DOI：10.7652/xjtuxb201702005

面向路网环境速度预测攻击的隐私保护

张磊[1,2]，马春光[1]，杨松涛[1,2]，李增鹏[1]
（1.哈尔滨工程大学计算机科学与技术学院，150001，哈尔滨；
2.佳木斯大学信息电子技术学院，154007，黑龙江佳木斯）

摘要：针对路网环境中攻击者利用速度预测获得用户位置隐私的问题，提出了一种提高当前路段查询密度值的密度压缩算法。该算法在用户真实位置附近添加大量噪声用户，通过噪声用户影响当前路段查询密度，进而降低速度预测的准确性，破坏攻击者通过概率转移矩阵预测用户行驶速度的攻击行为，以此保护用户在路网环境中的位置轨迹隐私。该算法通过密度压缩使真实用户和噪声用户表现出相同速度，提高了真实用户与噪声用户之间的相似程度，降低了噪声用户被识别的机率，进一步隐藏了真实用户。实验结果表明，与其他主流算法相比，密度压缩算法能够更有效地抵抗基于速度预测的攻击行为，具有更好的隐私保护能力。在执行时间和隐私保护成功率等方面的实验结果进一步表明，该算法更适合在路网环境下提供隐私保护服务，具有广阔的应用前景。

关键词：轨迹隐私；隐私保护；速度预测；查询密度
中图分类号：TP311 **文献标志码**：A **文章编号**：0253-987X(2017)02-0027-06

A Privacy Preserving Method from Attacks of Velocity Prediction in Road Network

ZHANG Lei[1,2], MA Chunguang[1], YANG Songtao[1,2], LI Zengpeng[1]
(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China;
2. College of Information and Electronic Technology, Jiamusi University, Jiamusi, Heilongjiang 154007, China)

Abstract: A density compression algorithm (DCA) to query density of current road segment is proposed to solve the problem of filching location privacy by velocity prediction. The algorithm produces a large number of dummy users and utilizes these users to increase the query density of current road segment and to decrease the prediction accuracy so that velocity prediction attacks based on the matrix of transition probability are destroyed. Thus the aim of location trajectory privacy preservation is realized. Moreover, the DCA also makes dummy users have the same velocity with the real user, which increases the similarity of dummy users with the real user and reduces the probability of dummy users to be identified so that the real user is further hidden. Experimental results and comparisons with other schemes show that the DCA resists the attacks from velocity prediction and achieves a better privacy preservation. In addition, the DCA also has a shorter running time as well as a higher success probability in privacy preservation. These characteristics show that the DCA may have a better utilization in location privacy of road networks and a more broad application prospect.

收稿日期：2011-07-19。 作者简介：张磊(1982—)，男，博士生；马春光(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金资助项目(61472097)；高等学校博士学科点专项科研基金资助项目(20132304110017)；黑龙江省自然科学基金资助项目(F2015022)。
网络出版时间：2016-12-30 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20161230.1629.004.html

Keywords: trajectory privacy; privacy preservation; velocity prediction; query density

连续位置服务产生的大量离散位置可按时间序列关联成位置轨迹。由于轨迹中含有大量的时空信息,使得攻击者更容易获得用户隐私。为有效地保护位置轨迹,研究者提出了大量的隐私保护方法,但这些方法多针对欧氏空间[1-5],在实际路网环境下存在局限,这使得人们更加关注路网环境下的位置轨迹隐私保护,并提出轨迹泛化[6-9]和后续位置扰乱[10-13]两种主要机制。在泛化的方法中,常见的有粗粒度[6-7]、锚点[8-9]和孤立索引[14]等主要方法,但泛化的方法受道路宽度和用户密度的影响较大,这使得人们更关注后续位置扰乱的方法。然而,现有的扰乱方法并不能有效地抵抗用户轮廓预测攻击,该攻击包含用户下一位置预测[15-19]、用户轮廓信息预测[20-21]和目的地预测[22]等。这些攻击方法在很大程度上可对部分隐私保护方法免疫。针对这种攻击,本文首先量化了基于速度的预测模型,然后在此模型的基础上提出了相应的攻击方法和基于密度压缩的隐私保护方法。实验证明密度压缩算法具有较好的算法执行效率和隐私保护能力。

1 预备知识

1.1 攻击模型

影响速度的因素主要有道路状况和用户密度,其中道路状况又影响用户密度。攻击者可根据用户密度预测不同路段中的速度变化,进而推测用户的潜在位置。在对速度进行预测之前,攻击者先从未被保护的轨迹中挖掘出历史速度,通过计算获得预测结果,再与不确定速度集合进行比较后识别真实位置。该攻击可用 $L_{v|d}^{\theta}$ 模型加以量化。

定义 1 $L_{v|d}^{\theta}$ 模型。设 L 是攻击者所掌握的最大长度速度变化轨迹,d 是 L 中所包含的 m 个路径密度差异,当 $P_{\mathrm{con}}(v_l=v_{\mathrm{c}}\mid P(v\mid d))\geqslant\theta$ 时,称攻击者获得了用户真实位置轨迹 T 中任意路段 l 的真实速度。其中,v_l 是当前路段真实速度;v_{c} 是攻击者预测速度;$P(v\mid d)$ 是通过 L 挖掘出的速度随查询密度变化的转换概率;$0\leqslant\theta\leqslant1$ 代表预测与真实速度的信息量。基于该模型并利用贝叶斯推论,可设计一种基于马尔可夫过程的速度预测方法。

1.2 隐私保护思想

在 $L_{v|d}^{\theta}$ 模型中,根据 $P_{\mathrm{con}}(v_l=v_{\mathrm{c}}\mid P(v\mid d))$ 可通过降低速度与真实速度之间的相关程度 P_{con} 来保护隐私。$P(v\mid d)$ 可表示为当前密度下的速度转换概率 $P(v_i\rightarrow v_{\mathrm{c}}\mid d_i\rightarrow d_{\mathrm{c}})$,$v_i$ 和 d_i 分别是 L 中距当前位置最近速度和密度;v_{c} 和 d_{c} 分别是当前速度和查询密度。在实际情况下,影响相关度 P_{con} 的因素取决于背景知识,由于 v_i 和 d_i 已被掌握,因此需改变 v_{c} 或 d_{c} 来实现隐私保护。

对于改变 v_{c} 或 d_{c},当前存在两种方法。一种是随机变化行驶速度,即频繁地变更在相同或不同路段上的行驶速度,但这种方法不符合行驶习惯,且频繁变更速度也不利于行驶安全。另一种方法是变更当前路段查询密度,破坏密度与速度之间的关联关系,进而影响相关度 P_{con}。基于该思想,本文针对 $L_{v|d}^{\theta}$ 模型提出了密度压缩算法(density compression algorithm,DCA)来保护位置隐私。

2 基于 $L_{v|d}^{\theta}$ 模型的攻击方法

根据 $L_{v|d}^{\theta}$ 模型预测当前速度 v_{c},需根据历史速度变化轨迹 L 挖掘出随查询密度变化的速度转移,获取当前速度 v_{c} 的先验概率,然后通过贝叶斯推论预测真实速度。该过程可分为训练和预测两个阶段。其中,训练是根据子轨迹和背景知识分析获得不同路段查询密度下的速度变化;预测是根据当前路段查询密度,结合先验概率计算当前速度后验概率,并根据极大后验假设预测当前速度。假设当前行驶速度为 v_{c},则根据路段查询密度得到当前速度的极大后验假设可表示为

$$v_{\mathrm{c}}=\arg\max P(v_i\mid d_{\mathrm{c}}) \tag{1}$$

式中:v_i 表示在查询密度 d_{c} 下的不同速度;$\arg\max P$ 表示极大后验假设;d_{c} 是攻击者通过路段中的服务请求数计算得出的查询密度;v_i 表示同一查询密度下的不同速度。因此,攻击者需要根据最近位置的行进速度预测潜在的速度变化率,并根据极大后验假设预测速度 v_{c}。

获得速度变化有两种方法:一是根据当前速度,按照当前位置与后续位置之间潜在的查询密度差异,逐段使用先验概率计算当前速度;另一种是通过先验概率建立马尔可夫一步转移概率矩阵,并通过查询密度差异设定转移步数来计算当前查询密度下的速度后验概率,进而根据极大后验假设预测当前速度。这两种方法各具优缺点:第一种方法能够较准确地预测出行进速度进而得出用户位置,但在多密度变换下计算量较大;第二种方法通过 n 步转移忽略了部分行驶距离,尽管预测结果与真实位置之

间存在一定偏差，但不需计算每个路段的查询密度，降低了计算开销。因此，本文主要以第二种方法来实现预测攻击。

假设在训练阶段通过历史速度变化轨迹 L 获得的路段查询密度分类数为 m，S 表示用户速度在查询密度变化时的速度转换，n 表示转移步数。通过 L 获得的速度转换，可构建 n 步转移概率矩阵 $\boldsymbol{M}^{(n)}=P(v)_{ij}^{(m+n)}$，条件概率 $P(v)_{ij}^{(m+n)}$ 可表示为

$$P(v)_{ij}^{(m+n)}=P\{X_{m+n}=f_{v_j|d_c}\mid X_0=f_{v_i|d_i}\},\quad m\geqslant 0;n\geqslant 1;v_i,v_j\in S \tag{2}$$

式中：$f_{v_j|d_c}$ 和 $f_{v_i|d_i}$ 分别表示当前查询密度下速度转换概率和初始位置（攻击者掌握的最近位置）处查询密度对应的速度概率。由此，f 可通过条件概率 $P(v_i\to v_c|d_i\to d_c)$ 计算得到。$v_i\to v_c$ 表示速度转移，$d_i\to d_c$ 表示查询密度转换。使用转移概率矩阵获取当前速度可描述为：首先根据速度与查询密度建立一步转移矩阵 $\boldsymbol{M}$；然后计算 d_i 到 d_c 之间存在的查询密度步数差 n；再计算 n 步转移矩阵 $\boldsymbol{M}'=\boldsymbol{M}^n$；最后根据 $p_{v_i^c v_i^c}^{d_i^c d_c}=\max\boldsymbol{M}'_{v_i}$ 获取极大后验假设。如何建立转移概率矩阵将在下例中详细描述。

如图 1 所示，设存在 A、B、C 共 3 种路段密度，用户速度可表示为 $v_i(1\leqslant v_i\leqslant 3)$。攻击者首先根据查询密度将公路划分为 5 个不同路段，然后按历史速度变化轨迹 L 计算每个路段的速度转换概率。以该值作为矩阵元素，根据查询密度变化导致的速度变化，可以得到速度一步转移概率矩阵

$$\boldsymbol{M}=\begin{bmatrix}
p_{11}^{AA} & p_{12}^{AA} & p_{13}^{AA} & p_{11}^{AB} & p_{12}^{AB} & p_{13}^{AB} & p_{11}^{AC} & p_{12}^{AC} & p_{13}^{AC}\\
p_{21}^{AA} & p_{22}^{AA} & p_{23}^{AA} & p_{21}^{AB} & p_{22}^{AB} & p_{23}^{AB} & p_{21}^{AC} & p_{22}^{AC} & p_{23}^{AC}\\
p_{31}^{AA} & p_{32}^{AA} & p_{33}^{AA} & p_{31}^{AB} & p_{32}^{AB} & p_{33}^{AB} & p_{31}^{AC} & p_{32}^{AC} & p_{33}^{AC}\\
p_{11}^{BA} & p_{12}^{BA} & p_{13}^{BA} & p_{11}^{BB} & p_{12}^{BB} & p_{13}^{BB} & p_{11}^{BC} & p_{12}^{BC} & p_{13}^{BC}\\
p_{21}^{BA} & p_{22}^{BA} & p_{23}^{BA} & p_{21}^{BB} & p_{22}^{BB} & p_{23}^{BB} & p_{21}^{BC} & p_{22}^{BC} & p_{23}^{BC}\\
p_{31}^{BA} & p_{32}^{BA} & p_{33}^{BA} & p_{31}^{BB} & p_{32}^{BB} & p_{33}^{BC} & p_{31}^{BC} & p_{32}^{BC} & p_{33}^{BC}\\
p_{11}^{CA} & p_{12}^{CA} & p_{13}^{CA} & p_{11}^{CB} & p_{12}^{CB} & p_{13}^{CB} & p_{11}^{CC} & p_{12}^{CC} & p_{13}^{CC}\\
p_{21}^{CA} & p_{22}^{CA} & p_{23}^{CA} & p_{21}^{CB} & p_{22}^{CB} & p_{23}^{CB} & p_{21}^{CC} & p_{22}^{CC} & p_{23}^{CC}\\
p_{31}^{CA} & p_{32}^{CA} & p_{33}^{CA} & p_{31}^{CB} & p_{32}^{CB} & p_{33}^{CB} & p_{31}^{CC} & p_{32}^{CC} & p_{33}^{CC}
\end{bmatrix}$$

对同一道路存在较多查询密度变换的情况，n 步转移需计算大量的矩阵乘法，令计算复杂度过高，因此根据每一查询密度路段均可遍历这一性质，使

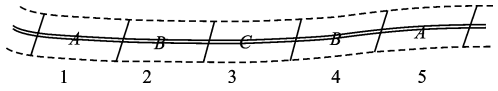


图 1　基于查询密度划分的路段

用平稳分布认定当前速度。平稳方程表示为

$$\pi_j=\lim_{n\to\infty}P(v)_{ij}^{(n)}>0(v_j\in S) \tag{3}$$

以平稳方程联立规范性条件 $\sum_{v_j\in S}P(v)_{ij}^{(n)}=1$ 可以得到关于 π 的方程组，求解之后可得长期行进中速度概率集，进而根据极大后验假设得出当前速度。

3　基于密度压缩的隐私保护方法

3.1　密度压缩算法

针对 $L_{v|d}^{\theta}$ 攻击模型可通过添加大量噪声查询的方法来改变当前查询密度，进而降低预测的准确性。基于该思想，本文提出一种密度压缩算法。

定义 2　密度压缩算法。针对用户提出的隐私保护申请，隐私保护服务器计算当前路段的真实用户数以及最大容纳，将生成的虚假请求与真实请求混合发给位置服务提供商，以此改变攻击者可获得的查询密度，该方法称为密度压缩算法。

更改查询密度不仅需要添加大量的虚假查询，还需要保障这些查询具有相似速度，可对真实查询加以扰乱，进而降低噪声位置的排除性。在密度压缩算法中，由于将查询密度压缩为最大密度，使得当前速度只能是速度分类中最慢的一种，间接地实现了速度匿名。

3.2　安全性分析

由 $L_{v|d}^{\theta}$ 模型中的 $P_{\mathrm{con}}(v_l=v_c|P(v|d))$，可知攻击成功率取决于预测位置与真实位置之间的关联阈值，仅破坏最大阈值使真实攻击阈值小于 θ 并不能保证攻击者通过速度关联排除虚假查询。密度压缩算法通过压缩当前查询密度，迫使当前路段中所有用户具有最大速度相似性，模糊了用户的真实位置，因此该方法可按真实速度模糊程度加以度量。

设 p_i 是攻击者根据 $L_{v|d}^{\theta}$ 模型获得的当前速度与真实速度的相似概率，$p_i=P_{\mathrm{con}}(v_l=v_i|P(v|d))$，若当前路段中存在 n 个用户，则真实速度的扰乱程度可用熵加以度量

$$H=-\sum_{i=1}^{n}p_i\mathrm{lb}p_i \tag{4}$$

泛化速度的目的是令攻击者无法准确识别出真实用户。根据最大熵定理可知，在 n 个用户中任选一个用户是真实用户的概率为 $1/n$，此时熵取最大值。由于添加的虚假用户在速度上与真实用户相似，使攻击者无法通过速度来提高或降低 p_i 取值，可认为在该算法下能够获得最大熵，即攻击者无法通过速度预测准确判断用户位置。

对于密度压缩算法，根据 $P_{\text{con}}(v_l=v_i\,|\,P(v|d))$ 可以设定一个在攻击者 A 与用户 U 之间的双方博弈。U 首先将当前路段和历史速度变化轨迹发送给 A，然后 A 指定任意两个不同路段和在此路段上的速度(v_0,v_1)给 U；U 随机选择 $b\in\{0,1\}$使得 v_b 是 A 所提供速度中的任意一个，同时将两个不同查询密度设为最大值 $d_{\max}$，并将其发送给 A；A 通过历史速度变化轨迹和 $d_{\max}$成功预测 $b'=b$，则攻击者 A 获胜。

定理 1 密度压缩算法可抵抗 $L^{\theta}_{v|d}$模型的攻击，对于任何攻击者，通过 $L^{\theta}_{v|d}$模型获得以上博弈中 U 选择速度的最大概率是 $1/2+l_{\text{neg}}(v)$，该概率等同于攻击者随机猜测。其中 $l_{\text{neg}}(\cdot)$表示安全参数的一个可忽略函数。由定理 1 以及式(4)可以得以下引理。

引理 1 密度压缩算法保护了用户位置隐私。

证明 攻击者可以获取到的背景知识包括历史速度变化轨迹和压缩后的查询密度，这使得攻击者通过式(2)计算得到的当前速度为最低值，该值与 v_0 和 v_1 均不存在关联关系，使得通过预测方法得到的速度无法与真实速度相关联，进而令预测结果等同于随机猜测。

4 实验验证

4.1 实验准备

文中所有算法均在 windows 7 系统上用Matlab 7 加以模拟，其环境为 1.70 GHz Intel Core i5，4 GB 内存。数据集采用 BerlinMOD Data Set 中的真实数据，并随机选择位置作为查询用户来评测攻击和隐私保护方法。表 1 为实验中采用的相关参数阈值。

表 1 实验参数阈值设定表

参数	取值范围	默认值
速度信息量	$0\leqslant\theta\leqslant1$	0
密度分级	$1\leqslant d_{\text{level}}\leqslant3$	1
速度分类	$1\leqslant v_{\text{classly}}\leqslant3$	2
转移次数	$1\leqslant n\leqslant30$	15
匿名值	$2\leqslant k\leqslant30$	10
隐私申请人数	$1\leqslant N\leqslant30$	15
路段宽度(人数)	$1\leqslant R_w\leqslant20$	10
路段长度(人数)	$1\leqslant R_l\leqslant30$	20
路段容量	$0\leqslant C\leqslant600$	150

其中，速度信息量默认为 0，表示任何高于 0 的相似概率均被收集，并应用于预测；密度分级和速度分级表示选择路段中的用户密度级别和速度级别；转移次数表示用户行进中的密度转换次数；匿名值表示隐私保护所要求的匿名用户数；隐私申请人数表示当前路段中提出隐私保护请求的用户数；路段宽度和长度用以计算当前路段的最大可容纳用户数；路段容量可通过路段宽度和路段长度计算获得，在本文中用以计算隐私保护成功率和添加噪声比例。

对速度预测攻击的评估主要查看攻击效果，以 BerlinMOD journey 中 141 个轨迹中 346 657 条数据作为基础，按照训练样本的比例变化完成攻击测试。对于隐私保护方法则分别从保护效果和算法效率两个方面加以评估。其中，保护效果通过攻击成功率和用户速度的模糊熵两个方面加以比较；算法效率根据隐私保护成功率、噪声数和算法执行时间 3 个方面加以考查。在保护效果的验证上与以下算法比较：时间耽搁的非矩形 mix-zone[13]、基于连续匿名的 CLAPPINQ[5]、基于锚点的 Cooperative[9] 以及粗粒度的 Snet[7]。算法效率方面无法比较，只能通过数值进行分析，这是由于目前缺乏类似算法可供比较。

4.2 实验结果

图 2 显示了基于 $L^{\theta}_{v|d}$模型的攻击方法的攻击成功率，该结果产生于随机选择的 10 000 个不同位置。由图 2 可以看出，该攻击对以扰乱为主的隐私保护方法具有较好的攻击效果，这是由于扰乱方法可提供真实位置给服务提供商，使得攻击者更易通过速度对比识别出真实位置。同时 mix-zone 算法比 CLAPPING 算法好，这主要是由于在 mix-zone 算法中攻击者无法获取当前查询密度影响预测准确性。在基于模糊的隐私保护方法中，锚点方法具有较好的抵抗能力，这是由于锚点方法隐藏了用户所在路段，降低了攻击者获得用户所在路段密度的概率。最后，DCA 算法表现最好，这是由于该算法将当前路段查询密度压缩为最大密度，使后验概率获取的用户速度与真实速度之间存在差异，进而导致

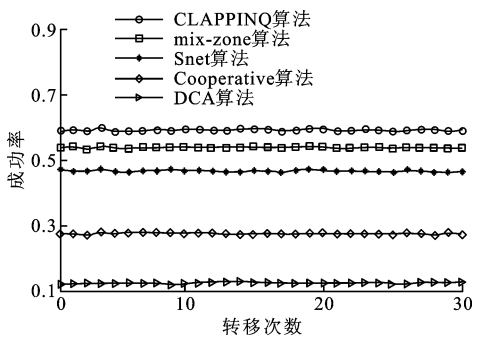


图 2 攻击成功率随转移次数的变化

攻击者获得真实速度的概率近似于随机猜测。

为比较熵变化，实验设定扰乱和模糊方法中的匿名用户具有相似轮廓。根据 Jaynes 最大熵原理，当攻击者从当前用户集合中推测出真实速度的概率彼此独立时存在最大熵。图 3 给出了不同算法速度扰乱熵随添加噪声数的变化，模糊和 DCA 算法由于攻击者无法分辨出真实用户与噪声用户，使得随噪声增加熵可取最大值，由于部分用户存在轮廓信息差异，扰乱方法使攻击者可通过差异排除匿名用户进而降低熵的取值。

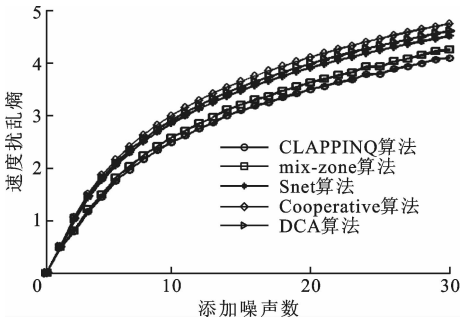
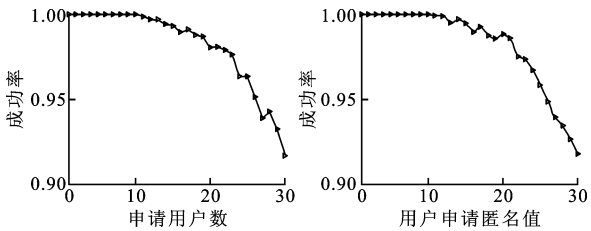


图 3　不同算法速度扰乱熵随添加噪声数的变化

如图 4 所示，DCA 算法的隐私保护成功率取决于当前路段的用户容量，若当前路段已达到最大容量，则无法改变查询密度，导致 DCA 算法失败。由图 4a 可以看出，在匿名值为 10 的情况下，当路段人数达到路段极限时，随着申请用户数的增加，隐私保护成功率逐渐下降。图 4b 中当申请用户数为 15 时，匿名值 k 的增大造成隐私保护失败的情况逐渐加剧，可见在申请用户较多的情况下随着基本匿名需求的增加，导致隐私保护的成功率降低。



(a)随申请用户数增加的成功率　(b)随匿名值增加的成功率

图 4　DCA 算法的隐私保护成功率

图 5 给出了添加噪声比例随申请用户数的变化，添加噪声的比例随着申请用户数线性下降，由于路段中的用户差异，这种线性下降在较小的申请用户数间隔内呈现不规则的波动，当申请用户数超过 470 左右时，当前路段达到最大密度，使得 DCA 算法执行失败，进而无法添加噪声，此时噪声比例为 0。由此可见，DCA 算法随申请用户数增加，其执行效率随着添加噪声数的降低而有所提高，但不会导致隐私保护程度的降低，因为在申请用户数增加的情况下，当前路段密度逐渐趋向饱和，更易实现密度压缩。

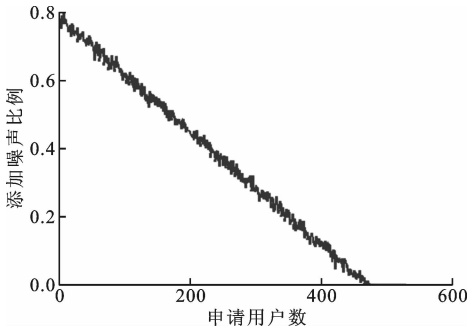


图 5　添加噪声比例随申请用户数的变化

图 6 给出了算法执行时间随申请用户数的变化，可见算法的执行时间随申请用户数的增加而减少，这是由于申请用户数的增加，使得当前路段的查询密度逐渐增大，进而添加的噪声量逐渐减少，降低了算法执行时间；当申请用户达到当前路段最大密度时，DCA 算法执行失败，此时算法的执行时间降为 0，表明算法不需执行。

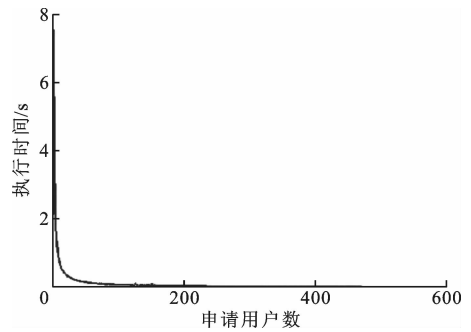


图 6　算法执行时间随申请用户数的变化

综上所述，DCA 算法在抵抗速度预测攻击的隐私保护能力和算法效率上都具有较好的表现，可以认为该算法在有效地抵抗基于 $L_{v|d}^{\theta}$ 攻击模型的速度预测攻击的基础上，具有较好的执行效率。

5　结　论

本文针对路网环境下已有的隐私保护方法无法有效地保护用户位置隐私的情况，结合已有的攻击方法量化了一种预测当前速度的攻击模型，并根据该模型提出了基于贝叶斯推论的速度预测攻击方法。同时，在分析该方法存在的优缺点的基础上，提出了针对该攻击的密度压缩隐私保护方法，以此来保护用户的位置隐私。实验证明，密度压缩算法能

够有效地保护用户的位置隐私,同时具有较好的算法效率。由于密度压缩算法需要添加大量的噪声数据,对于隐私保护服务器的负载较大,今后的研究将在既有效地破坏预测准确性、又能更好地降低隐私保护服务器负载方面展开。

参考文献:

[1] WANG Yong, HE Longping, PENG Jing, et al. Privacy preserving for continuous query in location based services [C]// Proceedings of the 18th IEEE International Conference on Parallel and Distributed Systems. Piscataway, NJ, USA: IEEE, 2012: 213-220.

[2] HWANG R H, HSUEH Y L, CHUNG H W. A novel time-obfuscated algorithm for trajectory privacy protection [J]. IEEE Transactions on Services Computing, 2014, 7(2): 126-139.

[3] ROMAN S, CHOW C Y, HUANG Qiong, et al. User-defined privacy grid system for continuous location-based services [J]. IEEE Transactions on Mobile Computing, 2015, 14(10): 2158-2172.

[4] PAN Xiao, XU Jian, MENG Xiaofeng. Protecting location privacy against location-dependent attacks in mobile services [J]. IEEE Transactions on Knowledge and Data Engineering, 2012, 24(8): 1506-1519.

[5] HASHEM T, KULIK L, ZHANG Rui. Countering overlapping rectangle privacy attack for moving *k*NN queries [J]. Information Systems, 2013, 38(3): 430-453.

[6] WANG Chi, LIU Hua, WRIGHT K L, et al. A privacy mechanism for mobile-based urban traffic monitoring [J]. Pervasive and Mobile Computing, 2015, 20(C): 1-12.

[7] WANG Yong, XIA Yun, HOU Jie, et al. A fast privacy-preserving framework for continuous location-based queries in road networks [J]. Journal of Network and Computer Applications, 2015, 53: 57-73.

[8] 马春光, 周长利, 杨松涛. 路网环境下保护 LBS 位置隐私的连续 *K*NN 查询方法 [J]. 计算机研究与发展, 2015, 52(11): 2628-2644.
MA Chunguang, ZHOU Changli, YANG Songtao. Location privacy-preserving method for LBS continuous *K*NN query in road networks [J]. Journal of Computer Research & Development, 2015, 52(11): 2628-2644.

[9] MA Chunguang, ZHOU Changli, YANG Songtao. A Voronoi-based location privacy-preserving method for continuous query in LBS [J]. International Journal of Distributed Sensor Networks, 2015, 3(11): 1-17.

[10] YING B D, MAKRAKIS D, MOUFTAH H T. Dynamic mix-zone for location privacy in vehicular networks [J]. IEEE Communications Letters, 2013, 17(8): 1524-1527.

[11] GAO Sheng, MA Jianfeng, SHI Weisong, et al. TrPF: a trajectory privacy-preserving framework for participatory sensing [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(6): 874-887.

[12] PALANISAMY B, LIU Ling. Effective mix-zone anonymization techniques for mobile travelers [J]. Geoinformatica, 2014, 18(1): 135-164.

[13] PALANISAMY B, LIU Ling, LEE K, et al. Anonymizing continuous queries with delay-tolerant mix-zones over road networks [J]. Distributed and Parallel Databases, 2014, 32(1): 91-118.

[14] KIM H, CHANG J W. *k*-nearest neighbor query processing algorithms for a query region in road networks [J]. Journal of Computer Science and Technology, 2013, 28(4): 585-596.

[15] 李雯, 夏士雄, 刘峰, 等. 基于运动趋势的移动对象位置预测 [J]. 通信学报, 2014, 35(2): 46-53.
LI Wen, XIA Shixiong, LIU Feng, et al. Location prediction algorithm based on movement tendency [J]. Journal on Communications, 2014, 35(2): 46-53.

[16] YANG Jie, XU Jian, XU Ming, et al. Predicting next location using a variable order Markov model [C]// Proceedings of the 5th ACM Sigspatial International Workshop on GeoStreaming. New York, USA: ACM, 2014: 37-42.

[17] OZER M, KELES I, TOROSLU, et al. Predicting the next location change and time of change for mobile phone users [C]// Proceedings of the Third ACM Sigspatial International Workshop on Mobile Geographic Information Systems. New York, USA: ACM, 2014: 51-59.

[18] BAUMANN P, KLEIMINGER W, SANTINI S. The influence of temporal and spatial features on the performance of next-place prediction algorithms [C]// Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing. New York, USA: ACM, 2013: 449-458.

[19] LARUSSO N D, SINGH A. Efficient tracking and querying for coordinated uncertain mobile objects [C]// Proceedings of the 29th IEEE International Conference on Data Engineering. Piscataway, NJ, USA: IEEE, 2013: 182-193.

(下转第 110 页)