Journal of Computer Applications
计算机应用, 2020, 40(5): 1364 - 1368
ISSN 1001-9081
CODEN JYIIDU
2020-05-10
http://www.joca.cn

文章编号:1001-9081(2020)05-1364-05
DOI:10.11772/j.issn.1001-9081.2019111982

增强现实中基于位置安全性的LBS位置隐私保护方法

杨　洋[1*],王汝传[2,3]

(1. 南京广播电视大学/南京城市职业学院 工程与信息学院,南京 211200;　2. 南京邮电大学 计算机学院,南京 210003;
3. 江苏省无线传感网络高技术研究重点实验室,南京 210003)

(*通信作者邮箱 nj.yangyang@163.com)

摘　要: 为了解决基于位置的服务(LBS)和增强现实(AR)技术快速发展带来的用户位置隐私泄露的隐患,分析了现有的位置隐私保护方法的优缺点,提出基于位置安全性的位置隐私保护方法。将区域安全度和伪装区域引入该方法中,将提示某区域是否需要保护这一度量标准定义为区域安全度,非安全区域(即需要给予保护的区域)的区域安全度设置为1,安全区域(即不需要保护的区域)设置为0,通过扩大区域安全度和识别等级来计算位置安全度。实验结果表明,该方法与未引入位置安全性的方法相比降低了平均定位误差,提高了平均安全性,从而有效地保护了用户的位置隐私,提高了LBS的服务质量。

关键词: 基于位置的服务;位置隐私保护;位置安全性;区域安全度

中图分类号: TP391.9　　**文献标志码:** A

Location based service location privacy protection method based on location security in augmented reality

YANG Yang[1*], WANG Ruchuan[2,3]

(1. *Institute of Engineering and Information*, *Nanjing Radio and TV University / Nanjing City Vocational College*, *Nanjing Jiangsu* 211200, *China*;
2. *College of Computer*, *Nanjing University of Posts and Telecommunications*, *Nanjing Jiangsu* 210003, *China*;
3. *Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks*, *Nanjing Jiangsu* 210003, *China*)

Abstract: Rapid development of Location Based Service (LBS) and Augmented Reality (AR) technology lead to the hidden danger of user location privacy leakage. After analyzing the advantages and disadvantages of existing location privacy protection methods, a location privacy protection method was proposed based on location security. The zone security degree and the camouflage region were introduced into the method, and the zone security was defined as a metric that indicates whether a zone needs protection. The zone security degree of insecure zones (zones need to be protected) was set to 1 while that of secure zones (zones not need to be protected) was set to 0. And the location security degree was calculated by expanding zone security degree and recognition levels. Experimental results show that, compared with the method without introducing location security, this method can reduce average location error and enhance average security, therefore effectively protecting the user location privacy and increasing the service quality of LBS.

Key words: Location Based Service (LBS); location privacy protection; location security; zone security degree

0　引言

增强现实是一种允许在正常感知现实上叠加由计算机形成的图片和信息的技术[1]。基于位置的服务(Location Based Service, LBS)是增强现实提供的常用服务之一,在LBS中移动终端用户的位置信息是通过移动的无线网络或外部定位方式来获取的,位置定位技术(Location Determination Technology, LDT)是获取用户位置信息的一种较好的技术,如全球定位系统(Global Positioning System, GPS)、高级时差检测定位技术(Enhanced Observed Time Difference, EOTD)等,这些都可以给出含有*X*-*Y*坐标的用户位置信息。近年来,由于GPS设备和移动信息技术的进步,LBS被公认为是一种重要的服务,虽然基于位置的服务非常便利,但它冒着用户隐私受到威胁的危险。要使用基于位置的服务,用户当前的位置必须被服务提供者获得,因此位置信息对情境感知服务提供者来说很重要,它也成为信息泄露的来源。通过结合用户的位置和其他信息,服务提供商可以侦查出用户的真实身份或相关信息如家庭地址和办公地点等。例如,用户*U*想查询离他最近的银行ATM(Automatic Teller Machine)在哪里,他首先要通过智能手机发送一个查询请求和他的位置给LBS提供商,LBS服务器将提供最近的银行ATM地址信息给用户*U*,但是对于移动用户来说,位置信息非常重要,而且将信息提交给不信任的LBS服务器会受到隐私威胁,极有可能暴露用户的个人信息如习惯、日常生活、健康状况等。

收稿日期: 2019-11-05;**修回日期:** 2019-12-19;**录用日期:** 2019-12-23。　**基金项目:** 国家自然科学基金资助项目(60973139,61170065,61171053);江苏省自然科学基金资助项目(BK2011755);江苏省科技支撑计划项目(BE2010197,BE2010198,BE2011844,BE2011189)。

作者简介: 杨洋(1980—),女,江苏南京人,副教授,硕士,主要研究方向:网格计算、增强现实、位置隐私保护;　王汝传(1943—),男,安徽合肥人,教授,博士生导师,主要研究方向:计算机软件、计算机网络、信息安全、移动代理、虚拟现实。

LBS服务器包含了大量的位置信息。用ATM举例,LBS服务器包含了ATM的位置纬度、经度、银行名称等,希望LBS能够保证这些数据只发送给授权用户。在LBS服务中,能够确保用户和服务器的安全非常重要,它意味着获取用户的位置隐私并保证服务器数据不被不合法用户访问,为了解决这个问题,位置匿名技术得到研究者关注。

1　现有位置隐私保护技术

所谓位置隐私保护,是指用户在使用位置服务的过程中,位置服务采用技术保护措施来有效确保用户的位置隐私信息不会泄露,从而避免泄露隐私信息给用户带来不必要的麻烦。

位置隐私分为三大类:一类是对位置信息本身的保护,是采用位置匿名技术来隐藏用户位置信息,使得用户的位置信息无法被识别出来,那么攻击者无法找到用户的真实位置信息,即使找到,也无法区分;第二类是在位置服务的数据通信过程采用一种位置隐私保护模型来保证用户和服务器之间数据传输的安全[2],例如差分隐私保护,它是通过在原始数据中加入噪声来保证数据的安全;第三类是针对服务器的查询过程,将用户的位置进行匿名化,这样用户的位置信息变成一个匿名的信息集合,其中包含了多个用户的位置信息,扩大用户的位置区域,此时攻击者无法获得用户的确切位置。

目前主要的位置隐私保护技术主要有以下三种。

1.1　假位置的位置隐私保护技术

用户在自己周围取一虚假位置,并将此位置信息作为自己的确切位置信息发送给位置服务器,通过发布假位置达到混淆视听的效果[3],但这种方法有一定的缺陷,当假位置距离真实位置较远时,服务质量差,但其隐私保护程度较高;当两者之间的距离较近时,服务质量好,但其隐私保护程度则低。研究者提出了一种SpaceTwist方案[4],在该方案中引入可信的第三方位置服务器,主要是为了降低用户执行服务请求时暴露位置信息的风险。在这个方案中,第三方位置服务器保护用户的位置隐私信息,位置服务器收到服务提供商的服务请求并定位用户后,首先它将用户的位置信息发送给匿名处理服务器,匿名处理服务器使用匿名算法处理用户的真实位置信息,生成一个虚假的位置信息,接着将这个虚假位置信息发送给服务提供商,服务提供商将虚假位置信息与自己数据库中的地理信息进行对比,定位用户和周围的服务信息,以虚假位置信息为中心覆盖真实用户附近的所有目标,并将这些目标汇总为一个目标集,最后发送给用户。

1.2　基于*K*-匿名的位置隐私保护技术

K-匿名技术是一种典型的模糊化保护技术,通过*K*值来确定匿名集的大小,匿名集内的用户位置信息匿名化后成为一个相同区域的位置信息。

在向LBS提供商提交前,先删除个人信息内容,发布较低精度的数据,使得各条记录至少与数据表中其他$K-1$条记录具有完全相同的准标识符属性值[5]。它主要通过对匿名区域进行划分,划分成模糊空间,这些模糊空间大小是均匀的,接着按照子空间里用户数量对子空间进行从大到小的排序,然后分段序列,最后从每一个分段中选取一个查询区域进行合并,构成*K*个查询匿名集。

在位置隐私保护中,不同的用户有不同的位置*K*-匿名需求,针对*K*-匿名法的局限性,由Gedik等[6]首先提出了个性化*K*-匿名法。为实现个性化,需要将*K*值定义为可变的,用户可以根据不同的环境自主设置*K*值,*K*的值决定了用户隐私保护级别的高低,*K*值越高隐私保护级别就越高,但是*K*值超过一定的值会造成查询处理负担过重,导致服务质量降低,所以个性化*K*-匿名法可以由用户来折中考虑。

1.3　基于混合区域的位置隐私保护技术

还有一种位置隐私保护技术是针对车辆自组网内的位置信息保护的,基于混合区域的位置隐私保护技术是指用户在建立通信过程中隐藏真实身份,攻击者无法将身份一一识别,从而保护车辆和用户身份信息。

实际上,基于混合区域的保护技术是一种假名技术,常使用于车辆自组网内,比如,在一个十字路口的混合区域中,车辆进入混合区域之前使用假名,进入混合区域之后更换假名,离开混合区域后车辆就以一个新假名出现在路网中。该技术的基本思想是,首先为即将进入混合区域的每个车辆配备多个可以隐藏真实身份的假名,当车辆进入混合区域时,可以自主更换假名[7],更换假名的方案主要有三种:第一种是每辆车配备自己的假名数据库,在经过混合区域时更换;第二种是在混合区域配备一个假名数据库,车辆进入混合区域时,随机得到一个新的假名来取代原来的假名;第三种是在车流量较大的地方设置混合区域,提取假名重新分配。除此之外[8],将假名更换和其他技术如路径混淆[9]、随机假名[10]等相结合提高匿名的效果,从而保护位置隐私。

1.4　三种位置隐私保护技术的比较

基于假位置的位置隐私保护技术中攻击者无法区分哪个是真实的或哪个是虚假的位置[11],用户的位置隐私得到保护,但该方法也有缺陷,其假设用户在一个固定的自由空间中活动,但是在现实生活中并非如此;另外,该方法的隐私保护程度不是固定不变的,当假位置距离真实位置较远时,服务质量差,但其隐私保护程度较高;当两者之间的距离较近时,服务质量好,但其隐私保护程度则低[12]。

基于*K*-匿名的位置隐私保护技术中可以设计出一个适当的间隔算法[13],该算法可以产生包含至少$k_{\min}$用户的时空cloaking box,利用此box作为位置信息发送给LBS提供商。但这种方法的局限性是不能抵制同质性攻击和背景知识攻击[14],攻击者很容易推断出个体相应的敏感属性数据,或者可以通过背景知识确定敏感属性数据和个体之间的对应关系,从而导致隐私泄露。

基于混合区域的位置隐私保护技术中攻击者无法识别真实身份[15],但实际上它是一种假名技术,所以隐私保护程度不是固定不变的。

2　基于位置安全性的位置隐私保护方法

随着问题背景和攻击模型的多样化,位置隐私还将继续面临新的问题,如造成敏感属性泄露、背景知识攻击的不确定性、敏感属性分布失衡等,因此,本文提出基于位置安全性的位置隐私保护策略。

2.1　准备知识

用户在不同的环境背景中会有不同的隐私要求,需要根据不同的环境分配不同的隐私等级,这样才能应用相应的隐

私保护策略。比如，最常访问地点是最接近于用户标识（最高位点），因此最高位点的隐私等级应被定义为高级别；另一方面，公共区域如风景区，可以被定义为低隐私保护等级，这就意味着低强度模糊处理同时保证其服务质量。

本文提出的基于位置安全性的方法介绍了将位置安全性作为新的评价度量标准。以往的研究均进行相似的处理过程，而不管这一点是什么区域，然而很多地方是不需要进行保护的，比如所有人通过的马路、不宜居住的区域、城市公园等，均不需要进行保护。本文将根据哪些区域需要保护哪些区域不需要保护，提出一种执行不同保护的方法。

本文将提示某区域是否需要保护这一度量标准定义为区域安全度，非安全区域（即需要给予保护的区域）的区域安全度将其设置为1，安全区域（即不需要保护的区域）将其设置为0。通过扩大区域安全度和识别等级来计算位置安全度。

2.2 相关定义

定义1 本文用三元组来表示网络实体$\langle u_k, Server, LServer\rangle$，其中$u_k$移动用户，$Server$表示中心服务器，$LServer$表示基于位置的服务器，并且$Server$是可信的，$LServer$是半可信的。

定义2 用户向$LServer$发起查询，用户查询内容Cj，$Cj=\{User, fQ, t, IDg, c, Q, Sp\}$，其中：$User$表示用户的标识符，$fQ$表示用户首次发送查询请求，$t$表示用户发送查询请求的时间，$IDg$表示用户所在位置，$c$表示该用户查询请求的服务内容，$Q$表示用户的隐私需求，$Sp$表示用户的速度。

定义3 与$Server$距离$dist(u_k, Server)<r_{\min}$的用户$u_k$构成的区域称作非安全区域，距离$r_{\min}\leqslant dist(u_k, Server)\leqslant r_{\max}$的用户构成的区域为安全区域，与$Server$距离$dist(u_k, Server)>r_{\max}$的用户$u_k$构成的区域也称作非安全区域。

2.3 算法描述

假设各节点的位置信息可通过GPS获得并设置成经纬度，每个节点都有区域安全度的状态变量。各节点规律性地向位置信息服务器汇报位置信息及周围情况，位置信息服务器显示所有节点的位置信息。此外，假设标识符不包括原始节点的重要信息，因为位置服务器提供的节点标识符随时间不断改变。

算法1

参数 广播报文B。

输入 广播报文；

输出 判断用户区域。

Procedure：

用户u_k收n个$Server$发来的报文集合$G=\{G_{s_1}, G_{s_2}, G_{s_3}\}$，其中$G_{s_i}=(Server_i, loc_i, r_{\min}, r_{\max})$

For each $G_{s_i}\in G$ do

Calculate $dist\left(loc_{u_k}, loc_{s_i}\right)$

If $dist\left(loc_{u_k}, loc_{s_i}\right)<r_{\min}$ then

用户处于非安全区域，丢弃其他报文

Else if $dist\left(loc_{u_k}, loc_{s_i}\right)>r_{\max}$ then

用户处于非安全区域，丢弃G_{s_i}

Else $r_{\min}<dist\left(loc_{u_k}, loc_{s_i}\right)<r_{\max}$

用户处于安全区域，向G_{s_i}登记报文并注册

End

算法1描述 用户接收报文集合，首先计算距离，当$dist\left(loc_{u_k}, loc_{s_i}\right)<r_{\min}$说明用户处于非安全区域，则丢弃其他报文；如果$dist\left(loc_{u_k}, loc_{s_i}\right)>r_{\max}$且处于非安全区域，用户丢弃$G_{s_i}$；否则用户向$G_{s_i}$登记报文并注册。

算法2

参数 用户查询集Q，隐私阈值E。

输入 用户查询集、隐私阈值；

输出 符合隐私阈值的$|Q|$。

Procedure：

WHILE $|Q|<E$

选取一个用户查询内容q_j建立查询集Q

直到$|Q|$符合隐私阈值E

END WHILE

算法2描述 各节点延伸其伪装区域的面积，除非该节点区域包括k节点。此处k指模糊参数，如果该节点位于安全区域，那此节点范围是非模糊的最小面积。

算法3

参数 位置信息L，隐私等级D。

输入 节点定位并从位置信息服务器中获取周围信息；

输出 位置信息存储在位置信息服务器。

Procedure：

IF 区域安全度=1 THEN

IF 最大伪装区域有其他节点 is TRUE THEN

位置信息模糊化

ELSE 移除模糊化后的信息

ELSE

位置信息存储在位置信息服务器

END IF

算法3描述 通过位置信息，节点定位并从位置服务器中获取周围信息，当区域安全度为1，如果最大伪装区域有其他节点，选取合适大小的区域作为伪装区域封装周围合适数量的其他节点，则位置信息模糊化；否则移除模糊化后的信息。如果区域安全度不为1，则将位置信息存储在位置信息服务器。

2.4 隐私度量

2.4.1 单独查询

在查询途径中，用户可为每一个查询获得P匿名，由于用户查询内容均被隐藏，所以不存在位置K匿名，此处研究的隐私保护度P_v，即在运用本文的P查询方式时，在单一查询中攻击者通过用户身份追寻查询主题的可能，计算公式如下：

$$P_v=\frac{1}{\max(E, Q)}$$

此处，Q是同簇中融合的查询数量，E是隐私阈值。可以发现，E和Q的值越高，P_v的值越低，隐私保护度就越高。

2.4.2 连续查询

在经典的K-匿名方法中，用户通过与其他$K-1$用户混淆标示和位置来获得隐私，因此，K值是位置隐私水平的度量标准。然而该隐私度量在连续的攻击模式下难以应用。在连续LBS中，攻击方通过关联一个用户查询的时间序列来提取

目标ID和位置信息。此时,攻击方需要追踪用户的连续查询。攻击方根据重复发生的查询主题来区分某个连续查询。因此,本文使用概率P_v来描述在LBS服务器中一段时间内超过2次的查询主题出现次数,以此来衡量隐私性。P_v值越高,攻击方越难以区分真实的查询主题,因此,连续攻击能够被有效阻止。

因为查询选择的随机性,LBS服务器中查询的随机性能够过程建模。本文假设查询主题Q在一段时间内在LBS服务器中出现的次数是随机变量X,因此X的分布计算公式如下:

$$P(X \geqslant c) = 1 - \sum_{i=0}^{c-1} \frac{\lambda^i}{i!} \cdot e^{-\lambda}$$

λ的值是查询主题Q在一段时间内在LBS服务器中发生几率的平均值,因此可以如下定义隐私度量P_v:

$$P_v = P(X \geqslant 2) = 1 - \sum_{i=0}^{1} \frac{\lambda^i}{i!} \cdot e^{-\lambda}$$

2.5　算法评价

为评价本文所提算法,使用两个标准来评价对于节点位置信息及匿名程度的服务质量。由于位置信息服务器提供的节点位置信息是模糊的,因此与直接从原始节点获得的高精度定位信息相比,此时将会出现定位误差,定义如下文所述。

首先本文假设节点的定位信息被处理成最小定位信息的间隔尺寸,表示为s和t。假设节点q的坐标为s_q和t_q,假设该节点的模糊后坐标为s_q'和t_q'。此外,假设伪装区域大小的x轴方向和y轴方向分别为a和b。此时,最高精度的定位信息由二维阵列$\boldsymbol{A}$处理。总而言之,对应节点$A[s_q, t_q]$坐标的组件$\boldsymbol{A}$将被增加值1,另外,模糊后的定位信息由二维阵列$\boldsymbol{B}$处理,本文使用阈值代表匿名水平,如阈值设为4,定位信息将被模糊到至少有4个节点拥有相同的定位信息。如果节点q的位置被模糊,则$1/(a,b)$的值将被分别加入$B(B[m][n], m = s_i', s_{i+1}', \cdots, s_{i+a-1}', n = t_i', t_{i+1}', \cdots, t_{i+b-1}')$,该值所有节点的值均被加入阵列。定位误差被定义为一个值,这个值是所有这些阵列的差异绝对值的总和除以终端数P,也就是说,定位误差定义为公式$D = \sum_{i=0}^{s_{\max}-1} \sum_{j=0}^{t_{\max}-1} |A[i][j] - B[i][j]/P|$,其中$s_{\max}$和$t_{\max}$是$s$、$t$方向的分段数。如果定位误差这个值很小,意味着提供的定位信息精确度很高,使得该值成为LBS的服务质量的指标。

接着,定义节点特征,本文将此节点特征称为正确节点的等级,并假设该初始值为1,也就是说首先指定该节点特征。当该节点遇到其他节点时,因为不能鉴别哪个是正确的节点,因此其特征值降为1/2;如果其随后遇到其他节点,节点特征值继续下降1/2;此外,如果其一次遇到两个或两个以上节点,节点特征值变为$1/l$(l是遇到的节点数加1)。

根据区域安全性和识别级别,区域安全性可被计算出来。在固定时间内,所有节点的平均安全性可被计算出来作为整个系统的安全性,那么该值被作为匿名程度。

3　实验结果及分析

本文实验采用Brinkhoff[16]提出的基于网络的移动对象生成器,选用德国奥尔登堡的地图作为实验背景,最小区域面积10 m^2,安全区域面积2 500 m^2,节点数量(100~800),实验环境为Windows7操作系统,内存为4 GB,基于安卓平台使用Java程序,本文将与未引入区域安全性的伪装区域法进行比较,评价平均定位误差和平均安全性。

3.1　平均定位误差的比较

随着节点数量增加,由于伪装区域变小,而遇到其他节点的几率增加,未引入位置安全性的位置隐私保护方法平均定位误差升高,而基于位置安全性的位置隐私保护方法虽然平均定位误差在升高,但表现仍然比未引入位置安全性的位置隐私保护方法要好。两种位置隐私保护方法的平均定位误差比较如图1所示。

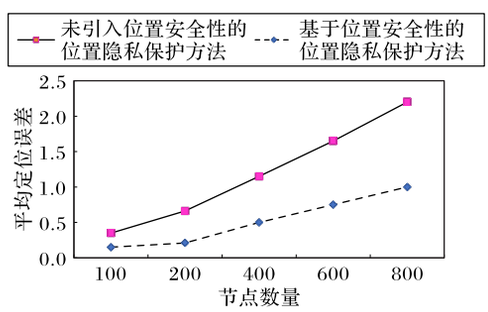

图1　两种位置隐私保护方法的平均定位误差比较

Fig. 1　Average location error comparison between two location privacy protection methods

3.2　平均安全性的比较

如图2比较了两种位置隐私保护方法的平均安全性,在节点数量相同的情况下,基于位置安全性的位置隐私保护方法的平均安全性要比未考虑位置安全性的位置隐私保护方法高,根据以上结果,本文方法不仅可以改善定位信息的质量而且提高区域的平均安全性。

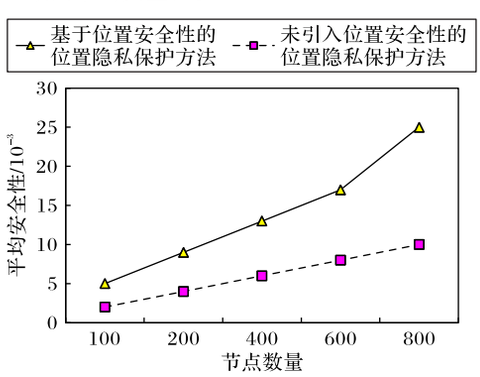

图2　两种位置隐私保护方法的平均安全性的比较

Fig. 2　Average security comparison of two location privacy protection methods

4　结语

目前的位置隐私保护方法都是在LBS服务质量和匿名度之间权衡,本文提出一个新的度量值“位置安全性”来缓解权衡的问题。从研究结论来看,所提方法没有降低位置安全性,并且位置信息服务的质量也很好。随着增强现实技术和无线网络的迅速发展,增强现实技术结合LBS使得人们将进入全新的位置搜索引擎时代、营造全新的社交方式。其中,LBS面

临的威胁是用户隐私泄露的威胁，目前这样的威胁已得到用户、服务提供商、政府管理部门和专家学者的关注，还没有一个十分完善的增强现实中LBS的位置隐私保护方法，还需进一步对相关问题进行研究。

参考文献（References）

[1] HÖLLERER T H, FEINER S K. Mobile augmented reality[M]// KARIMI H A. Telegeoinformatics: Location-Based Computing and Services. Boca Raton: CRC Press, 2004:392.

[2] 张啸剑，孟小峰. 面向数据发布和分析的差分隐私保护[J]. 计算机学报, 2014, 37(4):927-949.（ZHANG X J, MENG X F. Differential privacy in data publication and analysis[J]. Chinese Journal of Computers, 2014, 37(4):927-949.）

[3] KIDO H, YANAGISAWA Y, SATOH T. Protection of location privacy using dummies for location-based services[C]// Proceedings of the 25th International Conference on Data Engineering Workshops. Piscataway: IEEE, 2005:1248-1248.

[4] YIU M L, JENSEN C S, HUANG X, et al. SpaceTwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services[C]// Proceedings of the IEEE 24th International Conference on Data Engineering. Piscataway: IEEE, 2008:366-375.

[5] 潘晓，郝兴，孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2011, 47(1):121-129.（PAN X, HAO X, MENG X F. Privacy preserving towards continuous query in location-based services[J]. Journal of Computer Research and Development, 2011, 47(1):121-129.）

[6] GEDIK B, LIU L. Protecting location privacy with personalized k-anonymity: architecture and algorithms[J]. IEEE Transactions on Mobile Computing, 2008, 7(1):1-18.

[7] 张建明，赵玉娟，江浩斌，等. 车辆自组网的位置隐私保护技术[J]. 通信学报, 2012, 33(8):180-189.（ZHANG J M, ZHAO Y J, JIANG H B, et al. Research on protection technology for location privacy in VANET[J]. Journal on Communications, 2012, 33(8):180-189.）

[8] RAYA M, HUBAUX J P. The security of vehicular ad hoc networks[C]// Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM, 2005:11-21.

[9] 胡兆玮，杨静. 轨迹隐私保护技术研究进展分析[J]. 计算机科学, 2016, 43(4):16-23.（HU Z W, YANG J. Survey of trajectory privacy preserving techniques[J]. Computer Science, 2016, 43(4):16-23.）

[10] WASEF A, SHEN X. REP: location privacy for VANET using random encryption periods[J]. Mobile Networks and Applications, 2010, 15(1): 172-185.

[11] REEM D. The geometric stability of Voronoi diagrams with respect to small changes of the sites[C]// Proceedings of the 27th Annual Symposium on Computational Geometry. New York: ACM, 2011: 254-263.

[12] CHOW C Y, MOKBEL M F, LIU X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments[J]. GeoInformatica, 2011,15(2):351-380.

[13] NERGIZ M E, GÖK M Z. Hybrid k-anonymity[J]. Computers and Security, 2014, 44:51-63.

[14] DWORK C. The promise of differential privacy: a tutorial on algorithmic techniques[C]// Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE, 2011:1-2.

[15] KALNIS P, GHINITA G, MOURATIDIS K, et al. Preventing location-based identity inference in anonymous spatial queries[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 19(12):1719-1733.

[16] BRINKHOFF T. A framework for generating network-based moving objects[J]. An International Journal on Advances of Computer Science for Geographic Information Systems (Geo Informatica), 2002,6(2): 153-180.

This work is partially supported by the National Natural Science Foundation of China (60973139, 61170065, 61171053), the Natural Science Foundation of Jiangsu Province (BK2011755), the Jiangsu Science and Technology Support Program (BE2010197, BE2010198, BE2011844, BE2011189).

YANG Yang, born in 1980, M. S., associate professor. Her research interests include grid computing, augmented reality, location privacy protection.

WANG Ruchuan, born in 1943, Ph. D., professor. His research interests include computer software, computer network, information security, mobile Agent, virtual reality.