路网环境下基于Voronoi图的位置隐私保护方法

赵 平[1,2] 马春光[1] 高训兵[1] 朱 蔚[3]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1] (中国人民解放军91446部队 涿州 072750)[2]
(中国人民解放军91619部队 秦皇岛 066000)[3]

摘 要 位置隐私泄露已经成为限制LBS应用普及的主要因素,而现有的位置隐私保护方法大都没有考虑移动用户所处的环境背景——道路网络。针对此问题,提出了一种基于路网环境的位置隐私保护方法,该方法主要包含3个部分:(1)利用Voronoi图原理构造路网V图,以满足用户路段多样性要求;(2)提出一种新的隐私模型——V_k-隐私模型,其兼顾匿名集内所有用户的隐私需求,并有效保证服务质量;(3)基于V_k-隐私模型提出一种新的位置匿名算法,它对同一V区内的多个用户进行共同匿名处理,以提高匿名效率和安全性。方法充分考虑了道路网络的结构特点,兼顾了用户的隐私需求与服务质量。通过理论分析论证了方法的抗推断攻击特性,并通过实验验证了方法的可行性。

关键词 基于位置的服务,位置隐私,道路网络,Voronoi图
中图法分类号 TP309 **文献标识码** A

Protecting Location Privacy with Voronoi Diagram over Road Networks

ZHAO Ping[1,2] MA Chun-guang[1] GAO Xun-bing[1] ZHU Wei[3]
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]
(Chinese People's Liberation Army (PLA) Troops 91446, Zhuozhou 072750, China)[2]
(Chinese People's Liberation Army (PLA) Troops 91619, Qinhuangdao 066000, China)[3]

Abstract Location privacy disclosure has become main constraint of LBS applications, while most existing location privacyprotection methods do not consider the background of mobile users——the road network. A location privacy protection method over road networks was presented. This method consists of three phases. First, in order to meet the requirement of segment l-diversity, the road-network Voronoi diagram is constructed based on the structure of the road network. Second, V_K-privacy model is put forward. It satisfies all the users' privacy requirement in the cloaking set and effectively insures the QoS of LBS. Finally, a clocking algorithm based on V_K-privacy model is presented, which improves processing efficiency and safety by cloaking multiple users in the same V-region together. The method takes full account of the structure characteristics of road networks and leverages users' privacy requirement and QoS of LBS. The robustness against inference attacksof the method was proved through theoretical analysis, and the feasibility of the method was proved by the experimental data.

Keywords LBS, Location privacy, Road network, Voronoi diagram

1 引言

随着无线通信和定位技术的日益成熟,基于位置的服务(Location-based service, LBS)[1]在人们的日常生活中逐渐普及。用户通过移动设备(如智能电话、PDA、RFID等),可以随时随地接受各种基于位置的服务,例如查询附近的医院、加油站、旅馆、电影院、公交路线等。LBS为人们的生活提供了巨大便利,但同时也带来了隐私威胁:用户必须先将自身的位置信息通过无线网络发送给位置服务提供商(如Google Maps),后者才能够依据此位置信息进行查询处理和提供服务,这些位置信息一旦被恶意攻击者截获,将对用户的位置隐私造成极大威胁[2]。

位置隐私安全问题引起了研究者们的广泛关注。2003年,Gruteser等[3]将Sweeney等[4]提出的K-匿名模型应用到位置隐私保护中,提出了位置K-匿名(Location K-anonymity)模型,该模型以区域化位置信息代替点位置信息,使攻击者无法将用户的位置与其他至少$K-1$个用户区分开来,从而有效保护了用户的位置隐私。位置K-匿名模型是目前最主要的位置隐私保护模型,对于此模型的改进和应用,研究者们提出了很多方法[5-9]。2006年,Machanavajjhala A等[6]

到稿日期:2012-09-12 返修日期:2012-12-23 本文受国家自然科学基金(61170241),博士后科研人员落户黑龙江科研启动资助金项目(LBH-Q10141),哈尔滨市科技创新人才专项资金(2012RFXXG086),黑龙江省教育厅科学技术研究项目(12513049)资助。
赵 平(1986—),女,硕士生,主要研究方向为位置隐私保护、物联网,E-mail:zj12345121@163.com;马春光(1974—),男,博士,教授,博士生导师,主要研究方向为密码学、信息安全、传感网与物联网、网络编码;高训兵(1987—),男,硕士生,主要研究方向为密码学、信息安全;朱 蔚(1985—),男,主要研究方向为信息安全、物联网。

在位置K-匿名基础上提出了l-多样性(l-diversity)概念，要求匿名集不仅要在数量上满足位置K-匿名，还要在分类上满足多样性，以增加攻击者的攻击难度。此外，具有代表性的匿名模型还有Casper模型[5]、Center Cloak模型[9]等。

以上研究都是基于欧式空间，没有考虑到实际的上下文环境。在现实生活中，用户的移动路线大都受限于道路网络，攻击者利用路网背景知识可将用户锁定于路网范围之内，并通过推断攻击进一步锁定用户所处路段[10]。因此，以上提到的位置隐私保护方法不能直接应用于路网环境，新的位置隐私保护方法必须将路网结构考虑在内。

2009年，Ting Wang等[10]将l-多样性[6]应用到路网环境中，提出了“路段多样性”(Segment l-diversity)概念，要求匿名框不仅要满足用户的位置K-匿名要求，还必须包含至少l条路段，以增加恶意攻击者在路网环境下推断攻击的难度。

文献[11,12]均引用了“路段多样性”概念，结合路网的结构特点构造出满足路段多样性的匿名模型。文献[11]提出“匿名蜂窝”模型，其利用相邻路径结点优先成组方法在“匿名蜂窝”内对用户进行匿名处理。文献[12]提出了“匿名环”和“匿名森林”两种子图结构，即在路网中寻找满足用户数和路段数要求的环路(或森林)，将环路(或森林)作为匿名区域发送给位置服务器。两种方法都能够较好地应对推断攻击，但均存在缺陷：前者不能保证匿名蜂窝内的路段数满足用户的路段多样性需求；后者在长路径环境下寻找到的环路面积过大，无法保证服务质量。

为了更好地平衡路段多样性与服务质量之间的矛盾，本文提出一种新的适用于路网环境的位置隐私保护方法——基于Voronoi图的位置隐私保护方法。本方法利用Voronoi图原理为整个路网构造“路网V图”，以满足路段多样性需求，并提出一种新的隐私模型——V_k-隐私模型，以兼顾用户隐私需求与服务质量，最后基于V_k-隐私模型提出一种高效的位置匿名算法。通过理论分析和实验，证明了方法的抗推断攻击特性和可行性。

2 系统模型

本节介绍方法所用的系统结构以及相关定义。

2.1 系统结构

中心匿名服务器结构[13]是位置隐私保护模型中最常见的系统结构，适用于处理大批量的服务请求。该结构由3部分组成：用户、位置匿名服务器和LBS服务器，如图1所示。

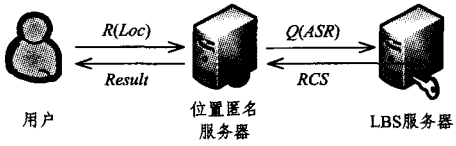

图1 系统模型

(1)用户

用户端设备一般具备自定位功能，在请求基于位置的服务时，将包含用户身份信息、位置信息(一般由坐标表示)、查询内容以及隐私需求的服务请求信息$R(Loc)$发送给位置匿名服务器。

(2)位置匿名服务器

位置匿名服务器接收到用户的服务请求后，利用自身的位置匿名算法对其进行位置匿名处理，并将处理后的位置信息和查询请求$Q(ASR)$发送给LBS服务器——信息在此过程中可能被攻击者截获。位置匿名服务器上还存储了系统范围内道路网络的详细信息，包括网络拓扑结构、用户分布等。

(3)LBS服务器

LBS服务器根据接收到的服务请求进行查询处理，将查询结果集RCS返回给匿名服务器，并由其进行求精处理后将查询结果Result发送给用户。

2.2 路网模型

以无向图$G=(V,E)$表示路网模型，其中，V是点的集合，E是边的集合，图的顶点表示路段交叉点，图的边表示两个交叉点之间的路段，交叉点连接的路段条数即为该交叉点的度(degree)。移动用户位于路段或交叉点上。图2是一个路网模型的例子。

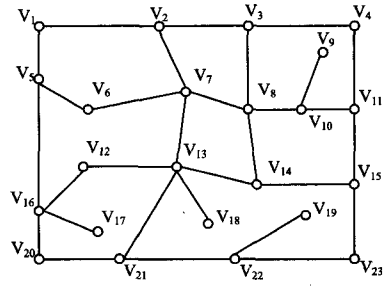

图2 路网模型

2.3 相关定义

定义1(位置K-匿名) 位置匿名服务器对用户的位置信息进行泛化处理，以区域化位置$[(X_1,Y_1)(X_2,Y_2)]$代替用户的准确位置(X,Y)，该区域称为匿名框(AR)。匿名框中包含了用户本身以及其他至少$(K-1)$个用户，它们共同构成匿名集(CS)。攻击者获取匿名框后，无法将发送请求的用户与其他至少$(K-1)$个用户区别开来，则该用户满足位置K-匿名。

定义2(位置隐私需求Q) 以三元组$(k,dist,T)$表示某用户的隐私需求Q，其包含以下3个方面含义：

(1)匿名度k表示匿名集中包含用户的最少个数。若用户满足位置K-匿名，且匿名度为k，在不考虑其他背景知识的情况下，攻击者锁定该用户位置的概率为$1/k$。

(2)空间容忍度$dist$表示该用户与匿名集中其他用户之间的最大限制距离。用户提供给LBS服务器的位置信息越准确，享受的服务质量就越高。设置空间容忍度$dist$以限制匿名框的大小，保证LBS的服务质量。

(3)时间容忍度T表示该用户能忍受的最大时延，该时延指的是位置匿名服务器从接收到用户请求信息到为该用户匿名成功之间的时间。若时延超过T，则此次服务请求失败。

定义3(路段差异度d_m) 路段差异度是路网环境下特定的隐私安全参数，表示对匿名框包含最小路段数的要求，防止路段太少(最坏情况下只有一条)而提高攻击者锁定概率。在本模型中，d_m的值由位置匿名服务器根据路网的实际结构进行设置。d_m不宜过大，否则导致匿名框面积过大，影响服务质量。

2.4 路网V图

为满足路段差异度要求，一种直观的思路是构造基于交叉点的匿名框，即令匿名框包含一个或多个路段交叉点，保证其连接的路段数满足路段差异度要求。那么选择什么样的交

叉点来构造匿名框、选取的交叉点为哪些用户构造匿名框呢？首先需要考虑交叉点的度，每个交叉点的度代表它连接的路段数，度较大的交叉点有利于构造较优的匿名框；其次考虑交叉点与用户之间的距离，寻找距离用户最近的交叉点为此用户构造匿名框，有利于构造较小匿名框。基于以上因素，本方法利用 Voronoi 图[12]为道路网络构造“路网 V 图”，在满足路段差异度的同时限制匿名框的大小。

Voronoi 图是一种广泛应用于空间分割的几何结构，它能够合理有效地表现空间目标之间的邻近关系。

定义 4(Voronoi 图) 设平面区域 A 内包含一个离散点集合 $P=\{P_1,P_2,\cdots,P_n\}$，定义 P_i 的 Voronoi 区域(简称 V 区)$V(P_i)$为 A 内所有到 P_i 距离最小点的集合：$V(P_i)=\{p\mid d(p,P_i)\leqslant d(p,P_j),p\in A,j\neq i,j=1,2,\cdots,n\}$。定义 P 的 Voronoi 图 $V(P)=\{V(P_1),V(P_2),\cdots,V(P_n)\}$，$P_i$ 称为 Voronoi 图生成元。Voronoi 图如图 3 所示。

文献[14]提出了构造 Voronoi 图的方法：将点集 P 中的每一个点与其周围的 n 个点做连线，对每一条连线做中垂线，则这 n 条中垂线相交围成一个 n 条边的 Voronoi 多边形。

Voronoi 图具有以下性质：

(1)相邻的 V 区共享同一条边；

(2)各个 V 区互不重合，组成的 V 图覆盖整个区域；

(3)每个 V 区内的点到本 V 区生成元距离小于到其他生成元距离。

将 Voronoi 图应用到路网中，以路网模型图 $G=(V,E)$ 中部分顶点的集合 $V_p\subseteq V$ 作为 Voronoi 图的生成元集合，构造出的 Voronoi 图称为路网 V 图。为满足路段多样性，要求 V_p 中各顶点的度均不小于 d_m。

定义 5(路网 V 图) $G=(V,E)$ 为一路网模型网，令 $V_p=\{V_i\mid degree(V_i)\geqslant d_m,V_i\in V\}$，$V_p$ 对应的 Voronoi 图称为路网 V 图。V_i 称为路网 V 图的生成元。

以图 2 所示的路网为例，构造路网 V 图：令 $d_m=3$，则有 $V_p=\{V_2,V_3,V_5,V_7,V_8,V_{11},V_{13},V_{14},V_{15},V_{16},V_{22}\}$，对应的路网 V 图如图 4(为使 V 图结构清晰，隐去了 G 的边)所示。

可以分析出路网 V 图具有以下性质：

(1)各 V 区均满足路段差异度要求；

(2)每个用户都位于路网 V 图的某个 V 区内；

(3)生成元的交叉点与其 V 区内的用户之间有最临近关系。假设 u 为 $V(V_i)$内的一个用户，则有

$d(u,V_i)\leqslant d(u,V_j),V_i,V_j\in V,i\neq j$

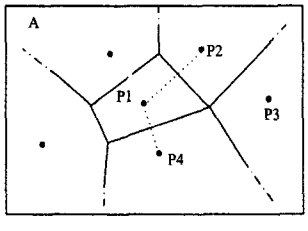

图 3 Voronoi 图

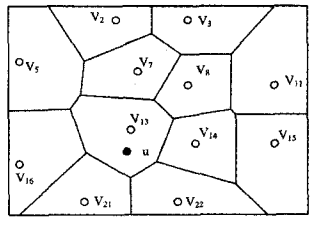

图 4 路网 V 图

3 隐私模型

现有的位置匿名方法[4,7-9]大都采取“各自匿名”策略，即为每个用户单独构造一个匿名集，每个匿名集只对其中的一个用户起匿名作用。若匿名服务器收到 N 条待匿名消息，即需运行 N 次匿名算法，构造 N 个匿名集。为提高匿名效率，提出一种新的隐私模型——V_k-隐私模型。采用“共同匿名”策略，为多个用户构造共同匿名集，此匿名集满足其中所有用户的位置隐私需求。

定义 6(V_k-隐私模型) 设匿名集 CS 中包含 K 个用户 $U_1,U_2,\cdots,U_K$，若 CS 满足以下性质：

(1)CS 内用户数量 K 满足其中任一用户的匿名度要求，即 $K\geqslant\max(U_1.k,U_2.k,\cdots,U_K.k)$；

(2)CS 内任意两个用户之间的距离不大于这两个用户的空间容忍度，即 $d(U_i,U_j)\leqslant\min(U_i.dist,U_j.dist),1\leqslant i,j\leqslant k,i\neq j$；

(3)CS 内包含的路段数 L 满足路段差异度要求，即 $L\geqslant d_m$。

则称匿名集 CS 满足 V_k-隐私模型(见图 5)。

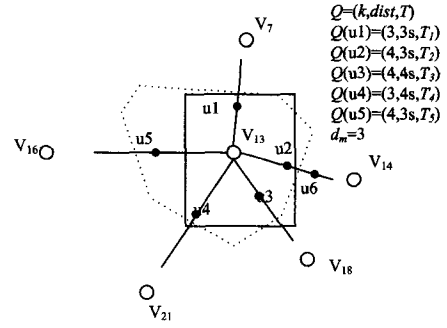

图 5 匿名框构造示意图

V_k-隐私模型保证匿名集满足其中每个用户的位置 K-匿名要求，同时满足路段多样性要求，并且通过空间容忍度的限制控制匿名框的大小，有效保证 LBS 的服务质量。

4 匿名算法

基于 V_k-隐私模型，提出一种新的匿名算法。算法的主要思想是在路网 V 图的各 V 区内，选择满足 V_k-隐私模型的 K(K 的设定见下文)个用户，构造共同匿名集。算法分为 4 个阶段：

(1)构造路网 V 图。首先由位置匿名服务器设定路段差异度 d_m。由于常见的路段交叉点连接的路段数不大于 4，一般设置 $2\leqslant d_m\leqslant 4$。若 $d_m\geqslant 5$，则需要合并相邻交叉点以得到满足度要求的虚拟交叉点[13]，此时一方面会增加路网 V 图的构造难度，另一方面会导致匿名框过大，影响匿名成功率和服务质量。根据设定好的 d_m 确定路网 V 图的生成元，构造相应的路网 V 图。

(2)选取头结点，确定匿名度。选取各 V 区内当前待匿名用户中匿名度要求最高的用户作为头结点 *point*，将其作为第一个成员加入匿名集，并以其匿名度要求作为此匿名集的匿名度。假设该用户的匿名度要求为 k，则 V 区内其他用户的匿名度要求均小于(或等于)k。令匿名集的匿名度 $K=k$，则该匿名集满足其中所有用户的匿名度要求，即满足 V_k-隐私模型性质 1。

(3)搜索匿名集成员。从 *point* 开始在其所属 V 区内进行广度优先搜索。当搜索到新用户 U 时，判断 U 与匿名集 $\{U_1,U_2,\cdots,U_r\}$中现有用户之间距离是否满足 V_k-隐私模型性质 2 即 $d(U,U_i)\leqslant\min(U.dist,U_i.dist),1\leqslant i\leqslant r$。若满

足，则将 U 添加入匿名集，否则仍作为“待匿名”用户等待下一轮匿名。当匿名集内的用户数 $K \geqslant k$，且用户所处的路段数 $L \geqslant d_m$ 时，停止搜索。

(4)扩展搜索。若在本 V 区内搜索到的匿名集无法满足 V_k-隐私模型的要求，则向本 V 区相邻 V 区(即与本 V 区有共享同一条边的 V 区)延伸，继续搜索，直至匿名成功。

算法伪代码如下：

```
输入：无向图 G；用户集 U，路段号集合 LID，路段差异度 d_m
输出：匿名集 CS
1. 为 G 构造 Voronoi 图；
2. for each V(V_i)
3.   选择头结点 point；
4.   将头结点 u 加入 CS，并将其路段号加入集合 LID，K=1，L=1；
5.   while 未搜索到本 V 区边界
6.     搜索用户；
7.     if 搜索到满足空间容忍度的用户
8.       将用户加入 CS，并将其路段号加入 LID，K=K+1；
9.       if 新用户的路段号与 LID 无交集
10.        L=L+1；
11.      end if
12.    end if
13.    end while
14.    if K≥k 且 L≥d_m
15.    匿名成功，返回匿名集 CS；
16.      else 扩展搜索；
17.    end if
18. end for
```

5 安全性分析

5.1 攻击者能力假设

大部分研究都认同位置隐私攻击者具备以下 3 项能力。

(1)攻击者有可能截获匿名服务器发送给 LBS 服务器的用户位置信息，这些位置信息经过位置匿名处理，一般是匿名框形式；

(2)攻击者掌握匿名服务器上的匿名算法；

(3)攻击者掌握路网结构以及其中用户的位置分布。

虽然第(3)种假设是从较坏的角度来考虑服务环境，但单凭这一点并不能导致用户隐私的泄露，因为只有当攻击者将用户身份与位置对应起来，才称攻击者获取了用户的位置隐私，单纯的位置信息不会造成用户隐私的泄露。

5.2 攻击方法

路网环境下攻击者是如何推断出用户的具体位置的呢？下面介绍两个定义。

定义 7(关联概率) 假设匿名框内包含路段集 S，用户 u 位于路段 e 上，$P(u \leftarrow e|S,K_{ad})$ 表示攻击者通过背景知识 K_{ad} 计算出的用户 u 位于 e 上的概率，称为 u 与 e 的关联概率。攻击者的背景知识 K_{ad} 主要包括：路网结构和匿名算法。

在截获某个匿名框 AR 后，攻击者根据路网结构背景知识，锁定匿名框 AR 中包含的路段集 S。理想的保护效果是使攻击者无法判断信息列表 T_q 中各条信息所对应的发送者处于 S 中的哪一条路段，即一个发送者与各路段的对应概率相同，均为 $1/|S|$。但通过有效的攻击，攻击者可能判断出用户与某条路段之间的关联概率超过 $1/|S|$。

定义 8(推断攻击) 攻击者利用位置匿名算法对匿名框内各路段上的用户分别进行匿名处理，得到相应的推断匿名框，称为推断攻击。

设匿名算法为 $F(\cdot)$，在路段 e 进行算法操作，得到相应的匿名框 $AR^e=F(e)$。根据背景知识找到 AR^e 包含的路段集 S^e，比较 S^e 与 S 重合的比例，从而判断出用户 u 处于此路段的概率，即 $P(u \leftarrow e|S,Kad)=|S^e \cap S|/|S|$。与用户 u 关联概率最大的路段就被攻击者认定为 u 所处的路段。

与其它匿名算法不同的是，本匿名算法构造出的匿名集对应的不是一个用户而是 K 个用户，即满足其内部 K 个成员的隐私需求。因此攻击者截获的匿名框 AR 满足 K 个用户的空间容忍度要求，即 AR 包含于各用户所对应的最大匿名框中。可以得出，同一 V 区内的匿名集成员对应的推断匿名框与 AR 的交集均为 AR 本身，即

$$P(u \leftarrow e|S,Kad)=|S^e \cap S|/|S|=|S|/|S|=1, e \in S$$

因此，用户 u 位于匿名框内各路段上的概率相等，攻击者无法推断出用户所处的路段。可见，本匿名方法具有良好的抗推断攻击特性。

6 实验及结果分析

6.1 实验设置

从两个方面来检验匿名算法的性能：匿名成功率和平均匿名执行时间。实验使用路网生成器(Network-based Generator of Moving Object)[15]对路网进行模拟，利用 C++编程语言实现本文提出的算法。实验数据集采用德国奥丁堡的公路网络数据，该公路网络包括 6105 个顶点和 7035 条边。实验分别在稀疏用户环境下和密集用户环境下测试算法的性能，分析其中的差别。设置移动用户量为 10000 和 15000，用户的隐私需求的均值设置如下：$2 \leqslant k_{avg} \leqslant 10$，$300\text{m} \leqslant dist_{avg} \leqslant 500\text{m}$，$T$ 统一设置 5 个时间单位，令 $d_m=3$。

6.2 实验结果分析

(1)匿名成功率

匿名成功率指的是成功匿名的信息数量与总共发送的信息数量之比，匿名成功率越高，算法越合理。图 6(a)和图 6(b)分别显示了随着 k 和 $dist$ 均值的变化，匿名成功率在稀疏用户环境与密集用户环境下的差别。显然在密集用户环境下，匿名成功率较高，在稀疏用户环境下，构造满足用户空间容忍度和匿名度的匿名集的成功率稍低。图 6(b)显示了当用户的空间容忍度足够高时，匿名操作能保持稳定的高成功率。

(2)平均匿名执行时间

平均匿名执行时间是指进行一次匿名集构造所需的平均时间，平均匿名执行时间越短，则算法效率越高，在要求实时服务的 LBS 中的可用性越强。图 6(c)显示了随着 k 均值的增加，两种环境下的平均匿名执行时间都有所增加，密集用户环境下的增量更大，因为随着 k 的增加，稀疏用户环境下的匿名操作容易失败导致操作的终止，减少匿名执行时间。图 6(d)显示了在密集用户环境下，随着 $dist$ 均值的增加，满足 V_k-隐私模型的用户增多，因此平均匿名执行时间减少；在稀疏用户环境下，首先随着 $dist$ 均值的增加，匿名成功率提高，导致平均匿名执行时间有所增加，待匿名成功率稳定之后，平均匿名执行时间减少。

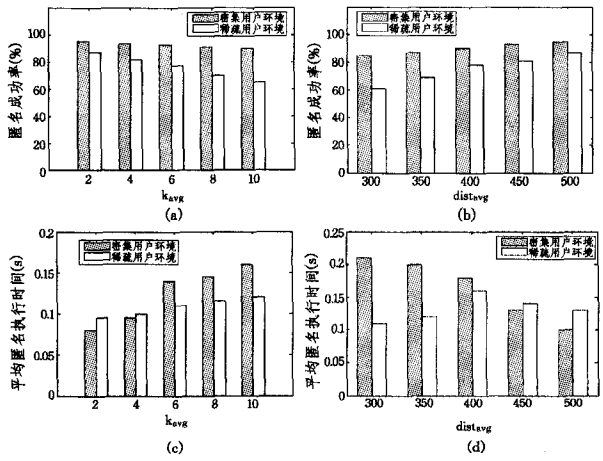

图 6 实验结果图

结束语 随着 LBS 在人们日常生活中的推广，位置隐私保护问题得到了广泛的讨论和研究。本文针对路网环境下的隐私保护特点，提出了基于路网 V 图的位置隐私保护方法，提出了新的位置隐私模型和匿名算法，用以对多个用户进行共同匿名，在保护用户隐私的同时提高匿名效率，保证服务质量。在今后的研究中，针对公路网络的结构特点，提出连续位置服务中的轨迹隐私安全保护方法，是下一步的研究目标。

参 考 文 献

[1] Freudiger J, Shokri R, Hubaux J-P. Evaluating the Privacy Risk of Location-Based Services[A]// 15th International Conference on Financial Cryptography and Data Security[C]. Gros Islet, St. Lucia, 2012: 31-46

[2] Cvrcek D, Kumpost M, Matyas V, et al. A study on the value of location privacy[A]// WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society[C]. New York, USA: ACM, 2006: 109-118

[3] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking[A]// Proceedings of the 1st International Conference on Mobile Systems, Applications and Services[C]. San Francisco, USA: ACM, 2003: 163-168

[4] Sweeney L. k-anonymity: a model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5): 557-570

[5] Mokbel M F, Chow C Y. Casper*: query processing for location services without compromising privacy[J]. ACM Transactions on Data Systems, 2009, 34(4): 24-48

[6] Machanavajjhala A, Kifer D, Gehrke J, et al. l-diversity: Privacy beyond k-anonymity[J]. ACM Transactions on Knowledge Discovery from Data, 2007, 1(1): 3

[7] Gedik B, Liu L. Protecting location privacy with personalized k-anonymity: Architecture and algorithms[A]// IEEE Transactions on Mobile Computing[C]. California, USA, 2008: 1-18

[8] Shin K G, Ju X, Chen Z, et al. Privacy protection for users of location-based services[J]. IEEE Communications Society, 2012, 19(1): 30-39

[9] Kalnis P, Ghinita G, Mouratidis K, et al. Preventing location-based identity inference in anonymous spatial queries[J]. Knowledge and Data Engineering, 2007, 19(12): 1719-1733

[10] Wang Ting, Liu Ling. Privacy-aware mobile services over road networks[J]. VLDB Endowment, 2009, 2(1): 1042-1053

[11] 徐建，徐明，林欣. 路网限制环境中基于匿名蜂窝的位置隐私保护[J]. 浙江大学学报，2011，45(3)：429-434

[12] 薛姣，刘向宇，杨晓春. 一种面向公路网络的位置隐私保护方法[J]. 计算机学报，2011，34(5)：865-878

[13] 魏琼，卢炎生. 位置隐私保护技术研究进展[J]. 计算机科学，2008，35(9)：21-25

[14] Wu Xiao-jun, Luo Xue-fang. The Algorithm for Creating Weighted Voronoi Diagrams based on Cellular Automata[A]// The 6th World Congress on Intelligent Control and Automation[C]. Dalian China: Luo Xue-fang, 2006: 4630-4633

[15] Brinkhoff T. Network-based generator of moving objects[A]// Proceedings of the 12th International Conference on Scientific and Statistical Database Management[C]. Oldenburg, Germany, 2000: 253-255

(上接第 88 页)

[8] Ozdemir S, Çam H. Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks[J]. IEEE/ACM Transactions on Networking, 2010, 18(3): 736-749

[9] Blundo C, Santis A, Herzberg A, et al. Perfectly-secure key distribution for dynamic conferences[J]. Proceedings of Crypto, 1992, 740: 471-486

[10] Du W, Deng J, Han Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(2): 228-258

[11] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(1): 41-77

[12] Karlof C, Sastry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks[C]// Proceedings of the 2nd international conference on Embedded networked sensor systems. New York, USA, 2004: 162-175

[13] Zhang W, Wang C, Feng T. Gp2s: Generic privacy-preservation solutions for approximate aggregation of sensor data[C]// Proceedings of IEEE PerCom. 2008: 179-184

[14] 陈娟，张宏莉. 无线传感器网络安全研究综述[J]. 哈尔滨工业大学学报，2011，43(7)：90-95

[15] 范永健，陈红，张晓莹. 无线传感器网络数据隐私保护技术[J]. 计算机学报，2012，35(6)：1131-1146

[16] 姚剑波，文光俊. 无线传感器网络中的隐私保护研究[J]. 计算机科学，2008，35(11)：19-22

[17] 杨庚，王安琪，陈正宇，等. 一种低耗能的数据融合隐私保护算法[J]. 计算机学报，2011，34(5)：792-800

[18] 张鹏，喻建平，刘宏伟. 传感器网络安全数据融合[J]. 计算机科学，2011，38(8)：106-108