北京航空航天大學

BEIHANG UNIVERSITY

第三十三届“冯如杯”竞赛主赛道项目论文模板

——基于 Latex 的论文模板

摘要

本 Latex 模板是北京航空航天大学大学第三十三届“冯如杯”竞赛主赛道论文模板，由北京航空航天大学校团委基于 GitHub 用户 ***Somedaywilldo*** 与 ***cpfy*** 的成果迭代开发而来。在此由衷感谢所有开发者对本模板的贡献与对“冯如杯”竞赛的大力支持。

摘要内容包括：“摘要”字样，摘要正文，关键词。在摘要的最下方另起一行，用显著的字符注明文本的关键词。

摘要是论文内容的简短陈述，应体现论文工作的核心思想。摘要一般约 500 字。摘要内容应涉及本项科研工作的目的和意义、研究思想和方法、研究成果和结论。

关键词是为用户查找文献，从文中选取出来用来揭示全文主题内容的一组词语或术语，应尽量采用词表中的规范词（参照相应的技术术语标准）。关键词一般为 3 到 8 个，按词条的外延层次排列。关键词之间用逗号分开，最后一个关键词后不打标点符号。

关键词：关键词 1，关键词 2，关键词 3，关键词 4，关键词 5

Abstract

This Latex template for the 33rd Fengru Cup Competition of Beihang University, is developed by Communist Youth League Committee of BUAA iteratively based on the contribution of GitHub users ***Somedaywilldo*** and ***cpfy***. Here, we would like to thank all the developers for their contributions to this template and for their support of the Fengru Cup Competition.

The abstract includes: the word "Abstract", the body of the abstract, and the keywords. On a separate line at the bottom of the abstract, indicate the key words of the text in prominent characters.

The abstract is a short statement of the content of the paper and should reflect the core ideas of the paper work. The abstract is usually about 500 words. The abstract should cover the purpose and significance of this scientific work, research ideas and methods, research results and conclusions.

Keywords are a set of words or terms selected from the text to reveal the subject content of the whole text for the user to find the literature, and the standardized words in the word list (refer to the corresponding technical terminology standards) should be used as much as possible. The keywords are usually 3 to 8, arranged according to the level of extensibility of the words. The keywords are separated by commas, and no punctuation marks are used after the last keyword.

Keywords: Keywords 1, Keywords 2, Keywords 3, Keywords 5, Keywords 6

目录

一、作品概述

本章首先介绍基于位置信息隐私保护的研究背景和研究意义，接着介绍国内外相关领域的研究现状，然后引出本文研究的主要内容，最后给出本文各章节的内容安排。

（一）研究背景与意义

近年来，移动用户数量迅猛增长，越来越多的用户选择使用移动设备来满足他们的日常活动需求，而不是依靠电脑。[czh_1.1] 在此背景下，基于位置的服务（Location Based Services, LBS）成为了一种趋势。基于位置的服务是指服务提供商根据用户提交的位置信息，返还给用户对应的基于位置信息的相应服务。比如大多数现代服务系统都会要求用户发送他们的位置信息，以提供更具适应性、符合用户实际需求和偏好的服务，例如关于天气、交通的警报服务或者提供出行的最佳路线。[czh_1.2]

在用户提交的位置信息中，最常用、便于服务提供商进行处理的位置信息是用户直接的地理位置信息，这也和用户个人隐私安全有着密切关系。但是，当移动应用频繁询问用户所在位置信息时，用户的位置信息面临着暴露的风险，甚至用户的其他隐私也不再安全。比如不可信的服务提供商可以利用用户的位置信息和上传时间，结合大数据分析手段绘制出用户的时间活动轨迹和活动热点图，进一步分析出用户的行为习惯、具体身份、社交信息等敏感隐私。在更极端的情况下，服务提供商还可以分析出用户的隐私画像，对匿名用户进行去匿名化，严重威胁用户隐私安全。

但是事实上相当多的移动应用都会询问用户的位置信息，这也带来了泄露位置信息、侵犯隐私的隐患。以 Google 应用市场为例，根据 2017 年的统计数据，在最受欢迎的 2800 个移动应用（aplication, 简称 app）中，4 成以上的 app 要求用户提供访问位置信息的权限，其中包括在后台可以直接访问位置的 app，[czh_1.3] 这在当时引起了用户群体一定的抗议。然而遗憾的是，当前大多数服务提供商对位置信息的保护力度远远不够。用户通常只能简单选择“是”或“否”给予服务提供商具体位置，而不能选择被上传的用户位置的精度，也没有对位置数据后续使用情况的追溯权限。服务提供商以使用用户地理位置提供精准服务的名义，将可能侵犯隐私的数据条款隐藏在繁杂的用户条款中，将用户摆在了无法反制的弱势地位上。现行的大多数隐私保护方案都基于通信渠道的安全性和授权，在获取位置信息后，服务提供方并没有对这些敏感信息给予应有的保护，[czh_1.4] 在这样的环境下，如何保护位置信息的隐私安全成为了一个新的问题。

需要注意的是，在保护位置信息隐私安全的同时，我们还应该保证位置信息的真实性以及用户获得的服务质量。如果忽略了位置信息的真实性，那么在一些特殊情景下，用户可能会向系统提供错误的位置信息来达成某些目的。比如攻击者可以向系统发送虚假的位置信息，以寻求系统的漏洞；或者用户可以在发生交通事故肇事逃逸后提交错误的位置信息，以逃避追责 [czh_1.5]。而保护隐私后的服务质量也同样需要保障。当前保护

位置隐私信息的一种重要方式是模糊用户的实际位置，将用户位置信息隐藏在虚假的位置或者一个模糊的范围中。这样固然对位置隐私起到一定的保护作用，却可能降低用户获得的服务质量，影响用户的服务体验。这两个需求也对现有位置隐私保护方案提出了更高的要求。

而现有的大多数位置隐私保护方案要么在在保护用户位置信息安全上存在漏洞，要么在满足上述两种需求上存在进一步提高的空间。并且用户基本只能选择同意授权获取位置权限或者拒绝，而难以在授权的同时控制暴露的位置信息的精度。因而服务提供商可以借提供服务的名义收集用户位置信息，这也使得用户处在一个难以保护自己隐私的弱势地位上。在这样的背景下，如果可以探索出一种新的位置隐私保护方案，这将为保护用户位置信息安全提供极大助力，并进一步促进隐私保护领域相关技术的发展。同时，如果将新的方案技术移植应用到其他领域，那将会为各行业的数据信息安全提供更可靠的保障。

（二）研究现状

现行的基于位置的隐私保护系统主要有 3 种结构：集中式结构、分布式结构以及混合式结构。国内外研究人员在这 3 种结构的基础上迭代出了很多高效、具有广泛适用性的位置信息隐私保护算法。本节将简要介绍这 3 种系统结构，并概括出各种结构的优缺点。

1. 集中式结构

集中式结构在基本已被淘汰的独立结构（仅由用户和服务提供方组成客户端/服务器结构[czh_2.1]）的基础上进行改进，在客户端和服务器之间加入位置匿名服务器，以分担客户端的计算、存储开销。集中式结构的示意图见图 1。

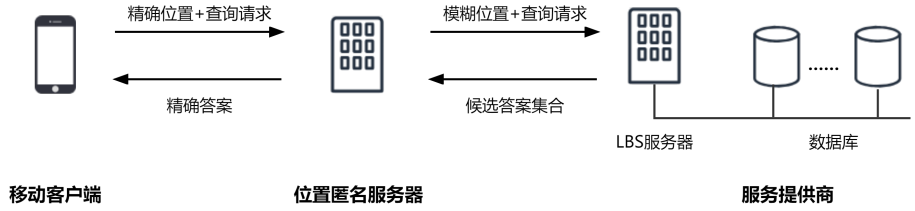

图 1 集中式结构系统示意图

在集中式结构的位置隐私保护系统中，用户发起查询请求后，由位置匿名服务器对用户的精确位置进行匿名处理。服务提供商受到位置匿名服务器提交的查询请求后，根据接受到的位置返回用户可能需要的答案集合，称为候选答案集合。位置匿名服务器接收到答案集合后，根据用户的精确位置进行筛选求精操作，最终把精确答案返还给用户。

[czh_2.2]

引入位置匿名服务器为系统性能带来了显著的提高。一方面，位置匿名服务器承担了位置匿名处理、候选答案求精的任务，从而减轻了用户端的负担，使得用户端的设计可以更为轻量。另一方面，引入位置匿名服务器后，原本一些在移动客户端上难以实现的复杂算法、功能也有了实现的可能，系统功能更加强大。

当然，位置匿名服务器本身也有一些缺点。随着系统的使用，服务器中存储的用户位置数据会逐渐积累。如果没有对服务器存储的数据进行处理，一旦服务器被攻击、或者服务器不再可信，这将会严重损害用户的位置信息隐私安全。此外，当系统用户频繁请求服务时，服务器自身的性能也可能成为限制系统性能的瓶颈。[czh_2.1]

2. 分布式结构

鉴于集中结构位置匿名服务器带来的安全问题和性能瓶颈问题，分布式结构去除了位置匿名服务器的存在，而是通过多台移动设备之间的协作来实现位置匿名效果。分布式系统结构示意图见图 2。

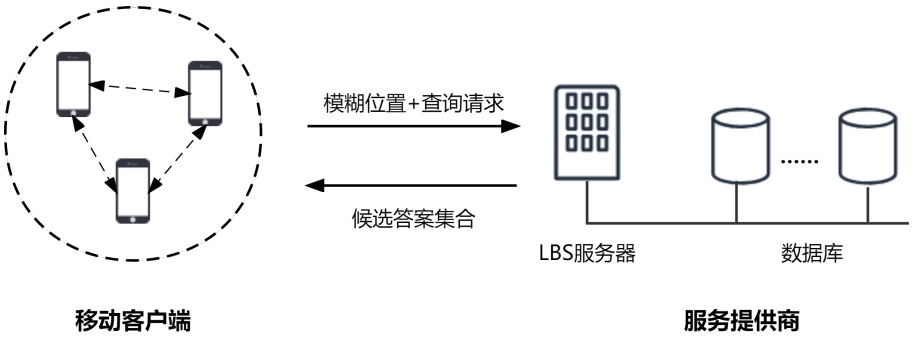

图 2 分布式结构系统示意图

在分布式结构系统中，用户发起查询请求后，一定区域内的多台移动设备相互协作并进行一定的通信，形成一个匿名区域。服务提供商根据接收到的区域返回相应的候选答案集合，用户接受到答案集合后进行筛选和求取精确答案的操作。

和集中式结构相比，分布式结构的系统进一步降低了用户位置信息泄露的隐患。但分布式结构也对用户移动设备的计算能力提出了一定的要求，以便进行协作匿名。这也限制了分布式结构系统的发展。[czh_2.1]

3. 混合结构

考虑到集中式结构系统的计算能力以及分布式结构系统的信息保密性，部分系统融合了上述两种结构，形成了兼具上述优点的新的系统结构——混合结构。混合结构的系

统示意图见图 3。

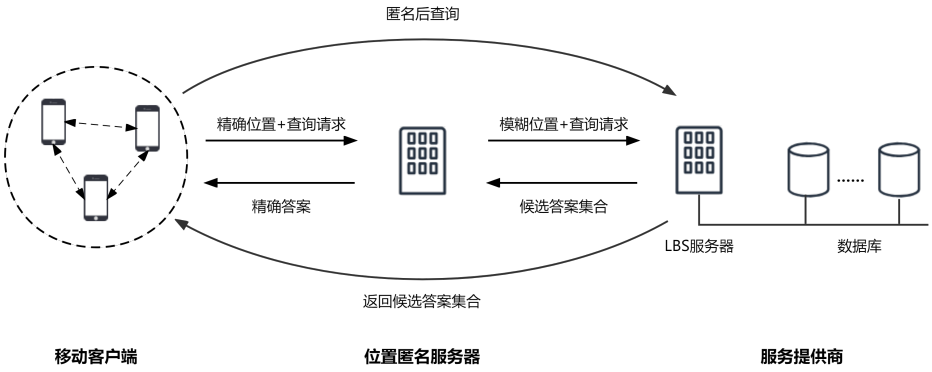

图 3 混合结构系统示意图

在混合结构系统中，用户发起查询请求后，系统可以选择让用户通过位置匿名服务器进行匿名查询，也可以联合多台移动设备，通过分布式的方式直接和 LBS 服务器取得联系，这将取决与系统中发起查询请求的用户数量。

值得一提的是，虽然混合结构吸收了先前两种结构的优点，使它看上去更为灵活。但实际上，在构建和维持混合结构时需要不断设置、调整系统参数，以决定系统什么时候通过哪种方式和 LBS 服务器建立联系。这也束缚了混合结构的进一步发展 [$czh\_2.3$]。

在上面的 3 个小节中，我们介绍了现行基于位置隐私保护系统的 3 种主要结构，它们各自的优缺点可以概括为表 1。

表 1 位置隐私保护系统 3 种结构对比

结构名称	优点	缺点
集中式结构	计算、存储性能提高	有泄露隐私的风险
分布式结构	提高安全性	对移动设备性能要求较高
混合结构	兼具安全性和性能	系统参数限制了应用

在以上 3 中位置隐私保护结构的基础上，国内外学者研发出了多种位置隐私保护技术。其中比较著名的有将用户位置信息隐藏在虚拟位置中的**K-匿名技术** [$czh\_2.4$]，在真实位置信息中添加虚假信息的**虚假位置技术** [$czh\_2.5$] 等等。由于本文主要在系统结构进行创新，这些技术不再一一说明。

（三）作品概述与创新点说明 (to be continued)

现有的位置隐私保护技术主要依靠添加虚假或者无关的位置信息，从而形成一个相对匿名的区域。用户实际位置信息隐藏在这个区域内，服务提供方和攻击者都难以从这个区域中采集用户的位置隐私。考虑到用户还是提交了位置信息，本文希望借鉴现有技术，提供一个用户在不暴露位置的同时获取服务的方法。

注意到区块链中的零知识证明技术具有正确性（证明结果可信）和零知识性（不会暴露关键信息）的优秀性质，并且这两个性质满足了位置隐私保护的需求，本文希望将零知识证明技术引入位置隐私保护，以改善现有模型。

零知识证明技术源于区块链中的 Zcash 货币应用体系。在用户之间进行交易前，付款的一方（prover）需要向另一方（verifier）证明自己的账户下有充足的余额。而零知识证明技术允许 prover 在证明自己账户余额足以完成交易的同时，保护 prover 自己的账户信息，防止敌手通过暴露的账户信息牟取利益。同时，零知识证明技术保证了 verifier 得到的证明结果是正确的，即 verifier 不会受到 prover 的欺骗。

本文借鉴了区块链中的零知识范围证明技术，对现有位置隐私保护系统进行改进优化，并提供一种在不提交用户位置信息的同时获取服务提供方服务的方法。具体创新成果如下。

1. 将零知识范围证明技术应用到位置隐私保护

现有零知识范围证明技术主要应用于区块链领域，而在其他领域的应用相当有限。同时，零知识范围证明技术满足了隐私保护的需求，但是现有位置隐私保护方案尚未将零知识范围证明技术投入应用。基于以上现状，本文将零知识范围证明技术应用到位置隐私保护领域，一方面可以开拓零知识范围证明技术的应用场景，为零知识范围证明技术的应用创造更多的可能。而另一方面，引入零知识范围证明技术可以改进现有位置隐私保护系统，为保护位置隐私提供一种新的思路。

2. 改进位置隐私保护系统的结构

引入零知识范围证明技术后，保护用户位置隐私不再需要第三方位置匿名服务器的参与，也不需要在多个用户端之间进行协作通信以达到匿名效果。同时，查询、提供服务与保护用户位置信息可以仅在移动用户端和服务提供商两方之间完成。所以本文在应用零知识范围证明技术的基础上，对现有位置隐私保护方案进行优化，改进了现有位置隐私保护系统的结构。

（四）内容结构安排 (to be continued)

二、预备知识

三、作品设计与实现

（一）需求分析

（二）系统概述

（三）关键技术

四、作品成果展示与可行性分析

五、前景展望

六、结论

七、参考文献

八、————————模板分割线————————

九、简介

第三十三届“冯如杯”主赛道论文一律由在计算机上输入、排版、定稿后转成 PDF 格式，在集中申报时通过网络上传。**论文封面及全文中不能出现作者姓名、学院、专业、指导老师的相关信息**。包括 5 个部分, 顺序依次为:

- 封面（中文）
- 中文摘要、关键词 (中文、英文)
- 主体部分
- 结论
- 参考文献

十、论文的书写规范

论文正文部分需分章节撰写，每章应另起一行。章节标题要突出重点，简明扼要、层次清晰。字数一般在 15 字以内，不得使用标点符号。标题中尽量不采用英文缩写词，对必须采用者，应使用本行业的通用缩写词。层次以少为宜，根据实际需要选择。三级标题的层次按章（如“一、”）、节（如“（一）”）、条（如“1.”）的格式编写，各章题序的阿拉伯数字用 Times New Roman 体。

（一）字体和字号

论文题目：二号，华文中宋体加粗，居中。

副标题：三号，华文新魏，居右（可省略）。

章标题：三号，黑体，居中。

节标题：四号，黑体，居左。

条标题：小四号，黑体，居左。

正文：小四号，中文字体为宋体，西文字体为 Times New Roman 体，首行缩进，两端对齐。

页码：五号 Times New Roman 体，数字和字母

（二）页边距及行距

学术论文的上边距：25mm；下边距：25mm；左边距：30mm；右边距 20mm。章、节、条三级标题为单倍行距，段前、段后各设为 0.5 行（即前后各空 0.5 行）。正文为 1.5 倍行距，段前、段后无空行（即空 0 行）。

（三）页眉

页眉内容为北京航空航天大学第三十三届“冯如杯”竞赛主赛道参赛作品，内容居中。页眉用小五号宋体字，页眉标注从论文主体部分开始（引言或第一章）。请注意论文封面无页眉。

（四）页码

论文页码从“主体部分（引言、正文、结论）”开始，直至“参考文献”结束，用五号阿拉伯数字连续编码，页码位于页脚居中。**封面、题名页不编页码。**

摘要、目录、图标清单、主要符号表用五号小罗马数字连续编码，页码位于页脚居中。

（五）图、表及其附注

图和表应安排在正文中第 1 次提及该图、表的文字的下方，当图或表不能安排在该页时，应安排在该页的下一页。

1. 图

图题应明确简短，**用五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，图的编号与图题之间应空半角 2 格。图的编号与图题应置于图下方的居中位置。图内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。曲线图的纵横坐标必须标注“量、标准规定符号、单位”，此三者只有在不必要注明（如无量刚等）的情况下方可省略。坐标上标注的量的符号和缩略词必须与正文中一致。

2. 表

表的标号应采用从 1 开始的阿拉伯数字编号，如：“表 1”、“表 2”、……。表编号应一直连续到附录之前，并与章、节和图的编号无关。只有一幅表，仍应标为“表 1”。表题应明确简短，用**五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，表的编号与表题之间应空半角 2 格。表的编号与表头应置于表上方的居中位置。表内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。

3. 附注

图、表中若有附注时，附注各项的序号一律用“附注 + 阿拉伯数字 + 冒号”，如：“附注 1：”。

附注写在图、表的下方，一般采用 5 号宋体。

4. 参考文献

凡有直接引用他人成果（文字、数字、事实以及转述他人的观点）之处，均应加标注说明列于参考文献中，以避免论文抄袭现象的发生。

标注格式：引用参考文献标注方式应全文统一，标注的格式为 [序号]，放在引文或转述观点的最后一个句号之前，所引文献序号用小 4 号 Times New Roman 体、以上角标形式置于方括号中，如“……成果”[1]。

十一、公式模板

公式示例展示如下：

$$\mathop{\mathrm{P}}_{\mathbf{I}_c \sim \mathfrak{S}_c}\Big(\mathcal{C}(\mathbf{I}_c) \neq \mathcal{C}(\mathbf{I}_c + \boldsymbol{\rho})\Big) \geq \delta \quad \text{s.t. } ||\boldsymbol{\rho}||_p \leq \xi, \tag{1}$$

十二、图表模板

图表示例展示如下：

图 4 example_caption

(a) 示意图 **1**

(b) 示意图 **2**

(c) 示意图 **3**

图 5 一行三张子图并排示意

(a) 示意图 **1**

(b) 示意图 **2**

(c) 示意图 **3**

(d) 示意图 **4**

图 6 2*2 四张子图示意

表 2 表格使用示例

表头 1	表头 2	表头 3	表头 4	表头 5
内容 11	内容 12	内容 13	内容 14	内容 15
内容 21	内容 22	内容 23	内容 24	内容 25

表 3 三线表使用示例

方法	**表头 1**	**表头 2**	**表头 3**	**表头 4**
方法 1	数据	数据	数据	数据
方法 2	数据	数据	数据	数据

结论

论文的结论单独作为一章，但不加章号。

注意: 文件大小不超过 5M。

参考文献

[1] 张志建．严复思想研究 [M]．桂林：广西师范大学出版社，1989．

[2]（英）霭理士．性心理学 [M]．潘光旦译．北京：商务印书馆，1997．

[3] 伍蠡甫．西方论文选（下册）[C]．上海：上海译文出版社，1979．

[4] 叶朗．《红楼梦》的意蕴 [J]．北京大学学报（哲学社会科学版），1989，（2）

[5] 谢希德．创造学习的新思路 [N]．人民日报，1998-12-25（10）

[6]Mansfeld, R.S. & Busse. *T.V. The Psychology of creativity and discovery*, Chinago：NelsonHall, 1981