面向海洋观监测传感网的移动终端位置隐私保护研究

苏新[1]，江苏[1]，周一青[2,3]
（1. 河海大学物联网工程学院，江苏 常州 231022；2. 中国科学院大学，北京 100049；3. 中国科学院计算技术研究所，北京 100190）

摘　要：移动边缘计算可支撑多类高可靠、低时延的海事应用，然而计算任务的卸载存在诸多安全隐患。为此，分析并量化了海洋移动终端由任务卸载导致的位置隐私泄露风险。建立有关位置隐私保护模型并提出一种基于动态缓存与空间匿名的位置隐私保护（DS-LPP, dynamic cache and spatial cloaking-based location privacy protection）算法。仿真结果表明，DS-LPP 算法在保护海洋移动终端位置隐私时，相比传统算法优构建匿名空间与中继节点选取性能更优，因而可有效应用于通信、计算资源相对匮乏的海洋观监测传感网，保障终端位置隐私保护连续性。

关键词：海洋观监测传感网；移动边缘计算；位置隐私保护；任务卸载
中图分类号：TN929.52
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2021.00244

Research on location privacy protection of mobile terminals for maritime monitoring sensor networks

SU Xin[1], JIANG Su[1], ZHOU Yiqing[2, 3]
1. College of Internet of Things Engineering, Hohai University, Changzhou 213022, China
2. University of Chinese Academy of Sciences, Beijing 100049, China
3. Institute of Computing Technology, Chinese Acadeny of Sciences, Beijing 100190, China

Abstract: Mobile edge computing can support various maritime applications with high reliability and low delay. However, many security problems in computing task offloading exist. The risk of location privacy leakage of maritime mobile terminals during task offloading was analyzed and quantified. The related location privacy protection model was established and a dynamic cache and spatial cloaking-based location privacy protection (DS-LPP) algorithm was proposed. Simulation results show that DS-LPP algorithm has better performance of constructing anonymous space and selecting relay node than traditional algorithms while protecting the location privacy of maritime mobile terminals. Therefore, the DS-LPP algorithm can be effectively applied to maritime monitoring sensor network with relatively scanty communication and computing resources, and ensure the continuity of location privacy protection.

Key words: maritime monitoring sensor network, mobile edge computing, location privacy protection, task offloading

1　引言

随着 5G/6G 时代的到来以及物联网、人工智能、区块链等新兴技术的发展[1-5]，我国正逐步加快海洋经济、海洋信息化建设。海洋立体观监测传感器网络（简称“传感网”）作为下一代海洋信息网络重要组成部分[6-7]，可实现全天候、全自动、高密度、多要素、多维度的全球海洋立体观监测，是汇聚海洋空间、环境、生态、资源等各类数据，保障先进海洋观监测的基础设施。加快研究与部署海洋立体观监测传感网，可为实现海洋强国战略目标打下坚实的基础。

收稿日期：2021−05−04；**修回日期：**2021−10−27
通信作者：苏新，leosu8622@163.com
基金项目：国家重点研发计划（No.2021YFE0105500）；国家自然科学基金资助项目（No.61801166）
Foundation Items: The National Key Research and Development Program of China (No.2021YFE0105500),The National Natural Science Foundation of China (No.61801166)

海洋立体观监测应用会在网络局部区域产生大量运算数据与网络负荷[6-7]。面向与海事高可靠、低时延相关应用的需求，基于传统岸基云计算的大数据处理模式时延长，已无法满足相应需求。移动边缘计算技术允许海洋移动终端将产生的海洋观监测数据与计算任务卸载至网络边缘侧的边缘计算节点进行处理，可有效地降低数据传输和处理时延，节省任务传输所需带宽与能耗，减轻岸基设施负荷，提高服务质量[6-7]。

面向海事实时定位、紧急救援等，计算任务的卸载处理存在诸多安全隐患[8-9]。若边缘计算节点为不可信节点，海洋移动终端可能会因任务卸载暴露自身位置隐私。

目前，移动边缘计算研究大多关注陆地组网与车联网特征[10-11]，部分研究涉及终端由任务卸载导致的隐私泄露问题，但主要围绕任务调度和卸载决策。例如，针对边缘计算中的位置隐私与使用模式隐私泄露，文献[12]提出一种基于约束马尔可夫决策过程的隐私感知任务调度算法，使移动用户在保持预先设定的隐私水平时，优化时延与能耗性能。基于文献[12]，文献[13]进一步分析边缘计算中的位置隐私和使用模式隐私泄露问题，综合计算时延、能耗和隐私级别 3 个参数，建立隐私感知卸载模型。针对用户位置隐私威胁，基于卸载任务至远距离边缘服务节点能较好保护用户位置隐私的原理，文献[14]权衡计算卸载中隐私保护与电池能耗的关系，利用深度“后决策”状态学习算法快速求解出最优卸载策略。

上述文献虽然考虑了边缘计算中相关隐私泄露问题，但只是在陆地组网中简单将隐私作为成本变量建立隐私感知卸载模型，针对面向海洋观监测传感网的海洋移动终端位置隐私保护，尚未进行合理隐私风险量化，也未曾提出相应隐私保护措施。此外，与陆地蜂窝网及车联网相比，海洋观监测传感网缺乏中心基础设施；通信带宽受限、通信环境复杂多变，易受天气、恶劣海况等因素影响；海洋移动终端计算、存储资源有限，对能耗敏感，较难在周围找到能源补给，且终端密度、速率、运行轨迹等难以预测，这些因素都对海洋移动终端位置隐私保护提出了严苛要求。

本文面向海洋观监测传感网，围绕海洋移动终端由任务卸载导致的位置隐私泄露问题开展研究。描述了基于移动边缘计算的海洋观监测传感网系统模型；分析并量化了海洋移动终端由任务卸载导致的位置隐私泄露风险；建立了一种基于分布式点对点通信制式的海洋移动终端位置隐私保护模型；提出了一种 DS-LPP 算法，能够确保海洋移动终端任务卸载时的位置隐私安全。

2　相关工作

据调研，海洋观监测传感网中针对移动边缘计算的安全与隐私保护研究工作尚处于初级阶段，相关研究成果匮乏。本文主要关注海洋移动终端任务卸载时的位置隐私保护。

当前，位置隐私保护研究主要围绕认知无线电[15]、无线传感网[16]、与基于位置服务（LBS, location-based service）3 类应用场景[17-21]。认知无线电中[15]，需要在用户与数据库之间单独架设中间查询服务器，使用户在确保位置隐私安全情况下获得分配信道。该方案应用于海洋观监测传感网时将产生高昂通信设施建造成本。无线传感网中[16]，源节点以随机多跳路由方式传输信息到汇聚节点确保位置隐私安全。但该措施将产生较高时延与网络通信开销，与移动边缘计算低时延、低带宽特点相违背。基于位置服务中[17-21]，当用户向 LBS 服务器发送真实位置并请求位置服务时，其位置隐私可能遭受 LBS 服务器非法贩卖交易。为此，文献[17]在实际用户周围添加虚拟用户，并将所有用户位置信息发送到 LBS 服务器，以此对攻击者造成位置信息干扰。上述方案可对用户位置隐私起到一定保护作用，但并未考虑用户移动速度。文献[18]将用户真实位置泛化成随机矩形，并以随机矩形中心位置取代用户真实位置发送到 LBS 服务器，但当用户移动速度较慢时，用户真实位置与矩形中心位置相当接近，无法有效保护用户位置隐私。文献[19]提出一种 Mix-Zone 方案，通过给用户分配多个“假名”，规定用户经过 Mix-Zone 并更换“假名”之后再与 LBS 服务器通信，以切断用户身份与位置的真实对应关系，保护用户位置隐私。基于文献[19]，文献[20]对 Mix-Zone 进行隐私分级得出基于联合熵的隐私度量模型，为系统构建最优 Mix-Zone 以及最大限度保护用户位置隐私提供判断依据，但该方案只是对规则道路拓扑进行数学建模与构建 Mix-Zone，无法有效应用于拓扑结构动态复杂的海洋观监测传感网。文献[21]提出 CloakP2P 算法与 Dual-active 算法两种协作节点搜索算法。用户与协作节点组成 *K*-匿名区域，并将 *K*-匿名区域信息发送到 LBS 服

务器确保位置隐私安全。然而 CloakP2P 算法利用逐跳洪泛搜索协作节点，用户每跳只能搜索少量协作节点，导致位置匿名时间延长。Dual-active 算法利用周期逐跳洪泛搜索协作节点，虽有效降低位置匿名时间，但增加了大量网络通信开销。

LBS 位置隐私保护措施主要针对陆地组网中的行人与车辆。它们无须单独建立通信基础设施且并不通过随机多跳路由传输信息确保位置隐私安全。虽然这些特性满足移动边缘计算业务需求，但由于研究背景差异，LBS 位置隐私保护措施难以直接应用于任务卸载时的海洋移动终端位置隐私保护。因此，本文结合海洋观监测传感网特性以及移动边缘计算特征，优化并改进现有针对 LBS 场景设计的隐私保护机制，最终提出切合海洋观监测传感网边缘计算场景的移动终端位置隐私保护方法。

3　系统模型与位置隐私

3.1　基于移动边缘计算的海洋观监测网络模型

基于移动边缘计算的海洋观监测传感网系统模型如图 1 所示。其中，海岸基站作为空中接口连接海洋节点与陆基服务器，同时具备一定的本地数据处理能力。近海水上节点包括助航、标示航道范围的水上浮标与执行海洋环境监测、资源开发的近海船舶等。近海水下节点包括环境感知的水下传感器和水底巡航机器人等。近海基站可实现本地海洋观监测数据处理，也可将数据通过海底光缆传输至陆基服务器集中处理。远海水上节点包括用于调研海洋水文、地质等特殊任务的科考船等；远海水下节点包括无人潜航器等。卫星系统可用于近、远海船舶的定位与导航。移动边缘计算可有效支撑各类海洋立体观监测应用并承担网络局部区域产生的大量运算[6-7]。海岸基站、近海基站等存储与计算能力较强的海洋网络节点可作为边缘计算节点，高效地支持各类高可靠、低时延海事信息服务。

3.2　位置隐私

本文定义海洋移动终端（以下简称终端）为计算存储能力较弱的节点，任务卸载时其位置隐私需要被保护。定义边缘计算节点（以下简称边缘节点）为计算存储能力较强的节点。边缘节点接收并处理终端卸载的任务，具有半诚信性质（不恶意删除、修改、窃取终端外包数据，但会窥探终端位置隐私）。任务卸载期间，边缘节点可根据信道信息推测与终端相对距离。若终端同时卸载任务至多个边缘节点，边缘节点可联合确定终端准确位置。

3.2.1　接收信号强度指示测距

接收信号强度指示（RSSI, received signal strength indicator）测距可通过计算信号在传播过程中的路径损耗，运用理论或经验信号传播模型将信号损耗转化为判定距离。自由空间无线电传播路径损耗模型为[22]

$$L = S - P = 32.44 + 20\lg d + 20\lg f \qquad (1)$$

其中，L 为信号传输过程中的损耗，S 为发射信号强度，P 为接收信号强度，d 为信号传播距离，f 为传输信号的频率。相比陆地通信，海洋通信环境

图 1　基于移动边缘计算的海洋观监测传感网系统模型

相对开放且缺少障碍物，可采用式(2)对数−正态分布模型进行描述[22]。

$$P_d = P_{d_0} - 10(m+n)\lg(d/d_0) + X_\sigma \tag{2}$$

其中，P_d 指距离发送端为 d 的接收信号强度，P_{d_0} 指距离发送端为参考距离 d_0 的接收信号强度，m 为与环境有关的路径损耗指数，n 为高斯白噪声，X_σ 为均值为 0、方差为 σ^2 的高斯随机变量。海上无线通信链路单位信号路径损耗可表示为

$$P_d = S - 32.44 - 20\lg d_0 - 20\lg f - 10(m+n)\lg(d/d_0) + X_\sigma \tag{3}$$

若已知 S 和 P_d，可根据式(3)判断传输距离 d。

3.2.2　终端位置隐私风险量化

如图 2 所示，以小型船舶表示终端，以海上基站表示边缘节点，终端同时将任务卸载至边缘节点 A、B、C。由于各边缘节点可基于 RSSI 测出与终端相对距离，因此以边缘节点为圆心、以 RSSI 测距（图 2 考虑测距误差）为半径作圆得 E、F、G 3 个交点，坐标分别为 (x_E, y_E)、(x_F, y_F)、(x_G, y_G)。连接 EF、EG、FG 得三角形 EFG 质心 ϖ，且 ϖ 被边缘节点估算作为终端位置。设终端真实位置坐标为 (x_T, y_T)，质心 ϖ 坐标为 (x_ϖ, y_ϖ)，其中，$x_\varpi = (x_E + x_F + x_G)/3$，$y_\varpi = (y_E + y_F + y_G)/3$。若终端同时卸载任务至 n 个边缘节点（$n \geqslant 3$），边缘节点联合确定终端位置时，可知平均距离误差 ADE 为

$$\mathrm{ADE} = \sum_{i=1}^{C_n^3} \sqrt{(x_{\varpi_i} - x_T)^2 + (y_{\varpi_i} - y_T)^2} \,/\, C_n^3 \tag{4}$$

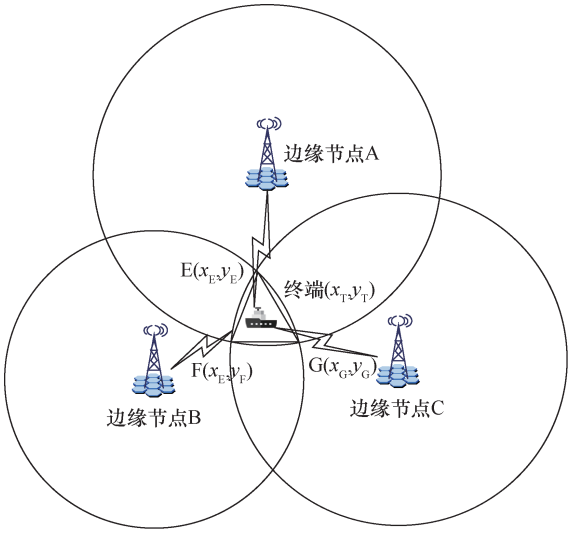


图 2　终端位置隐私泄露

本文以参数 $\Pr = 1/(1+\mathrm{e}^{-\mathrm{ADE}})$ 作为终端位置隐私泄露风险量化指标，$\Pr \in (0,1)$。Pr 越小，终端位置隐私泄露风险越高。

4　终端位置隐私保护算法

4.1　算法相关定义及说明

针对终端任务卸载时存在的位置隐私泄露风险，本文提出一种 DS-LPP 算法确保终端位置隐私安全。DS-LPP 有关定义如下所示。

位置匿名请求：记为 req= (ID_t, Brotime, Loc_t, K, h)，其中，ID_t 为终端身份信息，Brotime 与 Loc_t 分别表示终端广播位置匿名请求时的时间与位置，K 为匿名参数，h 为跳数。

协作节点：响应终端 req 的节点。

候选中继节点：终端根据匿名参数 K 选出的 $K-1$ 个协作节点。

节点信息：记为 Node_Info = (ID, Loc, T_s, Maxspeed)。ID 表示节点身份，Loc 与 Maxspeed 分别表示在 T_s 时刻节点的位置与最大速率。

本地缓存：节点存储空间，存放相邻节点的节点信息 Node_Info。

位置匿名响应：记为 res=(ID, Loc, T_s, Maxspeed)，即响应终端 req 有关节点的 Node_Info。

图 3 以小型船舶表示终端，以海上基站表示边缘节点，描述了本文所建立的海洋移动终端位置隐私保护模型。各船舶之间组成互联网络，并且假设船舶联网内的各船舶是可信的，船舶之间可互相交换位置隐私信息。DS-LPP 算法思想在于：若船舶 A 此时需要卸载任务，根据第 3.2.2 节内容，直接卸载任务至海上基站，可能会引发位置隐私泄露风险。因此船舶 A 可选取其他船舶作为中继，将任务卸载至海上基站，确保自身位置隐私安全。

具体实现为：船舶 A 向所在船舶联网中广播 req 搜索到协作节点为船舶 B、C、D、E、F；在协作节点中根据 K-匿名需求选出候选中继节点为船舶 B、C、D、E，并构成匿名空间。之后船舶 A 根据相关策略选出船舶 C 作为中继，首先传输卸载任务至船舶 C，继而由船舶 C 传输该任务至海上基站。此时海上基站联合确定的位置为船舶 C 的位置，而非原始具有任务卸载需求船舶 A 的位置，从而确保船舶 A 位置隐私安全。由于船舶 A 在匿名空间中可选择 $K-1$ 个中继节点完成任务卸载。因此，船舶 A 的位置被海上基站正确识别的概率降低至 $1/K$。

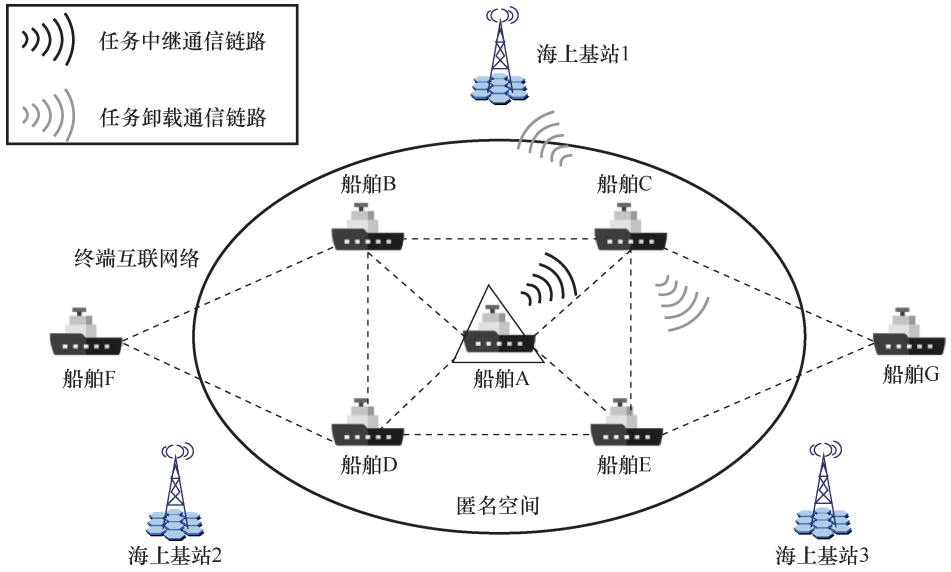


图 3　海洋移动终端位置隐私保护模型

4.2　DS-LPP 算法描述

为确保终端任务卸载时的位置隐私安全，终端首先向所在终端互联网络广播 req 搜索协作节点并构建匿名空间，之后在匿名空间中根据相关策略选出中继节点，并通过中继节点卸载任务以确保位置隐私安全。在构建匿名空间之前，为保证终端收集的协作节点信息具有准确性与时效性，要求终端互联网络中各节点可动态更新本地缓存。结合图 3，本文提出的 DS-LPP 算法包括本地缓存更新、构建匿名空间、中继节点选取 3 个步骤。

1）本地缓存更新

节点频繁接入与退出终端互联网络，需要持续更新网络各节点本地缓存信息，以确保协作节点信息的准确性与时效性。如算法 1 所示，节点在接入网络后或退出网络前，会向邻居节点发送接入或退出网络请求。首先需要判断节点状态，当节点为接入网络状态时，其邻居节点查看本地缓存是否存在该节点 ID，若存在，则覆盖之前的信息记录，实时更新本地缓存数据；若不存在，则将该节点信息存入本地缓存并广播自身节点信息至相邻节点。当节点退出网络，邻居节点查看本地缓存中是否存在该节点的 ID，若存在，则从本地缓存中删除该节点信息。海洋网络节点快速移动会导致部分节点驶离网络却不能完成本地缓存信息的及时清理。为此在算法 1 中设置了本地缓存中允许保留节点信息时间参数 T。每个节点需要根据 T_c、T_s 及时删除超出 T 的节点信息，以更新释放本地缓存。

算法 1　本地缓存更新

初始化　N.status=节点状态

N.ID=节点身份

T_c=系统当前时间

T=本地缓存中允许保留节点信息时间

switch (N.status)

Case-1(接入网络)

if(N.ID 存在于邻居节点本地缓存)

覆盖之前存储的节点信息

else

邻居节点将接入网络节点信息存入本地缓存

并广播自身节点信息至相邻节点

end if

Case-2(退出网络)

if (N.ID 存在于邻居节点本地缓存)

邻居节点从本地缓存中删除退出网络节点信息

end if

end switch

if ($T_c - T_s > T$)

各节点从本地缓存中删除超出 T 的节点信息

end if

2）构建匿名空间

传统协作节点搜索算法 CloakP2P 算法与 Dual-active 算法[21]需要消耗大量时间成本与网络通信开销，难以应用于环境恶劣以及通信、计算资源相对匮乏的海洋观监测传感网。为满足高可靠、低时延海事应用需求，DS-LPP 算法利用上述本地缓

存概念搜索协作节点，以有效节约终端构建匿名空间所需时间成本与通信开销，并提高终端位置隐私保护服务效率与质量。

以图 4(a)为例，终端互联网络包含 13 个船舶节点。假设终端 N_1 具有任务卸载与位置隐私保护需求。N_1 要求匿名参数 K=4，并搜索自身本地缓存得到节点集合 U_1={N_4, N_6, N_8, N_{13}}，数量满足 K-匿名要求。因此，N_1 无需广播 req，可直接更新 U_1 中的节点位置信息并选出距离最近的 3 个节点构建匿名空间。若 N_1 要求匿名参数 K=6，以图 4(b)为例，首先 N_1 搜索自身本地缓存，得到节点集合 U_1={N_4, N_6, N_8, N_{13}}，但无法满足 K-匿名要求。因此，N_1 需要向邻居节点广播 req 以收集更多节点信息。如图 4(b)所示，N_4 收到位置匿名请求后将本地缓存节点集合 U_2={N_1, N_2, N_6, N_{13}}发送到 N_1；同理，N_6, N_8, N_{13} 分别将 U_3={N_1, N_4, N_5}、U_4={N_1, N_9, N_{13}}、U_5={N_1, N_2, N_4, N_8, N_{12}}发送到 N_1。此时，N_1 收集的协作节点集合 U 为

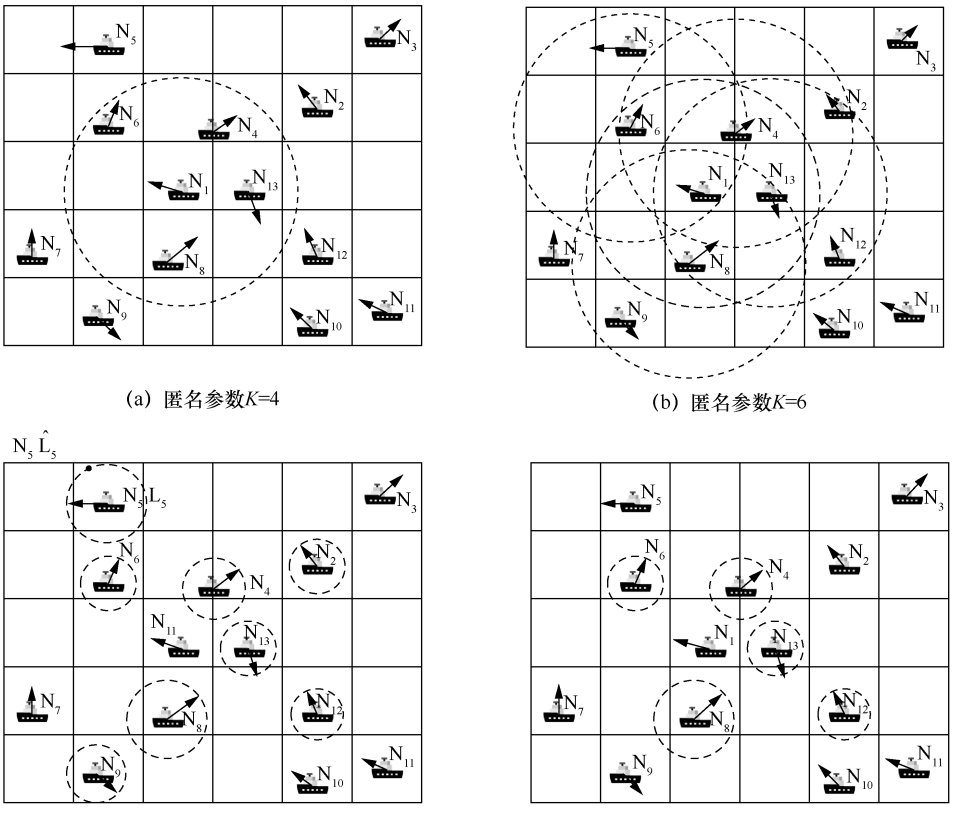
$$U=\{N_2,N_4,N_5,N_6,N_8,N_9,N_{12},N_{13}\} \tag{5}$$

数量满足 K-匿名要求。N_1 停止广播 req，并更新 U 中的节点位置信息。

面对终端互联网络中快速移动的海洋节点，DS-LPP 算法需要对终端收集的协作节点位置信息实时更新。但因终端无法确定其他船舶节点运动方向，因此本文采用保守位置信息更新方法。图 4(c)以终端 N_1 与协作节点 N_5 为例，设 N_5 在 T_s 时刻所处位置为 L_5，最大速率为 V_5，N_1 在 T_c 时刻所处位置为 $\hat{L}_1$。以 N_5 为圆心和$(T_c-T_s)\times V_5$ 为半径作圆，该圆内的“点集合”为 T_c 时刻 N_5 所有可能位置。连接 N_1 和 N_5 与圆交于 $\hat{L}_5$。采用保守位置估计方法即要求 N_1 与 N_5 在 T_c 时刻的距离最大，因此 $\hat{L}_5$ 为 N_5 在 T_c 时刻所处的位置，且 N_1 和 N_5 在 T_c 时刻的距离表示为

$$\left|\hat{L}_1\hat{L}_5\right|=\left|\hat{L}_1L_5\right|+(T_c-T_s)\times V_5 \tag{6}$$

终端更新协作节点位置信息之后，开始构建匿名空间。本例中终端 N_1 要求匿名参数 K=6，需要选出 5 个候选中继节点。为节约中继能耗，可选择距离终端最近的 5 个节点作为候选中继节点。如图 4(d)所示，在 T_c 时刻，距离终端 N_1 最近 5 个节



(a) 匿名参数K=4　　(b) 匿名参数K=6

(c) 调整收集节点位置　　(d) 构建匿名空间

图 4　构建匿名空间流程

点分别为 N_4、N_6、N_8、N_{12}、N_{13}，这些节点与终端 N_1 构成匿名空间。

在终端运行的构建匿名空间算法如算法 2 所示，终端首先统计本地缓存节点数量，若满足 K-匿名要求，执行位置调整与构建匿名空间；否则，向其邻居节点广播 req，搜索协作节点。若连续两次搜索到相同协作节点，说明周围已经没有符合条件的节点，此时继续增加跳数已经无法找到新的协作节点，需要跳出循环。算法 3 在协作节点运行，协作节点会收到 req 与 res 两类消息，且收到 req 时，将根据跳数 h 采取不同转发行为。

算法 2 构建匿名空间（终端）

Step 1 搜索协作节点

初始化 h=1 //设置初始跳数为 1

U=终端本地缓存节点集合

K_P=|U| //终端本地缓存节点数量

while (K_P<K−1)

终端以跳数 h 广播 req，搜索协作节点

U_P=终端广播 req 收集的协作节点

U=U∪U_P

K_P=|U|

if(终端连续两次搜索到相同节点)

跳出循环，转入位置调整与构建匿名空间

end if

h = h+1

end while

Step 2：位置调整与构建匿名空间

if (K_P⩾K−1)

for(集合 U 中的每一个节点)

计算节点在系统当前时刻 T_c 的位置

end for

在 T_c 时刻，选择距离终端最近的 K−1 个节点构建匿名空间 AS

else return 构建匿名空间 AS 失败

end if

算法 3 构建匿名空间（协作节点）

初始化 消息类型

switch(消息类型)

case−1(位置匿名请求 req)

读取 h 的值

if (h = 1)

将自身本地缓存节点信息发送到终端

else if (h>1)

将自身本地缓存节点信息发送到终端

h = h−1

将更新 h 后的 req 转发到下一跳节点

end if

case-2 (位置匿名响应 res)

转发 res 到上一跳节点

end switch

3）中继节点选取

终端成功构建匿名空间后，需要在匿名空间中采用相关策略选出中继节点（可为终端本身），之后将任务转发至中继节点并通过中继节点卸载任务以确保位置隐私安全。然而，海洋通信环境复杂多变且海洋节点具有较强移动性，为使终端顺利转发任务至中继节点，中继节点选取策略应考虑海洋节点移动性以及终端与各候选中继节点之间在任务转发时间 τ 内的链路稳定性。为此，本文提出一种基于链路稳定性的中继节点选取（LS-RNS, linkstability-based relay node selection）策略。定义节点间连通性参数 $C_{\tilde{t}} = R/|\boldsymbol{d}_{\tilde{t}}|$，其中，$R$ 为节点有效通信半径，$|\boldsymbol{d}_{\tilde{t}}|$ 表示 $\tilde{t}$ 时刻两节点之间的实际距离。

如图 5 所示，设终端 N_1 的匿名空间中某一候选中继节点为 N_2，t 时刻 N_1 位置为 (x_1, y_1)，N_2 位置为 (x_2, y_2)，$\boldsymbol{N}_1\boldsymbol{N}_2 = \boldsymbol{d}_t = (x_2 - x_1, y_2 - y_1)$。$N_1$ 与 N_2 之间的距离为 $|\boldsymbol{d}_t|$，且 $C_t = R/|\boldsymbol{d}_t|$。当 N_1 和 N_2 分别以速度 $\boldsymbol{v}_1$ 和 $\boldsymbol{v}_2$ 行驶时，$\boldsymbol{v}_1$ 与 $\boldsymbol{d}_t$ 之间的夹角为 γ，$\boldsymbol{v}_1$ 与 $\boldsymbol{v}_2$ 之间的夹角为 α，速度差 Δv=$\boldsymbol{v}_1 - \boldsymbol{v}_2$ 与 $\boldsymbol{v}_2$ 之间的夹角为 β。经过任务转发时间 $\tau = \hat{t} - t$ 之后，$\hat{t}$ 时刻，N_1 和 N_2 分别运动到位置 $(\hat{x}_1, \hat{y}_1)$，$(\hat{x}_2, \hat{y}_2)$。此时 $\boldsymbol{N}_1\boldsymbol{N}_2 = \boldsymbol{d}_{\hat{t}} = (\hat{x}_2 - \hat{x}_1, \hat{y}_2 - \hat{y}_1)$ 且 $C_{\hat{t}} = R/|\boldsymbol{d}_{\hat{t}}|$，其中，$\boldsymbol{d}_{\hat{t}} = \boldsymbol{d}_t - \Delta\boldsymbol{d} = \boldsymbol{d}_t - \Delta\boldsymbol{v}\cdot\tau$。设 $\Delta\boldsymbol{d}$ 与 $\boldsymbol{d}_t$ 之间的夹角为 θ=$\gamma - \beta + \alpha$，则在 $\hat{t}$ 时刻 $|\boldsymbol{d}_{\hat{t}}| = \sqrt{|\Delta\boldsymbol{d}|^2 + |\boldsymbol{d}_t|^2 - 2|\Delta\boldsymbol{d}||\boldsymbol{d}_t|\cos\theta}$。

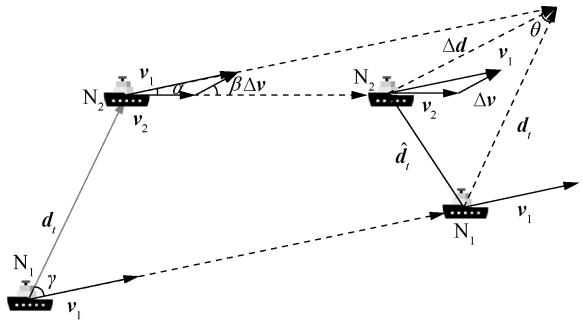


图 5 节点链路稳定性分析

如果以在 $\hat{t}$ 时刻终端与候选中继节点仍保持通信的概率来表示链路稳定性，需要计算在 $\hat{t}$ 时刻 $C_{\hat{t}} \geqslant 1$ 的概率，记为 $P\left(C_{\hat{t}} \geqslant 1\right)$，则有

$$P\left(C_{\hat{t}} \geqslant 1\right)=P\left(\left|\boldsymbol{d}_{\hat{t}}\right| \leqslant R\right)= P\left(\left|\Delta \boldsymbol{v}\right| \leqslant \frac{\left|\boldsymbol{d}_t\right| \cos \theta+\sqrt{R^2-\left|\boldsymbol{d}_t\right|^2 \sin ^2 \theta}}{\tau}\right) \tag{7}$$

假设终端与匿名空间中各候选中继节点之间的速度差值 $\left|\Delta \boldsymbol{v}\right|$ 服从均值为 u、方差为 σ^2 的正态分布，即 $\left|\Delta \boldsymbol{v}\right| \sim N\left(u, \sigma^2\right)$，则有

$$P\left(C_{\hat{t}} \geqslant 1\right)=\frac{1}{\sqrt{2 \pi} \sigma} \int_0^{l / \tau} \exp \left(-\frac{\left(\left|\Delta \boldsymbol{v}\right|-u\right)^2}{2 \sigma^2}\right) \mathrm{d}\left|\Delta \boldsymbol{v}\right| \tag{8}$$

其中，$l=\left|\boldsymbol{d}_t\right| \cos \theta+\sqrt{R^2-\left|\boldsymbol{d}_t\right|^2 \sin ^2 \theta}$，$u=\sqrt{\left|\boldsymbol{v}_1\right|^2+\left|\boldsymbol{v}_2\right|^2-2\left|\boldsymbol{v}_1\right|\left|\boldsymbol{v}_2\right| \cos \alpha}$。

式(8)表示在任务转发时间 τ 内，终端与候选中继节点之间的链路稳定性。终端需要计算与各候选中继节点的链路稳定性，并选择在时间 τ 内具有最大链路稳定性的候选中继节点作为最终中继节点。从而在复杂多变海洋通信环境下确保任务顺利转发到中继节点，实现终端位置隐私保护连续性。

5　仿真实验与分析讨论

本节针对提出的 DS-LPP 算法进行仿真实验。实验硬件平台为 Intel i7-9700 CPU(3.0 GHz)，16 GB 内存，Windows 10 操作系统。实验软件平台为 MATLAB R2016b。仿真实验参数设置见表 1。

表 1　　仿真实验参数设置

参数描述	参数值
船舶互联网络拓扑范围 Area	1 200 m×1 200 m
船舶节点数量 Num	20～65
匿名参数 K	3～15
船舶节点有效通信半径 R	300 m
船舶节点最大行驶速率 Maxspeed	[9.72 Knot, 19.44 Knot]
位置匿名请求消息字节 reqsize	32 byte
实验重复次数 freq	1 000 次

5.1　DS-LPP 算法评价指标定义

5.1.1　DS-LPP 算法位置隐私保护度

定义 ψ 为 DS-LPP 算法位置隐私保护度。记边缘节点通过网络窃听或数据挖掘等手段获取的相关背景知识为 B。δ 表示边缘节点通过背景知识获知的匿名空间中并非原始卸载终端的节点数量。当边缘节点具有背景知识时，匿名空间中原始卸载终端被正确识别的概率记为 $P\{A \mid B\}$。当边缘节点不具有背景知识时，匿名空间中原始卸载终端被正确识别的概率记为 $P\{A\}$。由于匿名空间中共有 K 个节点，则 ψ 满足

$$P\{A \mid B\}-P\{A\}=\frac{1}{K-\delta}-\frac{1}{K} \leqslant \psi \tag{9}$$

由式(9)可知，ψ 越小，DS-LPP 算法针对原始卸载终端的位置隐私保护效果越好。

5.1.2　DS-LPP 构建匿名空间性能

1）构建匿名空间成功率

定义构建匿名空间成功率 $\overline{S}$ 为终端成功构建匿名空间次数与实验重复次数之比。该指标反映 DS-LPP 算法对终端位置匿名请求的处理能力。$\overline{S}$ 越高，DS-LPP 算法处理终端位置匿名请求能力越好。

2）构建匿名空间平均响应时间

响应时间为终端从开始进行位置匿名到成功构建匿名空间所消耗的时间。定义构建匿名空间平均响应时间 $\overline{T}$ 为终端成功构建匿名空间响应时间总和与成功构建匿名空间实验次数之比。该指标反映了 DS-LPP 算法运行效率，$\overline{T}$ 越小，DS-LPP 算法运行效率越高。

3）构建匿名空间平均通信开销

通信开销为网络中产生的位置匿名请求消息 req 总和，包括终端发送到其邻居节点的 req 与邻居节点转发到其邻居节点的 req 之和。定义构建匿名空间平均通信开销 $\overline{W}$ 为终端成功构建匿名空间通信开销总和与成功构建匿名空间实验次数之比。该指标反映了 DS-LPP 算法网络带宽消耗，$\overline{W}$ 越小，DS-LPP 算法所需网络带宽消耗越低。

5.2　DS-LPP 算法位置隐私保护度分析

DS-LPP 算法终端位置隐私保护度的仿真结果如图 6 所示，终端位置匿名参数 K 一定时，边缘节点通过背景知识获知匿名空间中并非原始卸载终端的节点数量 δ 增多，位置隐私保护度 ψ 随之增大，终端位置隐私保护效果变差。由于 DS-LPP 算法位置隐私保护度 ψ 与位置匿名参数 K 值有关，因此改善方法是增加 K 值，图 6 中参数 ψ 随之减小，终端位置隐私保护效果变好。

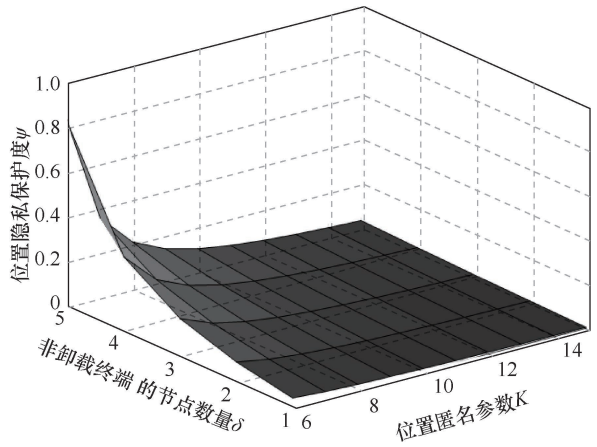


图 6　DS-LPP 算法终端位置隐私保护度的仿真结果

5.3　DS-LPP 算法构建匿名空间性能分析

DS-LPP 算法构建匿名空间成功率的仿真结果如图 7 所示，当固定船舶节点数量 Num 时，K 值越小，$\overline{S}$ 越高。当固定 K 值时，随着船舶节点数量 Num 增加，此时终端本地缓存节点数量增多，并且在广播 req 搜索协作节点时，每一跳搜索到新的协作节点概率增加，$\overline{S}$ 逐渐有所提升。特别地，当 Num ≥30 时，3 种 K 值仿真时获得的 $\overline{S}$ 值均在 84.9%以上，进一步说明了 DS-LPP 算法对终端位置匿名请求具有较好的处理能力。

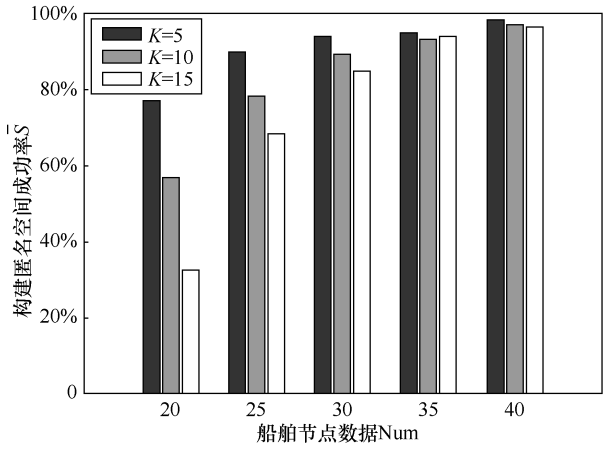


图 7　DS-LPP 算法构建匿名空间成功率的仿真结果

图 8 描述了 DS-LPP 算法在构建匿名空间平均响应时间 $\overline{T}$ 上的性能优势。CloakP2P 算法利用逐跳洪泛搜索协作节点，收到 req 的节点仅将自身节点信息发送至终端。终端需要较长时间才能收集足够数量的节点，$\overline{T}$ 最大（平均为 56.43 ms）。DS-LPP 算法利用动态缓存搜索协作节点，收到 req 的节点将自身本地缓存所有节点信息发送至终端，$\overline{T}$ 平均为 14.63 ms；相比 CloakP2P 算法，性能优势提升了 74%。尽管 Dual-active 算法由于周期性广播 req 收集协作节点，可以快速构建出匿名空间，$\overline{T}$ 最小（平均为 5.45 ms）；但相比 DS-LPP 算法，优势不够明显，两者 $\overline{T}$ 差距随着 Num 的增大逐渐缩小。

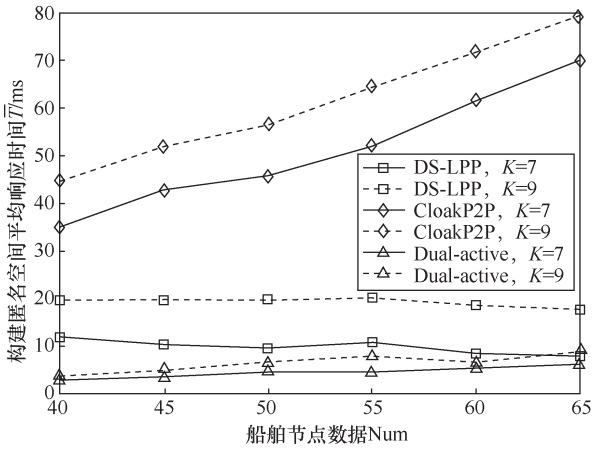


图 8　DS-LPP 算法构建匿名空间平均响应时间

图 9 描述了 DS-LPP 算法在构建匿名空间平均通信开销 $\overline{W}$ 上的性能优势。Dual-active 算法为了快速构建匿名空间，需要终端周期性广播 req 收集协作节点，$\overline{W}$ 最大（平均为 1 171 byte）。与 Dual-active 算法不同，CloakP2P 算法仅要求终端存在位置匿名需求时广播 req 收集协作节点，因此可节约部分通信开销（平均为 717 byte）。DS-LPP 算法不需要终端周期性广播 req，并且利用动态缓存搜索协作节点。因此，终端以较少跳数广播 req 即可收集大量协作节点并成功构建匿名空间，$\overline{W}$ 最小（平均为 71byte）。相比 Dual-active 算法与 CloakP2P 算法，DS-LPP 算法可分别节省通信开销 94%和 90%。

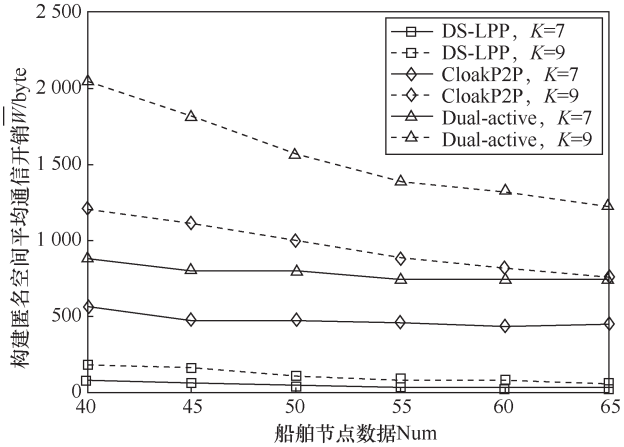


图 9　DS-LPP 算法构建匿名空间平均通信开销

5.4　DS-LPP 算法中继节点选取性能分析

DS-LPP 算法中继节点选取策略仿真结果如图 10 所示。实验设置终端坐标为(500,500)（单位：m），速度(v_x,v_y)（单位：Knot）为(5.84,7.78)。设置 5 个候选中继节点坐标分别为(640,430)、(420,640)、(330,520)、(450,360)、(600,356)，速度(v_x,v_y)分别为(11.67,3.89)、(7.78,9.73)、(0,−11.67)、(5.84,−9.73)、(−11.67,−1.95)。随机策略指终端随机选取匿名空间中某个节点作为中继节点，在不同任务转发时间 τ 内，链路稳定性 $\overline{P}$ 变化剧烈，严重影响终端转发任务效率。相比之下，本文提出的 LS-RNS 计算终端与匿名空间各候选中继节点链路稳定性并选择最大链路稳定性对应的节点作为中继节点，$\overline{P}$ 变化平缓。因而面对复杂多变海洋通信环境以及移动性较强的海洋节点，可确保终端顺利转发任务至中继节点，实现终端位置隐私保护连续性。LS-RNS 在链路稳定性方面，总体性能高出随机策略 54.8%。

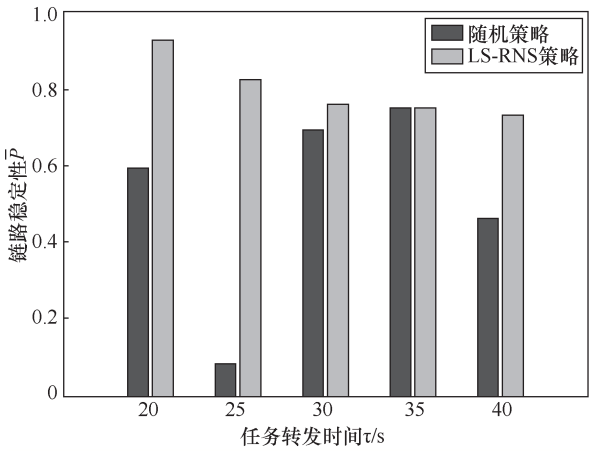


图 10　DS-LPP 算法中继节点选取策略仿真结果

6　结束语

本文描述了基于移动边缘计算的海洋观监测传感网系统模型，分析并量化了海洋移动终端由任务卸载导致的位置隐私泄露风险。建立有关位置隐私保护模型，并提出 DS-LPP 算法确保终端位置隐私安全。仿真结果表明，增大 DS-LPP 算法中匿名参数 K 可提升终端位置隐私保护效果。在构建匿名空间方面，DS-LPP 算法相比 CloakP2P 算法，可节省响应时间 74%，可节省通信开销 90%，相比 Dual-active，可节省通信开销 94%。在中继节点选取方面，DS-LPP 算法中 LS-RNS 算法策略总体链路稳定性高于随机策略 54.8%。研究成果可有效应用于环境恶劣以及通信、计算资源相对匮乏的海洋观监测传感网并保障终端位置隐私保护连续性。DS-LPP 算法假设终端互联网络内各节点是可信的，可互相交换位置信息，与现实情况有所偏差。下一步将结合差分隐私相关概念进一步完善该算法。

参考文献：

[1] ZHOU Y Q, LIU L, WANG L, et al. Service-aware 6G: an intelligent and open network based on the convergence of communication, computing and caching[J]. Digital Communications and Networks, 2020, 6(3): 253-260.

[2] XU H, KLAINE P V, DE ONIRETI O, et al. Blockchain-enabled resource management and sharing for 6G communications[J]. Digital Communications and Networks, 2020, 6(3): 261-269.

[3] LIU L, ZHOU Y Q, YUAN J H, et al. Economically optimal MS association for multimedia content delivery in cache-enabled heterogeneous cloud radio access networks[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(7): 1584-1593.

[4] LIU L, ZHOU Y Q, ZHUANG W H, et al. Tractable coverage analysis for hexagonal macrocell-based heterogeneous UDNs with adaptive interference-aware CoMP[J]. IEEE Transactions on Wireless Communications, 2019, 18(1): 503-517.

[5] LIU L, ZHOU Y Q, VIRGILE G, et al. Load aware joint CoMP clustering and inter-cell resource scheduling in heterogeneous ultra dense cellular networks[J]. IEEE Transactions on Vehicular Technology, 2018, 67(3): 2741-2755.

[6] LIANG M Z, SU X, LIU X F, et al. Intelligent ocean convergence platform based on iot empowered with edge computing[J]. Journal of Internet Technology, 2020, 21(1): 235-244.

[7] SU X, MENG L L, HUANG J. Intelligent maritime networking with edge services and computing capability[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13606-13620.

[8] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
ZHANG J L, ZHAO Y C, CHEN B, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21.

[9] SHA K W, YANG T A, WEI W, et al. A survey of edge computing-based designs for IoT security[J]. Digital Communications and Networks, 2020, 6(2): 195-202.

[10] QI Y L, TIAN L, ZHOU Y Q, et al. Mobile edge computing-assisted admission control in vehicular networks: the convergence of communication and computation[J]. IEEE Vehicular Technology Magazine, 2019, 14(1): 37-44.

[11] LI H D, FANG F, DING Z G. Joint resource allocation for hybrid NOMA-assisted MEC in 6G networks[J]. Digital Communications and Networks, 2020, 6(3): 241-252.

[12] HE X F, LIU J, JIN R C, et al. Privacy-aware offloading in mobile-edge computing[C]//Proceedings of GLOBECOM 2017 - 2017 IEEE Global Communications Conference. Piscataway: IEEE Press, 2017: 1-6.

[13] MIN M H, WAN X Y, XIAO L, et al. Learning-based privacy-aware

offloading for healthcare IoT with energy harvesting[J]. IEEE Internet of Things Journal, 2019, 6(3): 4307-4316.

[14] HE X F, JIN R C, DAI H Y. Deep PDS-learning for privacy-aware offloading in MEC-enabled IoT[J]. IEEE Internet of Things Journal, 2019, 6(3): 4547-4555.

[15] GRISSA M, YAVUZ A A, HAMDAOUI B. Location privacy in cognitive radios with multi-server private information retrieval[J]. IEEE Transactions on Cognitive Communications and Networking, 2019, 5(4): 949-962.

[16] FAN L H, LIU L, GAO H, et al. Secure K-Nearest neighbor queries in two-tiered mobile wireless sensor networks[J]. Digital Communications and Networks, 2021, 7(2): 247-256.

[17] KASORI K, SATO F. Location privacy protection considering the location safety[C]//Proceedings of 2015 18th International Conference on Network-Based Information Systems. Piscataway: IEEE Press, 2015: 140-145.

[18] XU J, YU H Z, XU C, et al. A dynamic spatial cloaking algorithm for location privacy[C]//Proceedings of IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012). IET2012: 1-6.

[19] ARAIN Q A, DENG Z L, MEMON I, et al. Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks[J]. China Communications, 2017, 14(4): 89-100.

[20] 冯霞, 刘亚伟. 基于联合熵隐私保护的自适应动态 Mix-zone 方案[J]. 通信学报, 2018, 39(3): 76-85.
FENG X, LIU Y W. Dynamic Mix-zone scheme with joint-entropy based metric for privacy-perserving in IoV[J]. Journal on Communications, 2018, 39(3): 76-85.

[21] 许明艳, 赵华, 季新生, 等. 基于用户分布感知的移动 P2P 快速位置匿名算法[J]. 软件学报, 2018, 29(7): 1852-1862.
XU M Y, ZHAO H, JI X S, et al. Distribution-perceptive-based spatial cloaking algorithm for location privacy in mobile peer-to-peer environments[J]. Journal of Software, 2018, 29(7): 1852-1862.

[22] SU X, YU H F. Case study for ship ad-hoc networks under a maritime channel model in coastline areas[J]. KSII Transactions on Internet and Information Systems, 2015, 9(10): 4002-4014.

[作者简介]

苏新（1986− ），男，博士，河海大学物联网工程学院教授、硕士生导师，主要研究方向为移动通信、边缘/雾计算、智慧海洋等。

江苏（1996− ），男，河海大学物联网工程学院硕士生，主要研究方向为海洋网络、边缘/雾计算、隐私保护等。

周一青（1975− ），女，中国科学院计算技术研究所研究员、博士生导师，主要研究方向为通信与计算融合、移动边缘计算、存储通信、干扰管控等。