# 一种主动扩散式的位置隐私保护方法

叶阿勇[1],林少聪[1],马建峰[1,2],许 力[1]
(1.福建师范大学密码技术与网络安全福建省重点实验室,福建福州 350007;
2.西安电子科技大学计算机学院,陕西西安 710071)

**摘 要:** 随着基于位置的信息服务的日益普及,位置信息的隐私保护已逐渐成为了一个突出的安全问题.因此,提出了一种基于主动共享机制的位置隐私保护方案,该方案引入位置服务信息的邻近共享机制,通过在邻居节点主动共享位置服务信息,有效降低了移动用户对位置服务器的依赖,从而提高了其位置信息的隐私性.论文分别采用病毒传播模型和仿真实验对方案进行理论分析和有效性验证.

**关键词:** 位置隐私保护; 位置服务; 网络安全
**中图分类号:** TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2015)07-1362-07
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.07.017

# An Active Diffusion Based Location Privacy Protection Method

YE A-yong[1], LIN Shao-cong[1], MA Jian-feng[1,2], XU Li[1]
(1. *Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian* 350007, *China*;
2. *School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi* 710071, *China*)

**Abstract:** In recent years, while the location-based services have become very popular, location privacy issue has also attracted more and more attention from researchers to users. In this article, we present a privacy preserving strategy based on an active diffusion mechanism. The sharing mechanism of location service information in the neighborhood was introduced to reduce the dependence of users on LBS server, thereby resisting the private information disclosure. Through theoretical analysis and simulation results, we have verified the effectiveness of our proposal.

**Key words:** location privacy protection; location based services; network security

## 1 引言

基于位置的服务(Location Based Services, LBS)是指在获取移动的位置坐标的基础上,为用户提供的各种信息增值服务[1].随着无线定位技术和移动互联网的快速发展,基于位置的服务已日益普及.普通用户都可以通过手机等智能设备获得各种丰富的位置服务,如导航、社交/交友、寻找附近的兴趣点、微博签到等.然而,用户在享受 LBS 带来各种便利的同时,也面临着位置隐私暴露的风险.用户在请求 LBS 时,需要向服务器发送自身的位置坐标,如果服务器系统存在安全漏洞,或者内部人员滥用这些位置信息,则用户就面临位置隐私暴露的安全威胁.

Reza Shokri 等在文献[2]中提出了一种协作机制来提高用户位置的隐私性.在该方案中,移动用户需要位置服务时,先尝试向附近用户请求协助,若没有邻居可共享 LBS 信息再向 LBS 服务器请求.这种协作机制可减少用户将自身位置暴露给服务器的机会,提高了位置的隐私性.但该方案在用户数量比较少或者停留时间较短暂的情况下,信息共享效率比较低下,隐私保护效果不明显.针对该问题,我们提出一种基于主动扩散的协作机制,用于提高 LBS 信息的共享效率,从而增强了用户位置的隐私保护.另外,本方案也可有效降低位置服务器的业务负载,提高系统的可扩展性.

## 2 相关工作

近年来,研究者们已提出了许多种用户位置隐私的保护方案.根据匿名原理的不同,已有方案大致可分为三大类:位置 $K$ 匿名模型[3~7]、位置匿名模型[8~10]和分布式协作模型[11~13].

收稿日期:2014-07-03;修回日期:2014-12-18;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61202452, No.U1405255, No.61202451, No.61202450);福建省工业科技重点项目(No.2014H0018);福建省教育厅产学研项目(No.JA12063);福建省 2013 战略性新兴产业技术开发(No.闽发改高技[2013]266 号)

文献[3]最早将 $K$ 匿名方法应用到位置隐私保护中.其基本原理是,用一个覆盖其他 $K-1$ 个用户的区域来代替用户的真实位置,这样,用户在该区域中被 LBS 服务器识别出来的概率为 $1/k$.但该方案在用户数量密度比较大的情况下,选取的区域可能比较小,从而在一定程度上会暴露了用户位置.为了解决这个问题,Gedik B 等人提出了一种支持个性化匿名的 Casper 方案[4],该方案增加了一个最小匿名区域 $A_{\min}$的安全保护,即这 $K$ 个用户的匿名区域不能太小.该方案的缺点是 $A_{\min}$值越大,则匿名区域面积也随之增大,QoS 依然也会下降.为提高匿名的成功率,文献[5]采用一种 Privacy Grid 网格的匿名方法,允许用户指定所需的隐私要求、位置多样性和所允许的最小匿名区域面积,该方案从多个方面保护了用户的隐私,因此匿名成功率很高;但计算开销和位置更新代价很大,并也会造成匿名区域过剩等问题.

位置匿名模型主要通过发布虚假位置或位置坐标区域化(或模糊化)等方法来实现位置隐私保护.例如,文献[8]提出了一种基于虚假位置的隐私保护方案,用户在提交自身真实位置坐标的同时,还发送其他伪造的虚假位置信息给位置服务器,使攻击者无法识别出用户的真实位置.但由于用户的精确位置还是混在报告信息之中,所以还是存在一定的安全隐患.文献[9]提出一种位置相似度的概念;该方案中,整个服务区域给细化分为网格,位置服务器先根据每个网格的兴趣点查询结果的相似度,计算出服务区域的相似地图,并传递给移动设备;用户再依据相似地图构造出一个服务轮廓(区域),用于代替自身位置向 LBS 服务器请求服务,从而实现位置保护.文献[10]提出了一种模糊区域和制造虚假节点相结合的方案,在用户数量比较多的地区,由第三方匿名服务器收集足够多的用户,构造成模糊的区域,利用模糊区域向位置服务器发送请求信息,这样,位置服务器就不能知道用户的具体位置,当用户数量比较少达不到要求时,匿名服务器利用算法构造虚假节点,利用虚假节点和相关用户构成匿名区域.该方案能在位置服务质量和系统开销方面得到一个平衡.

分布式协作模型是指用户之间通过协作实现匿名的方法,这种匿名过程不依赖于第三方可信服务器.例如,文献[11]提出了一种基于 TTP Free Protocol 的位置隐私保护方案,用户间自主形成若干个组,并把将自身真实位置发送给组长,当某个用户需要位置服务信息时,组长首先向数据中增加噪声来隐藏位置信息,然后将整个组内所有请求发送给位置服务器;该方案的优点是避免多个用户同时发送请求,对位置服务器造成信道冲突,在保护位置隐私的同时提高系统的效率.缺点是组长要对组内其他成员的信息进行处理,增加了组长的负担.

## 3　主动扩散式位置隐私保护机制

### 3.1　方案的基本描述

传统的 LBS 系统主要由两部分组成:位置服务器和移动用户.如图 1 所示,当移动用户需要位置信息服务时,如查找周边的兴趣点或者附近好友,需要向服务器发送服务请求和自身的位置信息;位置服务器利用用户的位置坐标计算出其所需的位置服务信息,并将结果返回给用户.在这种模式中,用户在每次服务请求时都需要把自身的精确位置报告给服务器,如果服务器系统存在安全漏洞或者内部人员非法使用这些位置信息,则请求用户就存在位置隐私暴露的安全威胁.

针对传统 LBS 模型存在用户位置隐私暴露隐患的问题,本文在 Reza Shokri 方案的基础上进行改进,提出了一种基于主动共享机制的位置隐私保护方案.在该方案中,邻居设备可以互相共享本区域的位置服务信息,从而减少将自身位置信息直接暴露给服务器的机会,提高了位置服务系统的隐私保护安全.具体设计方案如下:在每个用户设备中都设置一个缓存,用于缓存从服务器或周边设备获取到的位置服务信息;为了确保服务信息的正确性,缓存中的信息都设有一个存活期,过期将被删除;为了提高通信效率,我们将位置信息划分成多个小区域;用户在移动过程中可以将自身拥有的信息主动“传染”给其他用户.

如图 2,假定 A 是需要位置服务信息的用户,如果用户 A 直接向服务器请求服务,会导致自身位置信息暴露给服务器;而如果用户 A 获得了邻近用户 B 共享的位置服务信息,则无需向服务器请求服务,因此,用户 A 的位置就不会暴露给服务器,位置隐藏成功.

该方案降低了用户对服务器的依赖,使得黑客不容易通过攻击位置服务器来获取用户位置信息.避免了系统的攻击中心与系统的安全瓶颈.该方案也不需要改动现有的 LBS 结构,也不需要引入第三方平台,大大降低了系统的改造成本.

### 3.2　历史踪迹的预分析

我们首先根据 CRAWDAD[14]采集的移动用户轨迹数据进行分析,该数据集收集了美国 San Francisco 市 Bay 区中 500 辆的士在 30 天内的移动轨迹数据.我们以的士模拟作为移动点,分别考察三个指标:(1)逗留时间,指移动点在参考半径 100 米范围内的平均逗留时间;(2)不同半径范围内的移动点数量统计;(3)一天 24 小时内,各时间段内的移动点数量分布;分析结果如图 3 所示.

由图 3 ~ 5 可得:多数移动点在 100m 参考半径内约有 100s 以上的平均逗留时间;半径越大的区域范围内移动点越多;不同时间段内,移动点数量有所不同.以上分析中可知,在每个时间段内,每个区域内都有一定

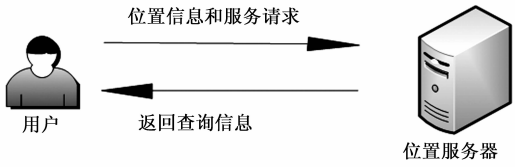


图1 传统的LBS的结构

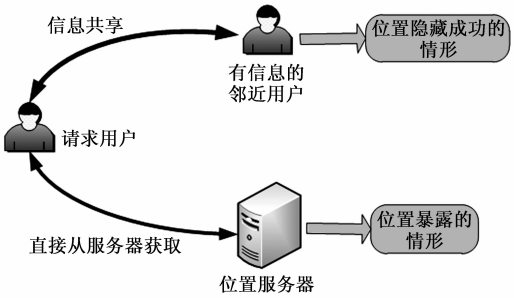


图2 基于信息共享的位置隐私保护方案

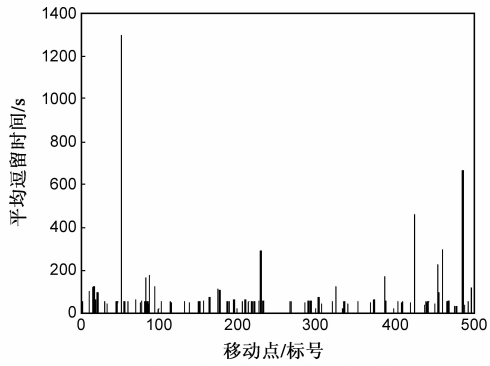


图3 移动点的平均逗留时间

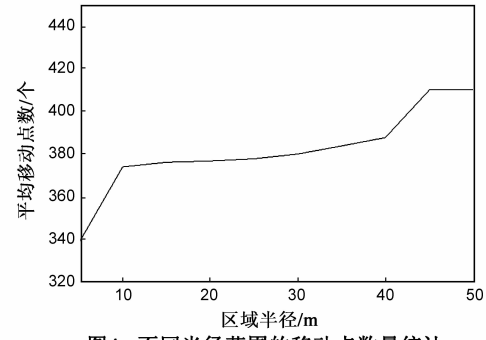


图4 不同半径范围的移动点数量统计

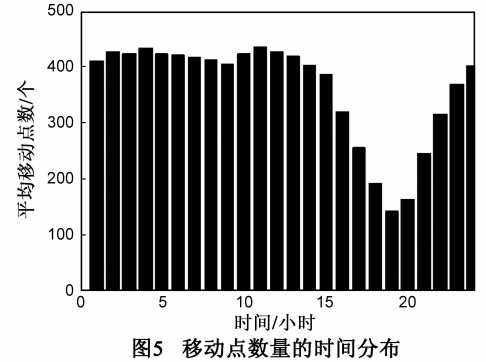


图5 移动点数量的时间分布

数量的移动点存在.因此,通过在每个区域内建立共享和传递机制是可行的,可以减少用户向位置服务器的请求次数,避免将自身位置信息直接暴露给服务器.

### 3.3 算法设计

我们在3.2节数据分析的基础上,提出一种主动式扩散机制算法,具体描述如下:

(1)将整个服务区域 $C$ 划分为一个 $n \times m$ 网格,并定义子区域为 $C_{ij}, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$.关于网格的大小,后面再讨论.

(2)每个移动点都设置了一个缓存,用于缓存从服务器或附近设备获得的位置服务信息.当移动点需要服务信息时,则先查询自身缓存,若没有,才向LBS服务器请求,并将返回结果保存在缓存中.为了保障信息扩散的安全,LBS需要对发布的消息进行签名;并且,每个服务信息都设有一个有效保存期,离开原区域或者过期都将作废.

(3)每个移动点如果拥有服务信息时,则周期向邻居广播一个信标,用于公告其拥有的服务信息.

(4)邻近区域中的其他移动设备,当收到信标信息时,如果自身没有该信息且对其感兴趣,则向源节点申请共享.移动点可能会收到多个来自不同移动点但主题相同的信标,可以选择向信号质量最好的邻居节点申请共享信息.

根据上述算法,设计了一个共享协议如图6所示.

Protocol of LBS sharing between neighbors

$p$: if has the $\mathrm{LBS}_{ij}^{a}$ then broadcast $\mathrm{Beacon}_{p}^{a} = \{i, j, a, p\}$ at each period $\Delta t$

$\{q \mid q \in N(p)\}$: if $\mathrm{LBS}_{ij}^{a}$ is unknown and interesting then

$q \rightarrow p$: LBS requisition

$p \rightarrow q$: $\mathrm{LBS}_{ij}^{a} = \{i, j, a, \mathrm{TTL}, E_{sk}(i, j, a, \mathrm{TTL})\}$

图6 邻居共享协议

其中,$\mathrm{LBS}_{ij}^{a}$表示LBS服务器在子区域 $C_{ij}$关于主题 $a$ 的服务信息;$E_{sk}(i, j, a, \mathrm{TTL})$为LBS服务器对信息的签名,用于防止消息被假冒和篡改;TTL为信息的有效保存期.$\mathrm{Beacon}_{a}^{p} = \{i, j, a, p\}$表示移动点 $p$ 广播的信标消息,其中:$(i, j)$指明区域,$a$ 为主题,$p$ 为节点ID.

## 4 理论分析

### 4.1 理论分析模型

我们利用SIR病毒传播模型[15]对本文方案进行理论分析.在SIR模型中,将一定区域内的生物体分为三类状态,一类是已感染状态 infection;一类是易感状态 susceptible;另一类是死亡或免疫后的被删除状态 removed,此种状态的生物体会结束该生物体带来重复感染的可能性.SIR的模型方程如下:

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t)\\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta I(t)S(t) - \gamma I(t)\\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t)\end{cases} \tag{1}$$

其中,参数 $\gamma$ 表示个体因感染或者获得免疫的比例,$\beta$ 表示传染率,$-\beta S(t)I(t)$表示易感者向感染者转换的增量.

根据位置信息的主动共享机制特征,我们在 SIR 模型的基础上建立本文方案的信息传播模型.为了便于描述,所以我们先定义以下参数,如表 1 所示.

**表 1　各个参数的代表含义**

| | |
|---|---|
| $\beta$ | 表示在一个区域和时间段内,用户与其邻近用户间的信息传染率. |
| $\mu$ | 表示在一个时间段内,外部用户进入某个区域的概率. |
| $\lambda$ | 表示在一个时间段内,内部用户离开某个区域的概率. |
| $\gamma$ | 用户询问请求的频率. |
| $\delta$ | 信息存在缓存里的存活周期. |
| $\omega$ | 用户接触服务器前的等待时间. |

我们依据是否位于本区域内、是否已获得相关位置服务信息以及对该信息是否感兴趣的情形,将系统用户分成 $S$、$S^*$、$I$、$I^*$、$R$、$R^*$ 等六类,具体含义如表 2 所示.

**表 2　用户类型**

| | |
|---|---|
| $S$、$S^*$ | 表示未获得 LBS 信息但对其感兴趣的用户,其中,$S$ 表示区域内,$S^*$ 表示区域外 |
| $I$、$I^*$ | 表示拥有 LBS 信息的用户,其中,$I$ 表示区域内,$I^*$ 表示区域外 |
| $R$、$R^*$ | 表示信息无兴趣、自身也没有 LBS 信息的用户,$R$ 表示区域内,$R^*$ 表示区域外 |

图 7 是用户类型的状态转换图.在每个时间段中,由于用户的获得信息,或者存储在用户缓存上的信息消逝,或者用户在区域间迁移,用户的状态都会发生变化.$R$、$R^*$、$S$、$S^*$、$I$ 和 $I^*$ 六个状态间会互相转换.为了简化模型,我们没有考虑 $R^*$ 和 $S^*$ 之间的状态迁移.

由图 7 分析可得,各用户类型的数量变化分别服从如下方程:

$$\begin{cases}\dfrac{\mathrm{d}}{\mathrm{d}t}S(t) = \mu S^*(t) - (\beta I(t) + \omega + \lambda)S(t) + \gamma R(t)\\ \dfrac{\mathrm{d}}{\mathrm{d}t}S^*(t) = \lambda S(t) - (\omega + \mu)S^*(t)\\ \dfrac{\mathrm{d}}{\mathrm{d}t}I(t) = \omega S(t) + (\beta S(t) - \delta - \lambda)I(t)\\ \qquad\qquad + \mu I^*(t) + (\gamma + \omega)R(t)\\ \dfrac{\mathrm{d}}{\mathrm{d}t}I^*(t) = \omega S^*(t) + \lambda I(t) - (\delta + \mu)I^*(t)\\ \dfrac{\mathrm{d}}{\mathrm{d}t}R(t) = \delta I(t) - (\gamma + \lambda)R(t) + \mu R^*(t)\\ \dfrac{\mathrm{d}}{\mathrm{d}t}R^*(t) = \delta I^*(t) + \lambda R(t) - \mu R^*(t)\end{cases} \tag{2}$$

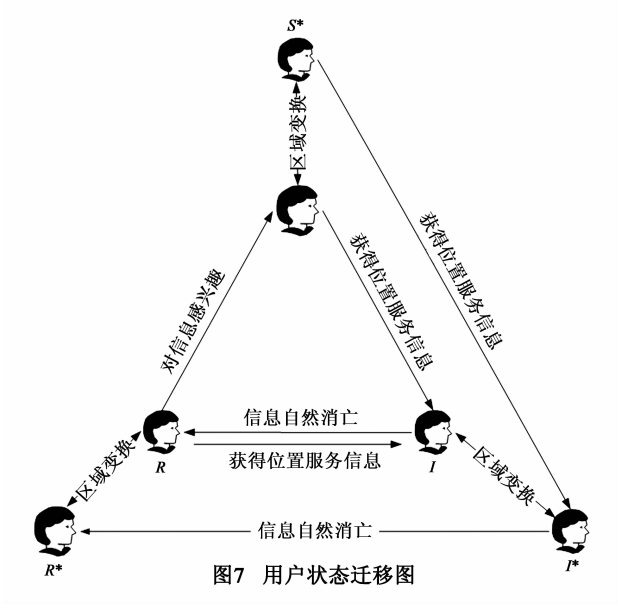


**图7　用户状态迁移图**

式(2)中第 1 个等式左边表示 $S$ 态的用户数量变化率,其等号右边的 $\mu S^*(t)$表示在单位时间内从区域外移动到区域内的 $S^*$ 用户的数量;$\lambda S(t)$表示在单位时间内从区域内移动到区域外的 $S$ 用户的数量;$-\beta I(t)S(t)$表示在单位时间内 $S$ 态用户转换为 $I$ 态的数量,$\omega S(t)$表示 $S$ 态用户由于得到服务器的信息变成 $I$ 态的数量,$\gamma R(t)$表示在单位时间内用户因为 $R$ 中的用户有询问的请求,所以从 $R$ 态变化为 $S$ 态的数量.

式(2)中第 3 个式子左边表示 $I$ 态的用户数量变化率,其等号右边的 $\omega S(t)$表示某些 $S$ 态的用户由于得到服务器的信息变成 $I$ 态,等号右边$(\beta S(t) - \delta - \lambda)I(t)$可拆分为 $\beta S(t)I(t)$、$-\delta I(t)$和 $-\lambda I(t)$,$\beta S(t)I(t)$表示单位时间内 $S$ 态用户转换为 $I$ 态的数量,$-\delta I(t)$表示用户由于信息的消逝而从 $I$ 状态转换为其他状态的用户数量,$-\lambda I(t)$表示用户 $I$ 由区域内移动到区域外的数量.等式右边的 $\mu I^*(t)$表示的是区域外用户 $I^*$状态进入区域内变成 $I$ 的数量.等式右边的$(\gamma + \omega)R(t)$表示的是 $R$ 状态的用户变成 $I$ 状态的用户数量.

式(2)中第 5 个式子左边表示 $R$ 态的用户数量变化率,其等号右边的 $\delta I(t)$表示区域内的 $I$ 状态的用户由于信息的消逝变成 $I$ 态用户数量.等号右边的$(\gamma + \lambda)R(t)$表示 $R$ 态用户转换为其他用户的数量,$\mu R^*(t)$表示区域外的用户进入区域内变成 $R$ 态用户数量.

式(2)中的第 2、4、6 个式子分别表示的是区域外 $S^*$,$I^*$,$R^*$ 态用户的变化率,分析方法跟区域内的 $S$、$I$、$R$ 态用户变化率类似.

### 4.2　隐藏概率的理论分析

隐藏概率指的是在一个给定的区域内,在每个时间单位用户发出询问请求不被服务器发现的概率.这

个概率越高,攻击者根据观测到的服务器的数据猜测出用户真实位置的成功率就越低.一些用户的请求信息可以被其他用户回应而不经过服务器.只有在 $R$ 和 $I$ 状态下,用户才有可能发出新的询问信息,所以只考虑这两种状态($S$ 状态的用户已经对信息感兴趣,无需发出新的询问请求,所以不考虑在内).在发出询问的请求时,用户是 $I$ 状态的概率为$\frac{I}{I+R}$,当用户是 $I$ 状态时,本身拥有该区域内的位置信息,只要读取自身的缓存即可,此时用户不必接触服务器,用户的位置信息不会暴露给服务器.在发出询问请求时,用户是 $R$ 状态的概率是 $\frac{R}{I+R}$,用户本身没有信息,用户必须向位置服务器发出询问请求信息,用户的个人位置信息就暴露给服务器,不能隐藏自身位置信息.所以,隐藏概率为:

$$HP=\frac{I}{I+R}*1+\frac{R}{I+R}*0=\frac{I}{I+R} \tag{3}$$

图 8 是 Reza Shokri 方案(下简称原方案)和本文方案(主动扩散式)位置隐私保护的 HP 理论值对比.其中,本文方案的参数设置如下:$\beta=0.1$, $\mu=0.1$, $\gamma=0.1$, $\delta=2$, $\omega=5$. 从图中可以看出,主动扩散式的方案比原方案的 HP 值有所提升,这是因为在主动扩散式的方案中,用户的信息传递效率比较高,有信息用户的点比原方案中的用户多,所以对服务器的依赖有所降低.

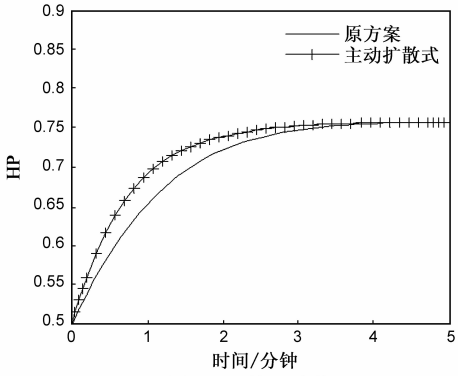


**图8 HP的理论值**

### 4.3 开销分析

主动式扩散机制必然会增大移动设备的通信和存储开销.因此,本文方案通过引入 $\Delta T$ 参数来降低协议开销.对于快速移动的设备,例如高速运动中的汽车,由于停留时间小于 $\Delta T$,因此不会参与共享机制,因此不会增加开销.对于停留时间较长的用户,其更新频率也不会大于 $\Delta T$.此外,由于服务区域被细划分成一个个较小的区域,因此各子区域内的兴趣点的信息交互量也相对较小.我们可以通过订阅主题的方法进一步减少通信和存储开销.

### 4.4 信息安全

在服务信息的共享过程中,恶意节点可能伪造假消息或者篡改服务器的消息.因此,我们引入数字签名机制来保障服务消息的安全性.LBS 服务器利用自身的私钥对服务信息进行签名,移动用户都可以利用 LBS 服务器的公钥来验证消息的真实性.另外,自私节点也可能不愿共享服务信息.但是个别自私节点并不会影响本文方案的总体运行;另外,也可以额外引入激励机制促进用户参与的积极性.

## 5 实验分析

我们在 CRAWDAD 采集的移动数据的基础上,采用 Matlab 系统进行模拟实验.

实验以 500 辆汽车作为移动对象,并随机选择一个 $100\times100$ 的方形区域,对区域内的移动点轨迹进行采样分析,采样周期 $T$ 设置为 100s(根据移动点的平均逗留时间来设置).实验中,$I$ 态用户就会主动地将已获取的 LBS 信息共享给周围邻近的其他用户;我们设置一个请求概率 $P$,在每个采样周期内随机选择一些用户进行 LBS 请求.每个 LBS 信息我们都设置一个有效存活时间 TTL.我们分析各个参数取值对位置隐藏概率的影响,并选择与 Reza Shokri 方案的位置隐私保护模型进行比较.

### 5.1 隐藏概率

隐藏概率的实验值 HP'的计算方法如下:

$$\mathrm{HP'}=\frac{C_{\mathrm{share}}}{C_{\mathrm{total}}} \tag{4}$$

其中,$C_{\mathrm{share}}$指通过共享机制获得 LBS 服务信息的次数统计,如果该用户能从其他用户获得信息则 $C_{\mathrm{share}}++$,$C_{\mathrm{total}}$指总的服务请求次数.

图 9 为本文方案和 Reza Shokri 方案的实验对比结果.其中,横坐标为模拟时间,以采样周期为单位,TTL $=2T$, $P=0.1$. 由图可得,随着模拟时间的推移,区域内有信息的移动点数量逐渐增多,越来越多的移动用户可以不经过服务器而获得 LBS 服务信息,因此隐藏的概率 HP 的值就不断上升,最后将收敛到一个稳定状态,与图 8 的理论分析吻合.而相对于 Reza Shokri 方案,本文方案由于其信息共享效率更高,因此位置隐藏概率明显提高.

### 5.2 信息存活时间

TTL 指的是 LBS 信息的有效存活时间,移动设备将删除缓存中过期的 LBS 信息.我们对比不同 TTL 值对隐藏概率的影响.

图 10 和图 11 分别表示 TTL 值对隐藏概率的实验值和理论值的影响,其中 $P=0.1$. 由图可得,理论值和实验结果的变化趋势基本吻合,TTL 越大,则获得共享

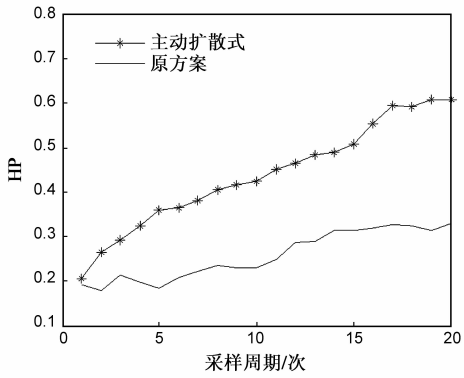

图9　方案实验对比

的机会也越多,因此隐藏概率也相应越大.由于理论模型和实验的参数设置不是完全匹配,因此图 10 的理论值和图 11 的实验值不会完全匹配.另外,TTL 越大,信息更新效率也越低,移动设备的存储开销也越小,因此,TTL 是一个需要折中考虑的取值.

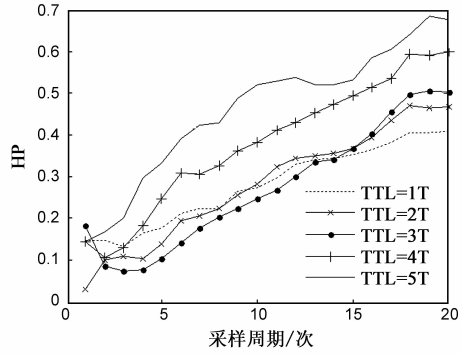

图10　TTL对HP '实验值的影响

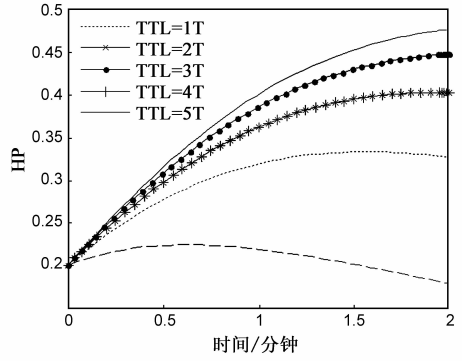

图11　TTL对HP理论值的影响

### 5.3　请求概率

请求概率 $P$ 指每个采样周期内一个用户发送 LBS 服务请求的概率. $P$ 越大,则需要服务的次数也越频繁.图 10 和图 11 分别表示 $P$ 值对隐藏概率的实验值和理论值的影响,其中 $TTL = 2T$.通过理论值与实验值分析可以看出,请求概率越高,则 HP 收敛的值越大.这是因为 $P$ 越大,则越多的用户需要位置服务,因此在初始状态下有更多的用户通过服务器获得位置服务信息,因此初始状态 $P$ 越大,则隐藏概率越小;但是,随着时间的迭代,$P$ 值越大,移动节点获得共享机会也越多,则隐藏概率也逐渐增大,最后收敛于更高的隐藏概率值.

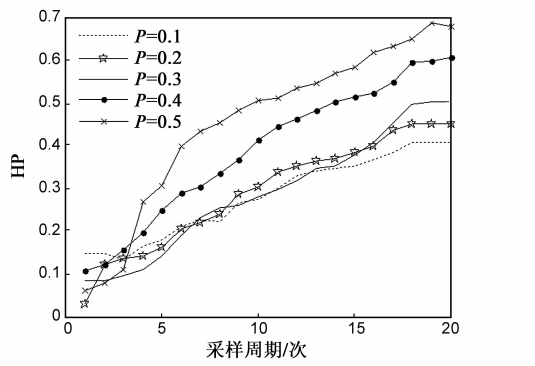

图12　P对HP'实验值的影响

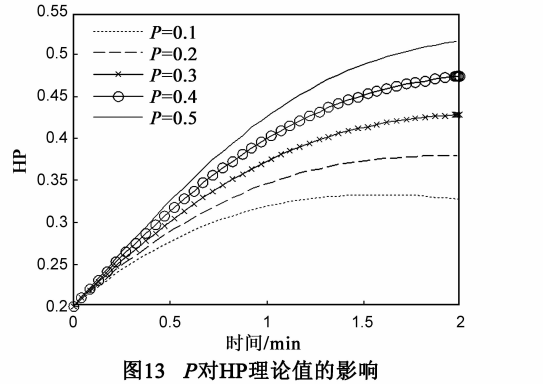

图13　P对HP理论值的影响

### 5.4　扩散周期

扩散周期 $\Delta T$ 对方案具有重要影响,图 14 和图 15 分别为 $\Delta T$ 对隐藏概率和通信开销的影响情况,其中通信开销指 LBS 信息的共享次数统计.由图可得,$\Delta T$ 越大,则用户间的消息共享频率越低,因此,移动设备的通信开销也随之越小,但是隐藏概率也会降低.因此,方案中可以根据隐藏概率的最低需求来选择合适的扩散周期 $\Delta T$,也可根据通信开销的限制来选择 $\Delta T$ 值.

## 6　总结

本文针对当前的 LBS 中存在的位置隐私泄露的问题,提出了一种主动扩散式的位置隐私保护方案,并分别采用病毒扩散模型和真实数据集对其进行理论和模拟实验分析.分析表明,本方案能充分利用邻居的位置服务信息,降低用户对 LBS 服务器的依赖,从而提高其位置的隐私安全.另外,本文提出的主动式扩散式方案不需要改变现有的 LBS 结构,也无需引入第三方可信平台,具有简单易行的优点.在下一步工作中,我们将继续完善该方案,拟通过引入主题订阅和概率机制来进一步降低方案的通信和存储开销.

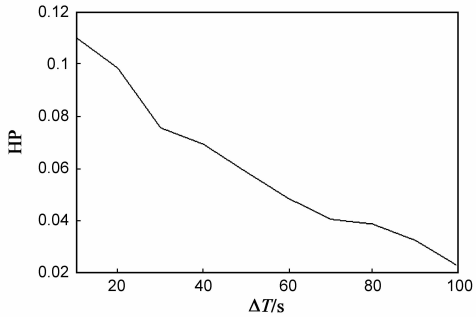


图14 $\Delta T$对HP的影响

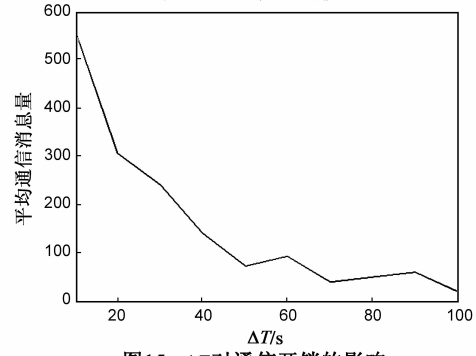


图15 $\Delta T$对通信开销的影响

## 参考文献


[1] Mokbel M F. Privacy in location-based services: State-of-the-art and research directions[A]. Proceedings of the International Conference on Mobile Data Management[C]. USA: IEEE, 2007.228.

[2] Reza Shokri. Hiding in the mobile crowd: location privacy through collaboration[J]. IEEE Transactions on Dependable Secure Computer, 2014, 11(3): 266 – 279.

[3] Gruteser M, Grunwal D. Anonymous usage of location-based services through spatial and temporal cloaking[A]. Proceedings of the International Conference on Mobile Systems Applications and Services[C]. USA: IEEE, 2003.163 – 168.

[4] M F Mokbel, C Y Chow, W G Aref. The new Casper: Query processing for location services without compromising privacy [A]. Proceedings of the International Conference on Very Large Data Bases[C]. USA: VLDB, 2006.763 – 774.

[5] Bhuvan B, Ling L, et al. Supporting anonymous location queries in mobile environments with privacy grid[A]. Proceedings of the 17th International Conference on WWW[C]. USA: ACM, 2008. 237 – 246.

[6] P Kalnis, G Ghinita, et al. Preventing location-based identity inference in anonymous spatial queries[J]. IEEE Transactions on Knowledge Data Engineering, 2007, 19(12): 1719 – 1733.

[7] 王丽娜,彭瑞卿,等.个人移动数据收集中的多维轨迹匿名方法[J].电子学报,2013,41(8):1653 – 1659.
Wang Li-na, Peng Rui-qing, et al. Multi-dimensional trajectory anonymity in collecting personal mobility data[J]. Acta Electronica Sinica, 2013, 41(8): 1653 – 1659. (in Chinese)

[8] H Kido, et al. An anonymous communication technique using dummies for location-based services[A]. Proceedings of IEEE ICPS[C]. USA: IEEE, 2005.88 – 97.

[9] Rinku Dewri. Exploiting service similarity for privacy in location based search queries[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(2): 374 – 383.

[10] Kenta Miura, Fumiaki Sato. A hybrid method of user privacy protection for location based services[A]. Proceedings of the 7th International Conference on Complex, Intelligent, and Software Intensive Systems[C]. Taiwan: CISIS, 2013.434 – 439.

[11] Agusti Solanas, Antoni Mart Ballest. A TTP-free protocol for location privacy in location based services[J]. Computer Communications, 2008, 31(6): 1181 – 1191.

[12] Kyriakos Mouratidis. Strong location privacy: A case study on shortest path queries[A]. Proceedings of IEEE 29th International Conference on Data Engineering (ICDE)[C]. USA: IEEE, 2013.136 – 143.

[13] 刘华玲,郑建国,孙辞海.基于贪心扰动的社交网络隐私保护研究[J].电子学报,2013,41(8):1586 – 1591.
Liu Hua-ling, Zheng Jian-guo, Sun Ci-hai. Privacy preserving in social networks based on greedy perturbation[J]. Acta Electronica Sinica, 2013, 41(8): 1586 – 1591. (in Chinese)

[14] M Piorkowski, N Sarafijanovic Djukic, M Grossg. CRAWDAD data set epfl/mobility[DB]. http://crawdad.cs.dartmouth.edu, 2009-02-24.

[15] 马知恩,周义仓.传染病动力学的数学建模与研究[M].北京:科学出版社,2004.


## 作者简介

**叶阿勇** 男,1977 年 1 月出生,福建漳州人,博士,福建师范大学副教授、硕士生导师,主要研究方向为网络与信息安全、位置信息处理等.

**林少聪** 男,1989 年 1 月出生,福建莆田人,福建师范大学硕士研究生,主要研究方向为位置隐私保护、位置信息处理.
E-mail: linscfujian@foxmail.com