置隐私保护能力。

现有的COVID-19接触者追踪应用通过使用匿名性 [220]，在位置隐私保护能力与数据效用之间实现平衡。这些应用，例如TraceTogether（新加坡） [219] 和COVIDSafe（澳大利亚） [188]，，会定期广播随机时变令牌，作为驾驶员的临时身份标识 [221]。这些应用记录驾驶员的接触信息，并利用这些信息报告感染风险。然而，即使这些应用并未有意收集个人信息 [221]，获得授权的实体仍然可以将临时身份标识与驾驶员的个人信息（例如轨迹、电话号码）关联起来。

车辆位置隐私与COVID-19跟踪之间的关联，为更广泛地理解车联网中管理位置隐私的挑战提供了重要insights。两种情境都涉及为公共利益收集和分析大量实时位置数据——无论是跟踪车辆移动以进行交通管理，还是在大流行病期间监测疾病传播。然而，这些情境也凸显了在确保接触者追踪等服务的数据效用与保护个人隐私之间存在的内在矛盾。在COVID-19跟踪中，车辆驾驶日志、GPS数据和邻近接触被用于绘制感染风险图谱，但这些相同的机制也带来了轨迹重建和身份推断的重大风险。同样，在车联网中，如果未得到适当保护，传感器数据和社交互动的聚合也可能导致意外的隐私泄露。

E. 关键要点

在本节中，通过对用户侧、服务器端和用户-服务器接口位置隐私保护机制进行全面分析，我们得出若干基本见解，有助于加深对该领域挑战与机遇的整体认识。

本节分析了位置隐私与数据效用之间的微妙平衡。高水平的隐私保护往往需要先进的密码学技术、数据扰动或混淆策略，这可能会显著降低基于位置的服务的准确性和及时性。反之，优先考虑数据效用可能导致隐私漏洞，尤其是在实时信息至关重要的动态车联网中。例如，基于区块链的位置隐私保护机制无需依赖中心化机构即可提供强大的隐私保护，但其计算开销可能会妨碍实时应用。同样，差分隐私及其变体能够实现强有力的隐私保障，但在边缘计算或高密度环境等实际场景中，往往难以维持较高的数据效用 []。这一发现强调，需要采用自适应机制，根据具体情境和用户需求优化隐私与效用。

本节的分析凸显了现有位置隐私保护机制在应对5G/6G中不断演变的威胁方面的局限性

车联网。主要挑战包括密码学方法的可扩展性、对可信第三方的依赖，以及实时隐私保护机制的计算需求。这些限制因车联网日益增加的复杂性而进一步加剧：高移动性、密集的通信环境以及先进的对抗能力，都要求解决方案具备稳健性、高效性和可扩展性。该综述表明，尽管群签名和同态加密等技术为安全数据交换提供了有前景的途径，但仍需进行大幅优化，才能满足6G网络对低延迟和高吞吐量的要求。

对车联网中位置隐私保护机制（LPPMs）的全面分析揭示了若干关键主题，这些主题界定了当前位置隐私保护的发展现状及其未来潜力。通过考察用户侧、服务器端以及用户—服务器接口机制，本节识别了现有方法中反复出现的优势与局限性。本节的主要观察结果如下：

- **权衡动态：** 有效的位置隐私保护机制必须在隐私和效用之间取得平衡，避免过度牺牲服务质量或使用户面临隐私风险。根据情境因素动态调整隐私参数的技术展现出良好的应用前景。

- **可扩展性与效率：** 现有的位置隐私保护机制（LPPMs）面临可扩展性方面的挑战，尤其是在大规模、高密度车联网中。未来的解决方案应优先采用轻量级密码学方法和去中心化框架，以减少对资源密集型操作的依赖。

- **新兴技术的集成：** 区块链、边缘计算和人工智能等技术的集成可以增强其稳健性 o

f

位置隐私保护机制。然而，采用这些机制需要仔细考虑其资源需求以及潜在的安全漏洞。

V. 5G/6G车联网中位置隐私保护机制的经验教训与未解决的挑战

本节首先介绍未来车联网中的定位技术，并将其与当前网络中的对应技术进行比较。通过讨论新型定位技术带来的位置隐私和数据效用新需求，我们指出了现有位置隐私保护机制在5G/6G车联网中的局限性。我们阐述了新通信技术所引入的未来跨层跟踪技术可能造成的位置隐私问题，并提出通过改进现有位置隐私保护机制来解决这些问题。

A. 定位与位置隐私的进展

在5G/6G赋能的车联网中，定位技术的进步既提升了精度，也增加了隐私风险。协作定位、基于机器学习的跟踪和多径利用定位等新兴技术，通过充分利用.....实现了更高的精度。

表 IX DIFFERENT 当前及5G/6G VEHICULAR 网络中的定位技术。

定位技术	5G/6G的特征 车联网	对应技术 当前车联网	差异
传统定位	高数据速率 高可扩展性	基于蜂窝无线电的跟踪	更多基站和用户设备 更频繁的信号传输 更准确的定位
协作定位	超低延迟 高可扩展性	基于感知基础设施的跟踪 基于蜂窝无线电的跟踪 基于上层消息的跟踪	更多传感器 更频繁的信号传输 基站与用户设备距离更近
基于人工智能的定位	高数据速率 高可扩展性	基于感知基础设施的跟踪 基于光学视觉的跟踪 基于上层消息的跟踪	更多传感器 更详细的数据集 海量设备
信道制图	高可扩展性	基于蜂窝无线电的跟踪 基于感知基础设施的跟踪 基于上层消息的跟踪	考虑信道状态信息
驾驶员跟踪定位	高数据速率 超低延迟	基于感知基础设施的跟踪 基于上层消息的跟踪	更多传感器 三维车联网
多径利用定位	超低延迟 高可扩展性	基于蜂窝无线电的跟踪	更多传感器
SLAM	高数据速率 超低延迟 高可扩展性	基于车辆驾驶日志的跟踪 上层基于消息的跟踪 基于蜂窝无线电的跟踪	更多传感器 考虑随时间变化的状态 更多固定地标
上下文感知定位	高数据速率 超低延迟	基于车辆驾驶日志的跟踪 基于上层消息的跟踪	智能预测 大量个人信息

密集的基站部署、传感器融合和机器学习算法能够以前所未有的精度精准确定车辆位置 [222]。然而，这种增强的定位能力带来了新的位置隐私挑战。随着定位、感知和通信系统趋于融合，共享时间-频率-空间资源，以及整合由5G/6G启用的跨层跟踪技术，使多源数据挖掘和轨迹重建面临安全漏洞。这些风险源于对高分辨率位置数据的大规模收集；一旦这些数据遭到泄露，便可能暴露有关驾驶员的敏感个人信息。现有的位置隐私保护机制是为当前网络设计的，无法有效应对这些新型定位技术引入的跨层跟踪。

1) 传统定位：虽然传统定位技术通过几何计算提供可靠的定位，但在第五代移动通信/第六代移动通信车联网中，它们在位置隐私方面存在显著局限。基站位置和用户设备约束已知这一假设，本身就会使系统面临隐私风险。例如，用户设备与基站之间的频繁通信，加上第五代移动通信/第六代移动通信网络中不断增加的基站密度，可用于生成高度精细的轨迹数据，使用户更容易遭受跟踪和轨迹重构攻击。此外，距离和角度测量技术需要持续交换信号，而对手可以拦截或分析这些信号，以推断敏感的移动模式。区域测量和跳数方法也会随时间聚合数据，使得这使恶意实体更容易绘制覆盖大范围区域的详细移动路径。由于这些方法本质上优先考虑定位精度，往往未能纳入稳健的隐私保护机制，从而留下可被利用的漏洞，导致未经授权的位置跟踪并危及用户的位置隐私。

传统定位技术可根据距离、角度、区域和跳数测量 [223],分类如下。

距离测量：定位中的距离测量技术**.**依靠到达时间差、接收信号强度指示和连通性条件等与距离相关的参数来计算用户设备 [224]的位置。尽管这些方法具有较高的精度，但由于依赖用户设备与基站之间持续的信号交换，因此带来了显著的位置隐私风险。计算距离所需的传输时间和信号强度数据很容易被对手截获，使其能够对车辆或用户的确切位置进行三角定位。这使距离测量技术特别容易遭受窃听和中间人攻击，恶意行为者可以利用信号的时间和强度来重建用户轨迹。此外，随着5G/6G网络引入更高的基站密度和更频繁的通信，位置数据的粒度也随之增加，进一步加剧了跟踪和画像分析的风险。现有的位置隐私保护机制可能难以处理这些测量产生的精细粒度数据，因为持续数据交换会增加彩票娱乐

位置推断攻击发生的可能性，因此，在此类高精度定位环境中，制定先进的混淆和加密策略以保护用户隐私至关重要。

- **角度测量：** 角度测量技术依靠三角学和几何计算，利用基站与目标设备之间的角度信息来估计目标（如车辆）的位置 [225]。尽管该方法能够实现较高的精度，尤其是在密集车联网中，但也带来了若干位置隐私挑战。基于角度的定位具有很高的精度，这意味着即使角度数据发生细微变化，也可能被用于跟踪车辆的细微移动，使对手更容易重构连续轨迹或预测未来位置。此外，为了准确收集角度和距离数据，需要与多个基站进行持续通信，这会增加数据交换的频率，从而加剧位置数据遭受潜在窃听的暴露风险。这些系统尤其容易受到交叉引用攻击：对手将来自多个来源的角度和距离信息结合起来，以确定精确位置，从而加大跟踪和身份推断的风险。随着未来网络变得更加互联且更加数据驱动，角度测量的细粒度特征对位置隐私构成了重大威胁，因此需要采用先进的混淆和加密方法，以降低未经授权的访问和敏感位置数据遭到利用的风险。

- **区域测量：** 区域测量定位通过计算多个基站覆盖区域的重叠部分的中心交点来估算位置。虽然这种方法通过缩小目标区域提高了精度，但也带来了显著的位置隐私挑战。随着区域范围收窄、精度提高，生成的位置数据也更加详细，用户的移动因此会在无意中变得更容易追踪。较小的交叠区域带来的高精度，会持续生成细粒度的轨迹数据；若未得到充分保护，这些数据可能遭到窃听和跟踪攻击。对手可能利用区域测量的精度重建用户的行进路线，进而暴露家庭或工作地址等敏感位置。此外，在基站更为密集的高密度网络环境中，区域测量方法会提供更多精细跟踪的机会，加剧位置推断和身份关联的风险。

- **跳数测量：** 跳数测量定位通过分析用户设备与基站或其他网络节点之间的通信跳数来估算目标的位置。虽然这种方法提供了一种简单高效的定位方式，尤其是在多跳无线网络中，但它在位置隐私方面存在显著局限。主要问题在于，跳数测量需要数据在多个节点之间持续传输，而每个节点都可能记录并转发位置信息。随着跳数增加，敏感数据暴露的风险也随之上升，从而为对手提供更多拦截和分析通信的机会。此外，跳数测量容易受到侧信道攻击，攻击者可利用时间模式或流量模式，推断用户在较长时间内的轨迹。在节点密度较高的网络中，跳数定位的精度会提高，但这也会增加精细跟踪的风险，因为对手可以通过交叉比对不同网络区段中的跳数数据，重建详细的移动路径。此外，由于跳数定位通常缺乏加密和混淆保护，因此尤其容易遭受窃听和轨迹推断攻击，进而损害动态车联网中的用户位置隐私。

2）协作定位：协作定位利用设备到设备（D2D）通信，使用户设备能够直接测量距离和角度信息，从而显著提高定位精度；但这也给车联网带来了严峻的位置隐私问题。用户设备之间距离较近，加上超低时延D2D链路，使定位能够达到很高的精度，也增加了隐私泄露的风险。随着5G/6G网络中连接的节点增多，用户设备之间交换的大量位置数据可能被对手利用，以重建极其详细的移动轨迹 [1]。众多设备频繁进行实时通信，使未授权实体更容易拦截、监视或窃听D2D链路，从而导致位置跟踪方面的严重安全漏洞。此外，虽然高信噪比能够提升定位精度，但也会增加精确时空数据的暴露风险，而这些数据可用于推断用户行为、监控驾驶模式，甚至锁定特定个人。若缺乏强有力的隐私保护机制，协作定位因其产生的数据流量庞大，以及联网车辆之间共享的位置信息具有细粒度特征，在保护位置隐私方面将面临重大挑战。

3）基于人工智能的定位：基于人工智能的定位利用机器学习构建高度精细的指纹数据库，其中存储信道状态信息（CSI）等环境信道参数，并根据参考点估算车辆位置 [222]。尽管这种以数据为中心的方法提高了 5G/6G 车联网中的定位精度，但也带来了显著的位置隐私风险。基于人工智能的定位所需数据集内容丰富、粒度精细，包括实时更新和多层环境数据整合，这增加了数据泄露的可能性。由于机器学习模型依赖大规模数据收集和环境特征分析，对手可能利用这些海量信息推断敏感模式、追踪车辆移动，甚至预测未来轨迹。此外，分层共存、灵活存储和灵活处理所产生的海量数据，也加大了数据泄露和未经授权访问的风险。基于人工智能的模型通常依赖集中式服务器或云系统进行训练和处理；如果数据加密和隐私保护措施不够完善，就可能产生安全漏洞

。此外，模型反演攻击——即对手试图对机器学习模型进行逆向工程以提取敏感信息——给基于人工智能的定位带来了独特的隐私挑战。因此，整合高级加密和隐私感知机器学习技术以降低这些风险至关重要。

表 X LOCALIZATION 车联网技术。

定位	基站密度	Cost	精度
传统	High	低 [226]	低 [227]
协作	Low	低 [228]	中等 [229]
基于人工智能的	中等	高 [230]	高 [230]
信道制图	取决于	取决于情况	取决于情况
驾驶员跟踪	中等	低 [231]	中等 [231]
多径利用	Low	媒介 [232]	高 [233]
SLAM	Low	取决于	高 [234]
上下文感知	High	媒介 [235]	高 [236]

4) 信道制图： 信道制图是一种人工智能驱动的定位技术，基于 CSI 创建虚拟地图，使车辆能够在不依赖精确地理坐标的情况下于车联网中实现跟踪。虽然该方法通过提供实时伪位置作为参考来提升数据效用，但也带来了严峻的位置隐私挑战。尽管生成的虚拟地图不会泄露实际位置，但基于 CSI 的跟踪仍可能暴露轨迹模式，而对手可以利用这些模式重建用户的移动轨迹。信道制图所采用的人工智能算法还可能在无意中学习并揭示伪位置与实际位置之间随时间变化的相关性，尤其是在通过重复观测收集更多数据之后 [237]。这增加了位置推断攻击的风险：攻击者可以将伪位置与现实身份关联起来，尤其是在密集型车联网中。此外，信道制图过程缺乏稳健的加密或混淆机制，因此与传统的基于加密的方法相比，其隐私保护能力较弱，使系统容易受到数据挖掘和模式识别技术的攻击。因此，尽管信道制图提高了定位精度，但仍必须通过更完善的位置隐私保护机制加以解决其位置隐私局限性，以防止推断攻击并保障用户匿名性。

5) 驾驶员跟踪定位：驾驶员跟踪定位会持续推断驾驶员的位置，以减少估计误差 [222]。这种定位技术可以利用车辆传感器数据预测驾驶员轨迹，具体如下。**被动感知：** 在 5G/6G 车联网中，被动感知也称为无源雷达或无源相干定位，它通过检测和处理来自车辆或行人等目标的反射信号来确定其位置 [237]。尽管这种方法能显著提高能效，并具有非侵入式跟踪的优势，但也带来了重大的位置隐私风险。被动感知面临的根本挑战在于，它不需要目标主动传输信号，因此用户很难知晓何时或如何收集自己的位置数据。这引发了人们对非自愿监控的担忧，因为被监控目标通常无法控制所采集的数据。在未来传感器密集的环境中，感知基础设施将无处不在，被动感知会持续收集位置数据，且可能未经用户同意，使敏感信息几乎无法避免泄露。此外，汇总来自多个来源的高分辨率传感器数据，可能使对手得以重建详细轨迹并识别个人的移动模式，从而大规模损害位置隐私。

- **主动感知：** 主动感知技术（如基于雷达的定位）越来越多地应用于车联网，支持自适应巡航控制和交叉路口来车预警等应用，并提供高精度的三维距离测量。在 5G/6G赋能的车联网中，这些传感器将共享大量位置相关数据，以支持实时应用所需的高精度定位。然而，这种数据共享带来了严峻的位置隐私挑战。网络间持续交换精确的传感器数据可能导致轨迹重建，使对手能够分析收集到的数据，详细追踪车辆移动。此外，主动感知的实时特性增加了数据传输频率，进而为窃听和位置推断攻击创造更多机会。这类网络中的三维定位精度虽然有助于提升安全性和效率，却反常地增加了身份关联和移动画像分析的风险，因为即使是车辆位置的细微差异，也可能被利用来识别特定用户。

6) 基于多径的定位： 基于多径的定位利用充当车辆周围环境镜像反射的多径分量，并将其与环境几何结构相结合，即使在非视距（NLOS）条件下，也能披露驾驶员的位置，从而提升精度 [238]。虽然该方法能够在城市地区等复杂环境中提供稳健的定位能力，但也带来了严重的位置隐私漏洞。对来自各种表面的反射信号进行解释，使基于多径的定位能够捕获比传统方法更多的位置相关数据，从而实现更细粒度的位置跟踪。在 5G/6G车联网中，车辆配备了发射雷达类信号的多个传感器，将传感器数据与多径信息融合会进一步放大轨迹重建和未经授权的跟踪风险。其固有局限在于，该技术会持续收集详细的环境数据和无线电反射信息，使对手更容易收集和分析侧信道信息，以推断车辆的精确位置。此外，支持5G/6G的车联网系统中的密集传感器网络，可能使传统位置隐私保护机制越来越难以有效混淆此类高分辨率数据，导致用户即使在无法进行直接视距跟踪的场景中，也容易遭受位置推断攻击。

7）同步定位与建图（*SLAM*）： 同步定位与建图（SLAM）是第五代移动通信/第六代移动通信车联网中的一项先进技术，利用高数据速率、超低延迟和可扩展性，实时估计车辆位置和环境地标 [239]。然而，尽管SLAM具有诸多优势，它仍然面临着显著的位置隐私挑战。在基于视觉的SLAM中，摄像头和传感器用于捕捉周围环境，持续收集和处理详细的视觉数据可能会暴露有关环境和车辆轨迹的敏感信息。对手可以截获或分析这些数据，以推断车辆的精确位置和移动模式，从而引发对未经授权的监视和隐私泄露的担忧。同样，基于雷达的SLAM利用无线电波检测物体并绘制环境地图，也会生成精确的位置数据，而这些数据可能被用于跟踪和轨迹重建。在这两种情况下，SLAM数据的细粒度和实时性都会增加位置推断攻击的风险，尤其是在密集且高度互联的车联网中。

在5G/6G车联网中，SLAM可分为以下两类：基于视觉的SLAM和基于雷达的SLAM。**基于视觉的SLAM**：基于视觉的SLAM依靠摄像头等图像传感器来检测地标、绘制环境地图，同时跟踪车辆的位置。尽管这种方法在动态环境中能够实现高精度定位，但由于视觉数据采集本身的特性，它也带来了显著的位置隐私风险。摄像头会持续拍摄周围环境，包括住宅空间或私人财产等敏感区域，可能在无意中泄露用户或旁观者的私人信息。对手可能利用这些图像传感器采集的数据进行位置推断，甚至识别人脸和物体，从而导致隐私泄露。此外，如果没有采用稳健的加密和匿名化机制，大量图像数据的存储与处理会增加数据泄露的风险。实时图像处理的频繁需求也使基于视觉的SLAM容易受到网络攻击：对手可能截获并分析视觉数据，以还原详细的轨迹和行为模式。

- **基于雷达的SLAM**：基于雷达的SLAM利用三维激光雷达点云和激光传感器，相较于基于视觉的系统具有更高的局部定位精度，因此是未来自动驾驶车联网的重要组成部分。然而，这些系统采集的三维空间数据精度更高、内容更丰富，也带来了显著的位置隐私风险。激光雷达生成的点云可用于详细的环境测绘；若与其他车辆数据和基础设施数据结合，便很容易重建车辆的确切移动和轨迹。这种细粒度的数据使车辆暴露于持续跟踪之中，让对手更容易实施轨迹推断攻击，并通过分析移动模式识别特定驾驶员或车辆。此外，基于雷达的SLAM生成的密集数据也增加了数据泄露的可能性，若未实施适当的加密和隐私保护机制，对手便可利用这些详细信息进行未经授权的跟踪。

5G/6G车联网中的实体可以利用雷达类信号，从其他车辆、固定基础设施和传感器收集位置信息。

8）上下文感知定位：5G/6G赋能的车联网中的上下文感知定位利用个人和公共数据，根据驾驶员的位置和情境提供智能的多模态定位 [236]。这种方法允许驾驶员根据周围环境动态切换通信信道和通信技术，从而提高定位的准确性和适应性，但也带来了严重的位置隐私漏洞。将高度个人化的数据（例如驾驶习惯、常去地点）与公共数据（例如交通状况、天气）相结合，会形成复杂的数据环境，对手可能利用上下文信息推断驾驶员行为和行踪中的敏感细节。这尤其令人担忧，因为上下文感知定位需要通过各种信道持续交换上下文信号，使攻击者更容易实施跨层跟踪和数据关联攻击。此外，根据情境切换通信技术可能暴露安全协议中的漏洞，导致某些信道更容易遭受窃听或消息拦截。依赖上下文数据进行定位也引发了对长期收集个人信息的担忧，这些信息可能被用于构建全面的用户档案，进一步损害位置隐私。

B. 面向未来上层位置隐私攻击的位置隐私保护机制的局限与机遇

随着车联网的发展，现有的位置隐私保护机制将面临新的挑战。如第 III 节和第 IV 节所述，现有的位置隐私保护机制主要针对上层基于消息的跟踪；对于采用其他跟踪技术的对手（即基于感知基础设施、光学视觉、车辆行驶日志和蜂窝无线电的跟踪），现有车联网无法有效抵御。然而，如表 XI 所示，在 5G/6G 车联网中，面对上层基于消息的攻击，现有的位置隐私保护机制无法提供可接受的位置隐私保护。

1）用户侧位置隐私保护机制：大多数现有的用户侧位置隐私保护机制无法满足 5G/6G 车联网的低延迟要求，例如传递并运行、证书和安全计算。尽管数据扰动能够满足延迟要求，但经数据扰动保护的位置数据无法为高精度定位应用提供高精度基于位置的服务。

- **传递并运行：** 通过即运行通信模型依赖车辆经由其他节点使用基于位置的服务，因此存在若干局限，尤其是在位置

表 XI CHALLENGE 第五代移动通信/6G 车联网中的位置隐私。

技术	新挑战	可用的位置隐私保护机制	需要改进的位置隐私保护机制
THz	小覆盖范围 频谱穿透能力 通过接入点实现厘米级精度	传递并运行 隐私证书 安全计算 同态加密 隐私信息检索 可搜索加密 安全通信	数据扰动 统计披露控制 可信第三方
VLC	信号散射 观测信号 有效传输要求	隐私证书 安全通信 可信第三方	传递并运行 数据扰动 安全计算 统计披露控制 隐私信息检索 同态加密 可搜索加密
毫米波	频繁交换信道状态信息 低延迟要求 容易窃听信道	隐私证书 安全计算 数据扰动 统计披露控制 同态加密 隐私信息检索 可搜索加密 可信第三方 安全通信	传递并运行
6 GHz以下频段	灵活的天线设计 伪基站和恶意设备 车载追踪	传递并运行 隐私证书 安全通信 可信第三方	安全计算 数据扰动 统计披露控制 同态加密 隐私信息检索 可搜索加密
卫星通信	传播时延长 难以分配 MIMO 通信资源分配	隐私证书 数据扰动 统计披露 安全通信 可信第三方	传递并运行 安全计算 同态加密 隐私信息检索 可搜索加密
QC	量子信道 量子计算机	隐私证书 安全计算 数据扰动 统计披露控制 安全通信 可信第三方	传递并运行 同态加密 可搜索加密 隐私信息检索

隐私方面。该方法面临的一项关键挑战是通信延迟较高，因为每辆车都要通过中间节点转发数据，从而增加了基于位置的服务请求的传递延迟。此外，这种多跳路由结构中的身份验证也会带来隐私风险。为确保数据安全路由而进行合法协作者身份认证，会增加通信延迟，因为每一跳都需要验证。这导致一种情况：车辆之间频繁的数据交换，无意中提高了基于信号的定位技术（如基本定位和基于蜂窝无线电的定位）的精度。随着车辆通信日益频繁，对手可能利用丰富的通信模式重建精细的轨迹，并更准确地追踪用户的移动，从而危及驾驶员的位置隐私。

在 5G/6G赋能的车联网中，先进的传感器网络可以通过让车辆全面了解道路网络和通信环境来缓解部分挑战。借助这些信息，驾驶员可以选择最优信道和路由路径，从而有望降低传输延迟并提升系统效率。然而，传感器的大量使用也引发了对数据聚合和隐私暴露的担忧，因为车辆和基础设施中的多个传感器会持续收集并传输敏感位置数据。此外，虽然区块链技术为信任管理提供了颇具前景的解决方案，能够实现去中心化身份认证和安全的证书分发，但在管理庞大的车辆网络时，它也会带来较高的计算成本和潜在的可扩展性问题 [240]。区块链固有的透明性也可能构成隐私风险，因为账本的不可篡改性可能使对手能够追踪车辆交互，并推断用户身份或轨迹

随时间推移。因此，尽管区块链能够解决信任问题，仍需谨慎设计，确保系统中嵌入的验证和可追溯机制不会损害位置隐私。

- **隐私证书：** 基于证书的位置隐私保护机制通过验证认证证书和签名，广泛应用于车联网中的身份认证，确保车辆与网络实体之间的通信安全。然而，这些传统的基于证书的位置隐私保护机制在5G/6G赋能的车联网中面临着显著局限。其主要局限之一是依赖可信证书颁发机构，这使原本高度去中心化且动态的系统出现了中心化。在数千辆车辆和传感器同时通信的大规模车联网中，由中央主管部门验证证书可能形成瓶颈，导致交通管理和事故预防等实时应用出现无法接受的时延。此外，单一可信主管机构会造成单点故障，使系统容易遭受攻击，进而危及整个网络的隐私。

基于证书的位置隐私保护机制的另一项显著局限，是管理众多节点上的证书所需的存储消耗。在5G/6G车联网中，大量车辆、路侧单元和传感器生成并交换数据，将增加证书管理的复杂性和存储需求。这可能会耗尽网络资源并降低通信效率。此外，由于每张证书都需要经过身份认证，身份认证延迟会随着网络规模扩大而增加，从而对车联网中典型的延迟敏感型服务造成负面影响。区块链技术通过提供不可篡改、去中心化且安全的共识机制来管理证书，为解决这些问题提供了潜在方案，但也带来了挑战，例如计算成本增加以及维护区块链所需的能耗。此外，收集传感器数据用于身份认证会引发隐私问题，因为对手可能利用这些数据进行位置跟踪或行为分析。

- **安全计算：** 虽然安全计算技术能够在不泄露实际内容的情况下处理加密数据，为保护车联网中的位置隐私提供了有效方案，但也存在显著的计算延迟。这种延迟是一项主要限制，尤其是在实时车联网环境中，导航、碰撞避免和交通管理等应用都离不开低延迟通信。同态加密及其他安全计算方法所带来的计算开销通常会增加处理时间，进而造成延迟问题并影响系统的整体性能 [130]。在 5G/6G赋能的车联网中，数据以极高的速率生成和传输，现有安全计算技术可能无法有效扩展，从而进一步加剧时延并限制其实用性。此外，随着车联网不断发展，需要处理更复杂的跨层跟踪和大数据分析，安全计算方法的处理需求预计也会不断增长，这给兼顾位置隐私与系统效率带来了更大的挑战。

因此，尽管安全计算能够提供强有力的隐私保障，但其在计算延迟和可扩展性方面的局限，意味着仍需进一步改进，才能满足现代车联网的实时需求。

- **数据扰动：** 数据扰动虽然是一种灵活且时延较低的位置隐私保护方法，但在 5G/6G 车联网中仍面临显著局限。当前的数据扰动技术通常只能达到米级精度，或许足以满足一般应用的需求，却无法达到 5G/6G 车载系统所要求的厘米级或毫米级精度。随着车联网不断发展，精准的位置数据对于自动驾驶和碰撞避免等关键服务至关重要，任何显著扰动都会损害数据效用。尝试优化扰动以提高精度，则可能大幅削弱这些机制的位置隐私保护能力 [15]。具体而言，将数据扰动到如此精细的程度，会使对手轻易地通过逆向分析还原原始位置，从而损害位置隐私。这种权衡凸显了当前基于数据扰动的位置隐私保护机制无法满足未来网络需求。为解决这一问题，必须将数据扰动与更稳健的隐私保护技术相结合，例如自适应噪声注入或多层加密，以便在满足未来车载应用严格精度要求的同时，确保高水平的隐私保护。

2) 服务器端位置隐私保护机制：低延迟要求也对现有的服务器端位置隐私保护机制构成挑战，因为服务器端的处理过程可能会导致计算时延。

- **统计披露控制：** 车联网中的统计披露控制依赖于服务器端位置隐私保护机制，例如数据扰动、安全计算和匿名化技术，以降低敏感位置数据暴露的风险 [30]。然而，用户侧位置隐私保护机制面临的相同局限性——例如计算成本、存储开销和数据管理复杂性——同样适用于服务器端，而在5G/6G赋能的车联网环境中，这些挑战会进一步加剧。随着5G/6G网络的超密集连接推动数据传输频率和数据量呈指数级增长，处理和存储这些海量涌入数据的需求对计算资源和存储基础设施造成了巨大压力。如果不加以谨慎控制，这种高频数据交换可能导致位置隐私方面的安全漏洞，因为对手可能利用频繁通信和大型数据集进行轨迹重建，并随着时间推移对用户进行画像。

尽管基于区块链的技术通过去中心化并保障数据交易，为优化数据管理和减少存储消耗提供了可能，但它们对减轻处理位置数据以实现隐私保护所需的计算开销作用甚微。例如，加密、匿名化和统

计披露控制的计算成本会随着数据流量的增加以及实时定位服务复杂性的提升而上升。此外，基于人工智能的位置隐私保护机制有望实现自适应隐私保护的自动化并简化数据分析，但也会增加模型训练和资源分配的复杂性，尤其是在应用于实时、高流量数据流时 [241]。此外，引入信任管理系统有助于通过对可信实体免除不必要的隐私保护来降低计算成本，但这些系统本身需要经过谨慎设计，以避免信任利用或内部人员攻击。

- **同态加密：** 同态加密是一种广泛用于安全计算的位置隐私保护方法，它允许在不泄露明文的情况下对加密数据进行运算。然而，由于计算延迟较高且资源消耗巨大，将其用于服务器端计算面临着重大挑战。同态加密运算的复杂性，尤其是全同态加密方案中的运算复杂性，会在加密、解密和处理过程中带来巨大的计算开销，因此难以应用于对低延迟要求极高的车联网实时应用。此外，传输大型加密数据集所产生的通信开销会进一步加剧网络拥塞；在启用 5G/6G 的环境中，数据传输速率较高，这一问题尤为突出。这些局限使得强位置隐私保护与系统效率之间难以兼顾。为缓解这些问题，亟需开发简化的同态加密流程，在维持足够隐私保护水平的同时降低计算负担。部分同态加密等技术，或将同态加密与边缘计算相结合，有助于缓解全加密计算带来的性能瓶颈，但仍难以满足大规模实时车联网所需的可扩展性。

- **隐私信息检索：** PIR 是一种很有前景的技术，通过允许用户从服务器检索数据而不泄露所访问的数据，从而确保位置隐私。然而，在车联网中的实际应用面临着重大挑战，尤其是在计算开销和可扩展性方面。在云端处理隐私信息检索查询所需的高昂计算成本，使得当前网络难以高效分配必要的资源。在支持 5G/6G 的车联网中，自动驾驶和交通管理等实时应用对低时延有着严格要求，PIR 的高额开销可能导致无法接受的延迟。此外，这些网络中不断增加的数据流量和查询频率进一步加剧了这一问题，使当前隐私信息检索方案难以实际部署。尽管 PIR 为增强位置隐私提供了稳健的框架，但其计算效率低下和资源需求高构成了重大限制，尤其是在高密度车载环境中，快速数据检索和实时通信至关重要。

- **可搜索加密：** 可搜索加密提供了一种方法来保护位置隐私，使驾驶员能够在不泄露敏感数据的情况下搜索基于位置的服务，但它也存在一些局限，尤其是在5G/6G车联网中。这些网络需要高精度位置数据来支持导航和交通管理等实时服务，而可搜索加密方案往往会导致搜索结果出现精度误差，从而降低用户的数据效用。尽管将可搜索加密与其他位置隐私保护机制（如基于证书的加密或同态加密）结合起来，可以提高搜索准确性和隐私保护水平，但这种集成会显著增加计算开销和处理时间，尤其是在大规模车联网中。计算负担加重可能导致实时服务交付延迟；对于低延迟和高效率至关重要的关键车载应用而言，这是不可接受的。此外，在分布式车联网中管理密码密钥并确保查询处理安全的复杂性，会增加出现安全漏洞的风险；如果系统的任何环节遭到破坏，位置数据就可能暴露。

可以利用 5G/6G车联网中传感器提供的信息来修正结果，因为届时将部署大量传感器。此外，还可以引入基于人工智能的位置隐私保护机制，根据驾驶员的历史信息优化结果，从而实现更精细的 [11]。

3) 用户-服务器接口位置隐私保护机制：与当前版本相比，用户-服务器接口位置隐私保护机制在 5G/6G车联网中将受到更多研究人员的关注，因为 5G/6G车联网会要求车辆通过频繁的 V2X通信来共享数据。保护通信信道中的位置隐私，是防御基础定位、信道制图定位和驾驶员跟踪定位的一种方法。

- **安全通信：** 尽管通过端到端加密实现的安全通信能够为车联网中的位置隐私提供强有力的保护，但它也存在若干局限，尤其是在5G/6G网络环境下。主要挑战在于，对大量实时位置数据进行加密和解密会带来计算开销，进而显著增加通信延迟。由于预计5G/6G车联网将处理高数据速率，并需要为自动驾驶和实时交通管理等关键服务提供低延迟通信，复杂加密协议带来的额外时延可能会降低基于位置的服务的数据效用。此外，受这些性能限制影响，端到端加密目前在车联网中并不常见。加密技术必须在传输的各个环节保护敏感位置数据，包括车辆之间、车辆与基础设施之间以及车辆与云服务器之间的传输，因此可能成为瓶颈，尤其是在数据交换频繁且实时响应至关重要的高密度城市环境中。此外，加密通信虽然能够保护数据机密性，但仍可能遭受侧信道攻击，对手可通过流量分析推断用户位置。

无需直接破解加密即可。

- **可信第三方（TTP）：**在当前车联网中，使用可信第三方（TTP）管理位置隐私通常被视为理想方案，但它也存在显著局限，尤其是在 5G/6G 车联网背景下。随着车联网不断扩展，并集成海量传感器和联网车辆，所产生的数据流量呈指数级增长，从而增加了 TTP 遭对手攻破的风险。即便是由政府实体控制的 TTP，也容易受到劫持或数据泄露的威胁，正如涉及从国家控制的数据库中窃取敏感数据的大规模事件所证明的那样 [3]。在如此庞大的网络中，TTP 一旦遭到攻破，就可能导致广泛的隐私侵犯，使用户的位置和行踪暴露给恶意行为者。此外，未来网络规模庞大且复杂，其特点是传感器、车辆和节点数量众多，这对集中式 TTP 模型的效率和可靠性构成挑战。依靠单一实体管理如此庞大网络中的信任，会造成单点故障。为克服这些局限，必须通过整合加密、区块链、基于人工智能的技术以及数据扰动等额外的隐私保护机制来增强 TTP 模型。这些互补方法有助于实现信任管理的去中心化，降低对单一实体的依赖，并提升5G/6G赋能的车联网中隐私保护策略的整体韧性。

C. 位置隐私挑战与新兴无线技术

与现有车联网不同，未来版本将通过新的通信媒介传输数据。这些新型通信媒介提高了车联网的效率，但也带来了新的跨层位置隐私问题。

- **6 GHz以下频段：**6 GHz以下频谱的范围为 0.45 GHz 至 6 GHz，凭借覆盖范围广、成本低以及支持车联网通信的能力，在车联网中得到广泛应用。然而，使用 6 GHz 以下频段也带来了若干位置隐私挑战。一个关键问题源于灵活的天线设计：它增强了通信能力，也使对手更容易跟踪车辆。攻击者可以利用伪造基站等恶意设备并监控多条 6 GHz 以下链路，收集距离和角度数据，从而准确计算车辆的位置 [242]。这种被动跟踪会严重损害车辆隐私，因为对手可以利用 6 GHz 以下信道开放的无线特性获取精细的轨迹数据。此外，安装在驾驶员移动设备上的恶意应用也会加剧隐私问题，因为手机的位置数据往往与车辆的位置相对应，尤其是在驾驶员开车时携带手机的情况下 [103]。

这些挑战要求采用更强大的物理层位置隐私保护机制，以降低 6 GHz 以下频谱带来的风险。现有的数据扰动和统计披露控制方法增加了识别非法实体的复杂性，使合法用户更难通过身份验证，也更难阻止窃听企图。虽然可以利用证书和可信第三方来识别并验证合法实体，但这些机制可能无法完全应对在 6 GHz 以下频段运行的伪造基站和恶意应用的隐蔽性。尤其是，攻击者可以利用多个基站的信号进行三角定位，重建精确的车辆位置，使车辆持续暴露于跟踪风险之中。6 GHz 以下通信的低延迟和普及性进一步加剧了这些隐私风险，使对手能够截获并分析实时车辆数据。

为保护6 GHz以下频谱中的车辆位置隐私，需要采用更先进的位置隐私保护机制，将用户-服务器接口和服务器端隐私保护纳入其中。这些方法结合人工智能和区块链技术，可以通过确保数据在传输前经过加密、混淆或阻止其被未授权实体访问，从而增强隐私保护。例如，人工智能算法可以检测恶意设备的异常行为，而区块链可以提供一种去中心化、防篡改系统，用于验证基站和移动设备的真实性。此外，驾驶员可以在位置数据中隐藏语义信息，或采用端到端加密，以防对手通过6 GHz以下信道重建其移动模式。

- **毫米波：**在5G/6G车联网中，毫米波技术工作于30 GHz至100 GHz的频谱范围内，可提供数千兆比特的高速传输，但也给车辆位置隐私带来了重大挑战。毫米波采用基于波束的定向传输，能够实现精确通信，但这种精度本身也增加了位置跟踪的风险。由于频率较高且波束较窄，毫米波信号的传输模式很容易被绘制和映射，使对手能够检测传输的方向和来源，进而推断车辆的位置 [243]。尤其是在基站密集且车辆移动频繁的环境中，为维持网络连接，持续交换信道状态信息（CSI）变得十分必要，而这一过程无意中提供了大量可能被利用于基于位置的攻击的数据。

此外，车辆位置频繁变化所导致的5G/6G车联网高度动态的拓扑结构，会加剧隐私风险。对低延迟V2X通信的需求，迫使车辆、路侧单元和传感器频繁交换信道状态信息，从而增加通信开销，并为对手窃听通信、提取位置信息提供更多机会 [244]。虽然可以采用数据扰动技术对位置数据进行匿名化处理，但当通信信道本身易受攻击时，这些技术往往不足以应对问题。窃听毫米波信号，尤其是在高速公路或城市地区等高机动性场景中，

[3] bleepingcomputer.com/news/security/hacker-claims-to-have-stolen-dat a-on url-1-billion-chinese-citizens/

即使消息的实际内容已加密，对手仍可通过反复观测信号来三角定位车辆位置 [245]。这会提高车联网中跟踪的精细程度，因此更需要强健的位置隐私保护机制。

一种有前景的解决方案是利用车辆高速相对运动所导致的毫米波传输固有的多普勒频移，以减轻这些风险。通过将多普勒效应与数据扰动和匿名化技术相结合，可以改变传输信号特征，从而混淆位置数据，使对手更难从截获的通信中推断实时位置 [246]。此外，还可采用同态加密、隐私信息检索和可搜索加密等先进的安全计算技术，防止对手即使截获信号也无法访问有用数据。这些密码学方法使车辆能够对加密数据进行计算，或从网络检索信息，而无需泄露其确切位置或身份。然而，这些技术也会带来自身的挑战，因为它们往往会增加计算和通信延迟，可能无法满足基于毫米波的车联网对低延迟的要求。

- **太赫兹（THz）通信：**太赫兹通信为车联网带来了机遇与挑战，尤其是在车辆位置隐私方面。太赫兹通信的频谱范围为 100 GHz 至 10 THz，波长极短（30–3000μm），具有实现高速数据传输和厘米级定位精度的潜力 [247]。然而，太赫兹波的小覆盖范围（不足 50 米）和有限的穿透能力引发了严重的隐私问题。基于太赫兹技术的车联网具备精准的定位能力，使对手能够以前所未有的精度追踪车辆移动，从而对位置隐私构成严重威胁。尽管太赫兹信号的有限传输距离似乎能够通过将通信限制在较短距离内来增强隐私保护，但高分辨率数据以及基站或接入点之间频繁的切换仍可能暴露精细的位置数据，使对手能够重建车辆的连续轨迹。太赫兹的小覆盖范围增加了依赖多个接入点实现无缝通信的可能性。这些接入点作为可信第三方，需要处理大量车辆数据，包括车辆所在位置、驾驶模式和道路状况，这显著增加了位置隐私泄露的风险。这些接入点的集中式架构虽然对于维持网络连接至关重要，但也可能成为网络攻击或数据拦截的目标，因为对手可能利用接入点中的安全漏洞获取敏感的位置信息。基于证书的位置隐私保护机制依赖密码凭证，未来可能会在太赫兹车联网中得到更广泛的应用，以解决信任问题，但这些解决方案也会带来管理开销和计算复杂度方面的挑战，尤其是在高密度城市环境中。在频繁发生切换的环境中 [248]。
除了信任管理和密码学方面的挑战外，现有的位置隐私保护机制（例如差分隐私和数据扰动技术）在基于太赫兹的通信中可能并不奏效。用户侧基于差分隐私的位置隐私保护机制依靠向位置数据添加受控噪声来保护隐私，但由于扰动候选项数量有限，在高精度太赫兹网络中可能难以维持隐私。太赫兹网络能够实现厘米级定位，因此即使是微小的扰动也可能不足以掩盖车辆的真实位置，使对手得以高精度推断移动模式 [16]。这一局限表明，需要转向服务器端基于差分隐私的位置隐私保护机制；采用上下文感知混淆和区块链增强型信任管理等更先进的隐私技术，或许能在不牺牲数据效用的前提下更有效地保护位置隐私。

- **可见光通信（VLC）：**车载网络中的VLC既带来了令人期待的机遇，也对位置隐私构成了重大挑战。VLC利用发光二极管（LED）设施（如交通信号灯、车辆前照灯和路侧灯）传输数据，具有能耗低、效率高的优势，并可使用从400 THz到800 THz的大频谱范围 [249]。在车载环境中，VLC有助于实现车联网通信，改善车辆与基础设施之间的数据传输。然而，尽管VLC具有诸多优势，但由于光传输的物理特征，它本质上容易受到位置隐私泄露的威胁。与无线电波不同，光信号容易发生散射，尤其是在室外环境中，这使对手能够窃听传输信号。即使采用非正交多址接入（NOMA）和伪表面波等先进技术来减轻信号衰减，也无法彻底消除信号被截获的风险 [250]。

VLC的室外部署加剧了位置隐私挑战，因为窃听者可以轻易截获散射的光信号。由于VLC依赖视距通信，发射源（如车辆灯光）在物理上的可见性，使对手只需观察或截获散射信号，就能推断位置数据。这对车辆位置隐私构成了独特威胁，因为窃听者可能无需采用复杂的黑客手段，就能跟踪车辆移动。在这种情况下，数据扰动或统计披露控制等传统位置隐私保护机制会失效，因为对手能够直接观察光源，从而绕过服务器端保护 [251]。VLC信号固有的物理可见性限制了数字混淆技术的作用范围，使车辆位置暴露于现实世界的跟踪威胁之下。

为应对这些挑战，基于认证的方法和用户-服务器接口位置隐私保护机制可为可见光通信系统提供更好的位置隐私保护。在短距离可见光通信中，基于认证的方法可确保只有经过认证的设备才能参与

数据交换，从而有效阻止未经授权的接收器访问通信信道。这有助于通过限制能够接收可见光通信信号的节点数量来降低窃听风险 [251]。然而，在远距离或远程通信场景中，还需采取额外措施。协作干扰和信道状态信息估计等技术是可行的物理层位置隐私保护机制，可防止窃听者获取敏感位置数据 [252]。协作干扰通过多个合法节点引入干扰信号，从而阻止窃听者访问通信信道。同时，信道状态信息估计使合法节点能够监测合法信道和窃听信道的状态，并动态调整传输以保护位置信息。

- **量子通信（QC）：**量子通信利用光的量子态，通过微观粒子承载量子信息来实现安全通信。

尽管量子密钥分发（QKD）借助海森堡不确定性原理和不可克隆定理等量子力学原理，为量子通信提供了无与伦比的安全性，但在保护车联网中的车辆位置隐私方面仍面临重大挑战 [253], [254]。虽然量子密钥分发能够检测窃听，并保护通信中使用的密码密钥的机密性，但它本身并不能保障位置隐私。具体而言，基于量子密钥分发的通信协议所使用的激光信号可能被用于推断源车辆和目的车辆的方向及相对位置。在车联网中，导航和碰撞避免等服务依赖持续的实时通信；通过分析通信模式以及所传输量子信号的物理特性，车辆的轨迹和位置可能会暴露。

这一局限造成了显著的隐私风险，因为对手可能利用侧信道攻击，根据量子密钥分发（QKD）所使用激光信号的时序、方向和强度来追踪车辆的位置。尽管 QKD 在保护数据完整性和防止窃听方面非常有效，但它缺乏必要的位置匿名化机制，无法防止高精度环境中的车辆跟踪。为缓解这些风险，研究人员提出了量子同态加密、量子可搜索加密和量子隐私信息检索等先进的量子密码学方法。这些技术能够在不泄露实际内容或查询信息的情况下，对加密数据进行处理、搜索和检索，从而应对量子计算的数据隐私问题。然而，这些方法并不能完全解决 QKD 在车联网中带来的特定位置隐私挑战，因为物理信号泄露仍可能危及位置机密性。将量子隐形传态（QT）引入车联网，会对车辆位置隐私带来重大挑战，尤其是在需要远距离通信时。QT 同时利用经典信道和量子信道来促进量子信息的传输，确保发送方的消息在传输过程中被销毁。尽管该方法有望用于高密度车联网中的安全通信，但它也同时扰乱了传统的位置隐私保护机制（LPPMs）。例如，传递并运行等基于路由的技术依赖中间节点安全地传输位置信息；而在量子通信环境中，这些技术会失效，因为 QT 通过纠缠量子态直接传输量子数据，无需此类路由机制 [255]。这形成了一种新的范式，在该范式下，传统的基于跳数的加密或混淆技术无法应用，从而使车辆位置数据面临 vulnerabilidad。QT 在车联网中的核心隐私挑战在于量子测量过程。量子信息被隐形传态后，原始消息会被销毁；而任何对传输过程的干扰——例如窃听或数据拦截——都会导致量子退相干，立即向双方发出警报。然而，依赖量子纠缠进行远距离通信，可能会因量子信道漏洞或侧信道攻击而暴露位置数据，尤其是在对手获得伴随量子数据传输的经典信道访问权限时。此外，利用量子中继器扩展通信范围也会带来数据泄露风险，因为对手可能通过监控与隐形传态过程相关的传统数据流，推断实时位置信息。这些问题表明，针对经典通信框架设计的现有位置隐私保护机制，需要进行重大调整或替换，才能确保量子通信环境中的位置隐私。将量子身份认证（QIA）和量子签名（QS）引入车联网，为安全通信带来了新的机遇，但也对车辆位置隐私提出了重大挑战。QIA 利用量子密码学原理提供基于认证的客观信任，通过使对手几乎不可能伪造身份或窃听量子信道来增强安全性。然而，量子通信更高的精度和细粒度，以及客观信任所需的可认证证据，可能对位置隐私造成潜在风险。每个认证实例都会生成有关车辆身份和通信端点的详细数据；如果管理不当，这些数据可能被用于位置跟踪和轨迹推断。对手可能利用量子安全信道收集可认证的位置数据，将其与实时通信关联起来，从而危及车辆和驾驶员的匿名性。

QS 旨在确保消息的完整性和真实性，但也会引入潜在的安全漏洞。虽然 QS 通过基于 TTP 的群组提供主观信任，并利用群组特定行为和特征，但对基于群组的信任模型的依赖可能会无意中暴露位置数据。例如，负责管理主观信任的 TTP 可能会汇总和处理大量位置相关元数据以确保真实性，

如果检测到车辆移动中的模式，就可能带来统计披露风险。量子签名与统计披露控制相结合，可能使对手能够分析通信模式的频率和上下文，从而识别隐私保护中的潜在薄弱环节。因此，尽管 QIA 和 QS 能够增强信任管理和安全性，但仍有必要开发更先进的位置隐私保护机制，以应对量子级数据收集带来的日益严峻的威胁，并确保在这些日益安全却更加透明的通信环境中，车辆的匿名性和位置隐私。

- **可重构智能表面（RIS）：**在车联网中部署可重构智能表面（RIS），为车辆位置隐私带来了新的挑战。RIS采用超材料和无源反射阵列，可通过操控电磁波增强无线通信，并提供全双工、全频段通信；但其在车路人一体化网络中的广泛应用也引发了重大的隐私问题 [256]。RIS具有动态、可编程的特性，能够精细控制信号反射，因此可能利用车辆与环境之间的反射及交互，实现对车辆的精准跟踪。由于RIS可轻松安装在道路附近的建筑立面和广告牌上，这种无处不在的基础设施可能被对手利用，通过持续监测和信号三角定位来推断车辆轨迹。RIS的计算和能耗较低，便于大规模部署，也因此进一步扩大了跟踪攻击的范围。此外，车辆的移动性以及车联网中的频繁断连，使位置数据难以得到保护：RIS不易适应动态拓扑，也难以从车辆收集可靠反馈以实施有效的隐私保护措施 [257]。

D. 网络融合带来的挑战

在融合车联网中，车辆可通过实时 V2X通信自动与其他车辆、路侧基础设施和行人交换信息并进行通信。在 V2X 技术的支持下，交通信息（例如车辆状态、实时道路状况和行人信息）促成了车—路—人融合网络的形成 [3]。具有 5G/6G 特征的车—路—人融合网络组件如下所示。

- **综合卫星与地面网络（ISTN）：**第五代移动通信/第六代移动通信车联网中的ISTN带来了车辆位置隐私方面的诸多挑战，这主要归因于卫星通信的独特特性。虽然卫星通信通过将覆盖范围扩展至偏远及难以到达的地区，实现了三维车联网服务，但它也面临着诸多显著限制，例如较长的传播时延、较高的传输延迟，以及高效管理多输入多输出（MIMO）方面的挑战。网络和通信资源分配 [3]。这些局限性不仅会影响服务质量，还会因长时间向对手暴露更详细的轨迹数据而增加位置隐私的脆弱性。传输时延的增加，加上卫星网络的分布式特性，使实时隐私保护更加困难，因为传统的位置隐私保护机制可能并未针对这类环境进行优化。

此外，依赖相邻车辆快速传输的传递并运行方法，由于卫星系统固有的传输延迟和通信滞后，在卫星网络中效果较差。同样，诸如同态加密和安全通信协议等先进的位置隐私保护机制本就计算密集，在 ISTN 中因延迟增加和资源受限而面临更大的挑战 [258]。这些因素严重限制了现有隐私保护机制的可扩展性和效率。为缓解这些挑战，可以将这些方法消耗的资源转移给可信第三方处理，并采用数据扰动技术（例如为位置数据添加噪声）以及统计披露控制机制，以更好地保护位置隐私。通过减少对实时计算的依赖，并转向更多批处理式隐私策略，或许能够有效平衡隐私需求与基于卫星的通信所带来的高延迟，从而更有力地防范支持 ISTN 的车联网中的位置隐私泄露。

- **人机交互：**车联网中的人机交互，尤其是行人、驾驶员和乘客携带移动设备所产生的交互，带来了显著的位置隐私挑战。移动设备增强了通信和数据处理能力，因此，车辆与人员之间的频繁交互正成为5G/6G车联网的核心组成部分，使车辆能够收集实时数据，并克服盲区等传感器局限 [259]。尽管这种数据共享能够支持情境报告和预警等关键服务，从而减少事故 [260]，但也加剧了跨层隐私攻击的风险。车辆与行人之间的频繁通信可能导致轨迹推断：对手结合不同层的信息（例如移动数据和车辆日志中的接触信息），以更高精度跟踪车辆。此外，车载传感器数据，包括驾驶日志和乘客信息，也可用于推断车辆的位置或行驶情况。因此，基于信任管理的位置隐私保护机制至关重要，可防范利用这些多源数据交互来定位驾驶员并侵犯其隐私的对手。随着车载生态系统中的人机交互日益增多，我们亟须采取更稳健的跨层隐私保护措施，以防范日益复杂的跟踪方法。

E. 关键要点

对5G/6G车联网中的位置隐私挑战和保护机制的研究揭示了现有位置隐私保护机制中的关键不足，也凸显了先进通信技术和集成系统所带来的复杂性。卫星地面网络、车联网（V2X）系统和可重构智能表面等多模态通信平台的融合，提升了定位能力的精度并扩大了其覆盖范围，因而使车辆面临新型隐私威胁。5G/6G车载环境所具有的超低延迟、高数据速率和广泛的设备互联，进一步加剧了这些威胁。

主要挑战之一在于解决整合感知基础设施、光学视觉和基于信道的跟踪技术所引入的跨层隐私漏洞。现有的位置隐私保护机制通常只关注单层威胁模型，因此难以有效防御多源数据关联和轨迹重构攻击。此外，尽管同态加密和量子通信等技术提供了颇具前景的解决方案，但其计算需求和延迟限制往往与车载应用严格的实时要求相冲突。

本节的关键观察如下：

- **可扩展性与适应性：** 当前的位置隐私保护机制缺乏必要的可扩展性，无法应对车载通信流量和联网设备数量的指数级增长。未来的解决方案必须纳入区块链等去中心化框架，以及能够根据网络条件和应用需求动态调整隐私保护的自适应机制。
- **先进技术的集成：** 包括量子通信、基于人工智能的定位和可重构智能表面在内的新兴技术，为位置隐私带来了新的维度。然而，必须谨慎管理这些技术的集成，以避免产生意外的安全漏洞，例如针对机器学习模型的对抗攻击或量子侧信道攻击。
- **跨层威胁缓解：** 未来的5G/6G车联网需要全面的隐私策略，以应对跨层交互。能够同时混淆用户侧数据、保护服务器端流程并保障通信接口安全的多层位置隐私保护机制，对于全面缓解隐私风险至关重要。

VI. 结论

本文全面研究了位置隐私保护机制的发展以及车联网中的位置隐私威胁。通过回顾车联网中的定位方法，我们阐述了定位引入的位置隐私威胁，并将位置隐私保护机制分为用户侧、服务器端和用户-服务器接口位置隐私保护机制。我们的分析评估了现有位置隐私保护机制在各种定位和通信场景下的性能，并提供了平衡位置隐私保护与数据效用的方法，以提升其有效性。

此外，我们还识别出未来车联网中新型通信技术所引入的潜在威胁，而现有研究忽略了这些威胁。我们的研究结果为现有位置隐私保护机制提供了潜在的发展方向，以助力未来研究，这对于位置隐私保护机制的设计十分重要。通过考虑与车联网中的位置隐私相关的挑战与机遇，我们可以开发出在数据效用与隐私保护之间实现平衡的有效位置隐私保护机制，从而增强驾驶员和乘客的安全性。

参考文献

[1] R. Zhang、Z. Su，“第五代移动通信网络赋能协作式自动驾驶车辆定位：一项综述”，*IEEE*《智能交通系统汇刊》，2024年。[2] F. Farouk、Y. Alkady 和 R. Rizk，“面向车载自组织网络系统中基于位置的服务的高效隐私保护方案”，*IEEE Access*，第8卷，第60 101–60 116页，2020年。[3] H. Guo、X. Zhou、J. Liu 和 Y. Zhang，“第六代移动通信中的车载智能：网络、通信与计算”，*Veh. Commun.*，第33卷，第100399页，2022年。[4] M. Deng、M. Ahmed、A. Wahid、A. A. Soofi、W. U. Khan、F. Xu、M. Asif 和 Z. Han，“可重构智能表面赋能的车载通信：最新进展与未来挑战综述”，*IEEE Trans. Intell. Veh.*，2024年。[5] Q. Xue、C. Ji、S. Ma、J. Guo、Y. Xu、Q. Chen 和 W. Zhang，“面向第六代移动通信的毫米波与太赫兹通信波束管理综述”，*IEEE Commun. Surv.Tutor.*，2024年。[6] J. Chen、X. Liang、J. Xue、Y. Sun、H. Zhou 和 X. Shen，“迈向第六代移动通信的RAN架构演进：动机、发展与赋能技术”，*IEEECommun. Surv. Tutor.*，2024年。[7] Q. Duan、J. Huang、S. Hu、R. Deng、Z. Lu 和 S. Yu，“融合联邦学习与边缘计算，迈向第六代移动通信网络中的泛在智能：挑战、最新进展与未来方向”，*IEEE Commun. Surv. Tutor.*，2023年。[8] K. Gao、C. Xu、P. Zhang、J. Qin、L. Zhong 和 G.-M. Muntean，“GCH-MV：面向第六代移动通信软件定义车载网络中多路径TCP的博弈增强型补偿切换方案”，*IEEE*《车辆技术汇刊》，第69卷，第12期，第16 142–16 154页，2020年。[9] Z. Sadreddini、E. Gu¨ler、M. Khalily 和 H. Yanikomeroglu，“MRIRS：智能反射表面辅助的移动自组织路由”，*IEEETrans. Cogn. Commun. Netw.*，第7卷，第4期，第1333–1346页，2021年。[10] B. Zhang、Q. Fan、X. Zhang、Z. Fu、S. Wang、J. Li 和 Q. Xiong，“B5G/6G网络中VNF转发图嵌入综述”，《无线网络》，第30卷，第5期，第3735–3758页，2024年。[11] N. M. Elfatih、M. K. Hasan、Z. Kamal、D. Gupta、R. A. Saeed、E. S. Ali 和 M. S. Hosain，“在第五代移动通信网络中利用人工智能技术进行车联网资源管理：现状与趋势”，*IET Commun.*，第16卷，第5期，第400–420页，2022年。[12] W. Hamdi、C. Ksouri、H. Bulut 和 M. Mosbah，“面向第五代移动通信及后续网络中车联网的基于网络切片的学习技术”，*IEEE Commun. Surv. Tutor.*，2024年。[13] B. Mao、J. Liu、Y. Wu 和 N. Kato，“第六代移动通信网络边缘的安全与隐私：综述”，*IEEE Commun. Surv. Tutor.*，第25卷，第2期，第1095–1127页，2023年。[14] C. Seroˆdio、J. Cunha、G. Candela、S. Rodriguez、X. R. Sousa 和 F. Branco，“作为IoE和专用网络支撑的第六代移动通信生态系统：愿景、需求与挑战”，*Future Internet*，第15卷，第11期，第348页，2023年。[15] B. Ma、X. Wang、W. Ni 和 R. P. Liu，“具有道路网络不可区分性的个性化位置隐私”，*IEEE*《智能交通系统汇刊》，第23卷，第11期，2022年。[16] B. Ma、X. Lin、X. Wang、B. Liu、Y. He、W. Ni 和 R. P. Liu，“面向道路网络不可区分性与位置隐私的新型伪装区域混淆”，载于第*25*届攻击、入侵与防御研究国际研讨会（*RAID*）论文集，2022年，第160–170页。[17] N. Malik、P. Nanda、A. Arora、X. He 和 D. Puthal，“面向车联网的基于区块链的安全身份认证与快速撤销框架”，载于第*17*届*IEEE*国际可信、安全与隐私计算及通信会议/第*12*届*IEEE*国际大数据科学与工程会议（*TrustCom/BigDataSE*）论文集。IEEE，2018年，第674–679页。[18] A. Qashlan、P. Nanda 和 M. Mohanty，“面向基于区块链的智能家居架构的差分隐私模型”，*Future Gener. Comput. Syst.*，第150卷，第49–63页，2024年。

[19] A. P. Mdee、M. M. Saad、M. Khan、M. T. R. Khan 和 D. Kim，“位置隐私保护方案对车载应用的影响”，Veh. Commun.，第100499页，2022年。[20] C. Zhang、L. Zhu、C. Xu、K. Sharif、K. Ding、X. Liu、X. Du 和 M. Guizani，“TPPR：一种基于信任且保护隐私的车载自组织网络车队推荐方案”，IEEE Trans. Serv. Comput.，第15卷，第2期，第806–818页，2022年。[21] A. Leander，“解析飞马座：以基础设施为视角探讨技术与瑞士安全政治之间的关系”，Swiss Political Sci. Rev.，第27卷，第1期，第205–213页，2021年。[22] Z. Lu、G. Qu 和 Z. Liu，“车载网络安全、信任与隐私最新进展综述”，IEEE《智能交通系统汇刊》，第20卷，第2期，第760–776页，2018年。[23] I. Ali、A. Hassan 和 F. Li，“车载自组网络（VANET）的认证与隐私方案：综述”，Veh. Commun.，第16卷，第45–61页，2019年。[24] A. Boualouache、S. Senouci 和 S. Moussaoui，“车载自组网络假名更换策略综述”，IEEE Commun. Surv. Tutor.，第20卷，第1期，第770–790页，2018年。[25] H. Talat、T. Nomani、M. Mohsin 和 S. Sattar，“车联网中部署的位置隐私技术综述”，载于第16届国际布尔班应用科学与技术会议（IBCAST）论文集，2019年。IEEE，2019年，第604–613页。[26] R. Hussain、F. Hussain 和 S. Zeadally，“车载自组织网络与第五代移动通信安全的集成：设计与实现问题综述”，Future Gener. Comput. Syst.，第101卷，第843–864页，2019年。[27] R. Lu、L. Zhang、J. Ni 和 Y. Fang，“第五代移动通信车对万物通信服务：面向安全与隐私做好准备”，Proc. IEEE，第108卷，第2期，第373–389页，2019年。[28] M. Wang、T. Zhu、T. Zhang、J. Zhang、S. Yu 和 W. Zhou，“第六代移动通信网络中的安全与隐私：新领域与新挑战”，Digit. Commun. Netw.，第6卷，第3期，第281–291页，2020年。[29] M. S. Sheikh、J. Liang 和 W. Wang，“车载自组织网络与车载云计算中的安全与隐私：综述”，Wirel. Commun. Mob. Comput.，第2020卷，2020年。[30] H. Jiang、J. Li、P. Zhao、F. Zeng、Z. Xiao 和 A. Iyengar，“基于位置的服务中的位置隐私保护机制：全面综述”，ACM Comput. Surv.（CSUR），第54卷，36，2021年1，1第期。[31] P. Mundhe、S. Verma 和 S. Venkatesan，“车载自组织网络中认证与隐私保护方案的全面综述”，Comput. Sci. Rev.，第41卷，第100411页，2021年。[32] M. Dibaei、X. Zheng、Y. Xia、X. Xu、A. Jolfaei、A. K. Bashir、U. Tariq、D. Yu 和 A. V. Vasilakos，“探讨利用区块链和机器学习保障车联网安全的前景：综述”，IEEE《智能交通系统汇刊》，第23卷，700，2022年2，第683页。[33] A. Boualouache 和 T. Engel，“第五代移动通信及后续车联网中基于机器学习的不当行为检测系统综述”，arXiv预印本 arXiv:2201.10500，2022年。[34] A. Haddaji、S. Ayed 和 L. C. Fourati，“用于缓解车联网网络攻击的人工智能技术：综述”，Comput. Electr. Eng.，第104卷，第108460页，2022年。[35] Y. Belal、S. Ben Mokhtar、H. Haddadi、J. Wang 和 A. Mashhadi，“面向时空移动性应用的联邦学习模型综述”，ACM Trans. Spatial Algorithms Syst.，2024年。[36] H. Rasheed、R. Md Noor、N. Abdul Ghani 和 I. Ahmad，“在基于位置的服务中保护位置查询隐私：综述”，Security and Privacy，第7卷，第5期，第e412页，2024年。[37] E. M. Mianji、M. Fardad、G.-M. Muntean 和 I. Tal，“车联网中多智能体强化学习应用综述”，载于2024年IEEE第99届车辆技术会议（VTC2024-Spring）。IEEE，2024年，第1–7页。[38] N. Kaaniche、M. Laurent 和 S. Belguith，“解决隐私与个性化悖论的隐私增强技术：分类体系与综述”，J. Netw. Comput. Appl.，第171卷，第102807页，2020年。[39] T. Feng、Z. Zhang、W.-C. Wong、S. Sun 和 B. Sikdar，“基于位置的服务中位置隐私保护与体验质量之间权衡的框架”，IEEE Open Journal of Vehicular Technology，2024年。[40] S. Su、X. Zeng、S. Song、M. Lin、H. Dai、W. Yang 和 C. Hu，“基于新型磁跟踪方法提高自动导引车辆的定位精度”，IEEE Intell. Transp. Syst. Mag.，第12卷，第4期，第138–148页，2018年。[41] P. Khoenkaw，“一种用于电感环车辆传感器的低成本微控制器可编程振荡器实现”，载于2021年联合国际会议*f. Dig*艺术、媒体与技术会议；*ECTI* 北方分会会议 *f.* 电气、电子、计算机与电信工程。IEEE，2021年，第31–36页。[42] M. W. Raad、M. Deriche 和 T. Sheltami，《基于物联网的校车与车辆跟踪系统：采用RFID技术和移动数据网络》，《阿拉伯科学与工程杂志》，第46卷，第4期，第3087–3097页，2021年。[43] N. Ismail、S. Wahid 和 N. Ahmad，《基于Arduino的RFID车辆跟踪，用于家庭安全》，载于《物理学杂志：会议系列》，第1529卷，第2期。IOP出版社，2020年，第022060页。[44] A. Motroni、A. Buffi、P. Nepa 和 B. Tellini，《采用低密度超高频RFID标签的室内车辆传感器融合与跟踪方法》，IEEE《仪器与测量汇刊》，第70卷，第1–14页，2020年。[45] Y. Zhang、X. Gong、K. Liu 和 S. Zhang，《基于无源超高频RFID信号相位差的室内自动驾驶车辆定位与跟踪》，《传感器》，第21卷，第9期，第3286页，2021年。[46] W.-C. Ma、I. Tartavull、I. A. Baˆrsan、S. Wang、M. Bai、G. Mattyus、N. Homayounfar、S. K. Lakshmikanth、A. Pokrovsky 和 R. Urtasun，《利用稀疏语义高清地图实现自动驾驶车辆定位》，载于《IEEE/RSJ智能机器人与系统国际会议（IROS 2019）论文集》。IEEE，2019年，第5304–5311页。[47] S. D. Khan 和 H. Ullah，《基于视觉的车辆再识别技术进展综述》，《计算机视觉与图像理解》，第182卷，第63页，2019年，第50–4页。[48] X. Cheng、D. Duan、S. Gao 和 L. Yang，《面向车载通信网络（VCN）的感知与通信一体化（ISAC）》，IEEE Internet Things J.，第9卷，第23期，第23 441–23 451页，2022年。[49] S. Pooja，《使用GPS的车辆跟踪系统》，《国际科学研究杂志》，第2卷，第9期，第128–130页，2013年。[50] E. Levy、A. Shabtai、B. Groza、P.-S. Murvay 和 Y. Elovici，《CAN-LOC：基于电压信号深层特征的车载控制器局域网总线欺骗检测与物理入侵定位》，arXiv预印本 arXiv:2106.07895，2021年。[51] A. Eldesoky、A. M. Kamel、M. Elhabiby 和 H. Elhennawy，《利用低成本集成传感器与GPS实现陆地车辆应用的实时定位方案》，《应用研究与技术杂志》，第18卷，第4期，第214–228页，2020年。[52] N. Saeed、H. Nam、T. Y. Al-Naffouri 和 M.-S. Alouini，《基于多维尺度定位技术的最新综述》，IEEE Commun. Surv. Tutor.，第21卷，第3583页，2019年，第4期，第3565–页。[53] R. M. Rao、A. V. Padaki、B. L. Ng、Y. Yang、M.-S. Kang 和 V. Marojevic，《远距离目标的基于到达时间的定位：等DOP曲面、渐近界与维度自适应》，IEEE《车辆技术汇刊》，第70卷，第10期，第11 089–11 094页，2021年。[54] P. Sinha 和 I. Guvenc，《天线方向图对利用地面传感器网络进行基于到达时间的三维无人机定位的影响》，IEEE《车辆技术汇刊》，第71卷，第7期，第7703–7718页，2022年。[55] S. Gezici、Z. Tian、G. B. Giannakis、H. Kobayashi、A. F. Molisch、H. V. Poor 和 Z. Sahinoglu，《利用超宽带无线电进行定位：展望未来传感器网络的定位方面》，IEEE《信号处理杂志》，第22卷，第4期，第70–84页，2005年。[56] D. S. Simbeye，《坦桑尼亚干线公路感应线圈车辆交通计数器的部署》，《坦桑尼亚工程技术杂志》，第41卷，第4期，2023年。[57] D. Das、S. Banerjee、U. Ghosh、U. Biswas 和 A. K. Bashir，《基于区块链和智能合约的去中心化车辆防盗系统》，《点对点网络与应用》，第14卷，第2788页，2021年，第5期，第2775–页。[58] X. Li、H. Zhang、Y. Ren、S. Ma、B. Luo、J. Weng、J. Ma 和 X. Huang，《 PAPU：基于差分隐私、具备可证明不可链接性的车载自组织网络假名交换方案》，IEEE Internet Things J.，第7卷，第12期，第11 789–11 802页，2020年。[59] S. A. A. Hakeem 和 H. Kim，《基于双线性配对密码学的多区域认证与隐私保护协议（MAPP），面向5G-V2X》，《传感器》，第21卷，第2期，第665页，2021年。[60] Y. Feng、G. Mao、B. Cheng、C. Li、Y. Hui、Z. Xu 和 J. Chen，《Mag-Monitor：通过磁传感器进行车辆速度估计与车辆分类》，IEEE《智能交通系统汇刊》，第23卷，第2期，第1311–1322页，2022年。[61] S. Su、H. Dai、S. Cheng、P. Lin、C. Hu 和 B. Lv，《一种基于图优化的稳健磁跟踪方法》，IEEE《仪器与测量汇刊》，第69卷，第10期，第7933–7940页，2020年。[62] A. Sassella、F. Abbracciavento、S. Formentin、A. G. Bianchessi 和 S. M. Savaresi，《通过感应线圈估计城市交通路口排队长度》，载于《2023年美国控制会议（ACC）》。IEEE，2023年，第1135–1140页。[63] R. A. Gheorghiu、V. Iordache 和 V. A. Stan，《城市交通检测器：感应线圈与磁传感器的比较》，载于《论文集》

第13届电子、计算机与人工智能国际会议（ECAI）2021）。IEEE，2021年，第1–4页。[64] Y. Liu、R. Chen、Y. Zhou、M. Liu、Y. Hui 和 N. Cheng，《利用虚拟宽带多频连续波的基于RFID的车辆定位》，IEEE《射频识别期刊》，2023年。[65] C. Spiess，《交通信号灯跟踪着你吗？关于西雅图一项市政监控技术的案例研究》，IEEE《技术与社会汇刊》，第2卷，第1期，第15–19页，2021年。[66] Z. Liu、Z. Liu、L. Zhang 和 X. Lin，《Marp：一种用于车载自组织网络的分布式抗攻击MAC层假名方案》，IEEE《可信与安全计算汇刊》，2018年。[67] H. Yang、J. Cai、M. Zhu、C. Liu 和 Y. Wang，《基于车辆再识别的交通信息感知多摄像头系统（TIMS）》，IEEE《智能交通系统汇刊》，第23卷，第17 200页，2022年，第10期，第17 189–页。[68] C. Yu、Z. Ye、Y. He、M. Gao、H. Luo 和 G. Yu，《基于预测波束成形的多RSU车载网络协作定位》，《电信年刊》，第79卷，第1期，第85–100页，2024年。[69] D. Burghal、G. Phadke、A. Nair、R. Wang、T. Pan、A. Algafis 和 A. F. Molisch，《利用车车MIMO链路进行相对车辆定位的监督学习方法》，载于《2022年IEEE国际通信会议（ICC）论文集》。IEEE，2022年，第4528–4534页。[70] M. A. Nazari、G. Seco-Granados、P. Johannisson 和 H. Wymeersch，《基于单个基站快照观测的毫米波六维无线电定位》，IEEE《车辆技术汇刊》，第72卷，第8928页，2023年，第7期，第8914–页。[71] H. Xu、W. Liu、M. Jin 和 Y. Tian，《基于大规模阵列增强到达方向估计的自动驾驶车辆定位与轮廓提取》，IEEE Internet Things J.，2023年。[72] S. Huang、B. Wang、Y. Zhao 和 M. Luan，《利用可重构智能表面的基于近场RSS的定位算法》，IEEE Sens. J.，第22卷，第4期，第3493–3505页，2022年。[73] T. Chen、A. Hu 和 Y. Jiang，《高移动性环境下基于射频指纹的专用短程通信智能车联网识别机制》，《可持续发展》，第14卷，第9期，第5037页，2022年。[74] X. Lin、D. Ai、B. Ma、X. Wang、G. Yu、Y. He、W. Ni 和 R. P. Liu，《利用控制器局域网报文统计信息的车载网络基于联邦学习的入侵检测系统》，载于《网络仿真与评估国际会议》。施普林格，2023年，第237–251页。[75] R. Rai、J. Grover 和 S. Pandey，《揭示威胁：车载网络攻击的全面分类体系》，载于《2023年第16届信息与网络安全国际会议（SIN）》。IEEE，2023年，第1–7页。[76] S. Guha、K. Plarre、D. Lissner、S. Mitra、B. Krishna、P. Dutta 和 S. Kumar，《AutoWitness：在容忍GPS和无线电中断的同时定位与跟踪被盗财物》，ACM《传感器与网络汇刊》，第8卷，第4期，第1–28页，2012年。[77] P. Bagga、A. K. Das、M. Wazid、J. J. Rodrigues 和 Y. Park，《车联网身份认证协议：分类体系、分析与挑战》，IEEE Access，第8卷，第54 314–54 344页，2020年。[78] S. Wang 和 N. Yao，《RSU辅助的分布式信任框架：用于基于假名的车载自组织网络隐私保护》，《无线网络》，第25卷，第3期，第1099–1115页，2019年。[79] R. Mendes、M. Cunha 和 J. P. Vilela，《考虑速度的地理不可区分性》，载于《第十三届ACM数据与应用安全和隐私会议论文集》，2023年，第141–152页。[80] I. Butun 和 M. Gidlund，《保障位置隐私的物联网》，载于ICISSP论文集，第19卷。捷克共和国布拉格，2019年，第1–8页。[81] B. Liu、W. Zhou、T. Zhu、L. Gao 和 Y. Xiang，《位置隐私及其应用：系统性研究》，IEEE Access，第6卷，第17 606–17 624页，2018年。[82] M. A. Al-shareeda、M. Anbar、I. H. Hasbullah 和 S. Manickam，《车载自组织网络认证与隐私方案综述》，IEEE Sens. J.，第21卷，第2期，第2422–2433页，2021年。[83] A. P. Mdee、M. T. R. Khan、J. Seo 和 D. Kim，《面向车载自组织网络位置隐私保护的安全合规协作式假名交换》，IEEE《车辆技术汇刊》，2023年。[84] S. Zhang、B. Hu、W. Liang、K.-C. Li 和 B. B. Gupta，《一种基于缓存的双重K匿名位置隐私保护方案，适用于边缘计算》，IEEE Internet Things J.，2023年。[85] A. Pfitzmann 和 M. Hansen，《数据最小化隐私术语：匿名性、不可链接性、不可检测性、不可观察性、假名性与身份管理》，2010年。

[86] I. Almalkawi、J. Raed、A. Alsarhan、A. Abdallah 和 E. Abdallah，《针对无线多媒体传感器网络全局攻击的新型高效基于优先级的跨层上下文不可观测性方案》，《国际在线工程杂志》，2022年。[87] M. N. Tahir、M. Katz 和 U. Rashid，《真实环境中车载自组织网络无线网络技术分析》，载于 IEEE 无线电与无线研讨会论文集，IEEE，2021年，第123–125页。[88] A. M. Vegni、C. B. Iglesias 和 V. Loscri，《MOVES：一种基于记忆的车载社交转发技术》，《计算机网络》，第197卷，文章108324，2021年。[89] L. Chao、C. Wu、T. Yoshinaga、W. Bao 和 Y. Ji，《车联网多路径TCP简要综述》，《传感器》，第21卷，第8期，文章2793，2021年。[90] K. N. Qureshi、A. Alhudhaif、A. A. Shah、S. Majeed 和 G. Jeon，《面向车联网的信任与优先级无人机辅助路由、移动性及面向服务的解决方案》，《信息安全应用》，第59卷，文章102864，2021年。[91] G. Karmakar、A. Chowdhury、R. Das、J. Kamruzzaman 和 S. Islam，《使用深度学习评估无人驾驶汽车的信任等级》，IEEE《智能交通系统汇刊》，第22卷，第7期，第4457–4466页，2021年。[92] A. A. Khadir 和 S. A. H. Seno，《降低雾车载网络时延的基于软件定义网络的卸载策略》，《点对点网络与应用》，第14卷，第3期，第1261–1275页，2021年。[93] X. Jiang、F. R. Yu、T. Song 和 V. C. Leung，《车联网视频流资源分配：综述、若干研究问题与挑战》，IEEE《智能交通系统汇刊》，第23卷，第7期，第5955–5975页，2022年。[94] H. R. Abdulshaheed、Z. T. Yaseen、A. M. Salman 和 I. Al Barazanchi，《WiMAX和Wi-Fi在车载自组网络（VANET）中的应用综述》，载于《IOP会议系列：材料科学与工程》，第870卷，第1期，IOP出版社，2020年，文章012122。[95] G. Kostadinov 和 T. Atanasova，《无线与网络基础设施的安全策略》，载于《工程、控制论与机器人问题》，第71期，保加利亚科学院，2020年，第14–19页。[96] L. Zhao、W. Zhao、A. Hawbani、A. Y. Al-Dubai、G. Min、A. Y. Zomaya 和 C. Gong，《面向边缘软件定义车载网络的新型基于在线序贯学习的自适应路由》，《IEEE无线通信汇刊》，第20卷，第5期，第2991–3004页，2020年。[97] A. R. Khan、M. F. Jamlos、N. Osman、M. I. Ishak、F. Dzaharudin、Y. K. Yeow 和 K. A. Khairi，《智能交通系统（ITS）中用于车到车（V2V）和车到基础设施（V2I）物联网系统的专用短程通信技术：综述》，《迈向工业4.0的机电一体化最新趋势：iM3F 2020精选文章》，马来西亚，第97–106页，2022年。[98] S. Chen、J. Hu、L. Zhao、R. Zhao、J. Fang、Y. Shi 和 H. Xu，《蜂窝车联网（C-V2X）》，施普林格·自然，2023年。[99] B. Ji、Y. Wang、K. Song、C. Li、H. Wen、V. G. Menon 和 S. Mumtaz，《第六代移动通信计算智能综述：关键技术、应用与趋势》，IEEE《工业信息学汇刊》，2021年。[100] C. Bettini，《基于位置的服务中的隐私保护：综述》，载于《移动数据隐私手册》，施普林格，2018年，第73–96页。[101] J. W. Kim、K. Edemacu 和 B. Jang，《移动群智感知中位置隐私的隐私保护机制：综述》，《网络与计算机应用杂志》，第200卷，文章103315，2022年。[102] C. Qiu、A. C. Squicciarini、C. Pang、N. Wang 和 B. Wu，《通过地理不可区分性实现基于车辆的空间众包位置隐私保护》，《IEEE移动计算汇刊》，第21卷，第7期，第2436–2450页，2022年。[103] M. Bradbury、P. Taylor、U. I. Atmaca、C. Maple 和 N. Griffiths，《保护实时车载位置上下文所面临的隐私挑战》，《IEEE Access》，第8卷，第207465–207484页，2020年。[104] J. Jiang、G. Han、H. Wang 和 M. Guizani，《无线传感器网络位置隐私保护综述》，《网络与计算机应用杂志》，第125卷，第93–114页，2019年。[105] S. Shen、D. Chen、Y.-L. Wei、Z. Yang 和 R. R. Choudhury，《利用附近墙壁反射进行语音定位》，载于第26届年度国际移动计算与网络会议论文集，2020年，第1–14页。[106] A. Bahramali、R. Soltani、A. Houmansadr、D. Goeckel 和 D. Towsley，《针对安全消息应用的实用流量分析攻击》，arXiv预印本 arXiv:2005.00508，2020年。[107] N. Lal、S. Kumar 和 V. K. Chaurasiya，《一种在智慧城市中实时捕获事件以提高车辆安全性的道路监测方法》，《无线个人通信》，第114卷，第1期，第657–674页，2020年。[108] X. Lin、B. Ma、X. Wang、G. Yu、Y. He、R. P. Liu 和 W. Ni，《ByCAN：从比特级到字节级逆向工程控制器局域网（CAN）消息》，《IEEE物联网杂志》，2024年。

[109] N. Xue、Y. Malla、Z. Xia、C. Po¨pper 和 M. Vanhoef，《绕过隧道：滥用路由表泄露VPN客户端流量》，载于第32届USENIX安全研讨会（USENIX Security 23），2023年，第5719–5736页。[110] L. Zhu、S. Wang、C. Li 和 Z. Yang，《基于车辆跟踪与结果整合的城市道路车牌识别》，《智能系统杂志》，第29卷，第1期，第1587–1597页，2020年。[111] R. P. Parameswarath 和 B. Sikdar，《汽车远程无钥匙进入系统的安全基于PUF的认证协议》，IEEE《车辆技术汇刊》，2024年。[112] R. Molina-Masegosa、M. Sepulcre、J. Gozalvez、F. Berens 和 V. Martinez，《车联网中协作感知消息真实生成的经验模型》，IEEE《车辆技术汇刊》，第69卷，第5期，第5713–5717页，2020年。[113] J. Clancy、D. Mullins、B. Deegan、J. Horgan、E. Ward、C. Eising、P. Denny、E. Jones 和 M. Glavin，《V2X通信的无线接入：研究、挑战与机遇》，IEEE Commun. Surv. Tutor.，2024年。[114] G. Bendiab、A. Hameurlaine、G. Germanos、N. Kolokotronis 和 S. Shiaeles，《自动驾驶汽车安全：利用区块链和人工智能应对挑战的解决方案》，IEEE《智能交通系统汇刊》，第24卷，第4期，第3614–3637页，2023年。[115] P. Verde、J. D´ıez-Gonza´lez、R. Ferrero-Guille´n、A. Mart´ınez-Gutie´rrez 和 H. Perez，《用于改善城市场景中本地无线传感器网络定位的模因链》，《传感器》，第21卷，第7期，文章2458，2021年。[116] C. Dunbar、M. Gao 和 G. Qu，《传递并离开：一种面向网络车辆的隐私保护容迟网络通信协议》，载于2013年国际互联车辆博览会会议（ICCVE），IEEE，2013年，第840–841页。[117] Z. Lu、M. Gao、Z. Liu、G. Qu 和 C. Dunbar，《传递并离开：一种面向网络车辆的隐私保护容迟网络通信协议》，《IEEE设计与测试》，第36卷，第6期，第56–62页，2019年。[118] S. F. Shahandashti 和 R. Safavi-Naini，《阈值基于属性的签名及其在匿名凭证系统中的应用》，载于《AFRICACRYPT 2009论文集：第二届非洲密码学国际会议》，施普林格，2009年，第198–216页。[119] H. K. Maji、M. Prabhakaran 和 M. Rosulek，《基于属性的签名》，载于《密码学研究轨道RSA会议（CT-RSA）论文集》，施普林格，2011年，第376–392页。[120] A. E. Kaafarani、E. Ghadafi 和 D. Khader，《去中心化可追踪基于属性的签名》，载于《密码学研究轨道RSA会议（CT-RSA）论文集》，施普林格，2014年，第327–348页。[121] N. Kaaniche 和 M. Laurent，《支持匿名认证的基于属性的签名》，载于《欧洲计算机安全研究研讨会（ESORICS）论文集》，施普林格，2016年，第279–300页。[122] H. Zheng、Q. Wu、B. Qin、L. Zhong、S. He 和 J. Liu，《用于审计匿名通信的可链接群签名》，载于《澳大拉西亚信息安全与隐私会议（ACISP）论文集》，施普林格，2018年，第304–321页。[123] L. Wu、J. Fan、Y. Xie、J. Wang 和 Q. Liu，《面向车载自组织网络的高效基于位置的条件隐私保护认证方案》，《国际分布式传感器网络杂志》，第13卷，第3期，文章1550147717700899，2017年。[124] P. Mundhe、V. K. Yadav、A. Singh、S. Verma 和 S. Venkatesan，《基于环签名的VANET条件隐私保护认证》，《无线个人通信》，第114卷，第1期，第853–881页，2020年。[125] P. Mundhe、V. K. Yadav、S. Verma 和 S. Venkatesan，《用于VANET消息认证的高效基于格的环签名》，《IEEE系统杂志》，第14卷，第4期，第5463–5474页，2020年。[126] Q. Mei、H. Xiong、J. Chen、M. Yang、S. Kumari 和 M. K. Khan，《具有条件隐私保护的高效无证书聚合签名》，《IEEE系统杂志》，第15卷，第1期，第245–256页，2020年。[127] G. Ateniese、D. H. Chou、B. d. Medeiros 和 G. Tsudik，《可净化签名》，载于《欧洲计算机安全研究研讨会（ESORICS）论文集》，施普林格，2005年，第159–177页。[128] D. Pa`mies-Estrems、N. Kaaniche、M. Laurent、J. Castella`-Roca 和 J. Garcia-Alfaro，《面向基于互联网的个人助理的生活日志保护方案》，载于《数据隐私管理、加密货币与区块链技术》，施普林格，2018年，第431–440页。[129] G. Sun、S. Sun、H. Yu 和 M. Guizani，《激励车联网中基于雾计算的隐私保护移动群智感知》，《IEEE物联网杂志》，第7卷，第5期，第4128–4142页，2019年。[130] J. Zhou、Z. Cao、Z. Qin、X. Dong 和 K. Ren，《LPPA：面向VANET基于位置服务的高效多密钥安全外包计算轻量级隐私保护认证》，《IEEE信息取证与安全汇刊》，第15卷，第420–434页，2019年。

[131] B. Niu、Q. Li、X. Zhu、G. Cao 和 H. Li，《在隐私感知的位置服务中实现 k-匿名》，载于 IEEE INFOCOM 2014——IEEE 计算机通信会议。IEEE，2014 年，第 754–762 页。[132] U´. Erlingsson、V. Feldman、I. Mironov、A. Raghunathan、K. Talwar 和 A. Thakurta，《通过洗牌实现放大：通过匿名性从局部差分隐私到中心化差分隐私》，载于第 30 届 ACM-SIAM 离散算法年度研讨会论文集。SIAM，2019 年，第 2468–2479 页。[133] M. E. Andre´s、N. E. Bordenabe、K. Chatzikokolakis 和 C. Palamidessi，《地理不可区分性：面向基于位置的系统的差分隐私》，载于 2013 年 ACM SIGSAC 计算机与通信安全会议论文集，2013 年，第 901–914 页。[134] H. Liu、X. Li、H. Li、J. Ma 和 X. Ma，《面向基于位置的服务的时空相关感知基于虚假数据的隐私保护方案》，载于 IEEE INFOCOM 2017——IEEE 计算机通信会议，2017 年，第 1–9 页。[135] L. Zhou、L. Yu、S. Du、H. Zhu 和 C. Chen，《在边缘辅助联网车辆中实现差分隐私位置隐私》，IEEE《物联网汇刊》，第 6 卷，第 3 期，第 4472–4481 页，2018年。[136] Q. Li、J. P. Queralta、T. N. Gia、Z. Zou 和 T. Westerlund，《自动驾驶车辆导航与制图的多传感器融合：城市环境中的精确定位》，《无人系统》，第 8 卷，第 03 期，第 229–237 页，2020年。[137] X. Li、Y. Ren、L. T. Yang、N. Zhang、B. Luo、J. Weng 和 X. Liu，《扰动隐藏：车联网中基于位置的服务的车辆隐私增强》，IEEE《网络科学与工程汇刊》，第 1–1 页，2020年。[138] S. Wang、N. Yao、N. Gong 和 Z. Gao，《车载自组织网络中用于位置隐私保护的基于触发器的假名交换方案》，《点对点网络与应用》，第 11 卷，第 3 期，第 548–560 页，2018 年。[139] S. Terzi、C. Savvaidis、K. Votis、D. Tzovaras 和 I. Stamelos，《利用区块链和自主主权身份保护智能车辆的排放数据》，载于 IEEE 区块链国际会议论文集 2020。IEEE，2020年，第 462–469 页。[140] Y. Gong、X. Chang、J. Mis˘ic´ 和 V. B. Mis˘ic´，《A2E：用于访问无人驾驶出租车服务的属性型匿名增强身份认证》，arXiv 预印本 arXiv:2407.11320，2024 年。[141] G. K. Verma、N. M. Wani 和 P. Gope，《抗量子无证书条件隐私保护认证方案》，arXiv 预印本 arXiv:2403.13743，2024年。[142] O. E. Ajibuwa、S. D. Fabiyi 和 G. E. Dada，《弹性隐私保护的阈值车辆公钥基础设施（VPKI）》，arXiv 预印本 arXiv:2308.02711，2023年。[143] G. Amjad、K. Yeo 和 M. Yung，《带公开元数据的 RSA 盲签名》，《隐私增强技术论文集》，2025年。[144] A. C. Yao，《安全计算协议》，载于第 23 届计算机科学基础年度研讨会（SFCS 1982）论文集。IEEE，1982 年，第 160–164 页。[145] A. Tadakaluru 和 X. Qin，《基于Voronoi图的语义均衡虚假位置生成框架》，《分析学》，第 2 卷，第 1 期，第 246–264 页，2023年。[146] B. Ma、Y. Zhao、X. Wang、Y. Jiang、J. Li、W. Ni 和 R. P. Liu，《车联网中利用希尔伯特曲线的基于差分隐私的位置隐私保护》，载于《国际网络仿真与评估会议》。施普林格，2023年，第 252–268 页。[147] Q. Li、H. Wu、X. Wu 和 L. Dong，《车载自组织网络中基于差分隐私策略的多级位置隐私保护》，载于 IEEE 第 89 届车辆技术会议（VTC2019-Spring）论文集，2019 年，第 1–5 页。[148] M. A. Al-Shareeda、M. Anbar、S. Manickam 和 I. H. Hasbullah，《车载自组织网络中基于安全假名的条件隐私保护认证方案》，《传感器》，第 22 卷，第 5 期，第 1696 页，2022年。[149] H. Li、X. Xue、Z. Li、L. Li 和 J. Xiong，《物联网中面向 LBS 的位置隐私保护方案》，《无线通信与移动计算》，第 2021 卷，第 1–18 页，2021年。[150] H. Li、L. Pei、D. Liao、G. Sun 和 D. Xu，《区块链遇上车载自组织网络：车载自组织网络中的身份与位置隐私保护架构》，《点对点网络与应用》，第 12 卷，第 5 期，第 1178–1193 页，2019年。[151] B. Luo、X. Li、J. Weng、J. Guo 和 J. Ma，《车载自组织网络中基于区块链的信任型位置隐私保护方案》，IEEE《车辆技术汇刊》，第 69 卷，第 2 期，第 2034–2048 页，2019年。[152] B. Amro，《利用混合区和虚拟假名更换保护车载自组织网络中的隐私》，arXiv 预印本 arXiv:1801.10294，2018年。[153] Q. Li、H. Wu、L. Liu、B. Pan 和 L. Dong，《车载自组织网络中用于位置隐私保护的基于群组的动态混合区方案》，载于第三届安全智能城市、工业控制系统与通信国际会议（SSIC）论文集 2018，2018 年，第 1–5 页。

[154] J. Meng、X. Zhang、T. Cao 和 Y. Xie，《基于物理不可克隆函数的物联网设备轻量级匿名双向认证协议》，《安全通信与网络》，第 2022 卷，第 1–11 页，2021年。[155] L. Zhu、M. Li、Z. Zhang 和 Z. Qin，《ASAP：车联网中的匿名智能停车与支付方案》，IEEE《可信与安全计算汇刊》，第 17 卷，第 4 期，第 703–715 页，2020年。[156] P. Singh、A. Agarwal、G. Nakum、D. Rawat 和 S. Nandi，《MPF-SLP：车载自组织网络中用于源位置隐私的源位置隐私伪装概率泛洪》，IEEE《车辆技术汇刊》，第 69 卷，11393，2020 10，11383 no. p. –。[157] S. Ghane、A. Jolfaei、L. Kulik、K. Ramamohanarao 和 D. Puthal，《保护联网车辆互联网中的隐私》，IEEE《智能交通系统汇刊》，第 22 卷，第 8 期，第 5018–5027 页，2020年。[158] Q. Miao、W. Jing 和 H. Song，《基于差分隐私的边缘计算位置隐私增强》，《并发计算：实践与经验》，第 31 卷，第 8 期，第 e4735 页，2019年。[159] W. Tong、J. Hua 和 S. Zhong，《面向拼车服务的联合差分隐私调度协议》，IEEE《信息取证与安全汇刊》，第 12 卷，第 10 期，第 2444–2456 页，2017年。[160] F. Yucel、K. Akkaya 和 E. Bulut，《电动汽车充电的高效隐私保护供应商匹配》，《自组织网络》，第 90 卷，第 101730 页，2019年。[161] V. Subramaniyaswamy、V. Jagadeeswari、V. Indragandhi、R. H. Jhaveri、V. Vijayakumar、K. Kotecha 和 L. Ravi，《轻度同态加密：用于物联网传感器信号边缘设备快速加密的环学习误差算法》，《安全通信与网络》，第 2022 卷，2022年。[162] H. Yu、H. Zhang、X. Yu、X. Du 和 M. Guizani，《PGRide：在线网约车服务中的隐私保护群组拼车匹配》，IEEE《物联网汇刊》，第 8 卷，第 7 期，第 5722–5735 页，2020年。[163] N. Prema，《使用全同态加密（FHE）实现车载自组织网络中的高效安全聚合》，《移动网络与应用》，第 24 卷，第 2 期，第 434–442 页，2019年。[164] M. A. Mohammed、B. Garcia-Zapirain、J. Nedoma、R. Martinek、P. Tiwari、N. Kumar 等，《面向交通应用的全同态加密安全任务卸载与调度系统》，IEEE《车辆技术汇刊》，第 71 卷，第 11 期，第 12 140–12 153 页，2022年。[165] Z. Tan、C. Wang、M. Zhou 和 L. Zhang，《车联网基于位置的服务中的隐私信息检索》，载于第四届 IEEE 物联网世界论坛（WF-IoT）论文集。IEEE，2018 年，第 56–61 页。[166] Z. Chen、J. Nie、Z. Li、C. Ge 和 W. Susilo，《无误报的几何可搜索加密及其应用》，《计算机杂志》，2022年。[167] H. Liu、X. Zheng、H. Peng 和 F. Li，《用于 LBS 中分布式 k-匿名隐私保护的位置可用性度量方法》，载于 2024 年大数据与隐私计算国际会议（BDPC）论文集。IEEE，2024 年，第 69–74 页。[168] Y. Jiang、B. Ma、X. Wang、G. Yu、P. Yu、Z. Wang、W. Ni 和 R. P. Liu，《物联网的区块链联邦学习：综合综述》，ACM《计算调查》，第 56 卷，37，2024 10，1no. pp. –。[169] B. Ma、X. Wang、Y. Jiang 和 X. Lin，《道路网络中的自适应伪装区域混淆》，载于 2024 年第三届全驱动系统理论与应用会议（FASTA）论文集。IEEE，2024 年，第 331–336 页。[170] X. Sun、F. R. Yu、P. Zhang、W. Xie 和 X. Peng，《基于同态加密的车载自组织网络安全计算综述》，《传感器》，第 20 卷，第 15 期，第 4253 页，2020年。[171] W. Cabral、C. Valli、L. Sikos 和 S. Wakeling，《Cowrie 工件的审查与分析及其被欺骗性使用的潜力》，载于 2019 年国际计算机科学与计算智能会议（CSCI）论文集。IEEE，2019 年，第 166–171 页。[172] W. Bai、M. Pearson、P. G. Kelley 和 M. L. Mazurek，《改善非专家对端到端加密理解的探索性研究》，载于 2020 年 IEEE 欧洲安全与隐私研讨会（EuroS&PW）论文集。IEEE，2020 年，第 210–219 页。[173] H. Hasrouny、A. E. Samhat、C. Bassil 和 A. Laouiti，《车载自组织网络安全挑战与解决方案：综述》，《车辆通信》，第 7 卷，20，2017 7pp. –。[174] E. M. Radi、N. Lasla、S. Bakiras 和 M. Mahmoud，《点对点能源交易生态系统中的隐私保护电动汽车充电》，载于 2019 年 IEEE 国际通信会议论文集。IEEE，2019 年，第 1–6 页。[175] F. Jamil、O. Cheikhrouhou、H. Jamil、A. Koubaa、A. Derhab 和 M. A. Ferrag，《PetroBlock：基于区块链的智能车辆加油支付机制》，《应用科学》，第 11 卷，第 7 期，第 3055 页，2021年。

[176] B. Chaudhary 和 K. Singh，《基于区块链的车载自组网络位置隐私保护方案》，Peer-to-Peer Netw. Appl.，第14卷，第5期，第3198–3212页，2021年。[177] Z. Lu、W. Liu、Q. Wang、G. Qu 和 Z. Liu，《基于区块链的车载自组织网络隐私保护信任模型》，IEEE Access，第6卷，第45 655–45 664页，2018年。[178] A. Boualouache、H. Sedjelmaci 和 T. Engel，《用于第五代移动通信赋能的车载雾计算中协作式位置隐私保护的联盟区块链》，IEEE《车辆技术汇刊》，第70卷，第7期，第7087–7102页，2021年。[179] O. Samuel、N. Javaid、F. Shehzad、M. S. Iftikhar、M. Z. Iftikhar、H. Farooq 和 M. Ramzan，《利用区块链保护智慧社区电动汽车隐私》，载于《国际宽带无线计算与通信应用会议论文集》，施普林格，2019年，第67–80页。[180] H. Wang、J. Gan、Y. Feng、Y. Li 和 X. Fu，《基于区块链和盲签名的车联网隐私增强方案》，载于《国际区块链与可信系统会议论文集》，施普林格，2021年，第368–387页。[181] Q. Tang、J. Shen、Z. Cao 和 X. Dong，《PSSBP：一种基于区块链、用于车联网停车场共享的隐私保护范围查询可搜索加密方案》，载于《第19届IEEE嵌入式与泛在计算国际会议（EUC）论文集》，IEEE，2021年，第1–8页。[182] R. Liang、B. Li 和 X. Song，《基于区块链的车载自组织网络隐私保护信任管理模型》，载于《国际高级数据挖掘与应用会议（ADMA）论文集》，施普林格，2020年，第465–479页。[183] D. Wang、L. Zhang、C. Huang 和 X. Shen，《基于区块链的车联网隐私保护信任管理系统》，载于《2021年IEEE无线通信与网络会议（WCNC）论文集》，IEEE，2021年，第1–6页。[184] H. Liu、Y. Zhang、S. Zheng 和 Y. Li，《基于区块链和智能合约的V2G网络电动汽车电力交易机制》，IEEE Access，第7卷，第160 546–160 558页，2019年。[185] M. Baza、M. Nabil、N. Lasla、K. Fidan、M. Mahmoud 和 M. Abdallah，《为自动驾驶车辆量身打造的基于区块链的固件更新方案》，载于《2019年IEEE无线通信与网络会议（WCNC）论文集》，IEEE，2019年，第1–7页。[186] Z. Zhang、G. Yu、C. Sun、X. Wang、Y. Wang、M. Zhang、W. Ni、R. P. Liu、A. Reeves 和 N. Georgalas，《TbDd：一种基于信任、由深度强化学习驱动的物联网区块链分片新框架》，《计算机网络》，第244卷，文章编号110343，2024年。[187] Z. Zhang、Y. Wang、G. Yu、X. Wang、M. Zhang、W. Ni 和 R. P. Liu，《一种面向社区的区块链分片策略：实现更经济的交易》，载于《2023年IEEE国际区块链会议（Blockchain）论文集》，IEEE，2023年，第370–376页。[188] D. J. Currie、C. Q. Peng、D. M. Lyle、B. A. Jameson 和 M. S. Frommer，《遏制传播：澳大利亚智能手机应用在控制COVID-19方面能发挥多大作用》，Public Health Res. Pract.，第30卷，第2期，文章编号3022009，2020年。[189] K. Aliyev，《阿塞拜疆COVID-19政策应对与公众舆论的探索性分析》，Cauc. Surv.，第9卷，第3期，第300–319页，2021年。[190] E. Mbunge，《将新兴技术融入COVID-19接触者追踪：机遇、挑战与陷阱》，Diabetes Metab. Syndr.: Clin. Res. Rev.，第14卷，第6期，第1631–1636页，2020年。[191] M. J. Hossain，《COVID-19大流行对孟加拉国医疗服务提供者的影响：系统综述》，Bangladesh J. Infect. Dis.，第S8–S15页，2020年。[192] P. M. Garrett、Y.-W. Wang、J. P. White、Y. Kashima、S. Dennis 和 C.-T. Yang，《台湾民众对COVID-19追踪技术的高度接受度：全国代表性调查分析》，Int. J. Environ. Res. Publich Health，第19卷，第6期，文章编号3323，2022年。[193] E´. Schultz、R. Touzani、J. Mancini 和 J. K. Ward，《从接触者追踪到COVID-19通行证持有者：法国TousAntiCovid接触者追踪应用程序的曲折历程》，Public Health，第206卷，第5期，第7–12页，2022年。[194] C. Herendy，《COVID-19期间及为应对COVID-19开发的应用程序是什么样的？——对用户需求评估与测试的调查》，载于《第11届IEEE认知信息通信国际会议（CogInfoCom）论文集》，IEEE，2020年，第000 503–000 508页。[195] S. Hsaini、H. Bihri、S. Azzouzi 和 M. E. H. Charaf，《抗击COVID-19大流行的接触者追踪方法：局限性与伦理挑战》，载于《2020年IEEE第二届电子、控制、优化与计算科学国际会议（ICECOCS）论文集》，IEEE，2020年，第1–5页。[196] M. N. Lintvedt，《COVID-19追踪应用程序作为法律问题：对挪威“Smittestopp”应用程序的调查》，Oslo L. Rev.，第8卷，第69页，2021年。

[197] J. Bay、J. Kek、A. Tan、C. S. Hau、L. Yongquan、J. Tan 和 T. A. Quy，《BlueTrace：一种用于跨境社区接触者追踪的隐私保护协议》，新加坡政府科技局，技术报告，2020年。[198] S. L. Zhou、X. Jia、S. P. Skinner、W. Yang 和 I. Claude，《中国COVID-19移动应用的经验教训》，J. Saf. Sci. Res.，第2卷，第2期，第40–49页，2021年。[199] Y. Lu 和 L. Zhang，《社交媒体微信推断COVID-19的发展趋势》，J. Infect，第81卷，第1期，第e82–e83页，2020年。[200] V. Q. Li、L. Ma 和 X. Wu，《COVID-19、政策变化与后大流行时代的数据治理：东亚接触者追踪应用程序案例分析》，Policy Soc.，2022年。[201] T. Sharma、M. M. Islam、A. Das、S. T. Haque 和 S. I. Ahmed，《大流行期间的隐私：全球范围内COVID-19应用程序隐私实践概览》，载于《ACM计算与可持续社会专题讨论会论文集》，2021年，第215–229页。[202] A. Skiljic，《“Stop COVID-19”：克罗地亚接触者追踪应用程序概述及隐私相关的不确定性》，Eur. Data Prot. L. Rev.，第6卷，第433页，2020年。[203] J. Stehl´ıkova´等，《新冠危机、数据保护与欧盟追踪应用程序：捷克和奥地利抗击病毒的COVID-19手机应用程序》，Mezina´rodn´ı vztahy，第56卷，第1期，第35–67页，2021年。[204] D. J. Leith 和 S. Farrell，《接触者追踪应用程序隐私：欧洲GAEN接触者追踪应用程序共享了哪些数据》，载于《IEEE INFOCOM 2021——IEEE通信会议论文集》，IEEE，2021年，第1–10页。[205] J. Rannikko、P. Tamminen、R. Hellsten、J. P. Nuorti 和 J. Syrja¨nen，《COVID-19数字接触追踪应用程序在芬兰的有效性》，Clin Microbiol Infect，2022年。[206] J. H. Reelfs、O. Hohlfeld 和 I. Poese，《Corona-Warn-App：追溯德国官方COVID-19暴露通知应用程序的启动》，载于《SIGCOMM’20海报与演示环节论文集》，2020年，第24–26页。[207] T. Alanzi，《COVID-19疫情暴发期间应用商店和Google Play商店中可用移动应用程序综述》，J. Multidiscip. Healthc.，第14卷，第45页，2021年。[208] P. Rodr´ıguez、S. Gran˜a、E. E. Alvarez-Leo´n、M. Battaglini、F. J. Darias、M. A. Herna´n、R. Lo´pez、P. Llaneza、M. C. Mart´ın、O. Ramirez-Rubio 等，《一项评估数字接触者追踪流行病学影响的基于人群的对照实验》，Nat. Commun.，第12卷，第1期，第1–6页，2021年。[209] S. Geber 和 T. N. Friemel，《基于类型学的方法研究COVID-19大流行期间追踪应用程序的采用：以SwissCovid应用程序为例》，J. Quant. Descr.，第1卷，在线发表，2021年。[210] H. Xu、L. Zhang、O. Onireti、Y. Fang、W. J. Buchanan 和 M. A. Imran，《BeepTrace：面向COVID-19大流行及后续时期的区块链赋能隐私保护接触者追踪》，IEEE Internet Things J.，第8卷，第5期，第3915–3929页，2020年。[211] S. Vaudenay，《DP3T分析——介于斯库拉与卡律布狄斯之间》，技术报告，2020年。[212] R. L. Rivest、J. Callas、R. Canetti、K. Esvelt、D. K. Gillmor、Y. T. Kalai、A. Lysyanskaya、A. Norige、R. Raskar、A. Shamir 等，《PACT协议规范》，私人自动化接触者追踪团队，麻省理工学院，美国马萨诸塞州剑桥，技术报告0.1，2020年。[213] R. Gupta、M. Bedi、P. Goyal、S. Wadhera 和 V. Verma，《印度COVID-19追踪工具分析：Aarogya Setu移动应用程序案例研究》，Digital Government: Research and Practice，第1卷，第4期，第1–8页，2020年。[214] G. Jung、H. Lee、A. Kim 和 U. Lee，《信息过载：评估韩国COVID-19患者接触追踪数据披露的隐私风险》，Public Health Front.，第8卷，文章编号305，2020年。[215] J. K. Liu、M. H. Au、T. H. Yuen、C. Zuo、J. Wang、A. Sakzad、X. Luo、L. Li 和 K.-K. R. Choo，《隐私保护的COVID-19接触者追踪应用程序：一种零知识证明方法》，密码学电子印本档案，2020年。[216] N. D. Shah、E. W. Steyerberg 和 D. M. Kent，《大数据与预测分析：重新校准预期》，Jama，第320卷，第27–28页，2018年。[217] A. M. Elbir、G. Gurbilek、B. Soner、A. K. Papazafeiropoulos、P. Kour-tessis 和 S. Coleri，《用于抗击全球大流行病的车联网：预防COVID-19传播》，Smart Health，第26卷，文章编号100353，2022年。[218] A. S. Hasan、D. Patel 和 M. Jalayer，《COVID-19防疫规定是否影响驾驶员分心行为？——新泽西州案例研究》，Transportation research part F: traffic psychology and behaviour，第99卷，第429–449页，2023年。

[219] H. Stevens和M. B. Haines，“TraceTogether：疫情应对、民主与技术”，Asian Sci. Technol. Soc.，第14卷，第3期，第523–532页，2020年。[220] T. Sharma和M. Bashir，“应用在COVID-19应对中的使用及隐私保护的丧失”，Nat. Med.，第26卷，第8期，第1165–1167页，2020年。[221] H. Cho、D. Ippolito和Y. W. Yu，“COVID-19接触者追踪移动应用：隐私考量及相关权衡”，arXiv预印本arXiv:2003.11511，2020年。[222] O. Kanhere和T. S. Rappaport，“面向未来蜂窝通信的位置定位：第五代移动通信及以后”，IEEE Commun. Mag.，第59卷，第1期，第70–75页，2021年。[223] F. Khelifi、A. Bradai、A. Benslimane、P. Rawat和M. Atri，“物联网定位系统综述”，Mob. Netw. Appl.，第24卷，第3期，第761–785页，2019年。[224] L. Italiano、B. C. Tedeschini、M. Brambilla和M. Nicoli，“利用5G技术在城市环境中进行行人定位”，载于2024年第22届地中海通信与计算机网络会议（MedComNet）。IEEE，2024年，第1–6页。[225] F. Naaz、A. Nauman、T. Khurshaid和S.-W. Kim，“利用RIS技术赋能车联网：最先进综述”，传感器，第24卷，第2期，第337页，2024年。[226] S. Tomic、M. Beko、R. Dinis、M. Tuba和N. Bacanin，《无线传感器网络中基于RSS-AoA的目标定位与跟踪》。River Publishers，2017年。[227] Y.-Y. Li、G.-Q. Qi和A.-D. Sheng，“混合ToA/AoA目标定位的最佳可实现精度性能指标”，IEEE Commun. Letter，第22卷，第7期，第1474–1477页，2018年。[228] B. XU、S. LI和H. ZHANG，“基于双模型的低成本多AUV协同定位方法”，J. Ship Res.，第15卷，第3期，2020年。[229] J. Lu、X. Chen、M. Luo和Y. Zhou，“基于测量值粗略估计的多个AUV协作定位”，Appl. Soft Comput.，第91卷，第106197页，2020年。[230] M. A. Ouameur、M. Caza-Szoka和D. Massicotte，“利用低功耗无线网络进行室内定位的机器学习赋能工具与方法”，IEEE Internet Things J.，第100300页，2020年。[231] C. Laoudias、A. Moreira、S. Kim、S. Lee、L. Wirola和C. Fischione，“网络定位、跟踪与导航赋能技术综述”，IEEE Commun. Surv. Tutor.，第20卷，第4期，第3607–3644页，2018年。[232] S. Wielandt和L. D. Strycker，“室内多径辅助到达角定位”，传感器，第17卷，第11期，第2522页，2017年。[233] J. Kulmer，“利用多径实现高精度定位以减少基础设施”，博士论文，格拉茨工业大学，第3卷，2019年。[234] T. Qin、T. Chen、Y. Chen和Q. Su，“Avp-slam：停车场中自动驾驶车辆的语义视觉建图与定位”，载于IEEE/RSJ智能机器人与系统国际会议论文集，IROS 2020。IEEE，2020年，第5939–5945页。[235] M. J. Piran和D. Y. Suh，“面向第六代移动通信的学习驱动无线通信”，载于计算机、电子与通信工程国际会议（ICCECE）论文集2019。IEEE，2019年，第219–224页。[236] A. Chorti、A. N. Barreto、S. Kopsell、M. Zoli、M. Chafii、P. Sehier、G. Fettweis和H. V. Poor，“面向第六代移动通信的上下文感知安全：物理层安全的作用”，arXiv预印本arXiv:2101 01536，2021年。[237] A. Bourdoux、A. N. Barreto、B. van Liempd、C. de Lima、D. Dardari、D. Belot、E.-S. Lohan、G. Seco-Granados、H. Sarieddeen、H. Wymeer-sch等，“关于定位与感知的6G白皮书”，arXiv预印本arXiv:2006.01779，2020年。[238] W. Ahmad、G. Husnain、S. Ahmed、F. Aadil和S. Lim，“车载自组织网络（VANETs）中基于接收信号强度的定位与车辆距离估计”，J. Sens.，第2023卷，第1期，第7826992页，2023年。[239] H. Saleem、R. Malekian和H. Munir，“自动驾驶地面车辆中基于神经网络的SLAM最新研究进展：综述”，IEEE Sens. J.，第23卷，第13期，第13829–13858页，2023年。[240] X. Wang、X. Zha、W. Ni、R. P. Liu、Y. J. Guo、X. Niu和K. Zheng，“物联网区块链综述”，Comput. Commun.，第136卷，第10–29页，2019年。[241] J. Posner、L. Tseng、M. Aloqaily和Y. Jararweh，“车联网中的联邦学习：机遇与解决方案”，IEEE Netw.，第35卷，第2期，第152–159页，2021年。[242] Y. Ge、M. Stark、M. F. Keskin、F. Hofmann、T. Hansen和H. Wymeer-sch，“6 GHz以下频段V2X侧链路定位分析”，载于2023年

IEEE 第三届国际联合通信与传感研讨会（*JC&S*）. IEEE，2023年，第 1–6 页。 [243] C. Han、Y. Wang、Y. Li、Y. Chen、N. A. Abbasi、T. Ku¨rner 和 A. F. Molisch，《太赫兹无线信道：关于测量、建模与分析的全面综述》，*IEEE Commun. Surv.*，第 24 卷，第 3 期，第 1670–1707 页，2022年。 [244] B. A. Jayawickrama 和 Y. He，《用于第五代移动通信 NR LDPC 的改进型分层归一化最小和算法》，*IEEE Wirel. Commun.*，第 11 卷，第 9 期，第 2015–2018 页，2022年。 [245] C. Wang、F. Lin、T. Liu、K. Zheng、Z. Wang、Z. Li、M.-C. Huang、W. Xu 和 K. Ren，《mmEve：通过商用现成毫米波设备窃听智能手机听筒》，载于第 *28* 届年度国际移动计算与网络会议（*MobiCom*）论文集，2022年，第 338–351 页。 [246] K. Ahuja、Y. Jiang、M. Goel 和 C. Harrison，《Vid2Doppler：从视频合成多普勒雷达数据，用于训练保护隐私的活动识别模型》，载于*2021*年 *CHI* 人类因素与计算系统会议论文集，2021年，第 1–10 页。 [247] C. Han、Y. Wu、Z. Chen、Y. Chen 和 G. Wang，《太赫兹集成感知与通信（THz ISAC）：物理层视角》，*arXiv* 预印本 *arXiv:2209.03145*，2022年。 [248] G. Ananthi 和 S. Sridevi，《用于太赫兹波车载自组网络的膨胀卷积自编码器堆叠波束成形》，*Wirel. Pers. Commun.*，第 126 卷，第 4 期，第 2985–3000 页，2022年。 [249] G. Singh、A. Srivastava、V. A. Bohara、M. N. Rahim、Z. Liu、D. Pesch 和 L. Hanzo，《迈向第六代移动通信车联网：用于车联网的混合射频-可见光通信》，*arXiv* 预印本 *arXiv:2208.06287*，2022年。 [250] M. Sarfraz、M. F. Sohail、S. Alam、M. Javvad ur Rehman、S. A. Ghauri、K. Rabie、H. Abbas 和 S. Ansari，《涉及非正交多址接入的下一代无人机通信容量优化》，*Drones*，第 6 卷，第 9 期，第 234 页，2022年。 [251] R. Shaaban，《室内和室外车到车通信中可见光通信的网络安全漏洞》，博士学位论文，北达科他大学，2021年。 [252] A. Kumar、S. Al-Kuwari、D. N. K. Jayakody 和 R. Alkanhel，《不精确信道估计条件下基于非正交多址接入的水下可见光通信系统安全性能分析》，*IEEEAccess*，2022年。 [253] P. Sharma、A. Agrawal、V. Bhatia、S. Prakash 和 A. K. Mishra，《量子密钥分发保障的光网络：综述》，*IEEE open j. Commun. Soc.*，第 2 卷，第 2049–2083 页，2021年。 [254] M. S. Sharbaf，《量子密码学：新一代信息技术安全系统》，载于第六届国际信息技术会议：新一代技术 *2009* 论文集。IEEE，2009年，第 1644–1648 页。 [255] S. Pirandola、J. Eisert、C. Weedbrook、A. Furusawa 和 S. L. Braunstein，《量子隐形传态的进展》，*Nat. Photon.*，第 9 卷，第 10 期，第 641–652 页，2015年。 [256] K. Alaaudeen、T. Aruna 和 G. Ananthi，《采用 I 形超材料结构的低成本、宽带、电小型微带天线，用于 WLAN/全球微波接入互操作性和第五代移动通信车载应用》，*Physica B Condens.*，第 643 卷，第 414144 页，2022年。 [257] Y. Liu、X. Liu、X. Mu、T. Hou、J. Xu、M. Di Renzo 和 N. Al-Dhahir，《可重构智能表面：原理与机遇》，*IEEE Commun. Surv. Tutor.*，第 23 卷，第 3 期，第 1546–1577 页，2021年。 [258] X. You、C.-X. Wang、J. Huang、X. Gao、Z. Zhang、M. Wang、Y. Huang、C. Zhang、Y. Jiang、J. Wang，等，《迈向第六代无线通信网络：愿景、赋能技术与新范式变革》，*Sci. China Inf. Sci.*，第 64 卷，第 1 期，第 1–74 页，2021年。 [259] J. Carmona、C. Guindel、F. Garcia 和 A. de la Escalera，《eHMI：自动驾驶车辆部署的综述与指南》，传感器，第 21 卷，第 9 期，第 2912 页，2021年。 [260] J. E. Domeyer、J. D. Lee、H. Toyoda、B. Mehler 和 B. Reimer，《驾驶员-行人感知模型揭示耦合关系：对车辆自动化的启示》，*IEEETrans. Hum. Mach. Syst.*，2022年。