计算机科学
COMPUTER SCIENCE

保护两方隐私的多类型的路网*K*近邻查询方案

曾聪爱, 刘亚丽, 陈书仪, 朱秀萍, 宁建廷

引用本文

曾聪爱, 刘亚丽, 陈书仪, 朱秀萍, 宁建廷. 保护两方隐私的多类型的路网*K*近邻查询方案[J]. 计算机科学, 2024, 51(11): 400-417.

ZENG Congai, LIU Yali, CHEN Shuyi, ZHU Xiuping, NING Jianting. Multi-type *K*-nearest Neighbor Query Scheme with Mutual Privacy-preserving in Road Networks [J]. Computer Science, 2024, 51(11): 400-417.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230900158

保护两方隐私的多类型的路网 K 近邻查询方案

曾聪爱[1,2,3]　刘亚丽[1,2,3]　陈书仪[1,2,3]　朱秀萍[1,2,3]　宁建廷[4]
1 江苏师范大学计算机科学与技术学院　江苏 徐州 221116
2 广西密码学与信息安全重点实验室(桂林电子科技大学)　广西 桂林 541004
3 河南省网络密码技术重点实验室　郑州 450001
4 福建省网络安全与密码技术重点实验室(福建师范大学)　福州 350007
(zengcongai@jsnu.edu.cn)

摘　要　在车联网场景中,现有基于位置服务的隐私保护方案存在不支持多种类型 K 近邻兴趣点的并行查询、难以同时保护车辆用户和位置服务提供商(Location-Based Service Provider,LBSP)两方隐私、无法抵抗恶意攻击等问题。为了解决上述问题,提出了一种保护两方隐私的多类型的路网 K 近邻查询方案 MTKNN-MPP。将改进的 k-out-of-n 不经意传输协议应用于 K 近邻查询方案中,实现了在保护车辆用户的查询内容隐私和 LBSP 的兴趣点信息隐私的同时,一次查询多种类型 K 近邻兴趣点。通过增设车载单元缓存机制,降低了计算代价和通信开销。安全性分析表明,MTKNN-MPP 方案能够有效地保护车辆用户的位置隐私、查询内容隐私以及 LBSP 的兴趣点信息隐私,可以保证车辆的匿名性,能够抵抗合谋攻击、重放攻击、推断攻击、中间人攻击等恶意攻击。性能评估表明,与现有典型的 K 近邻查询方案相比,MTKNN-MPP 方案具有更高的安全性,且在单一类型 K 近邻查询和多种类型 K 近邻查询中,查询延迟分别降低了 43.23%～93.70%,81.07%～93.93%。

关键词:基于位置的服务;两方隐私保护;K 近邻查询;不经意传输协议;车联网;多类型
中图分类号　TP309

Multi-type K-nearest Neighbor Query Scheme with Mutual Privacy-preserving in Road Networks

ZENG Congai[1,2,3],LIU Yali[1,2,3],CHEN Shuyi[1,2,3],ZHU Xiuping[1,2,3] and NING Jianting[4]
1 College of Computer Science and Technology,Jiangsu Normal University,Xuzhou,Jiangsu 221116,China
2 Guangxi Key Laboratory of Cryptography and Information Security,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China
3 Henan Key Laboratory of Network Cryptography Technology,Zhengzhou 450001,China
4 Fujian Provincial Key Laboratory of Network Security and Cryptology,Fujian Normal University,Fuzhou 350007,China

Abstract　In the Internet of vehicles scenario,existing location-based service privacy-preserving schemes have issues such as not supporting parallel query of multi-type K-nearest neighbor points of interest,difficulty to protect the privacy of both the in-vehicle users and the location-based service provider(LBSP),and unable to resist malicious attacks. In order to solve the above issues,a multi-type K-nearest neighbor query scheme with mutual privacy-preserving in road networks,named as MTKNN-MPP is proposed. By applying the improved k-out-of-n oblivious transfer protocol to the K-nearest neighbor query scheme,it is realized that multi-type K-nearest neighbor points of interest can be queried at a time while protecting the privacy of the query content of in-

到稿日期:2023-09-27　返修日期:2023-11-11
基金项目:国家自然科学基金(61702237,61972094,62032005);徐州市科技计划项目(KC22052);广西密码学与信息安全重点实验室(桂林电子科技大学)研究课题(GCIS202114);河南省网络密码技术重点实验室研究课题(LNCT2021-A07);福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(NSCL-KF2021-04);江苏师范大学研究生科研与实践创新计划项目(2022XKT1545,2021XKT1387,2021XKT1396);教育部产学合作协同育人项目(202101374001);江苏省自然科学基金(BK20150241);徐州市推动科技创新专项资金项目(KC18005);江苏省高校自然科学基金(14KJB520010);江苏政府留学奖学金
This work was supported by the National Natural Science Foundation of China(61702237,61972094,62032005),Science and Technology Planning Foundation of Xuzhou City(KC22052),Opening Foundation of Guangxi Key Laboratory of Cryptography and Information Security(Guilin University of Electronic Technology)(GCIS202114),Opening Foundation of Henan Key Laboratory of Network Cryptography Technology(LNCT2021-A07),Opening Foundation of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund(Fujian Normal University)(NSCL-KF2021-04),Postgraduate Research & Practice Innovation Program of Jiangsu Normal University(2022XKT1545,2021XKT1387,2021XKT1396),Cooperative Education Project of the Ministry of Education(202101374001),Natural Science Foundation of Jiangsu Province(BK20150241),Special Foundation of Promoting Science and Technology Innovation of Xuzhou City(KC18005),Natural Science Foundation of the Higher Education Institutions of Jiangsu Province(14KJB520010) and Jiangsu Provincial Government Scholarship for Overseas Studies.
通信作者:刘亚丽(liuyali@jsnu.edu.cn)

vehicle user and the privacy of the points of interest information of LBSP. The addition of the onboard unit caching mechanism reduces computational cost and communication overhead. The security analysis shows that the MTKNN-MPP scheme can effectively protect the location privacy of in-vehicle users, query content privacy of in-vehicle users, and the privacy of points of interest information of LBSP, which ensures the anonymity of the vehicle's identity and can resist malicious attacks such as collusion attacks, replay attacks, inference attacks, and man-in-the-middle attacks. Performance evaluation shows that compared with the existing typical K-nearest neighbor query schemes, the MTKNN-MPP scheme has higher security and the query latency in single-type K-nearest neighbor query and multi-type K-nearest neighbor query is reduced by 43.23% ~ 93.70% and 81.07% ~ 93.93%, respectively.

Keywords Location-based service, Mutual privacy-preserving, K-nearest neighbor query, Oblivious transfer protocol, Internet of vehicles, Multi-type

1 引言

车联网(Internet of Vehicles, IoV)[1]打破了车辆信息共享的局限性，能够实现车与车、车与人、车与云平台、车与基础设施的通信。通过集成全球定位系统、射频识别和无线通信等关键技术，IoV 能够实现智能化交通管理、智能动态信息服务和车辆智能化控制[2]。基于位置的服务(Location-Based Service, LBS)[3-4]作为智能动态信息服务的一种，在车联网中得到了广泛应用[5]，比如兴趣点(Point of Interest, POI)信息查询、地图导航、位置感知社交网络等。其中，兴趣点信息查询是用户使用最普遍的服务之一，车辆用户[5-6]向 LBSP 提交真实位置和查询请求信息，以获取附近的餐厅、医院等兴趣点信息[5]。然而，由于车联网节点之间通过开放信道实现信息交互[7]，可能会受到恶意攻击者的攻击，因此，在车联网场景下使用 LBS 存在隐私泄露的风险。若车辆用户的当前位置被泄露，则攻击者可以跟踪车辆，从而对用户的安全造成威胁；若车辆用户的查询内容被泄露，则攻击者可以据此推断出用户的兴趣爱好、身份职业等，从而可能给用户推送一些广告信息，给用户造成困扰[6,8-9]；若 LBSP 的兴趣点信息被泄露，则会造成 LBSP 的资产流失[10-11]。因此，面向车联网的 LBS 隐私保护是一个亟待解决的问题。

现有 LBS 隐私保护的相关研究[5,8-9]大多仅考虑保护用户的隐私，而忽视了 LBSP 的兴趣点信息的隐私保护。由于兴趣点信息是 LBSP 的资产，因此，车辆用户向 LBSP 提出查询兴趣点信息的需求时需要使用 4G/5G 流量[8]，即支付一定的费用。在未支付兴趣点查询费用时，LBSP 不能把兴趣点信息暴露给未支付费用的用户，因此，LBSP 的兴趣点信息隐私也应该受到保护[10]。虽然现有部分方案[10-11]考虑了同时保护车辆用户和 LBSP 两方的隐私，但其面向欧氏空间设计，以直线距离代表两点之间的距离，不适用于车联网场景。

若用户计划获取离自己距离最近的兴趣点信息，即近邻点，则查询任意一个兴趣点的方案已无法满足用户的需求[10]。此外，用户可能想一次查询多个近邻点以综合考虑选取哪个兴趣点，即 K 近邻(K-nearest Neighbor, KNN)查询[12-13]。尽管现有部分研究已实现了 KNN 查询[9,11]，但它们仅仅考虑一次查询一种类型的 KNN 兴趣点，并不支持多种类型 KNN 兴趣点的并行查询。在实际场景中，用户希望一次获取多种类型的 KNN 兴趣点，以便根据查询结果作出计划，例如，车辆用户需要同时获取附近的娱乐场所、餐厅和停车场等位置信息，以便提前安排出行计划。现有方案[9,11]若要实现这种场景下的多种类型的 KNN 兴趣点查询，则需要分别提交多次查询，这在一定程度上增加了用户的查询时间。因此，设计并实现保护两方隐私的多类型的路网 KNN 查询方案具有重要的研究意义和实践价值。

综上所述，为了解决现有研究大多面向欧氏空间设计不适用于车联网场景、难以同时保护车辆用户和 LBSP 两方的隐私、不支持多种类型 KNN 兴趣点的并行查询等问题，本文提出了一种保护两方隐私的多类型的路网 K 近邻查询方案 MTKNN-MPP。本文的主要贡献如下：

1)针对车联网路网环境下现有研究不支持一次查询多种类型 KNN 兴趣点的问题，创新性地提出了 MTKNN-MPP 方案，以实现多种类型 KNN 兴趣点的并行查询。

2)针对现有研究难以同时保护车辆用户以及 LBSP 两方隐私的问题，设计了改进的 k-out-of-n 不经意传输协议，实现了车辆用户的查询内容以及 LBSP 的兴趣点信息隐私保护，并利用 k 匿名、锚点技术实现了车辆用户的位置隐私保护。

3)提出了一种改进的环签名方案，保证了车辆传输信息的真实性和完整性，在保障车辆匿名性的同时，实现了车辆合法性的验证以防止恶意车辆获取兴趣点。此外，通过随机化同一车辆的临时身份，成功阻止了攻击者获取同一车辆的行驶轨迹，实现了车辆的不可链接性。

4)利用车载单元缓存机制，降低了计算代价和通信开销，提高了查询效率；采用最近最少使用算法定期更新车载单元缓存，解决了缓存溢满的问题。与现有典型的 KNN 查询方案相比，本文方案在查询一种类型 KNN 兴趣点和多种类型 KNN 兴趣点两种情况下，查询延迟分别降低了 43.23% ~ 93.70%，81.07% ~ 93.93%。

5)与现有典型的 KNN 查询方案相比，本文方案具有较高的安全性，有效地保护了车辆用户的位置隐私、查询内容隐私以及 LBSP 的兴趣点信息隐私，有效地抵抗了合谋攻击、重放攻击、推断攻击、中间人攻击等恶意攻击。

2 相关工作

LBS 隐私保护方案可分为两类：保护用户隐私的方案以及保护用户和 LBSP 两方隐私的方案。

1)保护用户隐私的方案

LBS 中保护用户隐私指保护用户位置隐私和查询内容隐私，Zhou 等[9]提出了路网场景下基于 Paillier 公钥密码

系统[14]的KNN兴趣点秘密检索方法，其假设除了用户，其余各方均不可信，采用锚点技术[15]和Paillier同态加密技术[14]，保护了用户的位置隐私和查询内容隐私，但存在计算代价较高的问题。上述方案以移动性较低的用户作为研究对象。为了适应移动性较高的车联网场景，研究者们提出了基于缓存的方案。Liu等[6]首次提出在车联网场景中使用路边单元(Roadside Unit，RSU)进行主动缓存的方案。RSU定期缓存兴趣点信息，之后广播车辆用户查询位置的兴趣点信息，车辆主动缓存兴趣点信息在其车载单元(Onboard Unit，OBU)中，然而该方案仅依靠用户从OBU获取到兴趣点信息的概率来进行隐私保护，当车辆用户未从OBU获取到兴趣点信息而向LBSP发送查询请求时，此方案没有对查询请求进行保护，导致查询内容泄露。Hu等[8]进一步提出了一种使用RSU缓存并结合k匿名[16]的方案，但该方案未考虑信道的安全性。RSU以明文形式向车辆广播兴趣点信息，若兴趣点信息被攻击者篡改，未认证兴趣点信息正确性的车辆将存储错误的兴趣点信息。为解决上述两个方案所面临的大规模部署RSU成本高以及RSU容易受到物理攻击等问题，Cui等[5]提出了使用公交车缓存替代RSU缓存的车联网位置隐私保护方案，公交车将行驶路程中的兴趣点信息广播给周围的私家车，私家车将兴趣点信息缓存在OBU中，当私家车发出查询请求时，可直接从OBU中获取。该方案保护了车辆用户的位置隐私，然而当车辆未获取到兴趣点信息时，其采用k匿名方式请求LBSP，未保护查询内容隐私，并且该方案未考虑私家车OBU缓存溢满的问题。并且，公交车也可能会被攻击，从而存在兴趣点信息被篡改的问题。此外，上述方案[5-6,8-9]均不支持多种类型KNN兴趣点的并行查询。

总之，保护用户隐私的方案存在不支持多种类型KNN兴趣点的并行查询、未能保护LBSP的兴趣点信息隐私，无法抵抗恶意攻击、无法实现匿名性和不可链接性、计算代价较高等问题。

2)保护用户和LBSP两方隐私的方案

上述方案[5-6,8-9]均未能保护LBSP的兴趣点信息隐私。为了同时保护用户隐私和LBSP的兴趣点信息隐私，Paulet等[17]在其方案中使用了不经意传输协议(Oblivious Transfer，OT)[18]以及私有信息检索技术[19]。但该方案被证实恶意用户仍然可以从LBSP获取请求之外的其他所有兴趣点信息，存在LBSP兴趣点信息隐私泄露的问题[20]。之后，Yadav等[21]提出了基于格的OT扩展协议的方案，该方案最小化了轮数，但是由于全程使用OT协议，存在计算代价和通信开销较高的问题。因此，Yadav等[10]在此基础上进行了改进，借助可提供无条件匿名性和自发性的环签名技术，提出了改进的可链接自发匿名组签名方案(Modified Linkable Spontaneous Anonymous Group，MLSAG)，其由可链接自发匿名组签名方案(Linkable Spontaneous Anonymous Group，LSAG)[22]改进而来，解决了LSAG方案在某些情况下无法提供匿名性和可链接性的问题，实现了可链接性、匿名性和自发性。同时文献[10]使用OT协议，保护了用户的位置隐私和查询内容隐私。虽然文献[10]在用户进行两次以上的查询时，不需要执行OT协议，降低了计算代价，但是MLSAG方案的可链接性会导致用户的行驶轨迹暴露，存在用户隐私泄露的风险；且文献[10]无法抵抗重放攻击、合谋攻击，存在通信开销较高等问题。此外，上述方案[10,17,20-21]均不支持多种类型兴趣点的并行查询。

上述方案均未能实现KNN查询。Liu等[11]采用OT协议以及基于密文策略的属性加密(Ciphertext-Policy Attribute-Based Encryption，CP-ABE)算法[23]，提出了不支持指定兴趣点类型的KNN查询方案以及支持指定兴趣点类型的KNN查询方案(T-KNN)两种方案，两者均保护了车辆用户的隐私和LBSP的兴趣点信息隐私，但其难以抵抗中间人攻击、合谋攻击等恶意攻击。Cui等[24]提出了一种可验证的安全KNN查询方案，其使用Paillier同态加密技术保护用户位置隐私和查询内容隐私，使用维诺图、划分格等方式为兴趣点设计了一个可验证的安全索引，并将安全索引上传到云服务器，在用户查询的过程中使用线性变换函数来保护LBSP的兴趣点信息隐私。但文献[24]在构造索引时存储了大量无用数据，导致其计算代价较高；此外，文献[24]中所有用户共用同一个Paillier同态加密私钥，若该私钥被任意一个用户泄露，将会导致兴趣点信息、查询请求和查询结果泄露。因此，Cui等[25]进一步提出了多用户的、安全可验证的KNN查询方案，解决了上述单一私钥泄露导致信息泄露的问题。然而，文献[24-25]均假设信道安全，未能实现匿名性和不可链接性，无法抵抗重放攻击、中间人攻击等恶意攻击。上述3个方案[11,24-25]均面向欧氏空间设计，不适用于车联网场景，不支持多种类型KNN兴趣点的并行查询。

总之，保护用户和LBSP两方隐私的方案存在不支持多种类型KNN兴趣点的并行查询、难以抵抗恶意攻击、面向欧氏空间设计不适用于车联网场景等问题。

上述LBS隐私保护方案的研究现状总结如表1所列。

表1 LBS隐私保护方案的研究现状总结

Table 1 Summary of existing studies on LBS privacy-preserving schemes

	文献[5]	文献[6]	文献[8]	文献[9]	文献[10]	文献[11]	文献[17]	文献[20]	文献[21]	文献[24]	文献[25]
保护用户位置隐私	√	√	√	√	√	√	√	√	×	√	√
保护用户查询内容隐私	×	√	√	√	√	√	√	√	√	√	√
保护LBSP的兴趣点信息隐私	×	×	×	×	√	√	×	√	√	√	√
匿名性	√	×	×	√	√	×	×	×	×	×	×
不可链接性	√	×	×	√	×	√	×	×	√	×	×
抵抗重放攻击	√	×	×	√	√	√	√	√	√	×	×
抵抗推断攻击	√	×	×	√	×	√	√	√	×	×	×
抵抗中间人攻击	√	×	×	√	√	×	√	√	√	×	×

（续表）

	文献[5]	文献[6]	文献[8]	文献[9]	文献[10]	文献[11]	文献[17]	文献[20]	文献[21]	文献[24]	文献[25]
抵抗合谋攻击	×	×	×	×	×	×	×	×	×	×	×
实现 KNN 查询	×	×	×	√	×	√	×	×	×	√	√
支持指定类型的 KNN 查询	×	×	×	√	×	√	×	×	×	×	×
路网场景下的 KNN 查询	×	×	×	√	×	×	×	×	×	×	×
车联网场景下的 LBS 查询	√	√	√	×	√	√	×	×	√	×	×
实现多种类型兴趣点的并行查询	×	×	×	×	×	×	×	×	×	×	×

3 预备知识

本章将介绍 OT 协议、椭圆曲线密码机制、路网模型以及锚点技术。

3.1 OT 协议

OT 协议具有两方，发送方（S）和接收方（R），具有 2-选-1 OT（1-out-of-2 OT）、n-选-1 OT（1-out-of-n OT）、n-选-k OT（k-out-of-n OT）3 种形式[18]。在目前的 LBS 隐私保护研究中，主要使用前两种形式。发送方为 LBSP，接收方为用户，当用户请求时，LBSP 将全部兴趣点信息发送给用户，用户仅能获取其请求的兴趣点信息而不能获取其他兴趣点信息，从而保护了 LBSP 的兴趣点信息隐私。由于 LBSP 不能识别用户发送的查询请求，因此保护了用户的查询内容隐私。为满足多种类型 KNN 兴趣点并行查询的场景需求，本文将 k-out-of-n OT 协议应用于 LBS 隐私保护中。k-out-of-n OT 协议如下[18]：

S 拥有 n 个消息，即输入 $\{m_0, m_1, \cdots, m_{n-1}\}$，$R$ 输入 h 个消息选择比特 $\{\gamma_1, \gamma_2, \cdots, \gamma_h\} \in \{0, 1, \cdots, n-1\}$。协议结束后，$R$ 最后仅得到所选择的消息 $\{m_{\gamma_1}, m_{\gamma_2}, \cdots, m_{\gamma_h}\}$，却无法得知其他未选择的消息，$S$ 无法得知 $\{\gamma_1, \gamma_2, \cdots, \gamma_h\}$ 的值。

3.2 椭圆曲线密码机制

$GF(p)$ 是大质数 p 对应的有限域[5]，在 $GF(p)$ 上存在一个椭圆曲线 $E: y^2 = x^3 + ax + b (\mathrm{mod} p)$，其中 $a, b \in GF(p)$ 且 $4a^3 + 27b^2 \neq 0$。若存在无穷远点 O，则 E 上的所有的点和 O 共同组成一个阶为大质数 q、生成元为 P 的椭圆曲线加法群 G，其具有以下运算规则和困难性假设[5,26]。

1）点加运算

设 $P(x_1, y_1)$，$Q(x_2, y_2)$ 为 G 上的两个点，若 $P = -Q$，即 $x_1 = x_2$ 且 $y_1 = -y_2$，则 $P + Q = O$，否则 $P + Q = J(x_3, y_3)$。

2）点乘运算

设 $P, Q \in G, t \in Z_q^*$，则 E 上的点乘运算为 $tP = P + \cdots + P$（t 个 P）。如 1）所示，若 $P = Q$，则 $J = P + P = 2P$。

3）椭圆曲线离散对数困难问题

在 E 上给定任意两个点 $P, Q \in G$，其中 $Q = tP$，$t \in Z_q^*$，在多项式时间内计算出 t 的值是困难的[5,7]。

3.3 路网模型

在实际车联网场景下，车辆行驶在有向路网图中，因此，本文方案面向路网空间设计，使用图 1 所示的有向路网图作为路网模型[9]，基于路网距离计算兴趣点与车辆、路网顶点之间的距离[9]。

1）有向路网图

图 1 所示的有向路网图模拟了局部城市道路场景，其中，$v_1 - v_{12}$ 表示路网顶点，代表公交站台或路口；$r_1 - r_{18}$ 表示有向边，代表城市道路；$p_1 - p_{15}$ 表示有向边上分布的部分兴趣点。本文假设兴趣点都分布在道路两侧，在进行 KNN 查询的计算时，兴趣点被映射到最近的道路上，它离最近道路的距离忽略不计[27]。

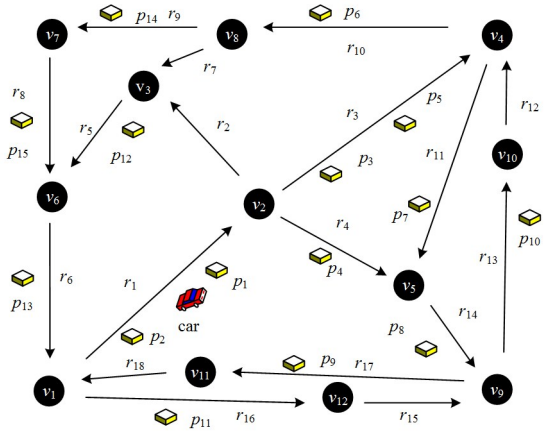


图 1 有向路网图

Fig. 1 Diagram of directed road network

2）面向欧氏空间设计与面向路网空间设计

（1）面向欧氏空间设计

面向欧氏空间设计的 KNN 查询方案[13]中，两点之间的距离是直线距离，被称作欧氏距离，表示为 d_c。

（2）面向路网空间设计

面向路网空间设计的 KNN 查询方案[9]中，两点之间的距离是路网距离 d_r，表示车辆从某一地点到另一地点行驶的最短路程，例如图 1 中从 v_2 到 p_6 的路网距离为 $d_r(v_2, p_6) = d_c(v_2, v_4) + d_c(v_4, p_6)$。

基于以上面向欧氏空间设计与面向路网空间设计的特点，可以得出：面向欧氏空间设计的 KNN 查询方案不适用于车联网场景，而面向路网空间设计的 KNN 查询方案更加符合车联网场景的需要。

3.4 锚点技术

锚点技术[15]指以一个假位置（锚点）替代用户真实位置发起查询请求[9]，具有构造灵活、易处理等特点，可以用于 LBS 查询的位置隐私保护[9]。

本文设定车辆以当前路段的前方固定路网顶点作为锚点[9]，该锚点可以替代单个车辆和多个车辆的真实位置，例如，图 1 中，car 的锚点为 v_2，处于 r_4，r_{11} 路段车辆的锚点为 v_5。当以锚点代替车辆真实位置发起查询请求时，攻击者不能推断出车辆的真实位置，保护了车辆用户的位置隐私。由于锚点位置固定，因此本文方案适用于车联网场景。

4 系统模型及安全模型

本章主要介绍本文方案的系统模型和系统安全模型。

4.1 系统模型

本节从系统实体和兴趣点分布结构两个方面介绍系统模型。

4.1.1 系统实体

本系统由可信机构(Trusted Authority,TA)、位置服务提供商和车辆3部分实体构成,各实体具体功能如下。

1)可信机构TA:诚实实体,具有强大的计算能力和足够的存储容量[5],可以抵御各种恶意攻击,主要负责为车辆分配公私钥对以及为合法车辆与LBSP分发通信的秘密值。

2)位置服务提供商LBSP:半诚实实体[11],遵守协议规则但好奇用户的隐私,试图从车辆发送的查询请求中推断出用户更多的隐私信息。本文设定将一个省以市为单位划分成多个区域,为每个区域分配单独的LBSP,用以存储本区域的兴趣点分布结构表,主要负责为车辆返回KNN兴趣点。

3)车辆:半诚实实体[11],遵守协议规则但试图从LBSP获取未请求的其他兴趣点的信息。该实体包括车辆用户(即车辆上的用户)和OBU两部分。车辆用户的手机或平板可通过WIFI接口与该车辆OBU进行通信[6],此外,OBU可以使用专用短程通信协议或蜂窝车辆对一切协议[5]与RSU进行通信。因此,车辆用户可通过OBU向LBSP发送查询请求并完成计算和存储功能。车辆配置的防篡改设备(Tamper Proof Device,TPD)用以存储车辆的公私钥对。

根据各实体间的交互过程,本文构建的系统模型如图2所示。下面以一个实际案例对图2进行说明。

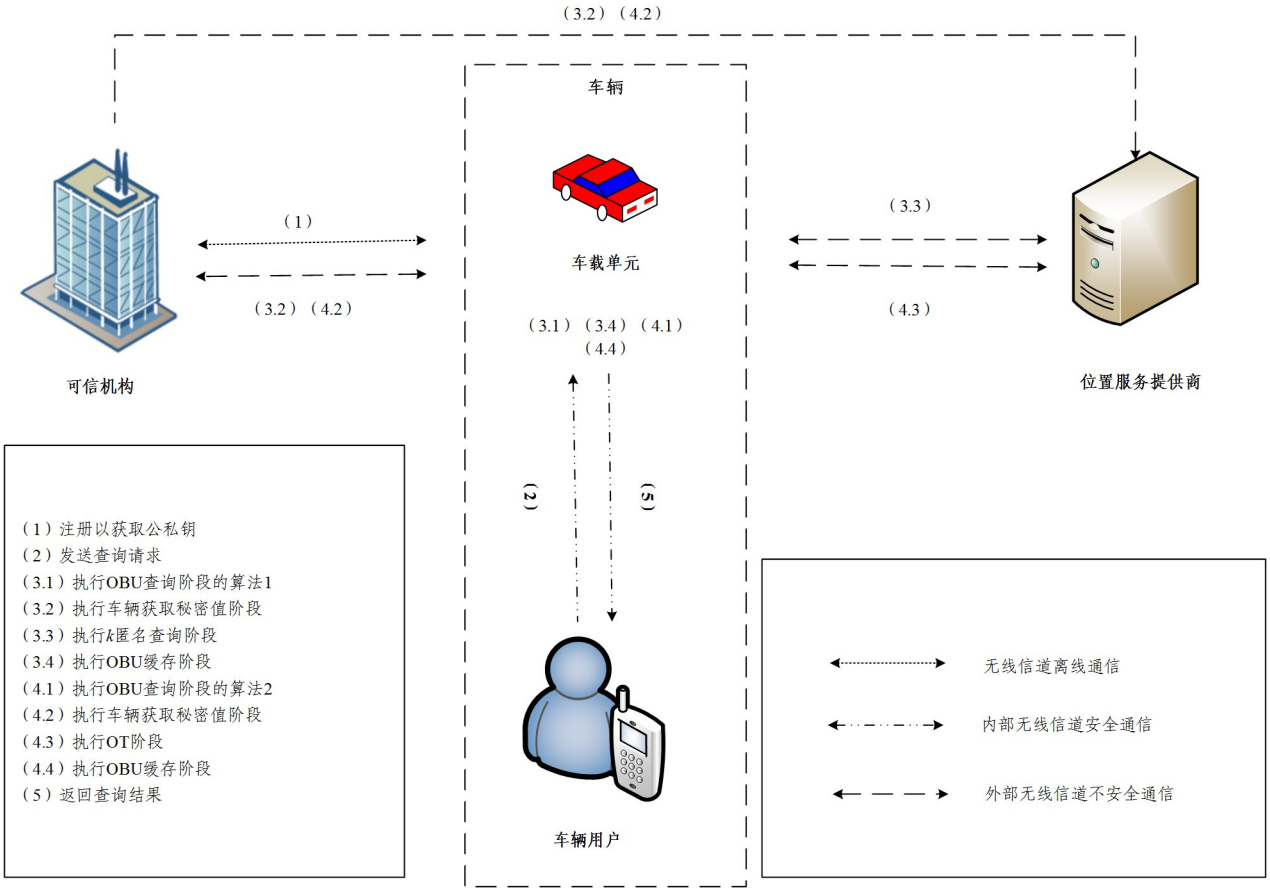


图2 系统模型

Fig. 2 System model

每辆车在享受兴趣点查询服务前都需要线下在TA中注册以获取公私钥对(即第1步)。若已完成第1步的车辆用户计划同时查询最近的5个餐厅和5个宾馆的相关信息,他可以使用手机或平板生成查询请求并发送给OBU(即第2步)。OBU首先执行OBU查询阶段的算法1查询自己的数据库中是否存有当前路段的兴趣点相关信息,且这些兴趣点信息均符合查询请求(即第3.1步)。若查询到的结果为空,则执行车辆获取秘密值阶段向TA获取与LBSP交互的秘密值(即第3.2步),之后执行k匿名查询阶段,从LBSP中查询当前路段的兴趣点信息(即第3.3步),再执行OBU缓存阶段,将该路段的所有兴趣点信息缓存到OBU中(即第3.4步)。若第3.3步查询到的结果少于5个餐厅和5个宾馆,比如仅获取到3个餐厅和2个宾馆的相关信息,则OBU以3个餐厅和3个宾馆为查询请求执行OBU查询阶段的算法2,获取以前方顶点为起始顶点的其他路段的兴趣点信息(即第4.1步)。若第4.1步查询到的兴趣点信息少于3个餐厅和3个宾馆,比如仅获取3个餐厅和0个宾馆,则执行车辆获取秘密值阶段,向TA获取秘密值(即第4.2步),再以3个宾馆为查询请求,执行OT阶段,获取3个宾馆的相关信息(即第4.3步),之后执行OBU缓存阶段,将第4.3步获取的兴趣点信息缓存到OBU中,最后综合上述查询结果,将最近的5个餐厅和5个宾馆的相关信息发送给车辆用户(即第5步)。若上述第3.1,4.1任意一步的查询结果满足5个餐厅和5个宾馆,则直接执行第5步,发送查询结果给用户。若上述第3.3,4.3

任意一步的查询结果满足 5 个餐厅和 5 个宾馆，则在分别执行第 3.4，4.4 步后直接执行第 5 步，发送查询结果给车辆用户。

4.1.2 兴趣点分布结构

本文采用锚点技术，将固定的路网顶点作为锚点以便查询路网顶点周围的兴趣点信息。在初始化阶段，LBSP 生成兴趣点分布结构表（见表 2）和兴趣点分布索引表（见表 3）[9]。

在表 2 中，路段起始顶点和终止顶点均为路网顶点，它们之间的路网距离不经过其他顶点。近邻兴趣点集指对某路段上的兴趣点进行类型划分后，针对每一类型兴趣点，根据其到路段起始顶点的距离进行升序排序而形成的集合。路网顶点对应的兴趣点指以该顶点为起始顶点对应的所有近邻兴趣集，其以类型分类并根据距离升序排序，从而形成有序集合。为了降低计算代价和通信开销，表 2 中没有记录未分布兴趣点的路段的相关信息。此外，本文设定路网顶点、路段索引与兴趣点类型索引均唯一，兴趣点类型索引与兴趣点类型一一对应，例如表 2 中每条路段的学校类型索引均为 50。

表 3 相较于表 2 缺失了近邻兴趣点集，此项内容因涉及 LBSP 的兴趣点隐私而未公开。表 3 包含内容覆盖某区域全部兴趣点的索引信息，车辆查询表 3 可以得到所需兴趣点的索引信息。

LBSP 保存表 2 并公布表 3，以便车辆根据前方顶点确定其所需的兴趣点类型索引，并把所需某种类型的兴趣点个数控制在其近邻兴趣点总数之内。

表 2 兴趣点分布结构

Table 2 POI distribution structure

路段起始顶点	路段终止顶点	路段索引	兴趣点类型索引	兴趣点类型	近邻兴趣点总数	近邻兴趣点集
v_1	v_2	e_1	50	hospital	n_1	$\{poi_1, poi_2, \cdots, poi_{n_1}\}$
			50	school	n_2	$\{poi_1, poi_2, \cdots, poi_{n_2}\}$
	v_{12}	e_{16}	14	cemetery	n_3	$\{poi_1, poi_2, \cdots, poi_{n_3}\}$
v_2	v_4	e_3	12	canal	n_4	$\{poi_1, poi_2, \cdots, poi_{n_4}\}$
			50	school	n_5	$\{poi_1, poi_2, \cdots, poi_{n_5}\}$
			57	tower	n_6	$\{poi_1, poi_2, \cdots, poi_{n_6}\}$
	v_5	e_4	57	tower	n_7	$\{poi_1, poi_2, \cdots, poi_{n_7}\}$
v_3	v_6	e_5	50	hospital	n_8	$\{poi_1, poi_2, \cdots, poi_{n_8}\}$
…	…	…	…	…	…	…

表 3 兴趣点分布索引

Table 3 POI distribution index

路段起始顶点	路段终止顶点	路段索引	兴趣点类型索引	兴趣点类型	近邻兴趣点总数
v_1	v_2	e_1	50	hospital	n_1
			50	school	n_2
	v_{12}	e_{16}	14	cemetery	n_3
v_2	v_4	e_3	12	canal	n_4
			50	school	n_5
			57	tower	n_6
	v_5	e_4	57	tower	n_7
v_3	v_6	e_5	50	hospital	n_8
…	…	…	…	…	…

4.2 系统安全模型

本节从系统所面临的安全威胁和系统安全性目标两个方面介绍系统安全模型。

4.2.1 系统威胁

根据 4.1.1 节对系统实体的描述，TA 是诚实的，LBSP 和车辆是半诚实的，它们均遵守协议规则，但试图通过观察的信息推断出更多的信息[11]。在信道安全方面，本文假设车辆用户与 OBU 之间的内部无线通信信道是安全的，车辆与其他实体间的外部无线通信信道是不安全的，可能受到外部攻击者的窃听、截获、篡改、重放等恶意攻击[6]。其中，外部攻击者的能力为多项式时间。因此，本文考虑对系统发起的威胁主要有以下 3 点：

1）LBSP 试图通过车辆提交的请求信息推断出车辆用户的隐私信息。

2）车辆用户试图从 LBSP 中获取除请求之外的兴趣点信息。

3）外部攻击者试图通过外部无线通信信道获取车辆与 LBSP 的交互信息，进而推断出车辆用户的隐私信息以及 LBSP 的兴趣点信息。

4.2.2 系统安全性目标

根据系统威胁中的描述，本文方案的安全性目标是实现匿名性、保护车辆用户的位置隐私和查询内容隐私、保护 LBSP 的兴趣点信息隐私、实现不可链接性和抵抗恶意攻击。系统安全性目标具体如下：

1）匿名性：保护车辆的身份信息不被泄露。

2）保护车辆用户的位置隐私：保护车辆用户的位置信息不被泄露。

3）保护车辆用户的查询内容隐私：LBSP 无法根据车辆提交的信息推断出车辆用户的查询内容和其他隐私信息。

4）保护 LBSP 的兴趣点信息隐私：车辆用户无法从 LBSP 数据库中获取尚未请求过的兴趣点信息。

5）不可链接性：当同一车辆连续请求时，攻击者不能把车辆临时身份和车辆真实身份联系起来，不能推断出车辆的行驶轨迹。

6）抵抗恶意攻击：车辆无法与其他车辆共谋获取未请求的兴趣点信息以抵抗合谋攻击。外部攻击者无法通过中间人攻击、重放攻击、推断攻击等恶意攻击方式获取车辆用户的隐私信息以及 LBSP 的兴趣点信息。

5 多类型的路网 K 近邻查询方案

为了解决现有车联网场景中 LBS 隐私保护方案存在的不支持多种类型 KNN 兴趣点的并行查询、难以同时保护车辆用户和 LBSP 两方隐私、无法抵抗恶意攻击等问题，本文提出了保护两方隐私的多类型的路网 K 近邻查询方案（Multi-

type K-nearest Neighbor Query Scheme with Mutual Privacy-preserving, MTKNN-MPP)。

5.1 MTKNN-MPP 方案符号及含义

MTKNN-MPP 方案常用符号及含义如表 4 所列。

表 4 MTKNN-MPP 方案常用符号及含义

Table 4 Common symbols of MTKNN-MPP and their meanings

符号	含义
K	用户查询的近邻兴趣点个数
k	k 匿名路段集大小
q	大质数
G	q 阶椭圆曲线加法群
H	哈希函数
P_0, P_1, P_2, P_3	G 的生成元
(pk_{car}, sk_{car})	车牌号为 car 的车辆公私钥对
(pk_{LBSP}, sk_{LBSP})	LBSP 公私钥对
$Table_3$	兴趣点分布索引表
$A_1, A_2, A_3, B_1, B_2, D_1, D_2, F_1, F_2$	信道中传输的消息集合
$edge\_id$	车辆当前所处路段索引
$\varphi list_0, \cdots, \varphi list_5$	兴趣点类型索引集合
φ_i	某个兴趣点类型索引
t_count	用户查询的兴趣点类型数
$edge\_poi$	车辆所处路段的兴趣点信息集
$edge\_tpoi$	车辆所处路段所需类型的兴趣点信息集
r_gpoi	车辆行驶前方的路段兴趣点查询结果集
$anchor\_id$	锚点
OBU_poi	缓存查询结果集
n_j	某锚点对应兴趣点类型所含兴趣点个数
num	环成员个数
Y	车辆临时身份
L	环成员公钥集
N	路网顶点对应的兴趣点类型个数
Γ	某个锚点对应兴趣点类型索引集
OT_poi	OT 阶段获取的 KNN 兴趣点查询结果集
v_n	车辆当前所处路段的前方顶点
$user\_poi$	用户查询结果集
d_r	路网距离
sh, sh'	秘密值

5.2 MTKNN-MPP 方案子阶段

MTKNN-MPP 方案由 7 个子阶段构成，分别是：初始化阶段、OBU 缓存阶段、OBU 查询阶段、车辆获取秘密值阶段、环签名阶段、k 匿名查询阶段、OT 阶段。各阶段具体描述如下。

5.2.1 初始化阶段

本阶段在线下进行，主要执行 TA 发布信息、车辆和 LBSP 生成公私钥对、LBSP 发布表 3($Table_3$)。

1) TA 发布信息：TA 确定 q 阶椭圆曲线加法循环群 G 的生成元为 P_0, P_1, P_2, P_3，选择哈希函数 $H: \{0,1\}^* \rightarrow Z_q^*$，公布 $A_1 = \{P_0, P_1, P_2, P_3, G, q, H\}$。

2) 车辆注册：TA 为前来注册的车辆分配公私钥对，对于车牌号为 car 的车辆，TA 分配给它的私钥为 $sk_{car} \in Z_q^*$，计算其公钥为 $pk_{car} = sk_{car} P_0$，把车辆的公私钥对存储在车辆的 TPD 中，并以 $(car, sk_{car}, pk_{car}, rtime)$ 的形式保存在自己的数据库中，其中，$rtime$ 表示注册时间。车辆公私钥对有效期为 1 年，到期需重新注册。

3) LBSP 初始化：LBSP 随机选取私钥 $sk_{LBSP} \in Z_q^*$，计算其公钥 $pk_{LBSP} = sk_{LBSP} P_0$，确定表 2 和 $Table_3$，公布 $A_2 = \{pk_{LBSP}, Table_3\}$。

4) LBSP 发布兴趣点更新表：LBSP 定期通过公告发布兴趣点更新表，以便用户查询所需类型的相应兴趣点是否更新。为保护 LBSP 的兴趣点信息隐私，若某路段的某兴趣点已更新，兴趣点更新表中仅会插入或更新该兴趣点对应的类型，而不会透露更新的具体兴趣点。该表的结构为 $(edge\_id, category\_id, utime)$，含义分别为更新兴趣点对应的路段索引、兴趣点类型索引以及更新时间。

5.2.2 OBU 缓存阶段

由于采用 RSU[6,8] 或公交车[5] 缓存兴趣点信息容易受到攻击，因此，本文不采用中间实体缓存的方法，而将查询到的兴趣点信息缓存到车辆本身的 OBU 中，方便后续执行 OBU 查询阶段直接从 OBU 中查询兴趣点信息，从而降低计算代价和通信开销。

OBU 缓存中具有路段兴趣点缓存表和顶点兴趣点缓存表两个表，其数据格式及含义均如表 5 所列。其中，路段兴趣点缓存表中数据按 rid 和 $category\_id$ 分类，顶点兴趣点缓存表中数据按 $start\_v_n$ 和 $category\_id$ 分类，每一类别的兴趣点均按照 $poi\_to\_start\_vn\_dis$ 从小到大排序后存储。

表 5 OBU 存储兴趣点的数据格式及含义

Table 5 Formats of OBU storage POI and their meanings

数据段	含义
poi_id	兴趣点索引
$start\_v_n$	路段起始顶点
$category\_id$	兴趣点类型索引
rid	兴趣点所处路段索引
$edge\_length$	兴趣点所处路段长度
$poi\_to\_start\_vn\_dis$	兴趣点距该路段起始顶点的路网距离
$ptime$	缓存时间

在执行完 k 匿名查询阶段和 OT 阶段后，执行本阶段分别将兴趣点信息缓存到路段兴趣点缓存表和顶点兴趣点缓存表中。在这两个表中缓存兴趣点信息时，若兴趣点在表中不存在，则直接插入；若存在，则替换已有的兴趣点信息，并更新 $ptime$。

为了防止缓存溢满，需要设置溢满的阈值。当缓存达到阈值时，OBU 将根据 $ptime$ 执行最近最少使用算法，定期更新缓存。对于路段兴趣点缓存表，需清理长时间未使用兴趣点的对应路段对应类型的全部兴趣点信息；对于顶点兴趣点缓存表，需清理长时间未使用兴趣点的对应起始顶点对应类型的全部兴趣点信息。

5.2.3 OBU 查询阶段

在执行 k 匿名查询阶段或 OT 阶段之前，执行 OBU 查询阶段，通过用户与 OBU 间的安全信道向 OBU 发起兴趣点信息查询请求，以降低通信开销并加强用户的隐私保护。

本阶段包括 OBU 查询当前路段兴趣点信息算法 1 和 OBU 查询锚点对应兴趣点信息算法 2。算法具体描述如下：

1) OBU 查询当前路段兴趣点信息算法

在执行 k 匿名查询阶段之前，执行该算法(见算法 1)，负责从 OBU 的路段兴趣点缓存表中查询当前路段所需类型的兴趣点信息，当且仅当所查兴趣点在表中且对应类型的所有兴趣点均未更新时，即可获取该类型的兴趣点信息。

算法 1 OBU 查询当前路段兴趣点信息算法

输入：edge_id, $\varphi list_0 = (\varphi_1, \cdots, \varphi_{t\_count})$

输出：edge_tpoi，已获取兴趣点的类型索引集 $\varphi list_1$

1. for $\varphi_i \in \varphi list_0$
2. 令 flag=0；/* 用于标识 */
3. 获取路段兴趣点缓存表中路段索引为 edge_id、兴趣点类型索引为 φ_i 的兴趣点信息；
4. 获取兴趣点更新表中路段索引为 edge_id、兴趣点类型索引为 φ_i 的更新时间 e_utime；
5. for 遍历每个兴趣点
6. if 某个兴趣点的缓存时间早于 e_utime
7. 令 flag=1；/* 表示该类型已更新 */
8. break；
9. end if
10. end for
11. if flag=0
12. 将 φ_i 对应的所有兴趣点信息加入 edge_tpoi 中，并将 φ_i 加入 $\varphi list_1$ 中；
13. end if
14. end for

2）OBU 查询锚点对应兴趣点信息算法

在执行 OT 阶段之前，执行该算法，如算法 2 所示。由于未在 OBU 的顶点兴趣点缓存表中获取到某类型的 KNN 兴趣点，执行 OT 阶段时，都会返回该路网顶点所查类型对应的全部 KNN 兴趣点，因此，本文设定车辆能够在 OBU 中获得锚点对应兴趣点信息的前提条件是：请求的兴趣点类型对应近邻个数不超过顶点兴趣点缓存表中该类型对应的兴趣点缓存个数，并且这些兴趣点均未更新。若满足该条件，车辆用户即可从 OBU 中获取该类型对应的兴趣点信息，后续查询也无需考虑该类型的查找；若不满足，则需执行 OT 阶段，获取该类型对应的兴趣点信息。

算法 2 OBU 查询锚点对应兴趣点信息算法

输入：anchor_id，K，$\varphi list_3$

输出：OBU_poi，已获取兴趣点的类型索引集 $\varphi list_4$

1. for $\varphi_i \in \varphi list_3$
2. 令 flag=0；
3. 获取顶点兴趣点缓存表中锚点为 anchor_id、兴趣点类型索引为 φ_i 的路段索引集 hedge_id，对应兴趣点个数 n_j 以及其他兴趣点信息；
4. 获取兴趣点更新表中路段索引集为 hedge_id、兴趣点类型索引为 φ_i 的更新时间集 etime；
5. if $n_j \geqslant K$
6. for 遍历 K 个兴趣点
7. if 某一个兴趣点对应的路段索引在兴趣点更新表中，且该表中该路段索引的缓存时间比顶点兴趣点缓存表中的缓存时间晚
8. 令 flag=1；
9. break；
10. end if
11. end for
12. end if
13. if flag=0
14. 把缓存中存在且未更新的 KNN 兴趣点加入 OBU_poi 中，将 φ_i 加入 $\varphi list_4$；
15. end if
16. end for

5.2.4 车辆获取秘密值阶段

车辆在从 LBSP 获取兴趣点之前，需要执行该阶段从 TA 获取与 LBSP 通信的秘密值，以验证车辆身份的合法性，防止未注册的恶意车辆获取兴趣点信息。

1）车辆生成时间戳 $vtime_0$，使用 SM2 公钥加密算法加密 $car, sk_{car}, pk_{car}, vtime_0$ 后得到 $B_1 = SM2E_{pk_{TA}}(car, sk_{car}, pk_{car}, vtime_0)$，发送 B_1 给 TA。

2）TA 使用 sk_{TA} 解密 B_1 后获取 $car, sk_{car}, pk_{car}, vtime_0$，若 car 存在，且对应 sk_{car} 正确，则随机生成秘密值 $sh \in Z_q^*$ 和时间戳 $stime$，使用椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）[28] 对 $sh, stime$ 签名后再使用 SM2 公钥加密算法对其加密后得到 $B_2 = SM2E_{pk_{LBSP}}(sh, stime, ECDSA_{sk_{TA}}(sh, stime))$，发送 B_2 给 LBSP；找出车辆注册时间 $rtime$，若 $vtime_0 - rtime < 1$ 年，发送 $B_3 = SM2E_{pk_{car}}(sh, ECDSA_{sk_{TA}}(sh))$ 给车辆；若 $vtime_0 - rtime \geqslant 1$ 年，则更新车辆公私钥对和注册时间为 $(sk'_{car}, pk'_{car}, rtime')$，并将其保存到数据库中，发送 $B_3 = SM2E_{pk_{car}}(sh, sk'_{car}, pk'_{car}, ECDSA_{sk_{TA}}(sh, sk'_{car}, pk'_{car}))$ 给车辆。

3）LBSP 获取到 B_2 后，使用 sk_{LBSP} 解密 B_2 并使用 pk_{TA} 验证成功后获取 $sh, stime$。

4）车辆使用 sk_{car} 解密 B_3 并验证成功后获取 sh，若其中含有 sk'_{car}, pk'_{car}，则更新 TPD 中的自身公私钥对。

5.2.5 环签名阶段

由于环签名具有无条件匿名性和自发性的特点[10]，适用于面向车联网的 LBS 隐私保护，可用于实现车辆身份的匿名性，因此，本文改进了 SM2 环签名方案[29]，提出了一种改进的环签名方案，解决了文献[29]无法抵抗重放攻击、未能实现不可链接性等问题，使得本文方案能够实现匿名性和不可链接性，能够验证车辆合法性，并且能够抵抗推断攻击、重放攻击等恶意攻击。

本文设计的环签名方案用于在 k 匿名查询阶段和 OT 阶段对发送的消息进行签名，其具有以下特点：1）在签名过程中使用 $sh, stime$ 验证车辆身份的合法性；2）随机选取 $num-1$ 个车辆的公钥加上自己的公钥构成环成员公钥集 L 进行签名，保证了车辆身份的匿名性；3）在签名过程中产生车辆临时身份 Y 以确保消息传输的准确性，实现车辆身份的不可链接性[5,10]，抵抗推断攻击；4）在签名过程中生成时间戳 $vtime_1$，其为车辆发送消息的时间，通过 LBSP 验证以防止重放攻击。

本阶段把环签名分为环签名生成算法 3 和环签名验证算法 4。假设请求车辆的公钥 pk_{car} 排在 L 中的第 z 个位置，则令 $pk_z = pk_{car}$，其对应私钥 $sk_z = sk_{car}$。算法 3 和算法 4 的具体描述如下。

算法 3 环签名生成算法

输入：要签名的消息 C，num，L，(pk_z, sk_z)，H，sh

输出：环签名值 sig

1. 生成时间戳 $vtime_1$，选择随机数 $u \in Z_q^*$，计算 $c_{z+1} = H(sh, L, Y, C, vtime_1, uP_0)$，其中 Y 为随机数，$Y \in Z_q^*$；
2. 选择 num−1 个随机数 $f_i \in Z_q^*$，其中 $i = 1, 2, \cdots, z-1, z+1, \cdots, num$，然后计算 $A_i = f_i P_0 + pk_i c_i$；
3. 计算 $c_{i+1} = H(sh, L, Y, C, vtime_1, A_i)$，并且记 $c_1 = c_{num+1}$；

4. 计算 $f_z=u-sk_z c_z \bmod q$，生成签名 $sig=(c_1,f_1,\cdots,f_{num},Y,vtime_1,H(sh))$。

算法 4 环签名验证算法

输入：sig，L，C，H，LBSP 的秘密值 sh′及对应 stime，秘密值有效期 Δstime

输出：回复值 ack

1. if $H(sh')=H(sh)$ and $vtime_1-stime<\Delta stime$
2. 对于 $1\leqslant i\leqslant num$，计算 $c_{i+1}=H(sh',L,Y,C,vtime_1,f_iP_0+pk_ic_i)$；
3. 若 $c_1=c_{num+1}$，则验证成功，返回 ack=1，否则返回 ack=0；
4. end if

5.2.6 *k* 匿名查询阶段

当表 3 公布后，车辆从表 3 中提取出全部的路段索引并存入 OBU 中。在执行 *k* 匿名查询阶段时，从 OBU 中获取 $k-1$ 个路段索引与当前路段索引构成匿名集。由于该匿名集从车辆自身的 OBU 选取而非从其他车辆获取，因此，该 *k* 匿名适用于车辆移动速度快、车辆与车辆之间无线连接时间短的车联网场景。

为了便于 LBSP 区分车辆发起的是 *k* 匿名查询阶段还是 OT 阶段，本文设定一个 *way* 值。当执行 *k* 匿名查询阶段时，令 *way*=1；当执行 OT 阶段时，令 *way*=2。*k* 匿名查询阶段的具体描述如下：

1）车辆发起 *k* 匿名路段查询

(1)令 *way*=1，车辆选择一个随机数 $ck\in Z_q^*$，计算 $car\_key=ck*P$。

(2)从 OBU 中随机选择不同于 *edge_id* 的 $k-1$ 个路段索引 $\{\theta_1,\cdots,\theta_{k-1}\}$ 与当前路段索引 *edge_id* 构成匿名集 $\theta list=\{\theta_1,\cdots,\theta_{k-1},edge\_id\}$（$\theta list$ 中 *edge_id* 的位置随机），采用 pk_{LBSP}，使用 SM2 公钥加密算法对 $\theta list$，*way*，*car_key* 加密，即 $C_1=SM2E_{pk_{LBSP}}(\theta list,way,car\_key)$。

(3)随机选择 $num-1$ 个车辆公钥加上自己的公钥构成公钥集 $L_1=(pk_1,pk_2,\cdots,pk_{num})$（$pk_{car}\in L_1$）。之后使用算法 3 对 C_1 签名后得到 sig_1，发送 $D_1=\{sig_1,C_1,L_1\}$ 给 LBSP。

2）LBSP 返回路段兴趣点查询结果

(1)在收到车辆发送的 D_1 后，验证 $ltime_1-vtime_1\leqslant\Delta time_1$ 是否成立，其中 $ltime_1$ 为 LBSP 收到 D_1 的时间，$\Delta time_1$ 为最大容忍时间。若成立，表明消息未遭受重放攻击，执行下一步；否则，终止连接。

(2)使用算法 4 验证签名 D_1，若 *ack* 为 1，则表明验证成功，说明车辆已经在 TA 中注册过，是合法车辆并且消息未被篡改，得到请求车辆的临时身份 *Y*，否则终止连接。验证成功后用 sk_{LBSP} 解密 C_1，获取 $\theta list$，*way*，*car_key*。

(3)由于 *way*=1，因此，检索表 2，查询 $\theta list$ 中所有路段的兴趣点信息，并将其加入 *k* 匿名路段的兴趣点信息集 θ_poi 中。

(4)将 θ_poi 编码到 *G* 中，为 θ_gpoi，计算 $lbsp\_\theta=car\_key\oplus\theta\_gpoi$。

(5)设置时间戳 $ltime_2$，用 ECDSA 对 $lbsp\_\theta$ 签名后得到 $ES_1=ECDSA_{sk_{LBSP}}(lbsp\_\theta,Y,ltime_2)$，把 $F_1=\{lbsp\_\theta,Y,ltime_2,ES_1\}$ 广播给车辆。

3）车辆获取路段兴趣点查询结果

(1)车辆 *car* 获取到 F_1 后，验证 $ltime_2-vtime_2\leqslant\Delta time_2$ 是否成立，其中 $vtime_2$ 为车辆收到 F_1 的时间，$\Delta time_2$ 为最大容忍时间。若成立，则使用 pk_{LBSP} 验证签名 ES_1，若验证成功，表明该消息确实来自于 LBSP，且消息未被篡改，执行下一步；否则，终止连接。

(2)比较自身的 *Y* 与获取的 *Y* 是否相等，若不相等，说明该兴趣点信息不是 LBSP 回应给 *car* 的，*car* 不应使用，否则将得到错误的兴趣点信息；若相等，则使用 *car_key* 计算 $\theta\_gpoi=car\_key\oplus lbsp\_\theta$，然后解码出 θ_poi，并从 θ_poi 中提取出 *edge_id* 路段的所有兴趣点信息 *edge_poi*，之后根据 $\varphi list_0$ 求出所需类型的兴趣点信息 *edge_tpoi* 以及对应的兴趣点类型索引集 $\varphi list_1$。

5.2.7 OT 阶段

本阶段使用锚点技术[9]，车辆以当前路段的前方顶点为锚点，并以此替代车辆真实位置提交查询请求，保护了车辆用户的位置隐私。

本阶段对文献[30-31]的 *k*-out-of-*n* OT 协议进行改进，解决了其中存在的合谋攻击、接收方无法从发送方得到查询信息，以及计算代价较高等问题，使其适用于多种类型 KNN 兴趣点并行查询的场景。改进的 *k*-out-of-*n* OT 协议一方面实现了多种类型 KNN 兴趣点的并行查询；另一方面，LBSP 在不清楚车辆提交的具体兴趣点类型的情况下，返回该锚点的全部 KNN 兴趣点，车辆用户仅能获取其提交的 *t_count* 种兴趣点，而不能获取其他兴趣点，有效保护了车辆用户的查询内容隐私和 LBSP 的兴趣点信息隐私。

由于车辆提交的兴趣点类型索引以及近邻个数是由前方顶点对应的数据决定的，因此，执行 OT 阶段后可以得到查询的兴趣点信息。

假设执行 OT 阶段的锚点为 *anchor_id*，*anchor_id* 对应的兴趣点类型索引为 $\Gamma=\{\tau_1,\tau_2,\cdots,\tau_N\}$，近邻数为 K'，兴趣点类型数为 t_count'，查询的兴趣点类型索引集为 $\varphi list_5=(\varphi_1,\varphi_2,\cdots,\varphi_{t\_count'})$（$1\leqslant t\_count'\leqslant N$）。其中，$\varphi list_5\subset\Gamma$，$\varphi_i\in\Gamma$，执行以下 3 个步骤获取兴趣点信息。

1）车辆生成查询请求

(1)随机选择 t_count' 个值 $s_i\in Z_q^*$，根据 $\varphi list_5=(\varphi_1,\varphi_2,\cdots,\varphi_{t\_count'})$（$1\leqslant t\_count'\leqslant N$），计算 $\beta_{\varphi_i}=s_iP_1+\varphi_iP_2$（$1\leqslant i\leqslant t\_count'$）。

(2)随机选择 $N-t\_count'$ 个值 $w_j\in Z_q^*$，计算 $\beta_j=w_jP_3$，其中 $j\in\Gamma$ 且 $j\neq\varphi_i$。

(3)令 *way*=2，采用 pk_{LBSP}，使用 SM2 公钥加密算法对 *anchor_id*，$\beta_{\tau_1},\cdots,\beta_{\tau_N}$，$K'$，*way* 加密，即 $C_2=SM2E_{pk_{LBSP}}(anchor\_id,\beta_{\tau_1},\cdots,\beta_{\tau_N},K',way)$。

(4)生成环成员公钥集 $L_2=(pk_1,pk_2,\cdots,pk_{num})$（$pk_{car}\in L_2$），然后使用算法 3 对 C_2 进行签名后得到 sig_2，发送 $D_2=\{sig_2,C_2,L_2\}$ 给 LBSP。

2）LBSP 发送兴趣点信息给车辆

(1)在收到车辆发送的 D_2 后，验证 $ltime_3-vtime_3\leqslant\Delta time_3$ 是否成立，其中 $ltime_3$ 为 LBSP 收到 D_2 的时间，$\Delta time_3$ 为最大容忍时间，$vtime_3$ 为环签名的时间。若成立，则使用算法 4 验证签名 D_2，若 *ack* 为 1，则表明验证成功，得到

请求车辆的临时身份 Y；否则终止连接。验证成功后用 sk_{LBSP} 解密 C_2 获取 $anchor\_id, \beta_{\tau_1}, \cdots, \beta_{\tau_N}, K', way$。

(2)由于 $way=2$，因此检索表 2，查询以 $anchor\_id$ 为路段起始顶点的兴趣点信息集 $start\_vn\_poi$，$start\_vn\_poi$ 包括兴趣点类型名称以及前 K 个近邻兴趣点集($K \leqslant n_j$，每种类型的 KNN 兴趣点为该类型的兴趣点按照与 $anchor\_id$ 的路网距离从小到大排序后的前 K 个兴趣点)。

(3)将 $start\_vn\_poi$ 中的信息按照兴趣点类型依次编码到 G 中，分别为 $M_{\tau_1}, M_{\tau_2}, \cdots, M_{\tau_N}$，之后随机选择 N 个值 $k_i \in Z_q^*$ $(i \in \Gamma)$，计算 $(a_i, b_i) = (k_i P_1, M_i + k_i(\beta_i - iP_2))(i \in \Gamma)$。

(4)设置时间戳 $ltime_4$，用 ECDSA 签名 $a_{\tau_1}, \cdots, a_{\tau_N}, b_{\tau_1}, \cdots, b_{\tau_N}, Y, ltime_4$ 得 $ES_2 = ECDSA_{sk_{LBSP}}(a_{\tau_1}, \cdots, a_{\tau_N}, b_{\tau_1}, \cdots, b_{\tau_N}, Y, ltime_4)$，广播 $F_2 = \{a_{\tau_1}, \cdots, a_{\tau_N}, b_{\tau_1}, \cdots, b_{\tau_N}, Y, ltime_4, ES_2\}$ 给车辆。

3)车辆提取兴趣点信息

(1)车辆获取到 F_2 后，验证 $ltime_4 - vtime_4 \leqslant \Delta time_4$ 是否成立，其中 $vtime_4$ 为车辆收到 F_2 的时间，$\Delta time_4$ 为最大容忍时间。若成立，则执行下一步；否则，终止连接。

(2)使用 pk_{LBSP} 验证签名 ES_2，若验证成功，则比较自身的 Y 与获取的 Y 是否相等。若不相等，则丢弃该信息；若相等，则使用 (s_i, φ_i) 计算请求的兴趣点信息查询结果 $M_{\varphi_i} = b_{\varphi_i} - s_i a_{\varphi_i}$ $(1 \leqslant i \leqslant t\_count')$，然后解码成 t_count' 个不同种类的 KNN 兴趣点查询结果集 OT_poi。

5.3 MTKNN-MPP 方案流程

本节介绍 MTKNN-MPP 方案流程，流程图如图 3 所示，算法如算法 5 所示。

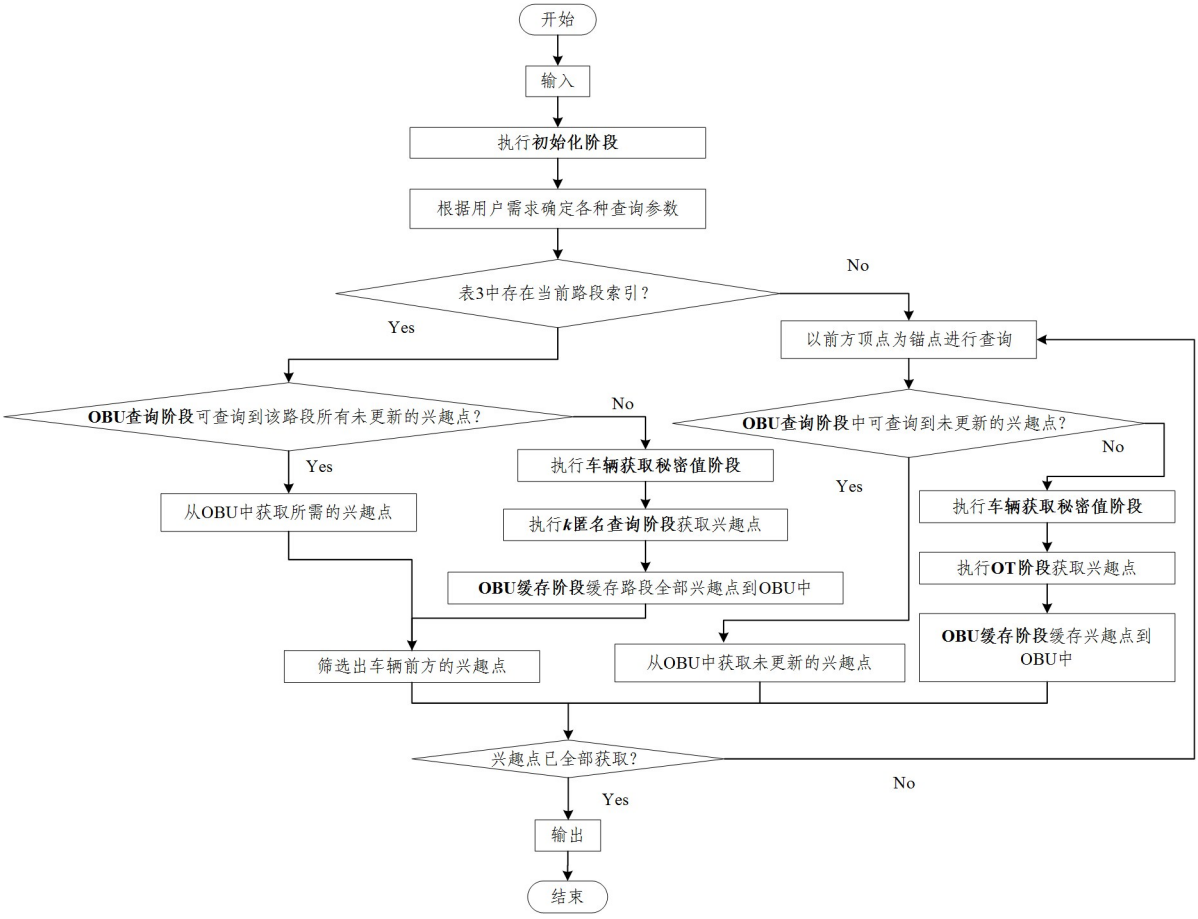


图 3 保护两方隐私的多类型的路网 K 近邻查询方案流程图

Fig. 3 Flowchart of multi-type K-nearest neighbor query scheme with mutual privacy-preserving in road networks

算法 5 MTKNN-MPP 方案

输入：t_count，PT，K，k

输出：用户查询结果集 user_poi，其包括所需的 t_count 种 KNN 兴趣点

1. 执行初始化阶段；
2. OBU 根据(t_count，PT，K，k)，确定(loc_{car}，edge_id，v_n，$\varphi list_0$)；
3. if 表 3 中存在 edge_id
4. 令路段索引为 edge_id，兴趣点类型索引集为 $\varphi list_0$，执行算法 1 获取 edge_tpoi 和 $\varphi list_1$；
5. if edge_tpoi=Ø
6. 执行车辆获取秘密值阶段；
7. 执行 k 匿名查询阶段获取 edge_poi，edge_tpoi 和 $\varphi list_1$；
8. 执行 OBU 缓存阶段将 edge_poi 缓存到 OBU 中；
9. end if
10. 调用算法 6 得到集合 r_gpoi 和 $\varphi list_2$；
11. 调用算法 7 得到 $\varphi list_3$ 以及 K′；
12. if $\varphi list_3 \neq \emptyset$
13. 令锚点为 v_n，兴趣点类型索引集为 $\varphi list_3$，近邻个数为 K′；
14. 执行算法 2 得到 OBU_poi 以及 $\varphi list_4$；
15. end if
16. 令 $\varphi list_5 \subset \varphi list_3$，且 $\varphi list_5 \cap \varphi list_4 = \emptyset$；
17. if $\varphi list_5 \neq \emptyset$
18. 执行车辆获取秘密值阶段；

19. 令锚点为 v_n，兴趣点类型索引集为 $\varphi list_5$，近邻个数为 K′，执行 OT 阶段获取 OT_poi；
20. 执行 OBU 缓存阶段，将 OT_poi 缓存到 OBU 中；
21. end if
22. 令 user_poi=r_gpoi∪OBU_poi∪OT_poi；
23. end if
24. if 表 3 中不存在 edge_id
25. 令锚点为 v_n，近邻个数 K′=K，兴趣点类型索引集 $\varphi list_3=\varphi list_0$，执行 14－21 步，得到集合 OBU_poi，OT_poi，然后令 user_poi=OBU_poi∪OT_poi；
26. end if

具体流程描述如下：

1）车辆用户查询 KNN 兴趣点前需执行初始化阶段，在 TA 中注册以获取车辆的公私钥对，即算法 5 第 1 行。

2）车辆用户把计划查询的兴趣点类型集 PT、类型个数 t_count、近邻个数 K 以及匿名数 k 发送给 OBU，OBU 确定车辆当前位置 loc_{car}、当前所处路段索引 $edge\_id$、前方顶点 v_n 以及兴趣点类型索引集 $\varphi list_0$，即算法 5 第 2 行。

3）车辆行驶到前方顶点的这段路程分布的兴趣点是离车辆最近的，因此车辆首先查看这段路程中是否存在兴趣点，即车辆查询 $edge\_id$ 在表 3 是否存在，若存在，则证明路段 $edge\_id$ 中分布了兴趣点，车辆行驶前方可能存在兴趣点，则需执行 OBU 查询阶段的算法 1，从 OBU 中获取当前路段的所需兴趣点信息 $edge\_tpoi$ 以及对应的兴趣点类型索引集 $\varphi list_1$，即算法 5 第 3－4 行。

4）若 $edge\_tpoi$ 为空，说明 OBU 中未存储 $edge\_id$ 路段的兴趣点信息，或者该路段的兴趣点信息已经发生了变化，可能新增、删除或更新了某些兴趣点信息。此时需首先执行车辆获取秘密值阶段，向 TA 获取秘密值 sh，然后执行 k 匿名查询阶段，向 LBSP 获取该路段的所有兴趣点信息 $edge\_poi$、所需类型的兴趣点信息 $edge\_tpoi$ 以及对应的兴趣点类型索引集 $\varphi list_1$。之后执行 OBU 缓存阶段，将 $edge\_poi$ 缓存到 OBU 中，以便后续从 OBU 中获取兴趣点，降低计算代价和通信开销，即算法 5 第 5－9 行。

5）在获取到 $edge\_tpoi$ 和 $\varphi list_1$ 后，需执行算法 6 筛选出车辆行驶前方的兴趣点信息 r_gpoi 以及对应的兴趣点类型索引集 $\varphi list_2$。为了提高查询准确率，需在算法 6 中设置距离阈值 Δd_r，避免查询完成时车辆已超越原先获取的前方兴趣点，即算法 5 第 10 行。

6）在获取到 r_gpoi 和 $\varphi list_2$ 后，需执行算法 7 得到尚未获取的兴趣点类型索引集 $\varphi list_3$ 以及新的近邻个数 K'，即算法 5 第 11 行。若 $\varphi list_3$ 不为空，表明还存在未获取的兴趣点信息，则令锚点为 v_n，兴趣点类型索引集为 $\varphi list_3$，近邻个数为 K'，即算法 5 第 12－13 行。

7）执行 OBU 查询阶段的算法 2，从 OBU 中获取 OBU 查询结果集 OBU_poi 以及兴趣点类型索引集 $\varphi list_4$，即算法 5 第 14－15 行。

8）在获取到 OBU_poi 和 $\varphi list_4$ 后，需把属于 $\varphi list_3$ 而不属于 $\varphi list_4$ 的类型索引加入新的类型索引集 $\varphi list_5$ 中，其为目前尚未获取的兴趣点对应的类型索引集。由于算法 2 设定找到 K' 个或 0 个兴趣点，因此，尚未找到的兴趣点类型对应的近邻个数为 K' 个。若 $\varphi list_5$ 非空，则首先执行车辆获取秘密值阶段，向 TA 获取更新的 sh，然后需使用 $\varphi list_5$ 和 K' 执行 OT 阶段，从 LBSP 中获取尚未得到的兴趣点信息，即 OT 查询结果集 OT_poi，之后执行 OBU 缓存阶段，将查询结果缓存到 OBU 中，即算法 5 第 16－21 行。

9）将以上查询结果 r_gpoi，OBU_poi，OT_poi 去除重复兴趣点后加入用户查询结果集 $user\_poi$ 中，即算法 5 第 22 行。

10）若表 3 中不存在 $edge\_id$，代表该路段并没有分布兴趣点，则令锚点为 v_n，近邻个数 $K'=K$，兴趣点类型索引集 $\varphi list_3=\varphi list_0$，执行 7）－8）步，获取集合 OBU_poi 和 OT_poi，查询结束后直接把 OBU_poi，OT_poi 中的兴趣点信息加入 $user\_poi$ 中，即算法 5 第 24－26 行。

算法 6 筛选车辆行驶前方兴趣点

输入：loc_{car}，Δd_r，v_n，K，该路段所需类型的兴趣点集合 edge_tpoi＝$\{1\leqslant j\leqslant t_n \mid m_{\varphi_j}\}$，其中，$t_n$ 表示 edge_tpoi 的兴趣点类型个数，m_{φ_j} 表示每种类型的兴趣点集合，poi∈m_{φ_j} 表示该类型的一个兴趣点

输出：r_gpoi，已获取兴趣点的类型索引集 $\varphi list_2$

1. 定义一个 count 集合，记录每种类型的兴趣点数量，并初始化为 0；
2. for 每种类型 $m_{\varphi_j}\in$ edge_tpoi
3. for 每个兴趣点 poi∈m_{φ_j}
4. if $d_r(poi,v_n)\leqslant d_r(loc_{car},v_n)-\Delta d_r$
5. if φ_j 的兴趣点数量 $count_{\varphi_j}<K$
6. 把 poi 放入集合 r_gpoi 中；
7. $count_{\varphi_j}++$；
8. end if
9. end if
10. end for
11. end for
12. 把 r_gpoi 中对应的兴趣点类型索引加入 $\varphi list_2$ 中。

算法 7 计算新兴趣点类型索引集 $\varphi list_3$ 以及新近邻个数 K′

输入：已获取的兴趣点类型索引集 $\varphi list_2$，用户查询的兴趣点类型索引集 $\varphi list_0$，近邻个数 K

输出：尚未得到 K 个兴趣点的类型索引集 $\varphi list_3$，新的近邻个数 K′

1. 定义字典 get_type，其键为 $\varphi list_2$ 中的兴趣点类型索引，值为该类型索引对应的兴趣点个数；
2. 定义字典 nget_type，其键为 $\varphi list_0$ 中的兴趣点类型索引，其值赋值为 K；
3. 遍历 get_type 与 nget_type 的键；
4. if $get\_type.key_i=nget\_type.key_j$
/ * 两个字典的某两个键相等 * /
5. $nget\_type[key_j]=K-get\_type[key_i]$；
6. end if
7. 删除 nget_type 中值为 0 的键值对；
8. K′=max(nget_type.values())；
/ * nget_type 中值的最大值即为 K′ * /
9. $\varphi list_3$=nget_type.keys()。

6 安全性分析

本文采用安全多方计算领域中的理想-现实模拟范式[32]来进行安全性分析，将现实世界映射到理想世界。理想世界具有理想函数 $\mathcal{F}$、模拟器 sim 和理想敌手 $ideal\_adv$，其中 $\mathcal{F}$

是一个完全可信的第三方，能正确地完成协议所执行的功能[33]。理想世界的物理信道是安全的，$ideal\_adv$ 仅能观察发送的信息[11]，对于能力为多项式时间的真实敌手 $real\_adv$，总是存在一个能力为多项式时间的理想敌手 $ideal\_adv$，使得真实协议 π 与 $real\_adv$ 间交互的输出结果（现实世界）和理想函数 $\mathcal{F}$ 与 $ideal\_adv$ 间交互的输出结果（理想世界）在计算上不可区分，则证明协议是安全的。

本章从匿名性、保护车辆用户的位置隐私、保护车辆用户的查询内容隐私、保护 LBSP 的兴趣点信息隐私、不可链接性和抵抗恶意攻击 6 个方面对 MTKNN-MPP 方案进行安全性分析（其中，$VIEW_{\text{real}}()$ 表示 $real\_adv$ 观察结果，$VIEW_{\text{ideal}}()$ 表示 $ideal\_adv$ 观察结果）。

1）匿名性

MTKNN-MPP 方案保证了车辆身份的匿名性。

证明：假设 LBSP 为 $real\_adv$，其试图识别车辆的身份。OT 阶段以及 k 匿名查询阶段使用环签名时 LBSP 获取到了 sig，此时 sim 在理想世界中模拟 LBSP，其随机选择 Y'，$vtime_1'$，$f_i' \in Z_q^*$，计算 $c'_{i+1}=H(sh,L,Y',C,vtime_1',f_i'P_0+pk_ic_i')$，获取 $sig'=(c_1',f_1',\cdots,f_{num}',Y',vtime_1',H(sh))$。由于 Y' 与 Y 是随机选择得到的，因此 $VIEW_{\text{real}}(Y)$ 与 $VIEW_{\text{ideal}}(Y')$ 在计算上不可区分；又由于哈希函数具有单向性，因此 $VIEW_{\text{real}}(sig)$ 与 $VIEW_{\text{ideal}}(sig')$ 在计算上不可区分；此外，Y 为车辆临时身份而非真实身份，且使用 num 个公钥形成公钥集进行签名。因此，MTKNN-MPP 方案保证了车辆身份的匿名性。

2）保护车辆用户的位置隐私

LBSP 无法根据车辆提交的请求信息推断出车辆用户的位置隐私。

证明：假设 LBSP 为 $real\_adv$，sim 在理想世界中模拟 LBSP。当执行 OT 阶段时，由于使用了锚点技术，因此 $real\_adv$ 与 sim 可以得到 $anchor\_id$。尽管 $VIEW_{\text{real}}(anchor\_id)$ 与 $VIEW_{\text{ideal}}(anchor\_id)$ 在计算上是可以区分的，但它们通过 $anchor\_id$ 仅能获取路网顶点位置，而无法获取车辆的当前位置。此外，若多辆车均以 $anchor\_id$ 发起查询请求，则 $real\_adv$ 与 $ideal\_adv$ 无法据此推断出各车辆的当前真实位置，因此实现了车辆用户的位置隐私保护。当执行 k 匿名查询阶段时，$real\_adv$ 与 sim 可以获取到 k 个路段索引，这 k 个路段索引在计算上不可区分。尽管推断出车辆所处真实路段的概率为 $1/k$，但该路段上仍存在其他车辆，且 OBU 查询阶段、OT 阶段的存在降低了 k 匿名查询阶段的执行概率，车辆用户位置隐私泄露的概率远远低于 $1/k$，该隐私保护程度已满足了用户的需求。因此，MTKNN-MPP 方案有效保护了车辆用户的位置隐私。

3）保护车辆用户的查询内容隐私

LBSP 无法获取车辆用户查询的兴趣点类型，也无法推断出车辆用户的其他隐私信息，在 k 匿名查询阶段仅能返回 k 个路段上的所有兴趣点信息给车辆，在 OT 阶段仅能返回路网顶点全部的兴趣点信息给车辆，保护了车辆用户的查询内容隐私。

证明：在 OT 阶段使用了改进的 k-out-of-n OT 协议，基于椭圆曲线的点加运算规则，$\beta_{\varphi_i}=s_iP_1+\varphi_iP_2$（$1\leqslant i\leqslant t\_count'$）中的 β_{φ_i} 与 $\beta_j=w_jP_3$（$j\in\Gamma$ 且 $j\neq\varphi_i$）中的 β_j 共有 N 个，两者在计算上不可区分。假设此时 LBSP 为 $real\_adv$，其获取到了信息 $\beta_{\tau_1},\cdots,\beta_{\tau_N}$，此时 sim 在理想世界中模拟 LBSP，其随机选择 $w_j',s_i',\varphi_i' \in Z_q^*$，计算 $\beta_{\varphi_i'}=s_i'P_1+\varphi_i'P_2$，$\beta_j'=w_j'P_3$，获取 $\beta_{\tau_1}',\cdots,\beta_{\tau_N}'$。由于 t_count' 不可知，因此 φ_i' 的个数也不可知，仅能确定 φ_i' 与 j 的总个数为 N。此外，由于椭圆曲线离散对数困难问题，$real\_adv$ 无法根据 $\beta_{\tau_1},\cdots,\beta_{\tau_N}$ 计算出 φ_i，且 $VIEW_{\text{real}}(\beta_{\tau_1},\cdots,\beta_{\tau_N})$ 与 $VIEW_{\text{ideal}}(\beta_{\tau_1}',\cdots,\beta_{\tau_N}')$ 在计算上不可区分。k 匿名查询阶段 LBSP 获取了 k 个路段索引，返回 k 个路段所具有的全部兴趣点信息，不知道车辆用户查询的具体兴趣点类型。因此，MTKNN-MPP 方案保护了车辆用户的查询内容隐私。

4）保护 LBSP 的兴趣点信息隐私

车辆用户仅能获取请求的兴趣点信息，而不能获取尚未请求过的兴趣点信息，保护了 LBSP 的兴趣点信息隐私。

证明：在 OT 阶段中，假设此时车辆为 $real\_adv$，其获取到了信息 (a_i,b_i)（$1\leqslant i\leqslant N$）以及部分兴趣点查询结果 M_{φ_j}（$\varphi_j\in\varphi list_5$），此时 sim 在理想世界中模拟车辆，其使用 φ_j' 计算 $M_{\varphi_j'}=b_{\varphi_j'}-s_ja_{\varphi_j'}$。由于 $s_j\in Z_q^*$ 为随机数，基于椭圆曲线离散对数困难问题及椭圆曲线点加运算规则，$VIEW_{real}(M_{\varphi_j})$ 与 $VIEW_{ideal}(M_{\varphi_j'})$ 在计算上不可区分。若此时 $\varphi_j'\notin\varphi list_5$，由于在 $(a_i,b_i)=(k_iP_1,M_i+k_i(\beta_i-iP_2))$（$i\in\Gamma$）中，$\beta_{\tau_1},\cdots,\beta_{\tau_N}$ 来自于 $\beta_j=w_jP$（$j\in\Gamma$ 且 $j\neq\varphi_i$）与 $\beta_{\varphi_i}=s_iP_1+\varphi_iP_2$（$1\leqslant i\leqslant t\_count'$），$\varphi_i$ 是查询提交时确定的，若以 φ_j'（$\varphi_j'\notin\varphi list_5$）进行计算，$\beta_{\varphi_j'}=w_{\varphi_j'}P_3$，则 $M_{\varphi_j'}$ 将不是正确的信息。在 k 匿名查询阶段，k 值由用户自主决定，查询费用与 k 成正比[8]，用户仅能获取 k 个路段上的兴趣点信息，而无法获取其他路段的兴趣点信息。因此，MTKNN-MPP 方案保护了 LBSP 的兴趣点信息隐私。

5）不可链接性

同一车辆连续请求的临时身份不同，攻击者不能把车辆的临时身份和真实身份联系起来，因此不能推断出车辆的行驶轨迹，从而实现了不可链接性，保护了车辆的隐私。

证明：在环签名方案中，每次请求都需要生成一个随机数 Y 作为车辆的临时身份。假设此时 LBSP 为 $real\_adv$，车辆第一次请求时获取 Y，第二次请求时获取 Y'，此时 sim 在理想世界中模拟 LBSP；车辆第一次请求时获取 Y''，第二次请求时获取 Y'''，由于 $Y,Y',Y'',Y''' \in Z_q^*$ 为随机数，因此 $VIEW_{\text{real}}(Y)$，$VIEW_{\text{real}}(Y')$，$VIEW_{\text{ideal}}(Y'')$ 和 $VIEW_{\text{ideal}}(Y''')$ 在计算上都是不可区分的，且 Y,Y',Y'' 和 Y''' 互不相同，实现了不可链接性。由于使用了环签名，车辆执行 k 匿名查询阶段与执行 OT 阶段的临时身份 Y 不同，$real\_adv$ 无法确定这两次查询是否是同一个车辆。因此，MTKNN-MPP 方案实现了不可链接性。

6）抵抗恶意攻击

MTKNN-MPP 方案能够抵抗重放攻击、推断攻击、中间人攻击、合谋攻击等恶意攻击。

证明：假设 $real\_adv$ 为多项式时间外部攻击者，$ideal\_$

adv 为理想世界中的多项式时间攻击者，MTKNN-MPP 方案中的秘密值不同且具有时效性，未注册的非法车辆截取的秘密值无法从 LBSP 获取兴趣点信息，此外，在环签名阶段中使用了时间戳，因此 MTKNN-MPP 方案有效抵抗了重放攻击。由于使用了环签名，$real\_adv$ 无法根据临时身份推断出车辆的身份，MTKNN-MPP 方案有效抵抗了推断攻击。在信道中传输信息时，由于使用了 SM2 公钥加密算法，则 $VIEW_{real}(B_1)$ 与 $VIEW_{ideal}(B_1')$、$VIEW_{real}(B_2)$ 与 $VIEW_{ideal}(B_2')$、$VIEW_{real}(B_3)$ 与 $VIEW_{ideal}(B_3')$、$VIEW_{real}(C_1)$ 与 $VIEW_{ideal}(C_1')$、$VIEW_{real}(C_2)$ 与 $VIEW_{ideal}(C_2')$ 在计算上均不可区分；由于椭圆曲线离散对数困难问题和哈希函数的单向性，因此 $VIEW_{real}(D_1)$ 与 $VIEW_{real}(D_1')$、$VIEW_{real}(D_2)$ 与 $VIEW_{real}(D_2')$ 在计算上均不可区分；由于使用了 ECDSA 以及借助椭圆曲线离散对数困难问题，则 $VIEW_{real}(F_1)$ 与 $VIEW_{ideal}(F_2')$、$VIEW_{real}(F_2)$ 与 $VIEW_{ideal}(F'_2)$ 在计算上均不可区分，从而说明 $real\_adv$ 无法识别或伪造信道中传输的消息，MTKNN-MPP 方案有效抵抗了中间人攻击。两个未注册的非法车辆由于未向 TA 获取秘密值，因此无法从 LBSP 中获取兴趣点信息；此外，车辆遵守协议规则，不会与其他车辆共享兴趣点信息。故 MTKNN-MPP 方案有效抵抗了合谋攻击，保护了 LBSP 的兴趣点信息隐私。因此，MTKNN-MPP 方案能够抵抗重放攻击、推断攻击、中间人攻击、合谋攻击等恶意攻击。

7 性能评估

由于 MTKNN-MPP 方案为面向路网空间设计的多类型的 KNN 查询方案，则本文选取的对比方案应为支持指定兴趣点类型的 KNN 查询方案，因此，本文从相关工作中选取文献[9]和文献[11]的 T-KNN 方案作为对比方案。两者均支持单一类型的 KNN 查询，不同之处在于文献[9]面向路网空间设计，而文献[11]的 T-KNN 方案面向欧氏空间设计(以下文献[11]均指文献[11]的 T-KNN 方案)。本章将从计算代价、通信开销、查询延迟、安全性等方面对 MTKNN-MPP 方案、文献[9]及文献[11]进行性能分析与对比。

7.1 计算代价

7.1.1 计算代价分析

计算代价由两部分构成：一部分为执行椭圆曲线点乘、点加等各种密码运算的运行时间，另一部分为执行除了密码运算的其他算法的运行时间。因此本节首先介绍 MTKNN-MPP 方案、文献[9]以及文献[11]的计算复杂度，之后介绍各方案中的密码运算时间总和。

1)计算复杂度分析

MTKNN-MPP 方案的计算复杂度由判断车辆当前行驶路段是否存在兴趣点、算法 1、车辆获取秘密值阶段、k 匿名查询阶段、算法 2、OT 阶段、算法 6、算法 7 以及 OBU 缓存阶段的计算复杂度构成，分别为 $O(1)$，$O(t\_count*\eta)$，$O(1)$，$O(k*edge\_m)$，$O(t\_count*K)$，$O(N*K)$，$O(t\_count*K)$，$O(t\_count)$ 和 $O(t\_count*K)$，其中 η 表示所需类型所含兴趣点个数的最大值，$edge\_m$ 表示随机选取路段所含兴趣点的最大值，则 MTKNN-MPP 方案的计算复杂度为 $O(N*K+t\_count*(K+\eta)+k*edge\_m)$。

文献[9]的计算复杂度由从缓存中获取兴趣点信息、用户端密文查询请求生成算法、LBS 服务器端查询请求处理算法以及用户端 K 近邻兴趣点精确结果计算算法的计算复杂度构成，分别为 $O(K)$，$O(N)$，$O(N^2)$ 和 $O(N+K)$，则文献[9]的计算复杂度为 $O(N^2+K)$。

由于 MTKNN-MPP 方案划分了区域但未划分单元格，为了统一，本文把文献[11]中的格设为 1，因此，文献[11]的计算复杂度由更新兴趣点集合以找出 KNN 兴趣点的计算复杂度构成，为 $O(K^2)$。

2)密码运算时间分析

各密码运算时间的符号如表 6 所列。由于文献[9]均以 Python 语言实现，没有单独的密码运算时间，因此本文仅列了 MTKNN-MPP 方案以及文献[11]的密码运算时间。

表 6 密码运算时间的符号

Table 6 Symbols of cryptographic operation time

符号	含义
T_{EM}	椭圆曲线点乘运算 aP 的执行时间，其中 $a\in Z_q^*$，$P\in G$
T_{EA}	椭圆曲线点加运算 $P+Q$ 的执行时间，其中 $P\in G, Q\in G$
T_{SM2E}	消息原长为 2kB 的 SM2 公钥加密算法加密时间
T_{SM2D}	消息原长为 2kB 的 SM2 公钥加密算法解密时间
T_{ECDSAE}	签名原长为 4kB 的 ECDSA 签名时间
T_{ECDSAD}	签名原长为 4kB 的 ECDSA 验签时间
T_{code}	将兴趣点信息编码到 G 中的编码时间
T_{decode}	将 G 中的点解码成兴趣点信息的解码时间
$T_{dec\_CP\text{-}ABE}$	CP-ABE 算法解密时间

MTKNN-MPP 方案在车辆获取秘密值阶段、环签名阶段、k 匿名查询阶段和 OT 阶段涉及密码运算，其中车辆获取秘密值阶段的密码运算时间总和为 $3T_{SM2E}+3T_{SM2D}+2T_{ECDSAE}+2T_{ECDSAD}$，环签名阶段的密码运算时间总和为 $(4num-1)T_{EM}+(2num-1)T_{EA}$，$k$ 匿名查询阶段的密码运算时间总和为 $(4num)T_{EM}+(2num-1)T_{EA}+T_{SM2E}+T_{SM2D}+T_{ECDSAE}+T_{ECDSAD}+T_{code}+T_{decode}$，OT 阶段的密码运算时间总和为 $(4N+2t\_count'+4num-1)T_{EM}+(2N+2t\_count'+2num-1)T_{EA}+T_{SM2E}+T_{SM2D}+T_{ECDSAE}+T_{ECDSAD}+T_{code}+T_{decode}$。

将文献[11]中的乘法群转换成椭圆曲线加法群，则其密码运算时间总和为 $15T_{EM}+3T_{EA}+T_{dec\_CP\text{-}ABE}$。

7.1.2 仿真实验

本节实验采用 California 真实路网数据集[34-35]仿真实现，该数据集共有 21048 个顶点、21693 条边、106904 个兴趣点、63 种兴趣点类型。本文将 California 地图分为 3 个区域，每个区域设置一个 LBSP，并以一个 LBSP 作为研究对象，因此本文实验的 California 路网数据集规模如表 7 所列。从表中可以得出，每个路网顶点对应的兴趣点类型个数不同。本文设置实验中路网顶点对应的兴趣点类型个数 $N=10$，k 匿名路段集 $k=10$，距离阈值 $\Delta d_r=0.010$km，环成员个数在文献[36]的基础上扩充为 5，10，15，20。

表 7 实验数据集规模

Table 7 Size of experimental dataset

顶点数量	边数量	兴趣点数量	兴趣点类型数
7136	5331	26308	63

实验在个人计算机上进行，除了 T_{EM} 与 T_{EA} 在处理器为 11th Gen Intel(R) i5-8250 @ 1.8 GHz、内存大小为 8 GB 的 WINDOWS 10 操作系统上进行[37]，其余实验均采用 Python 语言在处理器为 11th Gen Intel(R) Core(TM) i5-11300H @ 3.10 GHz 2.61 GHz、内存大小为 16GB 的 WINDOWS 10 操作系统上进行。下面首先介绍单个密码运算的实现时间，然后对 MTKNN-MPP 方案与文献[9]、文献[11]的计算代价进行对比分析。

1)单个密码运算的实现时间

T_{EM} 与 T_{EA} 使用 C++语言并借助 MIRACL 数据库实现[37]。设 G 为一个阶为大质数 q、生成元为 P 的椭圆曲线加法群，其由椭圆曲线 $E:y^2=x^3-3x(\mathrm{mod}\ p)$ 上所有的点和 O 共同组成，其中，p 为 512 位，q 为 160 位，P 为128 bytes，则在 G 上实现的椭圆曲线点乘运算的运行时间 $T_{EM}\approx 4.141$ ms、点加运算的运行时间为 $T_{EA}\approx 0.033$ ms。由于普通加减法运算、异或运算以及普通哈希函数运算的运行时间相对于 T_{EM} 与 T_{EA} 可以忽略不计[7]，因此，在计算 MTKNN-MPP 方案以及文献[11]的计算代价时忽略此 3 种运算的运行时间。

MTKNN-MPP 方案使用的 ECDSA 采用 SHA256 哈希函数。根据 7.2.1 节设定的各参数长度，可以计算得出 MTKNN-MPP 方案的 ECDSA 签名原长小于 4 kB，因此 ECDSA 的运行时间采用文献[38]中签名原长为 4 kB，基于曲线 secp256k1 测试得出的时间 $T_{ECDSAE}\approx 0.370$ ms，$T_{ECDSAD}\approx 0.415$ ms。

MTKNN-MPP 方案使用的 SM2 公钥加密算法采用 SM3 哈希函数。根据 7.2.1 节设定的各参数长度，可以计算得出 MTKNN-MPP 方案需加密的消息原长小于 2 kB。因此，SM2 公钥加密算法的执行时间采用文献[38]中加密消息原长为 2 kB 测试得出的时间 $T_{SM2E}\approx 0.837$ ms，$T_{SM2D}\approx 0.431$ ms。

本文使用 Python 语言实现将兴趣点信息编码到 G 中。假设曲线 $E:y^2=x^3-3x(\mathrm{mod}\ p)$ 中 $p=502807$，将信息编码到 G 中所消耗的时间 T_{code} 与信息大小的关系以及解码该编码结果所消耗的时间 T_{decode} 如表 8 所列，表中数据均为运行 200 次的平均时间。

表 8 编码和解码运行时间

Table 8 Encoding and decoding runtime

算法运行时间/ms	T_{code}	T_{decode}
512 bytes	0.242	0.050
1 kB	0.439	0.084
2 kB	1.143	0.144
4 kB	2.904	0.205

在虚拟机中使用 Python 语言实现 CP-ABE 算法[11]，得出 CP-ABE 解密时间为 $T_{dec\_CP\text{-}ABE}\approx 4.732$ ms。

2)实验结果分析

当车辆查询一种类型 KNN 兴趣点时，即固定兴趣点类型数 $t\_count=1$，改变 K 值为 1，5，10，15，20[24]，得到查询一种类型 KNN 兴趣点时的计算代价对比，如图 4 所示。当车辆查询两种类型及以上的 KNN 兴趣点时，即固定近邻个数 $K=5$，改变 t_count 值为 2，3，4，5，6，得到查询多种类型 KNN 兴趣点时的计算代价对比，如图 5 所示。图 4 及图 5 的计算代价均为 200 次实验的平均值。

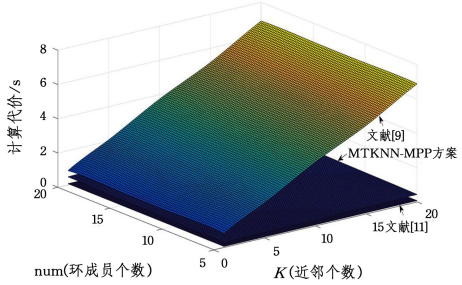


图 4 查询一种类型 KNN 兴趣点时的计算代价对比

Fig. 4 Computational cost comparison when querying a type of KNN points of interest

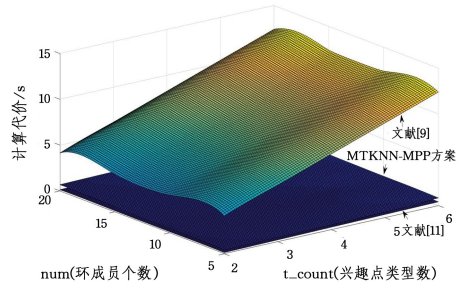


图 5 查询多种类型 KNN 兴趣点时的计算代价对比

Fig. 5 Computational cost comparison when querying multiple types of KNN points of interest

从图 4 和图 5 中可以得出，MTKNN-MPP 方案的计算代价均低于文献[9]，略高于文献[11]。然而文献[11]面向欧氏空间设计，不适用于车联网场景，而 MTKNN-MPP 方案面向路网空间设计，更加符合实际场景的需要。

7.2 通信开销

7.2.1 各参数长度设置

根据文献[37-39]，列出本文设置的各参数长度如下。

由 7.1.2 节可知，本文所使用的椭圆曲线加法群 G 的生成元 P 为 128 bytes，阶 q 为 160 位，则 G 中的元素长度为 128 bytes，Z_q^* 中的元素长度为 20 bytes，$car\_key\in G$ 长度为 128 bytes，Y，f_i，c_i，$sh\in Z_q^*$ 以及 $H:\{0,1\}^*\rightarrow Z_q^*$ 的哈希值长度均为 20 bytes[37]，ECDSA 签名值的长度为 $2*20=40$ bytes[38]，Paillier 同态加密生成的密文长度为 256 bytes[39]。

本文设定的其他参数长度：时间戳长度为 4 bytes[37]，用户假名 $u_k'\in Z_q^*$ 长度为 20 bytes，路网顶点位置 loc_{v_n} 长度为 20 bytes，char 数据类型的 way 长度为 1 bytes，int 数据类型的 K 长度为 4 bytes，car、锚点、路段索引、兴趣点类型索引、兴趣点索引、路段长度以及兴趣点距起始顶点的距离均为 varchar 数据类型，长度均为 8 bytes，因此一个兴趣点长度(即表 5 中存储的一条信息)为 $4+6*8=52$ bytes。SM2 密文字节数由待加密的消息 $len(C)$、椭圆曲线点乘值、SM3 哈希值长度(32 bytes)[38]组成，因此 SM2 的密文字节数为 $len(C)+160$ bytes。

7.2.2 通信开销分析

在 MTKNN-MPP 方案中，由于 OBU 查询阶段未与外界交互，因此通信开销产生于车辆获取秘密值阶段、k 匿名查询阶段和 OT 阶段。

1)车辆获取秘密值阶段：车辆发送给 TA 的消息为 B_1，其通信开销为 320 bytes；TA 发送给 LBSP 的消息为 B_2，其通信开销为 224 bytes。若 TA 发送给车辆的消息为 $B_3=SM2E_{pk_{car}}(sh,ECDSA_{sk_{TA}}(sh))$，则其通信开销为 220 bytes；若 TA 发送给车辆的消息为 $B_3=SM2E_{pk_{car}}(sh,sk'_{car},pk'_{car},ECDSA_{sk_{TA}}(sh,sk'_{car},pk'_{car}))$，则其通信开销为 368 bytes。取两者平均值，则 TA 发送给车辆的通信开销为 294 bytes，因此，车辆获取秘密值阶段的通信开销为 838 bytes。

2)k 匿名查询阶段：车辆发送给 LBSP 的消息为 D_1，其通信开销为 $8k+148num+353$ bytes；LBSP 发送给车辆的消息为 F_1，其通信开销为 192 bytes。因此 k 匿名查询阶段的通信开销为 $8k+148num+545$ bytes。

3)OT 阶段：车辆发送给 LBSP 的消息为 D_2，其通信开销为 $128N+148num+237$ bytes；LBSP 发送给车辆的消息为 F_2，其通信开销为 $64+256N$ bytes。因此 OT 阶段的通信开销为 $301+148num+384N$ bytes。

由于车辆从 OBU 中获取到所需兴趣点信息后将不会执行车辆获取秘密值阶段或 k 匿名查询阶段或 OT 阶段，因此 MTKNN-MPP 方案的通信开销为 $838t\_s+(8k+148num+545)t\_k+(301+148num+384N)t\_ot$，其中，$t\_s$，$t\_k$，$t\_ot$ 分别表示一次 KNN 查询中车辆获取秘密值阶段、k 匿名查询阶段、OT 阶段的执行次数。

文献[9]中，用户发送给 LBSP 的消息为 $Q=(u_k',loc_{v_n},time,K,ct)$，其中 $time$ 为发送时间，ct 表示执行了 N 次 Paillier 同态加密生成的密文，则其通信开销为 $48+256N$ bytes；LBSP 发送给用户的消息为兴趣点信息累乘结果，字节数与 Paillier 同态加密生成的密文字节数相等，则其通信开销为 256 bytes。由于用户从缓存中获取到兴趣点信息后将不会向 LBSP 查询兴趣点信息，因此文献[9]的通信开销为 $(304+256N)t\_paillier$ bytes，其中 $t\_paillier$ 表示一次查询中向 LBSP 请求兴趣点信息的次数。

文献[11]的通信开销来自于以下 3 个部分：

1)从雾节点下载某区域的兴趣点信息：设某区域的兴趣点个数为 all_poi，则通信开销为 $52all\_poi$。

2)生成 SK 隐私保护算法：车辆发送给 LBSP 的消息为哈希值，LBSP 发送给车辆的消息为 $(D,D_j,D_j')(1\leqslant j\leqslant l)$。由于本文仅考虑一个属性，因此 $l=1$，则通信开销为 $20+3*128=404$ bytes。

3)不经意密钥传输算法：经与 Liu 等[11]确认，其使用的 1-out-of-2 OT 协议参考文献[40]，通信中的 $\beta_0,\beta_1,\alpha_0,\alpha_1,r_0,r_1\in G$，则通信开销为 $128*6=768$ bytes。

因此，文献[11]的通信开销为 $52all\_poi+1172$ bytes。

7.2.3 通信开销对比分析

根据 7.1.2 节中的参数设置 $k=10$，$N=10$，$all\_poi=26308$，num 取 5，10，15，20，结合 7.2.2 节的通信开销分析，得到查询一种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[9]、文献[11]的通信开销对比，分别如图 6、图 7 所示，以及查询多种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[9]、文献[11]的通信开销对比，分别如图 8、图 9 所示。

由图 6 可知，在查询一种类型 KNN 兴趣点时，MTKNN-MPP 方案的通信开销在 $num\leqslant 10$ 时均低于文献[9]，仅在 $num>15$，$num=15(K<10)$ 时略高于文献[9]。但 MTKNN-MPP 方案保护了车辆和 LBSP 两方的隐私，能够有效抵抗合谋攻击、中间人攻击等恶意攻击，成功解决了文献[9]未能保护 LBSP 的兴趣点信息隐私且难以抵抗合谋攻击的问题。因此，MTKNN-MPP 方案以牺牲少量通信开销为代价，赢得了较高的安全性。

由图 7 可知，在查询一种类型 KNN 兴趣点时，MTKNN-MPP 方案的通信开销低于文献[11]。

由图 8、图 9 可知，在查询多种类型 KNN 兴趣点时，MTKNN-MPP 方案的通信开销均低于文献[9]和文献[11]。

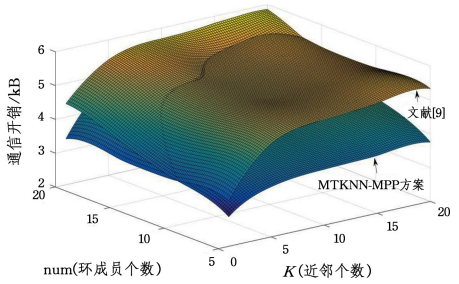


图 6 查询一种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[9]的通信开销对比

Fig. 6 Communication overhead comparison between MTKNN-MPP and reference [9] when querying a type of KNN points of interest

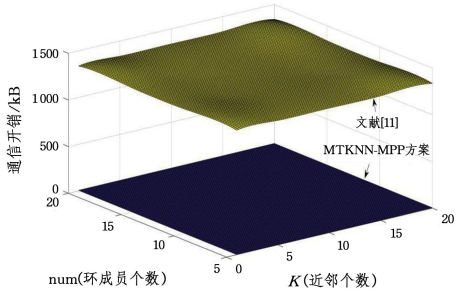


图 7 查询一种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[11]的通信开销对比

Fig. 7 Communication overhead comparison between MTKNN-MPP and reference [11] when querying a type of KNN points of interest

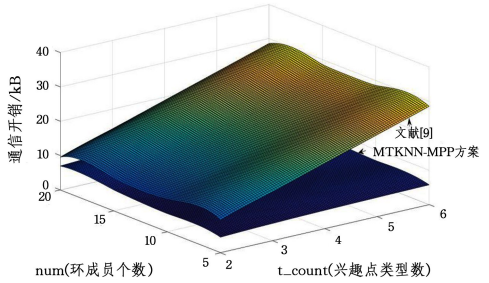


图 8 查询多种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[9]的通信开销对比

Fig. 8 Communication overhead comparison between MTKNN-MPP and reference [9] when querying multiple types of KNN points of interest

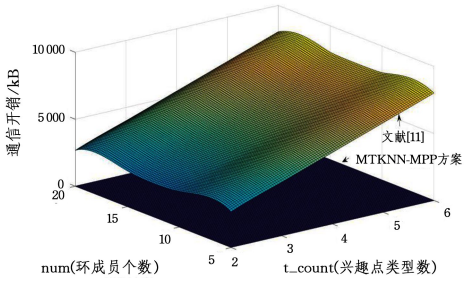


图 9 查询多种类型 KNN 兴趣点时 MTKNN-MPP 方案与文献[11]的通信开销对比

Fig. 9 Communication overhead comparison between MTKNN-MPP and reference [11] when querying multiple types of KNN points of interest

7.3 查询延迟

本文使用查询延迟[11]来评估方案的性能，该方法是 LBS 隐私保护中用于评估性能的重要指标之一。查询延迟指车辆从提交查询请求到收到兴趣点信息查询结果过程中所花费的总时间，即在线计算延迟与通信延迟的总和[11]。在线计算延迟即计算代价；通信延迟为发送时延、传播时延、处理时延以及排队时延之和。由于处理时延较小，可忽略不计，数据帧长度不影响传播时延(即每个方案具有相同的传播时延)，排队时延不确定且不影响方案查询延迟对比结果[41]，因此，本文的通信延迟不考虑处理时延、排队时延以及传播时延，仅考虑发送时延。其计算公式为数据帧长度(即通信开销)除以发送速率，则查询延迟的计算公式为：

$$\text{查询延迟}=\text{计算代价(s)}+\frac{\text{通信开销}}{\text{发送速率}}\text{(s)} \tag{1}$$

本文设置发送速率为 6 Mbit/s[5]，则根据上述计算代价和通信开销，可以得到查询一种类型 KNN 兴趣点时的查询延迟对比，如图 10 所示，以及查询多种类型 KNN 兴趣点时的查询延迟对比，如图 11 所示。

由图 10 可知，当 num 为 5，10，15，20 时，随着 K 值逐渐增大，MTKNN-MPP 方案的查询延迟增加幅度均较低，且均低于文献[9]和文献[11]。虽然 MTKNN-MPP 方案的计算代价略高于文献[11]，但其通信开销远低于文献[11]，而查询延迟由计算代价与通信开销共同决定，因此 MTKNN-MPP 方案的查询延迟低于文献[11]。

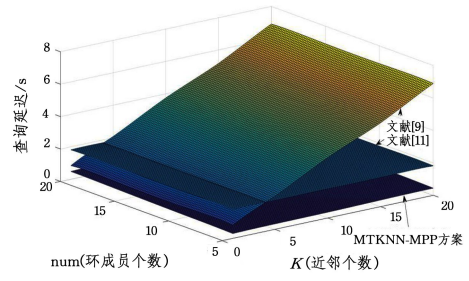


图 10 查询一种类型 KNN 兴趣点时的查询延迟对比

Fig. 10 Query latency comparison when querying a type of KNN points of interest

由图 11 可知，当 num 为 5，10，15，20 时，随着 t_count 逐渐增加，MTKNN-MPP 方案的查询延迟增加幅度均较低，均低于文献[9]和文献[11]。相比文献[9]和文献[11]，MTKNN-MPP 方案的查询延迟较低的原因在于其可以根据用户的需求支持多种类型 KNN 兴趣点的并行查询，文献[9]和文献[11]则不支持。若使用文献[9]及文献[11]查询多种类型的 KNN 兴趣点，则需要提交多次查询，进而导致计算代价、通信开销均呈倍数增加。因此，在查询多种类型 KNN 兴趣点时，MTKNN-MPP 方案的查询延迟明显低于文献[9]和文献[11]。

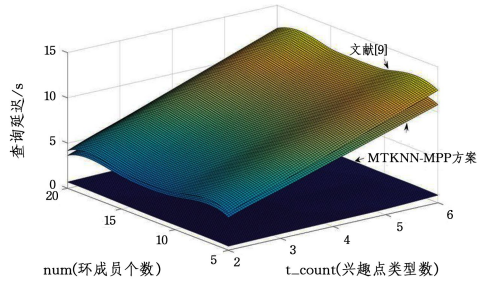


图 11 查询多种类型 KNN 兴趣点时的查询延迟对比

Fig. 11 Query latency comparison when querying multiple types of KNN points of interest

综合图 10 与图 11，MTKNN-MPP 方案相比文献[9]与文献[11]的查询延迟降低百分比如表 9 所列。其中，当 $t\_count=1$，$K=1$，$num=20$ 时，MTKNN-MPP 方案较文献[9]的查询延迟降低百分比为 $\frac{(0.835-0.474)}{0.835}\approx 43.23\%$；0.835 s与 0.474 s 分别表示在 $t\_count=1$，$K=1$，$num=20$ 时文献[9]和 MTKNN-MPP 方案的查询延迟。表 9 中的查询延迟降低百分比均以此方式计算得出。43.23%～63.36%表示当 $t\_count=1$，$K=1$，num 取 5，10，15，20 时，MTKNN-MPP 方案相比文献[9]的查询延迟降低百分比范围，表 9 中其余数据均以此方式表示。从表 9 可以得出，查询一种类型 KNN 兴趣点时，MTKNN-MPP 方案相比文献[9]和文献[11]查询延迟降低百分比分别为 43.23%～93.70%，65.61%～83.09%；同理可得，在查询多种类型 KNN 兴趣点时，MTKNN-MPP 方案相比文献[9]和文献[11]查询延迟降低百分比分别为 83.48%～93.93%，81.07%～93.04%。

表 9 MTKNN-MPP 方案查询延迟降低百分比

Table 9 Query latency reduction percentage of MTKNN-MPP

种类	文献[9]	文献[11]
$t\_count=1,K=1$	43.23%～63.36%	73.78%～83.09%
$t\_count=1,K=5$	74.55%～83.43%	70.84%～81.01%
$t\_count=1,K=10$	85.40%～90.38%	69.75%～80.07%
$t\_count=1,K=15$	88.52%～92.14%	67.14%～77.52%
$t\_count=1,K=20$	90.97%～93.70%	65.61%～76.01%
$K=5,t\_count=2$	83.48%～88.95%	81.07%～87.34%
$K=5,t\_count=3$	87.45%～91.44%	85.62%～90.20%
$K=5,t\_count=4$	89.87%～93.03%	88.39%～92.02%
$K=5,t\_count=5$	91.32%～93.93%	90.05%～93.04%
$K=5,t\_count=6$	91.20%～93.29%	89.91%～92.31%

7.4 安全性

MTKNN-MPP 方案相比文献[9]和文献[11]具有更高的安全性，安全性对比结果如表 10 所列。

表 10 MTKNN-MPP 方案与文献[9]和文献[11]的安全性对比

Table 10 Security features comparison between MTKNN-MPP and references [9,11]

	文献[9]	文献[11]	MTKNN-MPP 方案
保护用户位置隐私	√	√	√
保护用户查询内容隐私	√	√	√
保护 LBSP 的兴趣点信息隐私	×	√	√
匿名性	√	×	√
不可链接性	√	√	√
抵抗重放攻击	√	√	√
抵抗推断攻击	√	√	√
抵抗中间人攻击	√	×	√
抵抗合谋攻击	×	×	√

结束语 本文提出了一种面向路网空间设计的保护两方隐私的多类型的 KNN 查询方案 MTKNN-MPP，相比面向欧氏空间设计的 KNN 查询方案，该方案更加适用于车联网场景。MTKNN-MPP 方案使用改进的 k-out-of-n OT 协议、k 匿名、环签名技术以及锚点技术，在保证车辆与 LBSP 两方隐私的前提下实现了多种类型 KNN 兴趣点的并行查询。MTKNN-MPP 方案通过 OBU 缓存机制有效降低了查询延迟。安全性分析表明，MTKNN-MPP 方案能够抵抗重放攻击、合谋攻击、推断攻击、中间人攻击等恶意攻击，具有匿名性、不可链接性等隐私属性，能够有效保护车辆用户的位置隐私、查询内容隐私以及 LBSP 的兴趣点信息隐私。性能评估表明，与现有典型的 KNN 查询方案相比，MTKNN-MPP 方案具有更高的安全性，且在查询一种类型 KNN 兴趣点和查询多种类型 KNN 兴趣点的场景下具有更低的查询延迟。未来的工作将考虑 LBSP 计算资源和存储资源受限的问题，在兴趣点信息被外包到云服务器的场景下，设计安全的 KNN 查询方案，并进一步降低 KNN 查询方案的计算代价和通信开销。

参 考 文 献

[1] SONG T, LI X H, LI H, et al. Overview of Research on Security Encryption Authentication Technology of IoV in Big Data Era [J]. Computer Science, 2022, 49(4): 340-353.

[2] DUAN W, GU J, WEN M, et al. Emerging technologies for 5G-IoV networks: applications, trends and opportunities[J]. IEEE Network, 2020, 34(5): 283-289.

[3] TU S P, ZHANG L, LIU X P. Double Dummy Location Selection Algorithm Based on Behavior Correlation[J]. Computer Science, 2023, 50(5): 348-354.

[4] NI W W, FENG Z G, YAN D. Location Privacy Preserving Nearest Neighbor Query Method Based on Circle Distribution on Road Networks[J]. Chinese Journal of Computers, 2020, 43(8): 1385-1396.

[5] CUI J, CHEN X F, ZHANG J, et al. Bus Cache-Based Location Privacy Protection Scheme in the Internet of Vehicles[J]. Journal on Communications, 2021, 42(7): 150-161.

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

[7] CHEN S Y, LIU Y L, LIN C L, et al. Lightweight Verifiable Group Authentication Scheme for the Internet of Things[J]. Acta Electronica Sinica, 2022, 50(4): 990-1001.

[8] HU L, QIAN Y, CHEN M, et al. Proactive cache-based location privacy preserving for vehicle networks[J]. IEEE Wireless Communications, 2018, 25(6): 77-83.

[9] ZHOU C L, CHEN Y H, TIAN H, et al. Location Privacy and Query Privacy Preserving Method for K-nearest Neighbor Query in Road Networks[J]. Journal of Software, 2020, 31(2): 471-492.

[10] YADAV V K, VERMA S, VENKATESAN S. Linkable privacy-preserving scheme for location-based services[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(7): 7998-8012.

[11] LIU S S, LIU A, YAN Z, et al. Efficient LBS queries with mutual privacy preservation in IoV[J]. Vehicular Communications, 2019, 16(2019): 62-71.

[12] NI W W, LI N Q, LIU J Q. Voronoi-R* -Based Privacy-Preserving k Nearest Neighbor Query over Road Networks[J]. Journal of Software, 2019, 30(12): 3782-3797.

[13] YI X, PAULET R, BERTINO E, et al. Practical approximate k nearest neighbor queries with location and query privacy[J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(6): 1546-1559.

[14] PAILLIER P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[C]// International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT). Berlin: Springer Press, 1999: 223-238.

[15] ZHOU C L, MA C G, YANG S T. Research of LBS Privacy Preserving Based on Sensitive Location Diversity[J]. Journal on Communications, 2015, 36(4): 129-140.

[16] CHEN J, HE K, YUAN Q, et al. Blind filtering at third parties: An efficient privacy-preserving framework for location-based services[J]. IEEE Transactions on Mobile Computing, 2018, 17(11): 2524-2535.

[17] PAULET R, KAOSAR M G, YI X, et al. Privacy-preserving and content-protecting location based queries[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 26(5): 1200-1210.

[18] YADAV V K, ANDOLA N, VERMA S, et al. A survey of oblivious transfer protocol[J]. ACM Computing Surveys(CSUR), 2022, 54(10): 1-37.

[19] NI W, GU M, CHEN X. Location privacy-preserving k nearest neighbor query under user's preference[J]. Knowledge-Based Systems, 2016, 103: 19-27.

[20] JANNATI H, BAHRAK B. An oblivious transfer protocol based on elgamal encryption for preserving location privacy[J]. Wireless Personal Communications, 2017, 97(2): 3113-3123.

[21] YADAV V K, VERMA S, VENKATESAN S. Efficient and secure location-based services scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13567-13578.

[22] LIU J K, WEI V K, WONG D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups[C]// Australasian Conference on Information Security and Privacy(ACISP). Berlin: Springer Press, 2004: 325-335.

[23] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy

Attribute-Based Encryption[C]// 2007 IEEE Symposium on Security and Privacy(S&P). Piscataway: IEEE Press, 2007: 321-334.

[24] CUI N N, YANG X, WANG B, et al. SVkNN: Efficient Secure- and Verifiable k-Nearest Neighbor Query on the Cloud Platform [C]// 2020 IEEE 36th International Conference on Data Engineering(ICDE). Piscataway: IEEE Press, 2020: 253-264.

[25] CUI N N, QIAN K, CAI T T, et al. Towards multi-user, secure, and verifiable kNN query in cloud database[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(9): 9333-9349.

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

[27] SONG W, SHI C L, SHEN Y, et al. Select the Best for Me: Privacy-Preserving Polynomial Evaluation Algorithm over Road Network[C]// International Conference on Database Systems for Advanced Applications(DASFAA). Cham: Springer Press, 2019: 281-297.

[28] WANG J, WU L B, LUO M, et al. Secure and Efficient Two-Party ECDSA Signature Scheme[J]. Journal on Communications, 2021, 42(2): 12-25.

[29] FAN Q, HE D B, LUO M, et al. Ring Signature Schemes Based on SM2 Digital Signature Algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 710-723.

[30] MU Y, ZHANG J, VARADHARAJAN V. M out of n Oblivious Transfer[C]// Australasian Conference on Information Security and Privacy(ACISP). Berlin: Springer Press, 2002: 395-405.

[31] TZENG W G. Efficient 1-out-n Oblivious Transfer Schemes [C]// International Workshop on Public Key Cryptography (PKC). Berlin: Springer Press, 2002: 159-171.

[32] HAZAY C, LINDELLl Y. Efficient Secure Two-Party Protocols: Techniques and Constructions[M]. Springer Science & Business Media, 2010.

[33] ZHANG Z Y, LIU X Y, LI W H, et al. Efficient and Cooperative Secure Two-Party Computation Based on Authenticated Garbled Circuit[J]. Chinese Journal of Computers, 2022, 45(11): 2433-2455.

[34] LI F F. Real Datasets for Spatial Databases[DB/OL]. [2022-11-16]. https://www.cs.utah.edu/lifeifei/SpatialDataset.htm.

[35] LI F F, CHENG D H, HADJIELEFTHERIOU M, et al. On Trip Planning Queries in Spatial Databases[C]// International Symposium on Spatial and Temporal Databases(SSTD). Berlin: Springer Press, 2005: 273-290.

[36] CUI Y Q, CAO L, ZHANG X Y, et al. Ring Signature Based on Lattice and VANET Privacy Preservation[J]. Chinese Journal of Computers, 2019, 42(5): 980-992.

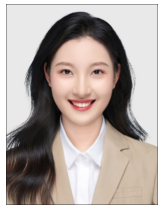
[37] CHEN S Y, LIU Y L, NING J T, et al. BASRAC: An efficient batch authentication scheme with rule-based access control for VANETs[J]. Vehicular Communications, 2023, 40: 100575.

[38] LAN X W. Optimization of ECC computation algorithms and their application in SM2 implementation[D]. Chengdu: University of Electronic Science and Technology of China, 2019.

[39] FENG Q. Research on data privacy preservation technologies using secure multi-party computation[D]. Hubei: Wuhan University of China, 2021.

[40] BELLARE M, MICALI S. Non-Interactive Oblivious Transfer and Applications[C]// Conference on the Theory and Application of Cryptology(CRYPTO). Berlin: Springer Press, 1989: 547-557.

[41] XIE X R. Computer networks[M]. Beijing: Publishing House of Electronics Industry, 2021.



ZENG Congai, born in 1999, postgraduate. Her main research interests include Internet of Vehicles security and location-based service privacy-preserving.

LIU Yali, born in 1981, Ph.D, professor, master's supervisor, is a senior member of CCF(No. 95313S). Her main research interests include information security, Internet of Things security and privacy-preserving technology, blockchain security and privacy, vehicular ad hoc networks, cryptographic algorithms and protocols as well as their applications in Internet of Things and mobile communication.

(责任编辑:杨雪敏)