计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200900021

基于生成对抗网络的位置隐私博弈机制

魏礼奇　赵志宏　白光伟　沈　航
南京工业大学计算机科学与技术学院　南京 211816
(201861220045@njtech.edu.cn)

摘　要　文中提出了一种以用户为中心的位置隐私博弈机制,目的是在满足LBS服务质量的基础上生成对应的保护策略,并减小计算规模和效用损失。该机制以Stackelberg博弈模型为基础,用户在请求LBS服务时,采用位置模糊机制对自身位置进行扰动后发送给LBS服务器,使攻击者难以推测自己的真实位置;攻击者根据已知的一部分背景知识,对匿名区域内用户的保护策略进行推断并调整攻击方式,最小化用户隐私水平。为了解决传统线性规划解法在现实场景中计算复杂度过高、实用性低的问题,文中采用生成对抗网络参与保护策略的生成,并尽可能降低效用代价。实验结果表明,该保护机制在隐私保护水平方面有着良好的表现,在损失一定服务质量的同时明显缩短了保护机制的生成时间。

关键词:隐私保护;服务质量;博弈论;机器学习;生成对抗网络
中图法分类号　TP393

Location Privacy Game Mechanism Based on Generative Adversarial Networks

WEI Li-qi,ZHAO Zhi-hong,BAI Guang-wei and SHEN Hang
College of Computer Science and Technology,Nanjing Tech University,Nanjing 211816,China

Abstract　This paper proposes a user-centered location privacy game mechanism,which is aimed to generate corresponding protection strategies based on the LBS service quality,and reduce the calculation scale and utility loss. This mechanism is based on the Stackelberg game model. When a user requests a LBS service,he/she uses the location ambiguity mechanism to disturb his/her location and send it to the LBS server,making it difficult for the attacker to predict his/her real location. Based on part of their known background knowledge,attackers infer the protection policies of users in the anonymous area and adjust their attack methods to minimize the level of user privacy. In order to solve the problem of large scale and long time calculation by traditional mathematical methods,this paper adopts generating countermeasures network to participate in the generation of protection strategy,and reduces the utility cost as much as possible. The experimental results show that the protection mechanism has good performance in terms of privacy protection level,and at the same time,it significantly reduces the generation time of the protection mechanism while losing some quality of service.

Keywords　Privacy protection,Service quality,Game theory,Machine learning,Generative adversarial networks

1　引言

近年来,随着互联网技术、通信技术的发展,如智能手机、智能手表等一大批智能移动设备的普及,丰富了人们的生活。而且随着移动定位技术的进步,以及移动定位设备的发展,基于位置的服务(LBS)已经渗透到人们的生活中,位置也成为了社会生活中不可或缺的关键信息。然而,用户在获取LBS时需要向服务提供商报告自己的位置和查询属性,其中包含用户位置隐私及其他个人敏感信息。通过收集用户LBS请求中的信息,如位置或POI(Point-of-Interest)等,恶意攻击者能够获取并推断出用户的诸多隐私:1)通过挖掘历史位置数据推断出用户的出行规律,并预测出其未来的位置和活动[1-3];2)通过分析特定时段的位置,推断出用户的家庭地址和工作单位[4];3)结合地图等背景知识,推断出用户健康状况和社会关系[5-6];4)通过分析室内位置,推断用户的工作角色、年龄、爱好等[7-8]。这些隐私的泄露将给用户带来难以估量的损失。

大数据技术的产生和机器学习的兴起,凭借其对海量数据进行强大分析的能力,进一步加剧了隐私问题。为了说明这一点,请考虑以下场景:一些用户向LBS服务器发送他们的身份和坐标,以获得某种帮助,如他们附近的POI。访问LBS的攻击者可以在一段时间内收集这些用户的跟踪信息,

到稿日期:2020-09-02　返修日期:2020-11-06　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61502230);江苏省自然科学基金(BK20150960)
This work was supported by the National Natural Science Foundation of China(61502230) and Natural Science Foundation of Jiangsu Province,China(BK20150960).
通信作者:白光伟(bai@njtech.edu.cn)

并使用机器学习技术和一些背景知识（如用户的家庭地址）推断更多有关这些用户的信息。例如，他可以训练一台机器来分类跟踪，将一个类关联到一个家庭地址，从而关联到一个用户，还可以将跟踪开始与它可能的延续联系起来。然后，攻击者可以使用计算机从一个新的跟踪（即使跟踪不包含家庭地址）中识别用户，或者预测用户可能访问的下一个位置。

位置偏移和模糊技术[9-11]通过加入噪声来降低位置的精确度，如真实位置的小范围移动或者以某个区域代替真实位置，来达到保护用户隐私的效果。更多的噪声显然意味着更多的隐私，但重要的是，一般来说，隐私并不是唯一关心的问题；良好的防御不仅必须阻止攻击者发现敏感信息，而且还要满足服务质量（QoS）的需求。在上文的示例中，用户可以向LBS报告一个模糊的位置，但他或她仍然期望得到服务回报，QoS通常会随着混淆程度的增加而降低。例如，报告固定地点或随机选择的地点将保证隐私，但会导致效用极低，因为所获得的POI将接近报告的地点，而该地点通常与真实地点相去甚远。因此，隐私与效用的权衡同样是隐私机制设计中面临的主要挑战之一。

隐私保护与QoS之间的权衡可以通过线性规划来实现。然而，将这种方法应用于现实的位置隐私保护场景中时会遇到困难，线性规划问题的高计算复杂度使得现有工具能处理的位置数上限仅为数百个，超过此上限时，求解时间将大大增加，失去实用意义。此外，背景知识和数据点之间的相关性会影响隐私，并且它们通常难以正式确定和表达。

本文拟研究一种基于机器学习、以用户为中心的位置隐私博弈机制。首先在一定区域内构建一个包含攻击者和用户双方的隐私博弈模型，用户在请求LBS服务时采用位置模糊策略在该区域内按一定保护策略发布虚假位置，使攻击者难以推测用户的真实位置，并尽可能最小化隐私保护代价；攻击者根据自身已知的一部分背景知识，通过分析用户历史发布的位置来反推用户的保护策略，最小化用户隐私水平。用户位于不同位置时，位置模糊的策略也不同。为了高效地生成保护策略，用户在部分位置采用线性规划求解的基础上，借助生成对抗网络（GAN）来生成该区域内其他位置的位置模糊策略。

本文第2节介绍了相关的现有位置隐私保护算法；第3节阐述了系统模型及具体算法；第4节主要介绍了实验的设计及实验结果；最后总结全文并展望下一步工作。

2 相关工作

基于位置模糊的LBS隐私保护技术受到了研究者的关注，其核心思想是对LBS查询中用户的原始数据进行必要的扰动，以避免攻击者获得用户的真实信息数据，同时保证不影响用户获得LBS服务。采用的技术主要有假名（删除或者用一个临时标志来替代用户）、随机化（添加哑元）、模糊化（泛化用户查询过程中的时空信息）和隐蔽化（隐蔽用户的整个查询）。Martucci等[12]将LBS查询中的用户位置用一个临时的假名代替，以打破用户身份与查询之间的联系。但仅仅采用假名并不能充分保护查询隐私，为了增强假名的有效性，文献[10]结合一些复杂的加密方法与假名技术配合使用以保护用户隐私。随机化指在LBS查询中加入随机的哑元，并将哑元和真实查询一起发送给LBS提供商。考虑到随意的随机化并不能很好地保护隐私，Schaub等[13]在使用随机化技术的同时，考虑了普适、拥挤、均匀等指标和与用户真实移动模式相近的哑元，使其看起来更为真实。但是由哑元组成的数据可能与真实数据有很大的差别，甚至产生了一些无效的位置（如在湖中），很容易被攻击者识别。文献[14]中提交给LBS服务器的是一个包含k个位置的匿名区域而非精确的位置，服务器需要在该区域选择参考位置来得到准确的结果，这无疑增加了服务器的负载、响应时间等，降低了服务质量，故需要在隐私与服务质量之间进行权衡。Shokri等[15]提出隐蔽化的方法，拥有一些具体信息的用户可以将这些信息传递给附近的用户，用户请求不是向LBS发起查询，而是由附近的用户来请求查询信息，实现对LBS的隐蔽查询。

上述方法不同程度地忽略了攻击者掌握的用户背景知识量对攻击效果的影响，攻击者利用收集到的数据对用户的位置信息进行推测分析，进而可以排除某些用户。Shokri等[15]提出了基于Stackelberg博弈的保护策略，该策略假设攻击者掌握用户的背景知识，让用户与攻击者轮流进行博弈。用户在确保服务质量损失小于给定阈值的情况下最大化隐私保护水平，而攻击者根据先验知识和偏移位置保证最小化隐私保护水平。通过博弈，该策略可以在保证最优化隐私保护水平的同时确保服务质量损失小于给定阈值，最后通过解最优化问题，得到用户的最优位置隐私保护策略和攻击者的最优攻击策略。

Tripathy等[16]提出了一种基于GAN的方法来构建提供最佳隐私效用交换的机制，并且他们考虑了类似的隐私和效用的概念。文献[16]与本文工作的主要区别在于其处理的是属性隐私，而不是位置隐私。Belghazi等[17]在文献[18]的启发下，提出了一种有效的交互信息神经估计方法，用于估计一类可表示为f-分歧的一般函数。这些方法也适用于连续查询情况和高维数据。Gu等[19]提出了基于预先缓存的连续查询隐私保护机制，降低了连续位置查询间的时间关联，提高了位置隐私保护水平。

综上所述，传统的假名、哑元等保护方法会因攻击者掌握的背景知识量不同而使隐私保护水平受到不同程度的影响；而且目前利用GAN的方法大多考虑的是多用户之间的属性隐私，而非位置隐私。线性规划方法可以在单用户和单攻击者的模型中达到纳什平衡，然而计算复杂度较高。本文将在Stackelberg博弈模型的基础上引入深度学习的方法，通过生成对抗网络生成对应的位置保护策略，在隐私保护水平接近的情况下缩短计算时间。

3 系统模型

本节首先阐述了本机制的隐私保护结构，其次对位置隐私保护中的一些度量进行了介绍，然后设计了攻击者的最佳攻击者策略、用户的最佳保护策略，最后讨论了它们之间的最佳平衡问题。

3.1 模型框架

本文采用基于可信第三方服务器的隐私保护框架，如图1所示。

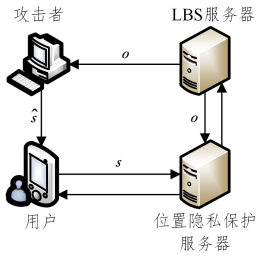


图 1 系统模型框架

Fig. 1 System model framework

(1)用户。在需要服务时发起 LBS 请求,并将自己的位置发送给位置扰动服务器。

(2)位置扰动服务器(Location Perturbation Server,LPS)。将用户的位置根据一定保护策略扰动为虚假位置,提供给 LBS 服务器。

(3)LBS 服务器。根据用户的 LBS 请求返回对应结果。

(4)攻击者。获取到经 LPS 处理后上报的虚假位置后,根据自己的背景知识对用户的真实位置进行推测攻击。

定义用户在发出 LBS 请求时的位置为 s,该 s 将与对应的服务请求共同被发送到 LPS 扰动服务器。LPS 根据自身的保护策略,将真实位置 s 扰动为虚假位置 o 并提交到 LBS 服务器。攻击者自身已经掌握了关于用户位置的背景知识,在获取到 o 之后进行推理攻击,得到推断出的用户位置 $\hat{s}$。

实际上,用户在区域内的位置 s 并不是单一值,它们构成一个集合 $S=\{s_1,s_2,s_3,\cdots,s_n\}$,而扰动后的虚假位置 o 和攻击者推断出的用户位置 $\hat{s}$ 也在此集合中($S=\{\hat{s}_1,\hat{s}_2,\hat{s}_3,\cdots,\hat{s}_n\}=\{o_1,o_2,o_3,\cdots,o_n\}$),其中 n 是可能的位置总数。

用户的位置 s 遵循如下概率分布:

$$\varphi(s)=\Pr(S=s) \tag{1}$$

同时,$\varphi(s)$ 也被攻击者所了解,成为了攻击者的背景知识。

3.2 服务质量代价度量

由于 LPS 将用户位置由真实位置 s 扰动到虚假位置 o,因此从 LBS 服务器得到的查询结果均是基于 o 的。在多数基于 LBS 的服务场景中,o 距离 s 越远,服务质量就越差,因此服务质量代价 Q_{loss} 可用如下公式表示:

$$Q_{loss}=\sum_{o,s}\varphi(s)\cdot p(o|s)\cdot d(o,s) \tag{2}$$

显然 Q_{loss} 不能过大,否则从 LBS 服务器得到的返回结果将失去可用价值。本文假定用户可以承受的最大服务质量代价为为 $Q_{loss}^{\max}$,则有 $Q_{loss}\leqslant Q_{loss}^{\max}$。

3.3 位置隐私保护水平度量

对于特定的位置 s,用户的隐私保护水平 l 可表示为攻击者推测到的位置 $\hat{s}$ 与 s 之间距离 $d(\hat{s},s)$ 的数学期望,如式(3)所示:

$$l=\sum_{o,\hat{s}}p(o|s)\cdot q(\hat{s}|o)\cdot d(\hat{s},s) \tag{3}$$

其中,$p(o|s)$ 为 LPS 的保护策略,$q(\hat{s}|o)$ 为攻击者的推断策略。

$$p(o|s)=\Pr\{O=o|S=s\} \tag{4}$$

$$q(\hat{s}|o)=\Pr\{S=\hat{s}|O=o\} \tag{5}$$

$d(\hat{s},s)$ 被定义为 $\hat{s}$ 与 s 的欧氏距离,$d(\hat{s},s)$ 越大,表示攻击者推断出的位置越不精确,即用户的隐私保护水平越高。

将位置 s_i 拓展到整个集合 S 中,可以得到整个区域中用户的隐私保护水平 L:

$$L=\sum_{s}\varphi(s)\sum_{s,o,\hat{s}}q(\hat{s}|o)\cdot p(o|s)\cdot d(\hat{s},s) \tag{6}$$

为了保证用户隐私,需要为 L 设定一个下限值 $L_{\min}$,且 $L\geqslant L_{\min}$。

3.4 最优攻击策略

攻击者的目标是尽可能减小推断位置与真实位置之间的距离 $d(\hat{s},s)$。对于所有可能的 s,其数学期望 $E(d(\hat{s},s))$ 为:

$$E(d(\hat{s},s))=\sum_{s}\varphi(s)\sum_{\hat{s}}\Pr\{\hat{s}|s\}\cdot d(\hat{s},s) \tag{7}$$

而 $\Pr\{\hat{s},s\}=q(\hat{s}|o)\cdot p(o|s)$,因此式(7)可改写为:

$$E(d(\hat{s},s))=\sum_{s,o,\hat{s}}\varphi(s)\cdot q(\hat{s}|o)\cdot p(o|s)\cdot d(\hat{s},s) \tag{8}$$

至此,可以构造一个线性规划问题:在已知用户背景知识 $\varphi(s)$ 与 LPS 保护策略 $p(o|s)$ 的情况下,求解出最优的攻击策略 q^*:

$$q^*=\arg\min_{q}E(d(\hat{s},s))=\sum_{s,o,\hat{s}}\varphi(s)\cdot q(\hat{s}|o)\cdot p(o|s)\cdot d(\hat{s},s) \tag{9}$$

3.5 最佳保护策略

用户的目标是在满足隐私保护水平 $L_{\min}$ 的前提下,尽可能降低服务质量代价 Q_{loss}。与攻击者的最佳攻击类似,在已知用户背景知识 $\varphi(s)$ 与最佳攻击策略 $q^*(\hat{s}|o)$ 的情况下,可以求解出最优的保护策略 p^*,并且满足隐私保护水平:

$$p^*=\arg\min_{p}Q_{loss}=\arg\min_{p}\sum_{s,o,\hat{s}}\varphi(s)\cdot p(o|s)\cdot d(o,s) \tag{10}$$

$$\text{s.t.}\quad\sum_{s,o,\hat{s}}\varphi(s)\cdot p(o|s)\cdot q^*(\hat{s}|o)\cdot d(s,s)\geqslant L_{\min} \tag{11}$$

由于求解 p^* 需要先求解 q^*,而求解 q^* 又需要已知用户的保护策略 p,因此式(9)和式(11)构成了一个博弈模型。

对攻击者而言,对于他接收到的任意 o,其最优攻击策略可表示为:

$$q^*(\hat{s}'|o)=\sum_{\hat{s}}q(\hat{s}|o)\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s) \tag{12}$$

其中,$\hat{s}'$ 表示任意 $\hat{s}$,则式(11)可改写为:

$$\min_{q^*(\hat{s}'|o)}\sum_{\hat{s}}q(\hat{s}|o)\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\geqslant L_{\min} \tag{13}$$

需要注意的是,$\hat{s}'$ 可以是 S 中的任意值,因此 $q^*(\hat{s}'|o)$ 实际上可以表示为如下数学期望:

$$q^*(\hat{s}'|o)=E(\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)) \tag{14}$$

那么必然存在一个 $s_0\in S$ 满足式(15)。

$$\min_{q^*(\hat{s}'|o)}\sum_{\hat{s}}q(\hat{s}|o)\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\geqslant \min_{s_0}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s) \tag{15}$$

且 s_0 满足如下条件:

$$s_0=\arg\min_{\hat{s}}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s) \tag{16}$$

注意到 $s_0\in S$,因此有:

$$\min_{q^*(\hat{s}'|o)}\sum_{\hat{s}}q(\hat{s}|o)\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\leqslant \min_{\hat{s}}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s) \tag{17}$$

由式(13)－式(17)可得：

$$\sum_{s,o,\hat{s}}\varphi(s)\cdot p(o|s)\cdot q^{*}(\hat{s}|o)\cdot d(\hat{s},s)=\min_{\hat{s}}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s) \tag{18}$$

这样，式(11)可以表示为：

$$\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\geqslant\min_{\hat{s}}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\sum_{o}\min_{\hat{s}}\sum_{s}\varphi(s)\cdot p(o|s)\cdot d(\hat{s},s)\geqslant L_{\min} \tag{19}$$

式(10)和式(18)中仅包含 p，不再包含 q^{*}，因此原问题转化为单一线性规划问题，可以求解。

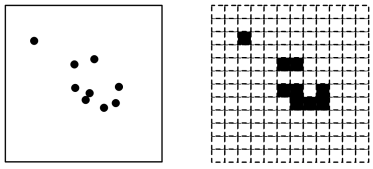
4 基于生成对抗网络的位置保护算法实现

第3节提出并证明了生成最优保护策略的线性规划算法，由于 p 的求解空间 P 包括区域内所有点 $s\in S$ 的 n 个保护策略 $p(o|s)$，$p(o|s)$的解空间又是以 n 为变量的指数函数，因此仅靠线性规划穷举求解开销过高，不适用于粒度划分比较细致的实际应用场合。

实际上，每个保护策略 $p(o|s)$都是一个二维的概率分布，因此可以将问题拆分为两步求解：先将保护区域划分为较粗的网格，在控制位置点数量的情况下使用第3节中的算法求出初步解；然后对网格进行更细粒度的划分，通过生成对抗网络(GAN)在初步解的基础上进行进一步的保护策略生成。

4.1 粒度划分

现实生活中的位置是一个连续变化的二维变量，因此需要先进行离散化，以便算法模型进行处理。本文采取常规的粒度化算法，即将一个区域等分成共有 a 行、b 列的正方形网格，所有处于此网格的用户都以该网格的中心点坐标作为自己的位置，如图2所示。



(a)粒度化前　(b)粒度化后

图2 粒度化过程

Fig. 2 Granulation process

假定原来的区域内分布着 n 个可能的位置(x_n,y_n)及其概率分布p_{x_n,y_n}，则具体的粒度化算法如下：

步骤1 获取区域的左下角、右上角的经纬度坐标(x_L,y_L)及(x_R,y_R)。

步骤2 根据划分粒度 a,b 计算出网格大小$x_0=\frac{x_R-x_L}{a}$，$y_0=\frac{y_R-y_L}{b}$。

步骤3 将原有点的经纬度坐标转换成网格坐标：$X_n=\mathrm{int}\left(\frac{x_n-x_L}{x_0}\right)$，$Y_n=\mathrm{int}\left(\frac{y_n-y_L}{y_0}\right)$，其中 int()为取整函数。

步骤4 计算每个网格的概率。

$$P_{X,Y}=\sum_{i=1}^{n}(p_{x_n,y_n}*exact(X,X_n)*exact(Y,Y_n))$$

其中，当 $x=y$ 时，$exact(x,y)$输出1，其余情况均输出0。

考虑到线性规划问题求解的规模不能过大，因此第一步划分的粒度一般应使 $a*b\leqslant 150$。

4.2 网络模型

本文提出了图3所示的条件生成对抗网络(Conditional GAN)模型。图3中，R 在初始条件下为使用第3节的算法在粗划分下生成的原始样本。G 和 D 分别为生成器和判别器，均由多层CNN组成。生成器 G 通过接收输入噪声 z，输出对应的概率分布 $x=G(z)$。判别器在接收 $G(z)$后将其与 R 中的样本进行对比，根据二者概率分布的相似程度输出 $y=D(G(z))$。y 的取值范围为(0，1)，越接近1，说明生成的 $G(z)$越接近 R。

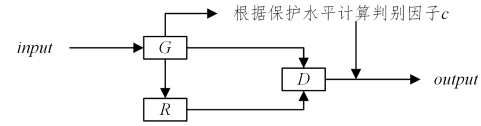


图3 条件生成对抗网络模型

Fig. 3 Conditional GAN model

实际上，即使 y 的值比较接近1，仍然会出现 $G(z)$的隐私保护水平 L 不满足 $L\geqslant L_{\min}$ 的情况。为了解决此问题，生成器 $G(z)$的输出会被复制一份，并使用式(6)计算其对应的隐私保护水平 $L(z)$。判别因子 c 采用式(20)来计算：

$$c=\begin{cases}\dfrac{\ln 2}{softplus(L_{\min},L(z))}, & L(z)<L_{\min}\\ 1, & L(z)>L_{\min}\end{cases} \tag{20}$$

其中，softplus 函数的定义为：

$$softplus(a,b)=\ln(1+e^{(a-b)}) \tag{21}$$

这个函数是非负的且单调递增的，当 $a<b$ 时它的值接近0，而当 $a>b$ 时它增长非常快。因此，当 $L(z)<L_{\min}$时，c 的分母会迅速变大，导致 c 迅速减小到一个接近于0的值。

有了判别因子 c 后，我们便可以修改 D 的输出。

$$y=c*D(G(z)) \tag{22}$$

当 $L(z)<L_{\min}$时，c 的值快速趋近于0，这会显著降低 D 的打分 y，促进训练过程向 $L(z)>L_{\min}$的方向进行。

5 实验与结果分析

本节将对上文提出的算法进行仿真实验，并分析实验结果。实验的硬件环境为 Intel Core i9-9900K CPU、GTX1080 GPU 和 32GB 内存，Ubuntu 18.04 LTS 操作系统，算法本体主要采用 Tensorflow 和 Keras 来实现。

5.1 基本模糊位置保护策略

定义模糊水平 k，在区域中找到离位置 s 最近的 $k-1$ 个位置$o_1,o_2,o_3,\cdots,o_{k-1}$，并设定保护策略 $p(o|s)$为：

$$p(o|s)=\begin{cases}\dfrac{1}{k}, & \text{if } o\in\{o_1,o_2,o_3,\cdots,o_{k-1},s\}\\ 0, & \text{otherwise}\end{cases} \tag{23}$$

式(23)表示 LPS 将位置 s 扰动到包括其自身的位置集合$\{o_1,o_2,o_3,\cdots,o_{k-1},s\}$中的任意一个位置中，并将该位置作为虚假位置 o 发送到 LBS。该机制的实现较为简单，常被作为其他位置隐私保护算法的对照。

5.2 贝叶斯攻击

假设 $P(B|A)$表示在 B 事件发生的情况下 A 事件发生

的概率，那么贝叶斯法可表示为：

$$P(A_i|B)=\frac{P(B|A_i)\cdot P(A_i)}{\sum_{i=1}^{n}P(B|A_i)\cdot P(A_i)} \tag{24}$$

其中，$A_1, A_2, \cdots, A_n$ 为完备事件组，即 $\bigcup_{i=1}^{n}A_i=\Omega$，$A_iA_j=\Phi$，$P(A_i)>0$。

对于攻击者来说，这里的 B 事件表示经匿名服务器匿名后发布的可观察数据，Ω 包含所有可能的原始信息的候选值。攻击者可根据式(24)进行贝叶斯攻击，并根据指定的度量选择最佳攻击结果。本文利用保护机制 $p(o|s)$ 对用户发布的原始数据进行处理，攻击者观察到的数据只有 o。攻击者在了解到 p 的具体保护机制后，可以运行贝叶斯攻击 q 来对用户的真实位置进行推测，如式(25)所示：

$$q(\hat{s}|o)=\frac{p(\hat{s}|o)\cdot p(o)}{\sum_{o}p(\hat{s}|o)\cdot p(o)} \tag{25}$$

5.3 实验设计

本实验将本文算法在实际用户的历史位置分布数据上进行计算，并评估其隐私保护水平、效用损失和计算时间。

实验采用的数据集来自微软亚洲研究院发布的 Geolife Trajectories 位置轨迹数据集 1.3 版本[1)]，取其中 10 个用户在三环路 13 km * 13 km 范围内的位置轨迹作为实验的初始数据集。表 1 列出了实验中基本参数的取值。

表 1 实验环境参数设置

Table 1 Experimental parameters

参数名称	参数值/范围
区域划分粒度(第一步)	10 * 10
区域划分粒度(第二步)	40 * 40
训练迭代次数	50000
基础模糊算法模糊水平 k	7
隐私保护水平最小值 $L_{\min}$	0.1 km

为了验证本文算法的有效性，实验引入了另外 4 个对照组，它们分别采用不同的攻击和保护算法组合，如表 2 所列。

表 2 实验组及对照组设定

Table 2 Experimental group and control group algorithm

组别名称	保护算法	攻击算法
Obfs,Bayes	基本模糊算法	贝叶斯攻击
Opt,Bayes	最优保护算法	贝叶斯攻击
Obfs,Opt	基本模糊算法	最优攻击算法
Opt,Opt	最优保护算法	最优攻击算法
GAN,Opt(实验组)	GAN	最优攻击算法

5.4 结果分析

(1)最大可容忍位置服务质量损失 $Q_{loss}^{\max}$ 与隐私水平 L 之间的关系

图 4 给出了不同最大可容忍位置服务质量损失 $Q_{loss}^{\max}$ 下的隐私保护水平。可以看出，随着最大可容忍位置服务质量损失 $Q_{loss}^{\max}$ 的增加，隐私保护水平 L 也随之增加，但趋势各不相同。在贝叶斯攻击下，基础模糊算法可以实现不错的隐私保护水平。然而，在最优攻击下 L 相比贝叶斯攻击大幅下降，这是由于在本实验取模糊水平 $k=7$ 的设定下，基础模糊算法的隐匿范围相对较小，攻击方通过线性规划可以很容易地逼近最优解；而当 k 取值过大时，基础模糊算法的时间复杂度将呈指数级增长，保护效果也不及最优保护算法。此外，最优保护算法的隐私保护水平也有显著降低，因此对攻击者而言，使用最优攻击算法显然是更好的选择。

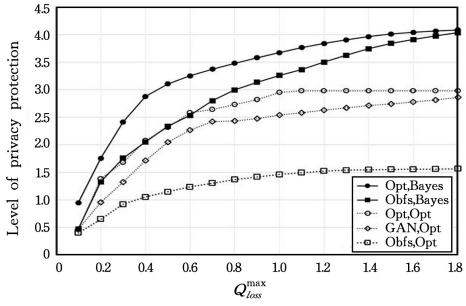


图 4 用户隐私保护水平

Fig. 4 Level of privacy protection of a user

本文比较了最优攻击下 3 种保护算法的效果，最优保护算法和本文利用 GAN 的算法的隐私保护水平均显著优于基础模糊算法。其中，最优保护算法的保护水平最高，并在 $Q_{loss}^{\max}\geqslant 1.1$ km 时为恒定值，表明攻击者和用户在此时已经形成纳什平衡。GAN 的隐私保护水平总体则比最优保护算法低 15%～18%。

(2)最大可容忍位置服务质量损失 $Q_{loss}^{\max}$ 与服务质量损失 Q_{loss} 之间的关系

图 5 给出了不同最大可容忍位置服务质量损失 $Q_{loss}^{\max}$ 下的服务质量损失。基础模糊算法的执行与攻击者采用何种攻击算法无关，因此在贝叶斯攻击和最优攻击两种情况下的 Q_{loss} 完全相等；最优保护算法在最优攻击下的隐私保护水平 L 相比贝叶斯攻击有显著降低，因此 Q_{loss} 也有所降低。基于 GAN 的保护算法下的 Q_{loss} 与最优保护算法相比基本相似。

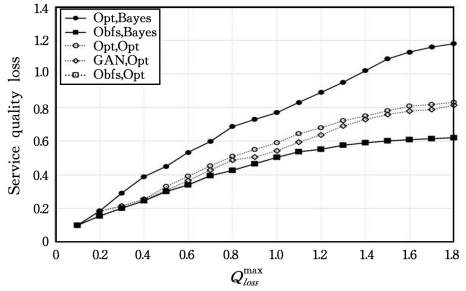


图 5 服务质量损失

Fig. 5 Service quality loss

(3)不同算法的计算时间对比

表 3 列出了不同算法下耗费计算时间的对比结果。最优保护算法由于涉及复杂度很高的线性规划求解，因此在贝叶斯攻击下的计算时长是采用基础模糊算法时的 20 多倍，达到了 21 h；而在最优攻击下又涉及联立线性规划方程组，计算时间进一步大幅增加到近 6 天。与之相比，基础模糊算法由于较为简单，在最优攻击算法下生成保护策略的时间最短，仅需 3 h 13 min。而本文基于 GAN 的算法用时约 16 h。

1) http://research.microsoft.com/apps/pubs/?id=79440

表 3 计算时间对比

Table 3 Calculation time comparison

组别名称	计算时间
Obfs，Bayes	40 min
Opt，Bayes	21 h 2 min
Obfs，Opt	3 h 13 min
Opt，Opt	139 h 36 min
GAN，Opt(实验组)	15 h 55 min

综上所述，本文算法在位置隐私保护方面有着较为良好的表现，在粗粒度划分的条件下利用基于博弈模型的算法保证了隐私保护水平 L 与服务质量损失 Q_{loss} 尽可能做到最优、均衡，而 GAN 的引入则在使隐私保护水平 L 相比最优保护算法降低不大的同时，显著缩短了计算时间。

结束语 本文提出了一种基于生成对抗网络的位置隐私保护机制，通过将传统的最优化求解方法与 GAN 相结合，使用位置扰动策略对用户在请求 LBS 服务时的真实位置进行模糊处理，防止暴露真实位置。实验结果表明，本机制在隐私性和实用性都有保证的前提下，相比最优保护算法缩短了计算时间，使隐私保护模型更具备实用性。

而现实场景中多数区域内的用户数量远不止一个，本机制只考虑了区域内仅有单用户场景下的隐私保护需求，因此第三方可信服务器的计算开销与用户数量成正比关系；如果用户较多，服务器的运算负担仍然会较重。实际上，多用户之间的位置隐私可以通过协作来实现，让扰动算法根据不同的用户 ID 来为群体提供位置隐私保护，以进一步优化隐私保护效果(类似的思路也被用在群智感知的任务分配上)。因此，我们将其作为后续的工作方向。

参 考 文 献

[1] SONG C，QU Z，BLUMM N，et al. Limits of predictability in human mobility[J]. Science，2010，327(5968)：1018-1021.

[2] PELLUNGRINI R，PAPPALARDO L，PRATESI F，et al. A data mining approach to assess privacy risk in human mobility data [J]. ACM Transactions on Intelligent Systems and Technology，2018，9(3)：1-27.

[3] YAO D，ZHANG C，HUANG J，et al. Serm：a recurrent model for next location prediction in semantic trajectories[C]// Procceding of ACM Conference on Information and Knowledge，Management (CIKM). 2017：2411-2414.

[4] ZHENG Y. Trajectory data mining：an overview [J]. ACM Transactions on Intelligent Systems and Technology，2015，6(3)：1-41.

[5] BACKES M，HUMBERT M，PANG J，et al. Walk2friends：Inferring social links from mobility profiles[C]// Procceding of ACM SIGSAC Conference on Computer and Communications，Security (CCS). 2017：1943-1957.

[6] FAWAZ K，SHIN K G. Location privacy protection for smartphone users[C]// Procceding of ACM SIGSAC Conference on Computer and Communications Security (CCS). 2014：239-250.

[7] XU Q，ZHENG R，TAHOUN E. Detecting location fraud in indoor mobile crowdsensing[C]// Procceding of the First ACM Workshop on Mobile Crowdsensing Systems and Applications (Crowd-SenSys). 2017：44-49.

[8] KONSTANTINIDIS A，CHATZIMILIOUDIS G，ZEINALIPOUR-YAZTI D，et al. Privacy-preserving indoor localization on smartphones[J]. IEEE Transactions on Knowledge & Data Engineering，2015，27(11)：3042-3055.

[9] ANDRES M E，BORDENABE N E，CHATZIKOKOLAKIS K. Geo-indistinguishability：differential privacy for location-based systems[C]// Procceding of the 20th ACM Conference on Computer and Communications Security (CCS). 2013：901-914.

[10] YIU M L，JENSEN C S，MOLLER J. Design and analysis of a ranking approach to private location-based services[J]. ACM Transactions on Database Systems，2011，36(2)：1-42.

[11] PERAZZO P，DINI G. A uniformity-based approach to location privacy[J]. Computer Communications，2015，64(1)：21-32.

[12] MARTUCCI L A，ZUCCATO A，FISCHER-HÜBNER S. Identity deployment and management in wireless mesh net-works [C]// IFIP International Summer School on the Future of Identity in the Information Society. Boston，MA：Springer，2007：223-233.

[13] SCHAUB F，MA Z，KARGL F. Privacy requirements in vehicular communication systems[C]// 2009 International Conference on Computational Science and Engineering. IEEE，2009，3：139-145.

[14] KIDO H，YANAGISAWA Y，SATOH T. An anonymous communication technique using dummies for location-based services [C]// Procceding of IEEE International Conference on Pervasive Services (ICPS'05). 2005：88-97.

[15] SHOKRI R，THEODORAKOPOULOS G，TRONCOSO C. Protecting location privacy：optimal strategy against localization attacks[C]// Procceding of ACM Conference on Computer and Communications Security. 2012：617-627.

[16] TRIPATHY A，WANG Y，ISHWAR P. Privacy-preserving adversarial networks，CoRR，2017：abs/1712.07008 [OL]. http://arxiv.org/abs/1712.07008.

[17] BELGHAZI M I，BARATIN A，RAJESHWAR S，et al. Mutual information neural estimation[C]// International Conference on Machine Learning. PMLR，2018：531-540.

[18] NOWOZIN S，CSEKE B，TOMIOKA R. f-GAN：training generative neural samplers using variational divergence minimization[C]// Procceding of the Annual Conference on Neural Information Processing Systems. 2016：271-279.

[19] GU Y M，BAI G W，SHEN H，et al. Precache Based Privacy Protection Mechanism in Continuous LBS Queries[J]. Computer Science，2019，46(5)：122-128.

WEI Li-qi，born in 1994，postgraduate. His main research interests include location privacy protection.

BAI Guang-wei，born in 1961，Ph. D，professor，doctoral supervisor，is a member of China Computer Federation Outstanding. His main research interests include mobile Internet，network security，location services and so on.