基于区块链的分布式 K 匿名位置隐私保护方案

刘 海[1),2),3),4)] 李兴华[2),3),4)] 雒 彬[2),3),4)] 王运帷[2),3),4)]
任彦冰[2),3),4)] 马建峰[2),3),4)] 丁红发[1)]

[1)](贵州财经大学信息学院 贵阳 550025)
[2)](西安电子科技大学网络与信息安全学院 西安 710071)
[3)](西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)
[4)](西安电子科技大学陕西省网络与系统安全重点实验室 西安 710071)

摘 要 由于无需可信第三方和复杂的密码技术就可为请求用户提供准确的查询结果,分布式 K 匿名已被广泛地用于保护基于位置服务中用户的位置隐私.然而,现有分布式 K 匿名位置隐私保护方案均未考虑匿名区构造过程中存在的位置泄露和位置欺骗行为,这使得自利的请求用户会泄露协作用户的真实位置;而自利的协作用户也会提供虚假的位置导致服务提供商能识别出请求用户的真实位置.因此,现有分布式 K 匿名方案并不能有效保护用户的位置隐私.为了解决上述问题,本文将匿名区的构造视为请求用户与协作用户间的两方博弈,利用区块链记录博弈双方以及协作用户提供的真实位置作为证据,通过惩罚具有位置泄露和欺骗行为的用户,使其作为请求者时不能成功构造出匿名区来约束他们的自利性.基于上文,本文提出一个基于区块链的分布式 K 匿名位置隐私保护方案.安全性分析和大量实验表明,本文所提方案不仅能激励协作用户提供真实位置参与匿名区构造,而且能防止请求用户泄露协作用户的真实位置,还可高效地生成匿名区,从而有效保护用户的位置隐私.

关键词 基于位置的服务;位置隐私保护;分布式 K 匿名;匿名区构造;协同构造博弈;区块链
中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2019.00942

Distributed K-Anonymity Location Privacy Protection Scheme Based on Blockchain

LIU Hai[1),2),3),4)] LI Xing-Hua[2),3),4)] LUO Bin[2),3),4)] WANG Yun-Wei[2),3),4)]
REN Yan-Bing[2),3),4)] MA Jian-Feng[2),3),4)] DING Hong-Fa[1)]

[1)](*School of Information, Guizhou University of Finance and Economics, Guiyang* 550025)
[2)](*School of Cyber Engineering, Xidian University, Xi'an* 710071)
[3)](*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071)
[4)](*Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an* 710071)

Abstract With the development of wireless communication and positioning technologies, location-based service (LBS) has become a part of our daily life. However, since LBS always requires the users to submit their locations, an unprecedented threat about location privacy of mobile users comes with the convenience of widely used technique. Therefore, LBS location privacy protection has attracted substantial attention. Among the existing LBS location privacy protection methods, the distributed K-anonymity technique is one of the most common and popular methods. In this

收稿日期:2018-04-24;在线出版日期:2018-12-29.本课题得到国家自然科学基金(U1708262,U1736203,U1405255)、国家"九七三"重点研究发展计划项目(2017YFB0801805)、贵州财经大学引进人才科研启动项目(2018YJ16)、贵州财经大学校级科研基金项目(2018XYB01)资助.**刘 海**,博士,主要研究领域为位置隐私保护和安全协议设计.E-mail:liuhai4757@163.com.**李兴华**(通信作者),博士,教授,主要研究领域为网络与信息安全、隐私保护和密码学.E-mail:xhli1@mail.xidian.edu.cn.**雒 彬**,博士研究生,主要研究领域为位置隐私保护和信任评估.**王运帷**,博士研究生,主要研究领域为区块链和隐私保护.**任彦冰**,硕士研究生,主要研究方向为区块链和位置隐私保护.**马建峰**,博士,长江学者特聘教授,主要研究领域为网络与信息安全、编码理论、密码学.**丁红发**,博士研究生,讲师,主要研究领域为数据隐私保护.

technique, without any trusted third party, the request user can submit an anonymous cloaking region that includes the locations of other cooperative users instead of his/her real location. In this way, the adversary can identify the request user's real location with a sufficient negligible probability. Furthermore, compared with other methods, the distributed K-anonymity method is able to provide precise query results without any requirement for complicated cryptographic technologies reduce the request user's computational burden. In light of these advantages, the distributed K-anonymity method has been widely used to protect the request user's location privacy when he/she enjoys LBS. However, the existing distributed K-anonymity location privacy protection schemes do not consider location leaking behaviors and location cheating behaviors during the construction of anonymous cloaking region. When directly adopting the existing schemes, on one hand, a selfish request user could disclose the cooperative users' locations to gain illegal benefits. On the other hand, a selfish cooperative user could provide a fake location, which leads that the constructed anonymous cloaking region cannot satisfy the privacy protection requirement of the request user and more seriously, the adversary could be used to directly identify the request user's real location. Therefore, these schemes cannot protect the users' location privacy completely. Fortunately, blockchain can provide an open and distributed ledger that guarantees that the recorded transactions are inherently resistant to modification. To address the problem mentioned above, this paper introduces blockchain into the distributed K-anonymity location privacy protection and proposes an advanced scheme. In the proposed scheme, the construction of anonymous cloaking region is firstly regarded as a two-party cooperation construction game between the request user and cooperative user to analyze their strategies and utilities, and then the security of distributed K-anonymity location privacy protection is given. Afterwards, by adopting blockchain to record the users involved in the construction of anonymous cloaking region and the provided locations as evidences, the corresponding users are punished with unsuccessfully constructing the anonymous cloaking in their future LBS queries when location leaking or cheating behaviors occur. The security analysis demonstrates that the proposed scheme not only prevents the request user from disclosing the cooperative users' locations but also promotes the cooperative users to provide the real locations, thereby effectively protecting location privacy of the request user and cooperative users. Extensive experiments indicate that the proposed scheme does not increase the computation delay and communication cost on both the request user side and the cooperative user side, which shows that the proposed scheme can construct the anonymous cloaking region efficiently.

Keywords　location-based service; location privacy protection; distributed K-anonymity; anonymous cloaking region construction; cooperation construction game; blockchain

1　引　言

基于位置的服务(Location-Based Service, LBS)[1-2]是根据用户提供的位置信息,在地理信息系统平台的支持下,为用户提供包括兴趣点查询、广告推送和娱乐游戏在内的增值服务.随着移动通信技术的不断发展以及智能终端设备的不断普及,LBS已被广泛地应用到电子商务、卫生医疗和移动社交等领域,成为人们日常生活必不可少的重要组成.据一项最新报告显示①,2017 年美国共有 2.20 亿 LBS 用户,占其人口总数的 68.09%,预计到 2018 年 LBS 用户将增至 2.42 亿.

然而,随着 LBS 的广泛应用,LBS 中的位置隐私泄露问题受到了用户的广泛关注[3-7].造成用户位置隐私泄露的主要原因是位置服务提供商(Location-based Service Provider, LSP)会利用数据挖掘等技

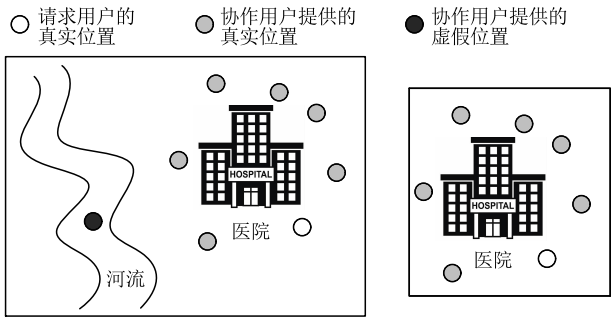
① https://www. statista. com/statistics/436071/location-based-service-users-usa.

术从用户提交的位置信息中非法获取用户的个人敏感信息[8-9]，如家庭/工作地址、个人嗜好、生活习惯等. K 匿名[10-11]是 LBS 位置隐私保护中最常见的一种方法，其基本思想是当发送 LBS 查询请求时，用户首先至少获取其他 $K-1$ 个协作用户真实位置后构建一个匿名区，然后再将该匿名区替代自己的真实位置提交给 LSP，从而有效保护自己的个人位置隐私. 与其他位置隐私保护方法相比，如差分隐私[12-13]、位置坐标变换[14-15]和基于密码学[16-17]的方法，K 匿名方法具有以下优势：(1) 不依赖复杂的密码技术；(2) 可有效地降低用户的计算开销；(3) 可让用户获取准确的查询结果，享受较高的 LBS 服务质量.

但是，在传统的 K 匿名方法[18-19]中，需要一个集中式的节点来当匿名服务器，为请求用户构造匿名区. 一旦匿名服务器被攻破，攻击者就能轻而易举地获取请求用户和协作用户的真实位置. 并且，集中式匿名服务器的存在，不仅使得用户(包括请求用户和协作用户)与匿名服务器间存在通信瓶颈，而且完全可信的第三方在现实环境中也难以找到. 这都导致集中式 K 匿名方法并不实用. 为了解决该问题，学者们又提出无需可信第三方的分布式 K 匿名位置隐私保护方法[18-35]. 在该方法中，请求用户可直接与周围协作用户进行协商并获取协作用户的真实位置，自主式地生成匿名区来保护自己的位置隐私. 然而，现有的分布式 K 匿名位置隐私保护方案却存在以下两个问题：

(1) 收到协作用户提供的真实位置后，自利的请求用户会将这些位置信息泄露给第三方以获取额外收益；或者恶意的攻击者会假扮为请求用户来获取协作用户的真实位置，从而导致协作用户位置隐私的泄露.

(2) 收到请求用户发送的协作请求后，即使某些协作用户位于敏感区域，但由于自利性，其仍会提供虚假位置给请求用户来提高自己的活跃度(或信誉值)，以便自己作为请求者时能高效地构造出匿名区. 如果自利的协作用户随机生成一个位于无移动用户区域内的虚假位置给请求用户来构造匿名区，由于 LSP 可利用背景知识如网络监视技术或区域监视技术识别出无用户区域[36]，LSP 就能缩小匿名区. 这不仅导致请求用户的位置隐私保护需求难以得到满足，甚至还使得 LSP 可直接推测出请求用户的隐私信息，如图 1 所示. 假设请求用户 Alice 使用分布式 K 匿名隐私保护方法保护其位置隐私. 当 Alice 发送匿名区构造协作请求后，协作用户 Bob 正在酒吧酗酒. 此时，他既不想提供自己的真实位置来泄露自己酗酒的不良嗜好，又想参与匿名区构造以提升自己的活跃度使得自己作为请求者时能获得他人帮助，因此 Bob 就随机生成了一个位于河流中心的虚假位置提供给 Alice. Alice 在收到协作用户 B 提供的位置后，将构造出的匿名区连同自己的查询内容提交给 LSP，如图 1(a)所示. 当收到 Alice 提交的匿名区后，LSP 识别出该匿名区中的无人区域，发现缩小后的匿名区属于医院区域，如图 1(b)所示. 此时，LSP 就能以极大概率推测出 Alice 的身体健康状况，从而非法获取请求用户 Alice 的个人隐私.



(a) 请求用户提交的匿名区　　(b) 被识别后的匿名区

图 1　协作用户提供虚假位置给请求用户的示例图

综上所述，由于未考虑匿名区构造过程中存在的位置泄露和欺骗行为，现有的分布式 K 匿名位置隐私保护方案并不能完全保护用户的位置隐私. 为了解决上述问题，本文提出了一个基于区块链的分布式 K 匿名位置隐私保护方案. 据作者所知，这是第一个利用区块链来研究 LBS 位置隐私保护的方案. 本文的主要贡献如下：

(1) 通过记录参与匿名区构造的请求用户、协作用户及其提供的位置信息作为证据，惩罚具有位置泄露和欺骗行为的用户，使其作为请求者时不能构造出匿名区，并设计一个交互记录机制来约束匿名区构造过程中请求用户和协作用户的自利性行为.

(2) 基于设计的交互记录机制，结合区块链技术，本文提出一个分布式 K 匿名位置隐私保护方案. 安全性分析证明该方案在有效防止请求用户泄露协作用户的位置信息的同时，还能激励协作用户提供真实位置来参与匿名区的构造.

(3) 大量实验表明，当请求用户使用本方案构造匿名区时，其与协作用户所需的计算开销、通信开销和存储开销较少，能高效地构造出匿名区. 这说明本方案具有较好的实用性.

2　相关工作

2.1　分布式环境下匿名区的构造方法

分布式 K 匿名位置隐私保护方法最早是由 Chow 等人[20]提出的，其基本思想是请求用户利用点对点通信方式获取至少其他 $K-1$ 个协作用户的真实位置构造匿名区，使得 LSP 仅能以不高于 $1/K$ 的概率从匿名区中猜测出请求用户的真实位置. 然而，在他们的方案中，请求用户和协作用户需要拥有两个独立的通信网络，分别用于 P2P 通信和 LBS 查询通信. 这极大地降低了该方案的实用性. Ghinita 等人[21]利用 Hibert 曲线将请求用户和协作用户的位置信息从二维空间映射至一维空间，并将每个用户的一维位置信息存储于 B+树的数据节点中，使得请求用户可快速获取相邻协作用户的真实位置来构造匿名区. 但是，当协作用户较多时，请求用户需从 B+树的根节点进行检索，从而增大了请求用户的计算开销. 为了解决该问题，文献[22]又利用环形结构替代 B+树结构存储所有用户的一维位置，使得请求用户可快速查找相邻用户构造匿名区. Chow 等人[23]指出请求用户在构造匿名区时需结合实际的道路交通网络，否则 LSP 就可根据道路交通网络从请求用户提交的匿名区中识别出某些协作用户的真实位置，乃至直接识别出请求用户的真实位置. 他们为请求用户在每条道路上进行 LBS 查询设置不同的服务质量，在确保服务质量的前提下，使得生成的匿名区中尽可能多地包含交叉路口，提高请求用户的位置隐私保护等级. Sun 等人[24]将网络中所有用户的真实位置进行分类，提出基于位置标签的分布式 K 匿名隐私保护方案. 在他们的方案中，请求用户构造的匿名区中不仅要至少包括 $K-1$ 个协作用户的真实位置，并且协作用户真实位置的类型也要与请求用户真实位置的类型一致.

2.2　分布式环境下协作用户位置的获取方法

当请求用户未收到 $K-1$ 个协作用户发送的位置信息时，上述方案均通过提高点对点通信跳数的方法来获取更多协作用户提供的位置信息. 这势必增加网络传输延迟，加重网络通信负担. 为了解决该问题，Chow 等人[25]提出利用历史协作用户的真实位置为请求用户构造匿名区. 在他们的方案中，请求用户在进行每次 LBS 查询后，均会将采用的协作用户的位置信息进行存储. 若下次 LBS 查询时获得的协作用户数量不满足其位置隐私保护需求，可直接利用历史协作用户提供的位置信息参与构造匿名区. 为了降低请求用户的存储开销，Kim 等人[26]采用 Hibert 曲线对历史协作用户的位置信息进行降维处理，并利用构造出的匿名区的信息熵来度量请求用户的位置隐私保护等级，提出了基于网格的分布式 K 匿名位置隐私保护方案. Peng 等人[27]通过让合法请求用户发送虚假查询的方式混淆自己的真实查询，提出了一个适用于分布式网络的 K 匿名位置隐私保护方案. 在他们的方案中，请求用户通过发送虚假协作请求获取协作用户的真实位置，并将它们存入缓存中. 当请求用户需要向 LSP 发送查询请求时，可利用缓存中存取的位置信息构造匿名区. 除采用历史协作用户的位置信息外，Zhong 和 Hengartner[28]、Takabi 等人[29]结合现有移动通信基础设施，分别提出了两个基于区域感知的分布式 K 匿名位置隐私保护方案. 他们的基本思想是让请求用户随机构造匿名区，通过向移动通信运营商询问该区域内包含的其他用户数量来确定该匿名区是否满足请求用户的隐私保护需求. 然而，这两个方案均不能抵抗来自移动通信运营商和 LSP 的合谋攻击. Che 等人[30]通过让网络中所有用户主动发送自己的真实位置以及自己周围邻居的位置信息表的方法，提出了一个双向主动的分布式 K 匿名隐私保护方案. Hwang 和 Huang[31]、Hwang 等人[32]提出请求用户可利用社交网络获取协作用户的真实位置来构造匿名区.

2.3　分布式 K 匿名中的激励机制

Yang 等人[33]指出原有的分布式 K 匿名隐私保护方案均假设协作用户是诚实的，他们在收到请求用户发送的匿名区协作构造请求后，会提供自己真实的位置给请求用户. 然而，在现实环境中，用户都是自利的. 若请求用户直接使用这些方案保护自己 LBS 查询时的位置隐私，将难以获得满足自己隐私保护需求的协作用户真实位置数量来构造匿名区. 他们利用单轮密封式双重拍卖机制允许多个请求用户通过拍卖的方式获取协作用户的真实位置，从而激励网络中的所有用户都参与到匿名区的构造. Zhang 等人[34]指出当请求用户的真实位置过于敏感时，若采用方案[33]的方法，其将难以拍卖到满足隐私保护需求的协作用户位置数量来构造匿名区. 为了解决该问题，他们利用贪心算法设计了一个中标判定规则，使得所有请求用户均能获得满足其隐私保护需求的位置数量来构造匿名区. Li 等人[35]指出上述两个方案均需要存在可信的拍卖者，否则

其可将请求用户与协作用户的位置信息泄露给LSP.他们将信誉引入到匿名区构造中,提出了基于信誉激励的分布式 K 匿名区隐私保护方案.在他们的方案中,协作用户只会帮助信誉值高的请求用户构造匿名区,而每个用户的信誉值则靠帮助其它用户构造匿名区来提升.此外,Gong 等人[36-37]指出为了更好地保护请求用户的位置隐私,请求用户与协作用户在参与匿名区构造时需要更换使用的假名.因此,为了激励协作用户更换假名,他们将参与匿名区构造的请求用户和协作视为一类特殊的社会群体,基于群体用户间的社会关系,通过最大化群体收益,激励协作用户在参与匿名区构造时更换自己的假名.

综上所述,现有的分布式 K 匿名位置隐私保护方案均未考虑匿名区构造过程中存在的隐私泄露和欺骗行为.这不仅使得自利的请求用户在收到协作用户的真实位置后可将这些位置信息泄露给第三方,还会使得自利的协作用户提供虚假位置给请求用户,使得最终生成的匿名区不能满足请求用户的位置隐私保护需求,甚至使得 LSP 可直接获知请求用户的位置隐私.因此,现有的分布式 K 匿名位置隐私保护方案不能完全保护用户的位置隐私.

3 预备知识

3.1 系统结构

如图 2 所示,本文采用点对点对等式结构[37],由请求用户、协作用户和 LSP 组成,无需第三方.假设请求用户与协作用户以及请求用户与 LSP 间存在安全的通信链路.当请求用户 P_0 向 LSP 发送查询请求时,他首先向周围用户发送协作请求以获取他们的真实位置.当收到协作用户 $P_1,P_2,\cdots,P_{K-1}$ 提供的位置 $Loc_1^{\text{real}},Loc_2^{\text{real}},\cdots,Loc_{K-1}^{\text{real}}$ 后,请求用户 P_0 构造匿名区 ACR,并连同查询内容一同提交给 LSP.

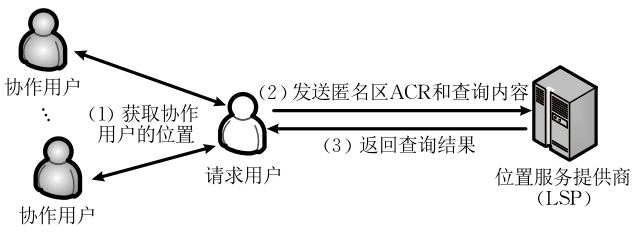


图 2 系统结构

当 LSP 认证通过请求用户 P_0 的身份后,他根据请求用户提交的匿名区和查询内容在数据库中进行检索,将所有结果返回给请求用户 P_0.在收到 LSP 发送的查询结果后,请求用户 P_0 根据自己的真实位置 Loc_0^{real} 对它们进行筛选,从而获得准确的查询结果.其中,Loc_i^{real} 表示第 $i(1\leq i\leq K-1)$ 个协作用户 P_i 的真实位置;匿名区 $ACR=Area(Loc_0^{\text{real}},Loc_1^{\text{real}},\cdots,Loc_{K-1}^{\text{real}})$;$Area(\cdot)$ 是匿名区构造函数;K 表示请求用户 P_0 的隐私保护需求.

此外,本文还假设请求用户与协作用户均是理性的,即在匿名区构造过程中,他们总是根据自身利益最大化进行策略选择.对于理性的请求用户 P_0 来说,他首先期望获得协作用户提供的真实位置用于生成匿名区 ACR;其次,在成功构造匿名区的同时,他会泄露协作用户的真实位置以获得更多额外收益.因此,在匿名区构造过程中,理性请求用户 P_0 的偏好满足:$\widetilde{U}^{+}>\widetilde{U}>\widetilde{U}^{-}>\widetilde{U}^{--}$.其中:

- $\widetilde{U}^{+}$ 表示请求用户 P_0 成功构造匿名区,且泄露协作用户 P_i 真实位置时的收益;
- $\widetilde{U}$ 表示请求用户 P_0 成功构造匿名区,但未泄露协作用户 P_i 真实位置时的收益;
- $\widetilde{U}^{-}$ 表示请求用户 P_0 未成功构造匿名区,但泄露协作用户 P_i 真实位置时的收益;
- $\widetilde{U}^{--}$ 表示请求用户 P_0 未成功构造匿名区,且未泄露协作用户 P_i 真实位置时的收益.

而对于理性的协作用户 P_i 来说,他首先期望能保护自己的位置隐私;其次,在有效保护自己位置隐私的同时,向请求用户提供协作帮助.因此,在匿名区构造过程中,理性协作用户 P_i 的偏好满足:$\widetilde{W}^{+}>\widetilde{W}>\widetilde{W}^{-}>\widetilde{W}^{f}>\widetilde{W}^{--}$.其中:

- $\widetilde{W}^{+}$ 表示协作用户 P_i 提供虚假位置 Loc_i^{fake} 给请求用户 P_0,且请求用户 P_0 采用该虚假位置构造匿名区时的收益;
- $\widetilde{W}$ 表示协作用户 P_i 提供自己的真实位置 Loc_i^{real} 给请求用户 P_0,且请求用户 P_0 未泄露该位置时的收益;
- $\widetilde{W}^{-}$ 表示协作用户 P_i 未提供位置信息来协作请求用户 P_0 构造匿名区时的收益;
- $\widetilde{W}^{f}$ 表示协作用户 P_i 提供虚假位置 Loc_i^{fake} 给请求用户 P_0,但被请求用户正确识别,未采用该位置构造匿名区时的收益;
- $\widetilde{W}^{--}$ 表示协作用户 P_i 提供自己真实位置 Loc_i^{real} 给请求用户 P_0,但请求用户 P_0 泄露自己真实

位置时的收益.

3.2　分布式 K 匿名位置隐私保护的安全性

本文分别将请求用户和周围协作用户视为攻击者. 在分布式匿名区的构造过程中，自利的请求用户在收到协作用户提供的位置信息后，会泄露这些信息给第三方以获取额外的收益. 而自利的协作用户在收到请求用户发送的匿名区构造协作请求后，其可能会提供虚假的位置信息给请求用户，使得请求用户构造出的匿名区不能满足其隐私保护需求，甚至使得 LSP 可直接推测出请求用户的个人隐私，如图 1 所示.

为了清晰地给出分布式匿名区构造的安全性定义，本文将匿名区的协同构造视为请求用户 P_0 和协作用户 P_i 间的两方博弈，首先形式化描述匿名区协同构造博弈.

定义 1(匿名区协同构造博弈). 匿名区协同构造博弈是一个五元组 $G_{\mathrm{ACR}}=\{P,A,H,F,U\}$，其中：

• $P=\{P_0,P_i\}$ 是理性用户集合；P_0 表示请求用户；P_i 表示协作用户.

• $A=\{A_0,A_i\}$ 是参与者的策略集合. 其中，$A_0=\{a_0^{(1)},a_0^{(2)}\}$ 是请求用户 P_0 的策略集合：$a_0^{(1)}$ 表示请求用户 P_0 在收到协作用户 P_i 提供的位置 Loc_i 后不将其泄露给第三方；$a_0^{(2)}$ 表示请求用户 P_0 在收到协作用户 P_i 提供的位置 Loc_i 后将其泄露给第三方. $A_i=\{a_i^{(1)},a_i^{(2)},a_i^{(3)}\}$ 表示协作用户 P_i 的策略集合：$a_i^{(1)}$ 表示协作用户 P_i 在收到协作请求后，提供自己的真实位置 Loc_i^{real} 给请求用户 P_0；$a_i^{(2)}$ 表示协作用户 P_i 在收到协作请求后，不提供位置信息给请求用户 P_0；$a_i^{(3)}$ 表示协作用户 P_i 在收到协作请求后，提供虚假的位置 Loc_i^{fake} 给请求用户 P_0. 并且，在匿名区协同构造博弈 G_{ACR} 中，请求用户和协作用户各选一个策略形成的向量 $\boldsymbol{a}=(a_0,a_i)$ 称为理性用户的策略组合. 其中，$a_0\in A_0$；$a_i\in A_i$.

• H 是历史集合. 任意一个历史 $\boldsymbol{h}\in H$ 表示其对应时刻理性用户选择的策略构成的策略组合. 显然，空字符 $\tau\in H$，其表示匿名区协同构造博弈开始. 对于任意的历史 $\boldsymbol{h}\in H$，在其之后可能出现的所有策略组合记为 $A(\boldsymbol{h})=\{\boldsymbol{a}\mid(\boldsymbol{h},\boldsymbol{a})\in H\}$. 如果存在 $\boldsymbol{h}'\in H$ 使得 $A(\boldsymbol{h}')=\varnothing$，则称该历史 $\boldsymbol{h}'$ 是终止的. 集合 Z 表示所有终止历史组成的集合.

• $F:(H/Z)\to P$ 是用户分配函数，它为没有终止的历史 $\boldsymbol{h}\in H\backslash Z$ 指定下一步进行策略选择的用户. 由于在匿名区协同构造博弈中，理性协作用户 P_i 率先进行策略选择，故 $F(\tau)=P_i$.

• $U=\{u_0,u_i\}$ 是理性用户的收益集合. 其中，$u_0\in\{\widetilde{U}^+,\widetilde{U},\widetilde{U}^-,\widetilde{U}^{--}\}$ 是理性请求用户 P_0 的收益函数；$u_i\in\{\widetilde{W}^+,\widetilde{W},\widetilde{W}^-,\widetilde{W}^f,\widetilde{W}^{--}\}$ 是理性协作用户 P_i 的收益函数.

基于形式化描述的匿名区协同构造博弈模型，下面给出分布式 K 匿名的安全性定义.

定义 2(分布式 K 匿名位置隐私保护的安全性). 假设 P_0 是理性请求用户，$P_1,P_2,\cdots,P_{K-1}$ 是 $K-1$ 个理性协作用户. 当理性请求用户 P_0 采用分布式 K 匿名隐私保护方案向 $P_1,P_2,\cdots,P_{K-1}$ 发送协作构造匿名区请求，且成功构造出匿名区 ACR 时，下述条件成立：

$$\begin{cases} u_0=\widetilde{U} & (1)\\ u_i=\widetilde{W} & (2)\\ \Pr_{\mathrm{LSP}}[Loc_0^{\mathrm{real}}\mid \mathrm{ACR}]\le 1/K & (3)\end{cases}$$

那么，该分布式 K 匿名位置隐私保护方案就称为是安全的. 其中，K 表示请求用户 P_0 在发送当前 LBS 查询时的位置隐私保护需求；$1\le i\le K-1$；$\Pr_{\mathrm{LSP}}[Loc_0^{\mathrm{real}}\mid\mathrm{ACR}]$ 表示 LSP 从请求用户 P_0 提交的匿名区 ACR 中正确识别出其真实位置 Loc_0^{real} 的概率.

在上述定义中，式(1)和式(2)是从匿名区构造的角度对分布式 K 匿名位置隐私保护的安全性进行定义. 其中，式(1)表示在匿名区构造过程中请求用户 P_0 不会泄露协作用户的位置；式(2)表示在匿名区构造过程中协作用户 P_i 提供自己的真实位置 Loc_i^{real} 给请求用户 P_0. 而式(3)是从 LBS 查询的角度对分布式 K 匿名位置隐私保护的安全性进行定义.

3.3　区块链

区块链[①]的基本思想是通过整合密码技术和点对点通信技术，基于数据分布式存储一致性的原理，利用智能合约来自动化执行预设脚本代码，在实现去中心化共享数据的同时，确保共享数据的不可篡改性和不可伪造性.

区块链的基础架构[39]可分为六层，自顶向下分别是：应用层、合约层、激励层、共识层、网络层和数据层，如图 3 所示.

(1) 应用层

应用层封装了区块链在社会活动中可应用的场景及实例.

① Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/[2018-07-28].

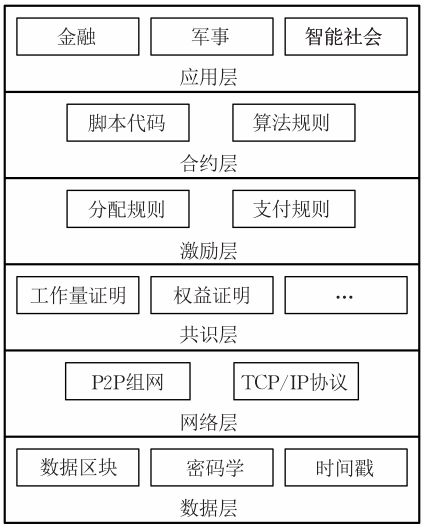


图 3 区块链基础架构

(2)合约层

合约层封装了各类脚本代码以及算法机制等,为用户提供可编程环境,从而实现智能合约.利用智能合约,区块链就可将各自业务规则转化成区块链系统中自动执行的合约,使得该合约的执行不依赖任何第三方.理论上智能合约一旦部署且符合其执行的条件,即可自动执行.

(3)激励层

在区块链中,数据是由所有节点共同维护的.为了激励节点积极参与到区块链的维护中,激励层封装了激励相容的分配规则和支付规则,在各节点参与维护区块链的同时,使其自身收益最大化.

(4)共识层

在区块链中,由于需要在无中心节点的情况下保证各个节点记账的一致性,此时需利用共识层中封装的各种共识机制在相互没有信任基础的个体间达成共识.

(5)网络层

网络层封装了区块链系统的组网规则——对等式组网,以及在该网络中节点间的交易账单和其他数据的传播、验证协议等.

(6)数据层

数据层利用 Hash 算法、Merkle 树等密码技术和时间戳技术将数据区块生成时间间隔内形成的所有交易账单以链式结构进行存储,确保区块链中存储的数据具有不可伪造、不可篡改和可追溯性.

4 基于区块链的分布式 K 匿名位置隐私保护方案

为了防止在分布式匿名区构造过程中请求用户泄露协作用户的位置以及协作用户提供虚假位置欺骗请求用户等情况的发生,本文首先利用加密和签名技术来防止其余用户非法获取协作用户提供的位置信息以及参与匿名区构造用户具有位置欺骗或泄露行为后的抵赖,并利用区块链分布式存储参与匿名区构造的博弈双方以及提供的位置信息作为证据,设计了一个分布式 K 匿名位置隐私保护方案.

4.1 共识机制

为了防止在分布式匿名区构造过程中请求用户泄露协作用户的位置以及协作用户提供虚假位置欺骗请求用户,本节首先设计了一个协作请求记录机制约束请求用户和协作用户的自利性行为;并且还提出了一个区块链记账权竞争机制,激励网络中所有用户参与区块链的维护中.

假设在任意第 q 次匿名区协同构造博弈中,策略 $a_0^{q-(1)}$ 表示请求用户 P_0 在收到协作用户 P_i 提供的位置 Loc_i^q 后并不将其泄露给第三方;策略 $a_0^{q-(2)}$ 表示请求用户 P_0 在收到协作用户 P_i 提供的位置 Loc_i^q 后将其泄露给第三方.策略 $a_i^{q-(1)}$ 表示协作用户 P_i 在收到协作请求后,提供自己的真实位置 Loc_i^{real} 给请求用户 P_0;策略 $a_i^{q-(2)}$ 表示协作用户 P_i 在收到协作请求后,不提供任何位置信息给请求用户 P_0;策略 $a_i^{q-(3)}$ 表示协作用户 P_i 在收到协作请求后,提供虚假的位置 Loc_i^{fake} 给请求用户 P_0.令 u_0^q 和 u_i^q 分别表示第 q 次匿名区协同构造博弈结束时请求用户 P_0 和协作用户 P_i 的收益.并且,令策略 $a_{0\to 0}^{q+j}$ 表示第 q 次匿名区协同构造博弈的请求用户 P_0 在之后的第 j 次博弈中仍作为请求者时选择的策略;策略 $a_{i\to 0}^{q+j}$ 表示参与第 q 次匿名区协同构造博弈的协作用户 P_i 在第 j 次博弈中作为请求者时选择的策略.那么,本文提出的协作请求记录机制如下所示.

定义 3(共识机制 I——交互记录机制).交互记录机制 $M_R=(\boldsymbol{a}^q,p^{[\tilde{q}+m]})$ 是一个二元组.其中,

- $\boldsymbol{a}^q=(a_0^q,a_i^q)$ 是在第 q 次匿名区协同构造博弈中,请求用户 P_0 和协作用户 P_i 选择的策略 a_0^q 和 a_i^q 形成的策略组合.
- $p^{[\tilde{q}+m]}=\{p_0^{[\tilde{q}+m]},p_i^{[\tilde{q}+m]}\}$ 是交互记录机制 M_R 根据请求用户 P_0 和协作用户 P_i 在第 q 次匿名区协同构造博弈中选择的策略,给予他们在之后的第 $\tilde{q}$ 次匿名区协同构造博弈 $G_{\text{ACR}}^{\tilde{q}}$ 至第 $\tilde{q}+m$ 次匿名区协同构造博弈 $G_{\text{ACR}}^{\tilde{q}+m}$ 的支付收益.对于任意 $j\in[\tilde{q},\tilde{q}+m]$,它满足:

$$p_0^j=\begin{cases}u_0^j(a_{0\to 0}^j,a_i^{j-(1)}), & a_0^q=a_0^{q-(1)}\\ u_0^j(a_{0\to 0}^j,a_i^{j-(2)}), & a_0^q=a_0^{q-(2)}\end{cases} \tag{4}$$

$$p_i^j=\begin{cases}u_{i\to 0}^j(a_{i\to 0}^j,a_{i'}^{j_{i'}-(1)}), & a_i^q=a_i^{q_i-(1)}\\ u_{i\to 0}^j(a_{i\to 0}^j,a_{i'}^j(\lambda_{i\to 0},\delta_{i'})), & a_i^q=a_i^{q_i-(2)}\\ u_{i\to 0}^j(a_{i\to 0}^j,a_{i'}^{j_{i'}-(2)}), & a_i^q=a_i^{q_i-(3)}\end{cases}\tag{5}$$

其中：m 表示惩罚轮数；$a_{i'}^j$ 表示在匿名区协同构造博弈 G_{ACR}^j 中协作用户 $P_{i'}$ 选择的策略；$\lambda_{i\to 0}$ 表示参与匿名区协同构造博弈 G_{ACR}^q 的协作用户 P_i 在参与博弈 G_{ACR}^j 时协助其他用户构造匿名区的次数；$\delta_{i'}$ 是匿名区协同构造博弈 G_{ACR}^j 中协作用户 $P_{i'}$ 的判断阈值. 当 $\lambda_{i\to 0}<\delta_{i'}$ 时，$a_{i'}^j(\lambda_{i\to 0},\delta_{i'})=a_{i'}^{j_{i'}-(2)}$；否则，$a_{i'}^j(\lambda_{i\to 0},\delta_{i'})=a_{i'}^{j_{i'}-(1)}$.

交互记录机制 M_R 就是通过记录参与匿名区构造的请求用户、协作用户及其提供的位置信息来约束他们的自利性行为. 也就是说，一旦发现匿名区协同构造博弈 G_{ACR}^q 中请求用户 P_0 泄露了协作用户的位置信息，那么其之后的 m 次服务查询中均不会有用户帮助其构造匿名区；同样地，如果发现匿名区协同构造博弈 G_{ACR}^q 中的协作用户 P_i 提供虚假位置，那么该协作用户在之后的 m 次服务查询中也不会有其他用户帮助其构造匿名区.

在本文提出的方案中，将利用区块链分布式存储参与匿名区构造的博弈双方以及协作用户提供的位置信息作为证据. 因此，为了激励网络中所有用户参与到区块链的维护中，本文还提出了一个区块链记账权竞争机制.

定义 4(共识机制 II——记账权竞争机制). 记账权竞争机制 $M_C=(\tilde{\lambda},\tilde{p})$ 是一个二元组. 其中：

• $\tilde{\lambda}=(\lambda_{\tilde{1}},\lambda_{\tilde{2}},\cdots,\lambda_{\tilde{n}})$ 是在竞争生成新区块 $block_M$ 时，参与竞争获取记账权的用户 $P_{\tilde{1}},P_{\tilde{2}},\cdots,P_{\tilde{n}}$ 历史上帮助其他用户构造匿名区的次数 $\lambda_{\tilde{1}},\lambda_{\tilde{2}},\cdots,\lambda_{\tilde{n}}$ 所形成的历史协同构造次数集合. $\lambda_{\tilde{i}}$ 是参与新区块生成记账权的第 $\tilde{i}$ 个用户 $P_{\tilde{i}}$ 历史帮助其他用户构造匿名区的次数.

• $\tilde{p}=\{\tilde{p}_{\tilde{1}},\tilde{p}_{\tilde{2}},\cdots,\tilde{p}_{\tilde{n}}\}$ 是记账权竞争机制 M_C 根据参与新区块生成记账权竞争的用户 $P_{\tilde{1}},P_{\tilde{2}},\cdots,P_{\tilde{n}}$ 历史上帮助其他用户构造匿名区构造的次数，给予他们在生成新区块时的收益. 对于任意 $\tilde{p}_{\tilde{i}}\in\tilde{p}$，其满足：

$$\tilde{p}_{\tilde{i}}=\begin{cases}0, & \text{其他}\\ \lambda_{\tilde{i}}+1, & \lambda_{\tilde{i}}=\arg\max\{\lambda_{\tilde{i}'}\bmod\lambda_{\max}^{M-1}\}\end{cases}\tag{6}$$

其中，$\lambda_{\max}^{M-1}$ 表示获得生成区块 $block_{M-1}$ 记账权的用户在当时曾帮助其他用户构造匿名区的历史次数；$\tilde{i}'\in[\tilde{1},\tilde{2},\cdots,\tilde{n}]$.

简单来说，本文提出的生成新区块记账权竞争机制 M_C 的基本思想是让参与匿名区构造次数最多的用户获取记账权. 但是，为了防止参与匿名区构造次数最多的用户始终获取记账权限，从而有机会伪造分布式匿名区协作构造区块链情况的发生，本文利用 $\lambda_{\tilde{i}}=\arg\max\{\lambda_{\tilde{i}'}\bmod\lambda_{\max}^{M-1}\}$ 使得区块链的记账权分散给网络中的各个用户. 此外，为了激励网络中所有用户来参与区块链的更新，本文将获得生成新区块的记账权视为参与匿名区构造的一种特殊方式. 显然，对于网络中任意用户 $P_{\tilde{i}}$ 来说，其帮助其他用户构造匿名区的历史次数 $\lambda_{\tilde{i}}$ 越大，那么 $P_{\tilde{i}}$ 作为请求者发送匿名区协同构造请求时就会有越多的用户提供自己的位置信息给他，使其能成功构造出匿名区的概率就越大. 这也能在一定程度上预防用户在区块链系统中频繁地使用新 cID.

值得注意的是，在本文提出的记账权竞争机制中，网络中的任何用户，即包括发送匿名区协同构造请求的请求用户、提供位置信息的协同用户以及收到匿名区协同构造请求未提供位置信息的其他用户均能参与到生成新区块记账权的竞争中.

4.2　本文方案

本文将请求用户获取协作用户真实位置的过程视为一类特殊的交易(Transaction)，在交易账单中记录交易双方的 ID 以及协作用户提供的位置信息，并将此账单存储至公有链中. 当请求用户指认协作用户提供虚假位置或者协作用户指认请求用户泄露自己位置时，可将该交易账单作为凭证用于仲裁. 一旦证实出现位置泄露或欺骗行为，那么具有上述行为的用户在作为请求者时将不会有其他用户给其提供帮助，使其不能成功地构造匿名区. 此外，为了激励网络中用户参与到区块链的维护中，每次生成区块的用户均会被视为帮助请求用户构造匿名区. 具体方案如下所示.

Step1.　请求用户 P_0 向协作用户发送匿名区构造协作请求

$$Req=\{T_{0-i},cID_0,\lambda_0,N(Tran_{l_1}),N(Tran_{l_2}),\cdots,N(Tran_{l_{\lambda_0}}),sign_{SK-cID_0}(\lambda_0\parallel T_{0-i})\}\tag{7}$$

其中，T_{0-i} 表示请求用户 P_0 发送匿名区构造协作请求时的时间戳；cID_0 是请求用户 P_0 在区块链系统中使用的假名；λ_0 表示请求用户作为协作者时曾参与匿名区构造的次数；$N(Tran_{l_k})$ 表示存储请求用户 P_0 协作其他用户构造匿名区的交易账单 $Tran_{l_k}$ 的交易账单号；$1\le k\le\lambda_0$；$SK-cID_0$ 是请求用户 P_0 在区块链系统中的私钥；$sign_{SK-cID_0}(\lambda_0\parallel T_{0-i})$ 表示利用

私钥 $SK-cID_0$ 对 $\lambda_0 \| T_{0-i}$ 的签名；“‖”是连接符.

Step2. 协作用户 $P_i(i\neq 0)$ 在收到请求用户发送的匿名区构造请求后，首先去分布式匿名区协作构造区块链 $Bloakchain=\{Block_1, Block_2, \cdots, Block_{M-1}\}$ 中统计请求用户 P_0 曾参与匿名区构造的次数 λ_0'，并在该区块链中查找是否存在记录请求用户 P_0 欺骗行为的惩罚交易账单.

• 当 $\lambda_0'=\lambda_0$ 且未找到记录当前请求用户 P_0 欺骗行为的惩罚交易账单时，协作用户 P_i 根据阈值 δ_i 决定是否发送自己的真实位置 Loc_i^{real} 给请求用户.

1）若 $\lambda_0<\delta_i$，则协作用户 P_i 不响应请求用户 P_0 的协作请求；

2）若 $\lambda_0\geq\delta_i$，则协作用户 P_i 将交易账单

$$Tran=\{T_{i-0}, cID_0, Enc_{PK-cID_0}(Loc_i^{real}\| T_{i-0}), sign_{SK-cID_i}(Enc_{PK-cID_0}(Loc_i^{real}\| T_{i-0}))\} \quad (8)$$

发送给请求用户 P_0.

• 当 $\lambda_0'=\lambda_0$，但在区块 $Block_{l'}$ 中找到记录当前请求用户 P_0 欺骗行为的惩罚交易账单时，协作用户 P_i 根据当前区块数量判断请求用户 P_0 是否仍在惩罚期内.

1）若 $M-1-l'\leq m$，即请求用户 P_0 仍在惩罚周期内，则协作用户 P_i 不响应请求用户 P_0 的协作请求，并广播惩罚交易账单

$$Tran_{Pun}=\{T_{i-0}, cID_0, cID_i, Punishment, sign_{SK-cID_i}(Punishment\| T_{i-0})\} \quad (9)$$

2）若 $M-1-l'>m$，即请求用户 P_0 已被惩罚完毕，则协作用户 P_i 将交易账单 $Tran$ 发送给请求用户 P_0.

• 当 $\lambda_0'\neq\lambda_0$ 时，协作用户 P_i 不响应请求用户 P_0 的协作请求，且广播惩罚交易账单

$$Tran_{\text{Pun}}=\{T_{i-0}, cID_0, cID_i, Punishment, sign_{SK-cID_i}(Punishment\| T_{i-0}), T_{0-i}, \lambda_0, sign_{SK-cID_0}(\lambda_0\| T_{0-i})\} \quad (10)$$

其中，M 表示请求用户 P_0 发送协作请求时分布式匿名区协作构造区块链中区块的数量；l' 表示记录请求用户 P_0 欺骗行为的区块序号，满足：$1\leq l'\leq M-1$；T_{i-0} 表示生成交易账单的时间戳；m 是惩罚阈值；$PK-cID_0$ 是请求用户 P_0 在区块链系统中的公钥；$SK-cID_i$ 是协作用户 P_i 在区块链系统中的私钥；$Punishment$ 是惩罚交易账单标识符；$Enc_{PK-cID_0}(Loc_i^{\text{real}}\| T_{i-0})$ 表示在区块链系统中使用请求用户 P_0 的公钥 $PK-cID_0$ 加密 $Loc_i^{\text{real}}\| T_{i-0}$ 后得到的密文.

Step3. 请求用户 P_0 在收到协作用户 P_i 发送的交易账单 $Tran$ 后，使用协作用户 P_i 在区块链系统中的公钥 $PK-cID_i$ 验证签名信息

$$sign_{SK-cID_i}(Enc_{PK-cID_0}(Loc_i^{\text{real}}\| T_{i-0})) \quad (11)$$

的正确性.

• 若验证通过，则利用自己的私钥 $SK-cID_0$ 解密 $Enc_{PK-cID_0}(Loc_i^{\text{real}}\| T_{i-0})$ 得到协作用户 P_i 的真实位置 Loc_i^{real}. 然后，计算 $Enc_{PK-cID_i}(Loc_i^{\text{real}}\| T_{i-0})$ 和 $sign_{SK-cID_0}(Enc_{PK-cID_i}(Loc_i^{\text{real}}\| T_{i-0}))$，并将其写入交易账单 $Tran$ 后进行广播.

• 若验证不通过，则不使用 Loc_i^{real} 构造匿名区 ACR，且广播发送惩罚交易账单

$$Tran_{\text{Pun}}=\{T_{i-0}, cID_0, cID_i, Punishment, sign_{SK-cID_0}(punishment\| T_{i-0}), Enc_{PK-cID_0}(Loc_i^{\text{real}}\| T_{i-0}), sign_{SK-cID_i}(Enc_{PK-cID_0}(Loc_i^{\text{real}}\| T_{i-0}))\} \quad (12)$$

当请求用户得到不少于 $K-1$ 个协作用户提供的真实位置后就可成功地构造出匿名区.

Step4. 网络中所有用户在收到广播发送的交易账单后分别验证其真实性. 若验证不通过，则分别生成新的惩罚交易账单并进行广播. 若验证通过，则保存交易账单用于生成新的区块 $Block_M$. 当要更新分布式匿名区协作构造区块链时，若

$$\lambda_j^M=\arg\max\{\lambda_{l'} \bmod \lambda_{\max}^{M-1}\} \quad (13)$$

则由用户 P_j 获得记账权，将生成新的区块 $Block_M$ 加入分布式匿名区协作构造区块链.

在上述方案中，用户的 cID 将作为索引，用于在区块链系统中检索包含该 cID 的所有历史交易账单，使得网络中每个用户均能追溯请求用户和协作用户的历史行为. 并且，当请求用户使用上述方案保护自己 LBS 查询时的位置隐私时，还可能出现以下三种情况：

（1）当请求用户在同一位置进行多次 LBS 查询时，用户无需广播发送构造匿名区协作请求. 其只需通过查找存储在区块链中的交易账单即可快速获得历史查询时协作用户提供的真实位置，从而高效地构造出匿名区，提高服务质量.

（2）当请求用户连续地进行 LBS 查询时，用户也无需广播发送构造匿名区协作请求. 此时，其同样通过查询存储在区块链中的交易账单即可快速获得上次查询时协作的用户，从而直接向这些用户发送协作请求，快速构造匿名区，提高服务质量.

（3）当生成新的区块时，若存在多个用户 P_{j_1}，

$P_{j_2},\cdots,P_{j_n}$ 使得

$$\lambda_{j_1}^M=\lambda_{j_2}^M=\cdots=\lambda_{j_n}^M=\arg\max\{\lambda_{i'}\bmod\lambda_{\max}^{M-1}\} \tag{14}$$

成立，则由网络中用户通过投票决定本次区块链的记账权由 $P_{j_1},P_{j_2},\cdots,P_{j_n}$ 中的哪个用户获得. 并且，为了降低网络中用户查询时的开销，在实际应用中，还可在上述方案中引入滑动窗口机制，减少区块链中存储交易账单的区块数量.

此外，如果在实际使用本方案时，位置隐私数据更新的频繁程度远远高于公有链网络中的交易产生速度时(即公有链网络中的交易产生速度与位置隐私数据更新的频繁程度不在一个数量级)，则可采用诸如区域划分的方法(即某个区域内所有用户构成一个群体)的方法，利用联盟链技术对本方案进行优化.

4.3　方案分析

4.3.1　安全性

本文假定网络中至少存在 $K-1$ 个用户 $P_i(1\leq i\leq K-1)$ 的阈值 $\delta_i\leq\lambda_0$，即请求用户 P_0 能成功地构造出包含其他 $K-1$ 个协作用户提供位置的匿名区 ACR. 并且，还假设如果请求用户 P_0 在收到这 $K-1$ 个用户提供的真实位置 $Loc_1^{\text{real}},Loc_2^{\text{real}},\cdots,Loc_{K-1}^{\text{real}}$ 后，其采用的匿名区构造方法 $Area(\cdot)$ 是安全的，即式(15)

$$\Pr_{\text{LSP}}[Loc_0^{\text{real}}\mid Area(Loc_0^{\text{real}},Loc_1^{\text{real}},\cdots,Loc_{K-1}^{\text{real}})]\leq 1/K \tag{15}$$

成立. 因此，本文仅从匿名区构造的角度证明本方案是安全的.

引理 1. 令 α 表示协作用户 P_i 正确识别出请求用户 P_0 具有位置泄露行为的概率，β 表示请求用户 P_0 识别出协作用户提供虚假位置的概率. 当网络中存在 $K-1$ 个用户 $P_i(1\leq i\leq K-1)$ 的阈值 $\delta_i\leq\lambda_0$ 时，若 $m>\max\left\{\left\lceil\dfrac{\widetilde{U}^+-\widetilde{U}}{\alpha\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil,\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^+-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil\right\}$，那么，本方案不仅能防止请求用户 P_0 泄露协作用户 $P_i(1\leq i\leq K-1)$ 的位置信息，还能确保协作用户 P_i 参与分布式匿名区构造时提供的是真实位置 Loc_i^{real}.

证明.　反证法.

假设当理性用户 P_i 的阈值 $\delta_i\geq\lambda_0$ 且 $m>\max\left\{\left\lceil\dfrac{\widetilde{U}^+-\widetilde{U}}{\alpha\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil,\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^+-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil\right\}$ 时，请求用户 P_0 在任意第 q 次匿名区协同构造博弈中，当收到理性用户 P_i 提供真实位置 $Loc_i^{q\text{-real}}$ 后将该位置泄露给第三方，即选择策略 $a_0^{q\text{-}(2)}$. 此时，对于请求用户 P_0 来说，他在博弈 G_{ACR}^q 中的收益为：

$$u_0(a_0^{q\text{-}(2)})=\widetilde{U}^+ \tag{16}$$

当理性协作用户 P_i 在任意时刻证实了 P_0 曾泄露自己的真实位置 $Loc_i^{q\text{-real}}$ 时，P_0 仍作为请求者在该时刻之后的 $a_i^{(2)}$ 次匿名区协同构造博弈 $G_{\text{ACR}}^{\tilde{q}},G_{\text{ACR}}^{\tilde{q}+1},\cdots,G_{\text{ACR}}^{\tilde{q}+m}$ 中的收益满足：

$$u_0^{\tilde{q}+j}(a_0^{\tilde{q}+j}\mid a_0^{q\text{-}(2)})=\widetilde{U}^- \tag{17}$$

其中，$1\leq j\leq m$.

因此，理性用户 P_0 选择策略 $a_0^{q\text{-}(2)}$ 在 $m+1$ 次博弈 $G_{\text{ACR}}^q,G_{\text{ACR}}^{\tilde{q}},G_{\text{ACR}}^{\tilde{q}+1},\cdots,G_{\text{ACR}}^{\tilde{q}+m}$ 的总体收益为：

$$\begin{aligned}\tilde{u}_0(a_0^{q\text{-}(2)})=&\alpha\cdot u_0(a_0^{q\text{-}(2)})+(1-\alpha)\cdot[u_0(a_0^{\tilde{q}}\mid a_0^{q\text{-}(2)})+\\&u_0(a_0^{\tilde{q}+1}\mid a_0^{q\text{-}(2)})+\cdots+u_0(a_0^{\tilde{q}+m}\mid a_0^{q\text{-}(2)})]\\=&\widetilde{U}^++m\widetilde{U}+\alpha\cdot m\cdot(\widetilde{U}^{--}-\widetilde{U})\end{aligned} \tag{18}$$

然而，若请求用户 P_0 在第 $a_i^{q\text{-}(1)}$ 次匿名区协同构造博弈中，在收到真实位置 $G_{\text{ACR}}^{\tilde{q}},G_{\text{ACR}}^{\tilde{q}+1},\cdots,G_{\text{ACR}}^{\tilde{q}+m}$ 后不将该位置泄露给第三方，即选择策略 $a_0^{q\text{-}(1)}$ 时，其在匿名区协同构造博弈 G_{ACR}^q 和 $G_{\text{ACR}}^{\tilde{q}},G_{\text{ACR}}^{\tilde{q}+1},\cdots,G_{\text{ACR}}^{\tilde{q}+m}$ 中的总体收益为：

$$\begin{aligned}\tilde{u}_0(a_0^{q\text{-}(1)})=&u_0(a_0^{q\text{-}(1)})+u_0(a_0^{\tilde{q}}\mid a_0^{q\text{-}(1)})+\\&u_0(a_0^{\tilde{q}+1}\mid a_0^{q\text{-}(1)})+\cdots+u_0(a_0^{\tilde{q}+m}\mid a_0^{q\text{-}(1)})\\=&\widetilde{U}+m\widetilde{U}\end{aligned} \tag{19}$$

根据假设可知：当且仅当 $\tilde{u}_0(a_0^{q\text{-}(1)})\leq\tilde{u}_0(a_0^{q\text{-}(2)})$ 时，请求用户 P_0 会泄露协作用户 P_i 提供的位置信息. 即

$$\widetilde{U}+m\widetilde{U}\leq\widetilde{U}^++m\widetilde{U}+\alpha\cdot m\cdot(\widetilde{U}^{--}-\widetilde{U}) \tag{20}$$

成立.

那么，$m\leq\dfrac{\alpha\cdot(\widetilde{U}^+-\widetilde{U})}{\widetilde{U}-\widetilde{U}^{--}}$，与已知 $m>\left\lceil\dfrac{\alpha\cdot(\widetilde{U}^+-\widetilde{U})}{\widetilde{U}-\widetilde{U}^{--}}\right\rceil$ 相矛盾. 故对于理性请求用户 P_0 来说，其不会泄露协作用户 P_i 的真实位置.

同理，假设在任意第 q 次匿名区协同构造博弈中，当 $m>\max\left\{\left\lceil\dfrac{\widetilde{U}^+-\widetilde{U}}{\alpha\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil,\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^+-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil\right\}$ 以及协作用户 $P_i(1\leq i\leq K-1)$ 决定帮助请求用户构造匿名区时，协作用户 P_i 提供虚假位置 $Loc_i^{q\text{-fake}}$，即选择策略 $a_i^{q\text{-}(3)}$. 此时，对于理性协作用户 P_i 来说，其提供虚假位置 $Loc_i^{q\text{-fake}}$ 被请求用户 P_0 正确识别的概率 β. 因此，协作用户在当前博弈 G_{ACR}^q 以及在被证实提供虚假位置之后作为请求者参与的 $a_i^{(2)}$ 次匿名区协同构造博弈 $G_{\text{ACR}}^{\tilde{q}},G_{\text{ACR}}^{\tilde{q}+1},\cdots,G_{\text{ACR}}^{\tilde{q}+m}$ 中的总体收益为

$$\tilde{u}_i(a_i^{q_-(3)})=\beta\cdot u_i(a_i^{q_-(3)})+(1-\beta)\cdot[u_{i\to 0}(a_0^{\tilde{q}}\mid a_i^{q_-(3)})+u_{i\to 0}(a_0^{\tilde{q}+1}\mid a_i^{q_-(3)})+\cdots+u_{i\to 0}(a_0^{\tilde{q}+m}\mid a_i^{q_-(3)})]$$
$$=(1-\beta)\cdot\widetilde{W}^{+}+\beta\cdot\widetilde{W}^{f}+\beta\cdot m\cdot(\widetilde{U}^{--}-\widetilde{U}) \tag{21}$$

其中，$u_{i\to 0}(\cdot)$表示匿名区协同构造博弈G_{ACR}^{q}中的协作用户P_0在之后的协同构造博弈中作为请求者时的收益函数.

而当协作用户P_i决定帮助请求用户构造匿名区且其提供真实位置Loc_i^{real}，即选择策略$a_i^{q_-(1)}$时，在博弈G_{ACR}^{q}和$G_{\mathrm{ACR}}^{\tilde{q}}$，$G_{\mathrm{ACR}}^{\tilde{q}+1}$，…，$G_{\mathrm{ACR}}^{\tilde{q}+m}$中的总体收益为

$$\tilde{u}_i(a_i^{q_-(1)})=u_i(a_i^{q_-(1)})+u_{i\to 0}(a_0^{\tilde{q}})+u_{i\to 0}(a_0^{\tilde{q}+1})+\cdots+u_{i\to 0}(a_0^{\tilde{q}+m})$$
$$=\widetilde{W}+m\widetilde{U} \tag{22}$$

根据假设可知：当且仅当$\tilde{u}_i(a_i^{q_-(1)})\leq\tilde{u}_i(a_i^{q_-(3)})$时，协作用户$P_i$会提供虚假位置给请求用户. 即下式

$$\widetilde{W}+m\widetilde{U}\leq(1-\beta)\cdot\widetilde{W}^{+}+\beta\cdot\widetilde{W}^{f}+\beta\cdot m\cdot(\widetilde{U}^{--}-\widetilde{U})$$

成立. 那么，$m<\dfrac{(1-\beta)\cdot(\widetilde{W}^{+}-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}$与已知$m>\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^{+}-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil$相矛盾. 故当协作用户决定帮助请求用户构造匿名区时，其会提供真实的位置.

证毕.

同理可得如下引理.

引理 2. 令α表示协作用户正确识别出请求用户P_0具有位置泄露行为的概率，β表示请求用户P_0识别出协作用户提供虚假位置的概率. 对于网络中的任意理性用户P_i来说，当$\delta_i\leq\lambda_0$且$m>\max\left\{\left\lceil\dfrac{\widetilde{U}^{+}-\widetilde{U}}{\alpha\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil,\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^{+}-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil\right\}$时，本方案能激励该用户$P_i$参与到分布式匿名区的构造中.

由引理 1 和引理 2 可总结出：

定理 1. 令α表示协作用户正确识别出请求用户P_0具有位置泄露行为的概率，β表示请求用户P_0识别出协作用户提供虚假位置的概率. 假设理性请求用户P_0采用本方案保护其 LBS 查询时的位置隐私且在网络中存在$K-1$个其他理性用户$P_i(1\leq i\leq K-1)$的阈值$\delta_i\leq\lambda_0$. 其中λ_0表示理性请求用户P_0历史上帮助其他用户构造匿名区的次数. 如果$m>\max\left\{\left\lceil\dfrac{\widetilde{U}^{+}-\widetilde{U}}{\alpha\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil,\left\lceil\dfrac{(1-\beta)\cdot(\widetilde{W}^{+}-\widetilde{W})}{\beta\cdot(\widetilde{U}-\widetilde{U}^{--})}\right\rceil\right\}$，本方案是安全的. 即本方案在促使协作用户$P_i(1\leq i\leq K-1)$提供自己的真实位置给请求用户$P_0$，并可防止请求用户$P_0$泄露这些位置的同时，还使得 LSP 从请求用户$P_0$提交的匿名区中识别其真实位置的正确率不高于$1/K$.

4.3.2 计算复杂性

本方案涉及加密、解密以及签名运算. 本文将签名运算视为一类特殊的加密运算. 并且由于解密运算是加密运算的逆运算，因此本文用$O(Enc)$表示进行加密、解密和签名运算时所需的计算复杂度.

在本方案中，当每个协作用户P_i收到请求用户P_0发送的匿名区构造协作请求后，其首先根据请求用户P_0的公钥$PK-cID_0$进行计算，验证签名数据$sign_{SK-cID_0}(\lambda_0\parallel T_{0-i})$的正确性，此时其所需的计算复杂度为$O(Enc)$. 若未通过正确性验证，则协作用户$P_i$计算$sign_{SK-cID_i}(Punishment\parallel T_{i-0})$，并广播惩罚交易账单. 此时其所需的计算复杂度为$O(Enc)$. 若通过正确性验证，协作用户$P_i$会通过查询区块链$Blockchain=\{Block_1,Block_2,\cdots,Block_{M-1}\}$中存储的交易账单，确定请求用户$P_0$帮助其他用户构造匿名区的次数$\lambda_0$的真实性，并在该区块链中查找是否存在记录$P_0$欺骗行为的惩罚交易账单. 当发现请求用户$P_0$发送虚假的$\lambda_0$或其仍在惩罚期内，则计算$sign_{SK-cID_i}(Punishment\parallel T_{i-0})$后广播惩罚交易账单. 此时，$P_i$的计算复杂度为$O(M)+O(Enc)=O(Enc)$. 当通过$\lambda_0$的正确性验证且未找到记录请求用户$P_0$欺骗行为的惩罚交易账单，那么协作用户$P_i$根据其阈值$\delta_i$决定是否提供自己的位置给请求用户$P_0$. 若$\lambda_0<\delta_i$，则不响应请求用户发送的匿名区构造协作请求，此时其所需的计算开销为$O(1)$；若$\lambda_0\geq\delta_i$，则在计算$Enc_{PK-cID_0}(Loc_i^{real}\parallel T_{i-0})$以及相应的签名$sign_{SK-cID_i}(Enc_{PK-cID_0}(Loc_i^{real}\parallel T_{i-0}))$后，将交易账单发送给请求用户$P_0$. 此时协作用户$P_i$所需的计算复杂度为$O(1)+O(Enc)+O(Enc)=O(Enc)$. 因此，当收到匿名构造协作请求后，协作用户$P_i$所需的计算复杂度上限为

$$O(Enc)+O(Enc)+O(Enc)=O(Enc) \tag{25}$$

同理可得，当收到协作用户P_i发送的交易账单后，请求用户所需的计算复杂度为$O(Enc)$；当生成新区块$Block_M$时，网络中参与新区块生成的用户所需的计算复杂度为$O(Enc)$.

综上所述，若请求用户采用本方案成功获取$r\geq K-1$个协作用户提供的真实位置时，网络中各用户的计算复杂度分别为

(1) 对于请求用户来说，其所需的计算复杂

度为

$$r \cdot O(Enc) + O(Enc) = O(Enc) \quad (26)$$

(2) 对于提供自己真实位置协作请求用户构造匿名区的用户来说，其所需的计算复杂度为

$$O(Enc) + O(Enc) + O(Enc) = O(Enc) \quad (27)$$

(3) 对于未响应匿名区协作构造请求的用户来说，其所需的计算复杂度为

$$O(Enc) + O(1) + O(Enc) = O(Enc) \quad (28)$$

4.3.3　方案对比

(1) 可保护位于人群稀疏区中用户的位置隐私

现有的分布式 K 匿名位置隐私保护方案[20-24, 33-37]是通过增加网络中点对点通信跳数的方法来确保请求用户能至少获取其他 $K-1$ 个协作用户的真实位置来构造匿名区，保护自己的位置隐私. 当请求用户位于人群稀疏区时，若直接使用这些方案势必会增加其通信时延，从而降低服务质量；甚至还会出现请求用户未能获取至少 $K-1$ 个协作用户的真实位置，难以成功构造匿名区的极端情形. 虽然方案[25-32]提出通过存储历史协作用户的真实位置或利用社交网络实现匿名区构造的方法，但是上述方案却存在以下要求：1) 请求用户拥有足够的存储空间用于存储大量历史协作用户的真实位置[25-27,30]；2) 依赖第三方的存在[28-29]；3) 当进行 LBS 查询时，其可通过社交网络找到至少 $K-1$ 个可信用户[31-32]. 显然，这些额外要求也限制了这些方案的实用性.

然而，在本方案中，当请求用户位于人群稀疏区进行 LBS 查询时，他无需通过点对点通信的方式获取至少 $K-1$ 个协作用户的真实位置，仅需通过查询分布式匿名区协作构造区块链就可获取曾帮助自己构造匿名区的协作用户位置，从而即可成功地构造匿名区来保护本次查询时自己的位置隐私.

(2) 可保护连续请求下用户的位置隐私

现有的大多数分布式 K 匿名位置隐私保护方案[22-27,30-37]均不能有效抵抗查询追踪攻击[38]. 如果请求用户直接采用这些方案保护自己连续查询时的位置隐私，LSP 可通过查找请求用户提交的匿名区中不同用户的方法来降低请求用户的位置隐私保护等级，乃至能直接识别出请求用户的真实位置. 造成上述问题的根本原因是当请求用户进行连续 LBS 查询时，其难以获得相同协作用户提供的真实位置来构造匿名区.

然而，在本方案中，当用户连续进行 LBS 查询时，其可通过查询分布式匿名区协作构造区块链来获取连续查询最初时刻帮助其构造匿名区的用户. 随后，可通过再次向这些用户发送协作请求以获取自己后续连续查询时他们的真实位置，使得自己连续查询时提交给 LSP 的匿名区中始终包含 $K-1$ 个相同协作用户的真实位置，从而有效保护自己连续查询时的位置隐私.

综上所述，与现有分布式 K 匿名位置隐私保护方案的对比结果如表 1 所示.

表 1　方案对比

方案	安全性		实用性		
	匿名区构造	LBS 查询	稀疏区域	连续查询	第三方
[20-21]	×	√	×	√	×
[22-24]	×	√	×	×	×
[25-27,30-32]	×	√	√	×	×
[28-29]	×	×	√	√	√
[33-35]	×	√	×	×	√
[36-37]	×	√	×	×	×
本方案	√	√	√	√	×

5　实　验

本实验首先选用国家密码管理局推荐的 SM2 椭圆曲线公钥密码(Elliptic Curves Cryptography)算法对协作用户提供的位置信息进行加密和签名. 椭圆曲线公钥密码算法是目前最适用于移动终端的加密/签名算法之一. 与其他公钥密码算法相比，如 RSA 加密算法，它在减少用户端计算开销的同时，还能提供更高的安全级别. 例如，密钥长度为 256 bit 的 ECC 算法的安全强度等同于密钥长度为 3072 bit 的 RSA 算法的安全强度.

其次，本实验还采用 Ethereum 1.5.5 版本构建分布式匿名区协作构造区块链. Ethereum 是目前最常使用的一个开源的、模块化且有智能合约功能的区块链平台. 在搭建的区块链网络中，共有 25 个网络节点，其中 1 个节点作为请求用户 P_0 节点，其余 24 个作为协作用户 $P_1, P_2, \cdots, P_{24}$ 节点. 通过生成随机数的方式为请求用户 P_0 节点生成其作为协作者时曾参与匿名区构造的次数 λ_0 以及为协作用户节点生成阈值 $\delta_1, \delta_2, \cdots, \delta_{24}$，使得至少有 $K-1$ 个协作用户 $P_{i_1}, P_{i_2}, \cdots, P_{i_{K-1}}$ 的阈值 $\delta_{i_1}, \delta_{i_2}, \cdots, \delta_{i_{K-1}} \leq \lambda_0$. 即当发送匿名区构造协同请求后，请求用户 P_0 至少能获得 $K-1$ 个协作用户提供的位置信息来构造匿名区. 此外，在搭建的区块链网络平台中，采用本文提出的共识机制 II——记账权竞争机制来决定网络中哪个用户获得新区块的生成权. 并且，在搭建

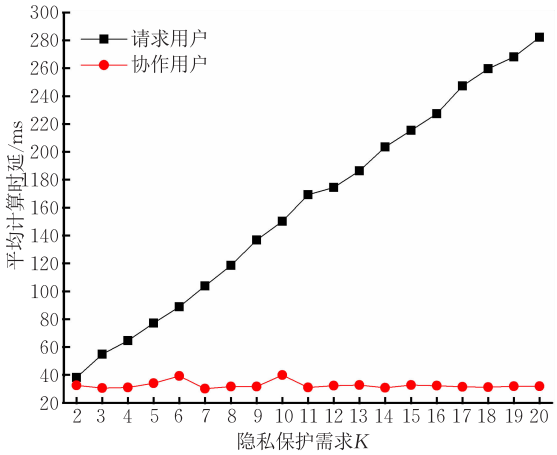
的区块链网络系统中，设定每个区块存储 100 个历史交易账单. 其中，每个交易账单用于记录匿名区协作构造过程中请求用户和协作用户关于协作用户提供的位置信息的密文和签名数据；设定当前区块链长度 $|Blockchain|=100$，即共存在 $100\times100=10\,000$ 个历史交易账单.

本实验设定请求用户的隐私保护需求 K 值从 2 变化到 20，针对不同的 K 值，重复执行 100 次所需算法. 所有的实验算法均采用 JAVA 编程语言实现，并使用了 JPBC 2.0 密码学库. 它是目前最常见的密码学库文件之一，其适用于 JAVA 编程环境，且预定义了大量的密码学计算运算，如有限域的生成、有限域上的加法和乘法运算等. 实验环境为 3.30 GHz Core i5-4590 CPU，4 GB DDR3-1600 RAM，操作系统为 Ubuntu 16.04 版本.

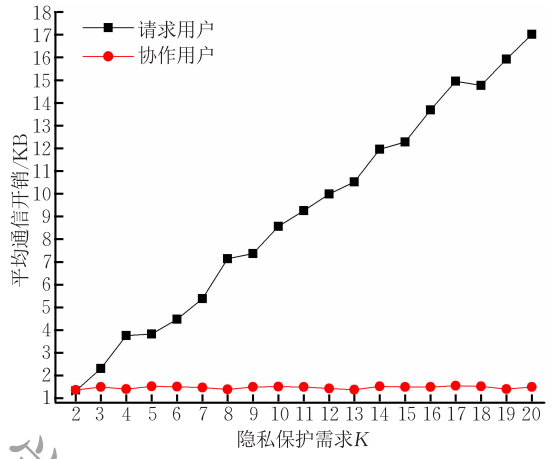
5.1 匿名区构造

在本部分实验中，假设请求用户曾提供自己的真实位置参与过 100 次匿名区的构造，即 $\lambda_0=100$. 当请求用户收到多于 $K-1$ 个协作用户提供的位置信息时，其任意选取 $K-1$ 个位置用于构造匿名区. 协作用户与请求用户在匿名区构造过程中所需的平均计算时延和通信开销分别如图 4 所示.

当请求用户采用本方案保护其 LBS 查询时的位置隐私时，随着隐私保护需求 K 的不断增加，其成功构造匿名区所需的平均计算时延呈递增趋势. 而对于协作用户来说，其所需的平均计算时延却与请求用户的隐私保护需求 K 值无关，如图 4(a)所示. 造成上述现象的原因是随着 K 值的不断增加，请求用户需要验证协作用户发送的签名数据的正确性以及解密获取协作用户真实位置的次数也不断增多. 然而，对于协作用户 $P_i(1\leq i\leq K-1)$ 来说，当收到请求用户 P_0 发送的匿名区构造协作请求且发现 $\delta_i\leq\lambda_0$ 后，其仅需发送利用请求用户公钥加密自己真实位置的密文以及该密文对应的签名数据给请求用户，所以请求用户所需的平均计算时延与 K 值无关. 此外，在匿名区构造过程中，请求用户所需的平均通信开销随着请求用户隐私保护需求 K 值的增大而增加. 其原因是随着 K 值的变大，请求用户需要接收更多协作用户提供的位置信息来构造匿名区，从而增大了请求用户的平均通信开销. 然而，对于协作用户来说，由于是采用点对点通信的方式提供自己的真实位置给请求用户，因此协作用户所需的平均通信开销并不随着请求用户隐私保护需求 K 值的变化而改变，如图 4(b)所示.



(a) 平均计算时延



(b) 平均通信开销

图 4 构造匿名区所需的平均计算时延和通信开销

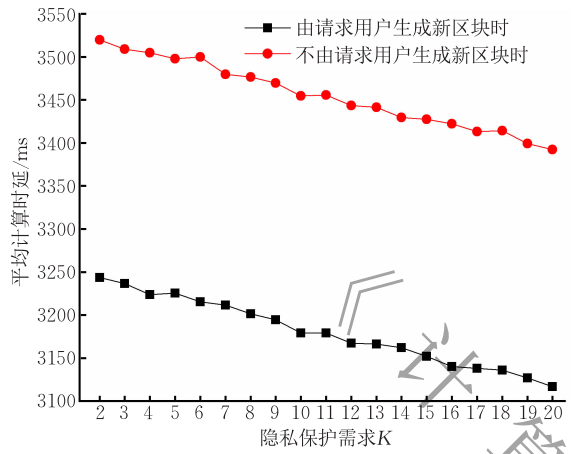
通过上述实验也可发现，当请求用户采用本方案成功生成匿名区时，请求用户端和协作用户端所需的计算时延和通信开销也极为有限. 例如，当 $K=20$ 时，请求用户的平均计算时延为 282.074 ms，其平均通信开销为 17.018 KB；而协作用户的平均计算时延为 31.776 ms，平均计算通信开销为 1.489 KB. 这就说明本方案具有较好的可用性，能高效地为请求用户生成匿名区.

5.2 区块链更新

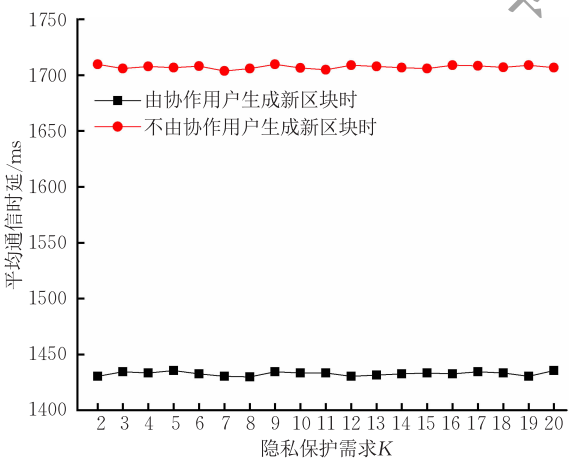
下面分析本方案中分布式匿名区协作构造区块链更新时用户所需的平均计算开销和存储开销. 在该部分实验中，设定生成新区块时包含的交易账单数量为 100.

在更新分布式匿名区协作构造区块链时，无论请求用户是否获得更新区块链的权限，其所需的计算时延随着自身隐私保护需求 K 值的增大而减少. 其原因是当 K 值增大时，请求用户在构造匿名区时已验证协作用户发送的关于其真实位置密文的签名数据的数量也随之增多，从而使其在更新区块链过

程中需要验证协作用户发送的关于其真实位置密文的签名数据的数量减少，如图 5(a)所示. 例如，当 K 值从 2 变化到 20 时，若请求用户未获得更新区块链的权限时，其在更新分布式匿名区协作构造区块链的过程中，所需的计算时延从 3528.703 ms 减少至 3374.681 ms；若请求用户获得更新区块链的权限时，其所需的计算时延也从 3242.084 ms 减少至 3125.916 ms.



(a) 请求用户所需平均计算时延



(b) 协作用户所需平均计算时延

图 5　区块链更新时请求用户和协作用户所需平均计算时延

对于协作用户来说，在更新分布式匿名区协作构造区块链时，无论请求用户是否获得更新区块链的权限，其均需要对请求用户广播发送的所有交易账单的正确性进行验证. 因此，其所需的计算时延并不受请求用户的隐私保护需求 K 值的影响，如图 5(b)所示. 并且，由于协作用户仅需验证每个交易账单中关于协作用户真实位置密文的签名数据的正确性，从而使其在更新分布式匿名区协作构造区块链过程中所需的计算时延远小于请求用户所需的计算时延. 例如，当协作用户未获得更新区块链的权限时，其在更新分布式匿名区协作构造区块链的过程中，所需的平均计算时延为 1733.583 ms；而当其获得更新区块链的权限时，所需的平均计算时延为 1439.428 ms.

5.3　交易账单数量对本方案的影响

这部分实验用于分析当前交易账单数量对区块链更新时所需的通信开销、生成新区块所需的计算时延以及新生成区块大小的影响. 设定生成新的区块时形成的交易账单数量从 100 变化至 1000.

在本方案中，存储至区块链中的交易账单最终是由请求用户进行全网广播的，这使得网络中的所有用户均能验证这些交易账单的正确性. 因此，请求用户在区块链更新过程中的通信开销随着交易账单数量的增加而增大，如图 6 所示. 并且，随着交易账单数量的增加，在生成分布式匿名区协作构造区块链的新区块时，需要存储的交易账单数量以及计算这些账单 Hash 值为叶子节点的 Merkle 树根节点所需的计算时延也随之增加. 这就导致生成新区块所需的计算时延以及生成的新区块大小随着交易账单数量的增加而增多，分别如图 7(a)和图 7(b)所示. 例如，当交易账单数量为 100 时，生成新区块所需的计算时延仅为 252.481 ms，生成的新区块大小为 998.333 KB；而当交易账单数量为 1000 时，生成新区块所需的计算时延为 7148.694 ms，生成的新区块的大小也增加至 9824.571 KB.

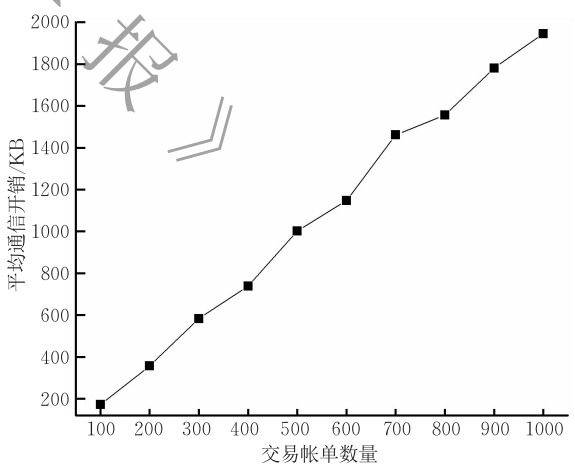
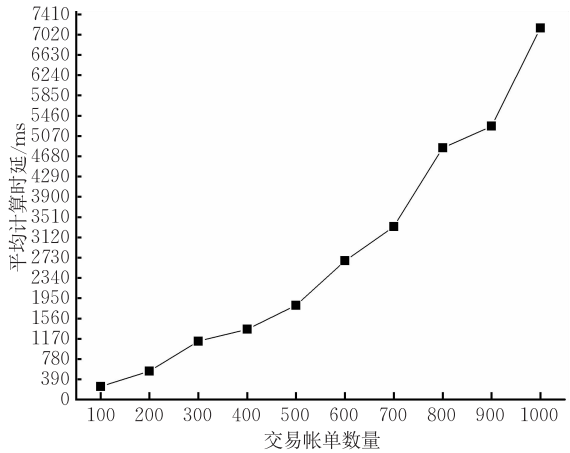
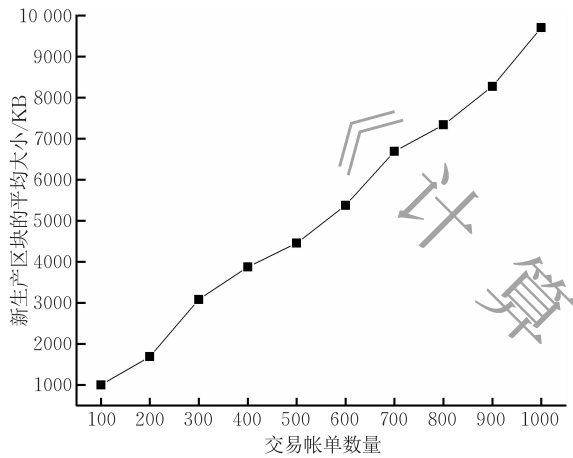


图 6　交易账单数量对区块链更新时请求用户所需平均通信开销的影响

通过上述分析可知，当生产新的区块时，随着交易账单数量的增加，网络中各用户的计算时延、通信开销和存储开销也会随之增加. 但是，对于请求用户来说，当其获得新区块的生成权时，他可先构造匿名区再进行新区块的生成. 从图 4(a)和图 4(b)可知，在使用本方案生成匿名区时，请求用户和协作用户

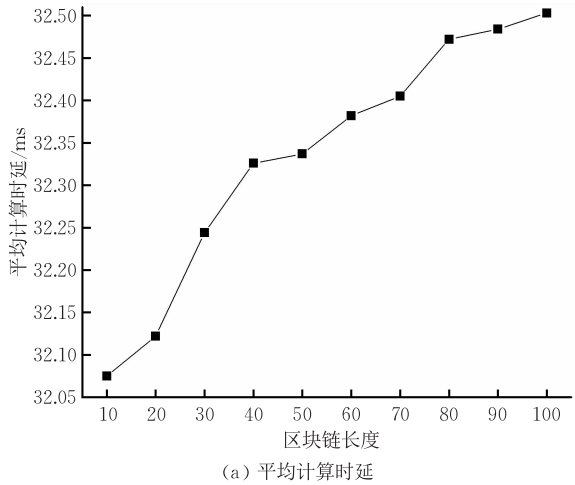


(a) 平均计算时延

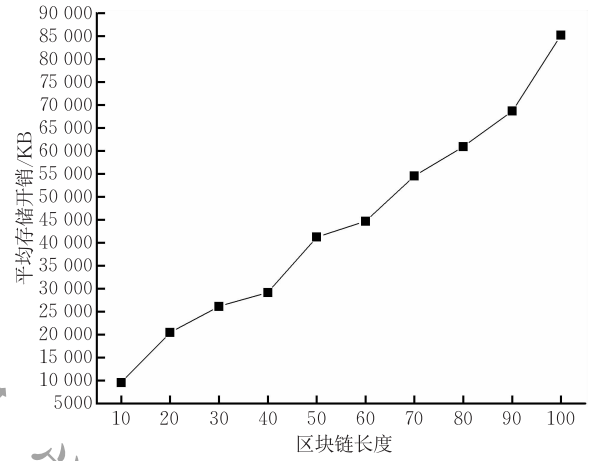


(b) 新生成区块的平均大小

图 7 交易账单数量对区块链更新时网络中用户的影响



(a) 平均计算时延



(b) 平均存储开销

图 8 区块链长度对协作用户的影响

所需的计算时延和通信开销均十分有限.这就说明本方案能高效地生成匿名区而且具有较好的实用性.

此外,在实际应用中,也可通过调整生成新区块的频率来减少用于生成新区块的交易账单数量,降低区块链更新时网络中各用户的计算时延、通信开销和存储开销,从而进一步提高本方案的可用性.

5.4 区块链长度对本方案的影响

本部分实验用于分析区块链长度(即区块链中区块的个数)对协作用户在匿名区构造过程中的存储开销和计算时延的影响,分别如图 8(a)和图 8(b)所示.

在该部分实验中,设定每个区块中均存储 100 个交易账单,区块链长度从 10 个区块增至 100 个区块.在本方案中,当收到请求用户发送的协作请求后,收到匿名区构造协作请求后,为了验证请求用户历史上是否存在位置隐私泄露或欺骗行为,协作用户需要下载并查询整个区块链中存储的交易账单.因此,随着分布式匿名区协作构造区块链长度的增加,协作用户在匿名区构造过程中所需的计算时延和存储开销也在不断增大.此外,由于协作用户查询整个区块链中存储的交易账单所需时间极为有限,因此当区块链长度增加时,在匿名区构造过程中协作用户所需的计算时延增长的极为缓慢.例如,当分布式匿名区协作构造区块链长度从 10 变化至 100 时,在匿名区构造过程中,协作用户所需的平均计算时延仅从 32.075 ms 增至 32.503 ms.

5.5 历史协作次数对本方案的影响

下面分析请求用户作为协作者参与匿名区构造的次数对其成功构造匿名区时所需通信开销的影响,如图 9 所示.

在本方案中,随着请求用户作为协作者参与匿名区构造的次数的增多,即 λ_0 的增大,请求用户需要提供的交易账单号的数量也随之增多,从而导致请求用户在匿名区构造过程中所需的通信开销也随之增大.此外,当收到匿名区构造协作请求后,为了验证请求用户历史上是否存在位置隐私泄露或欺骗行为,协作用户需要查询整个区块链中存储的交易账单.因此,请求用户作为协作者参与匿名区构造的

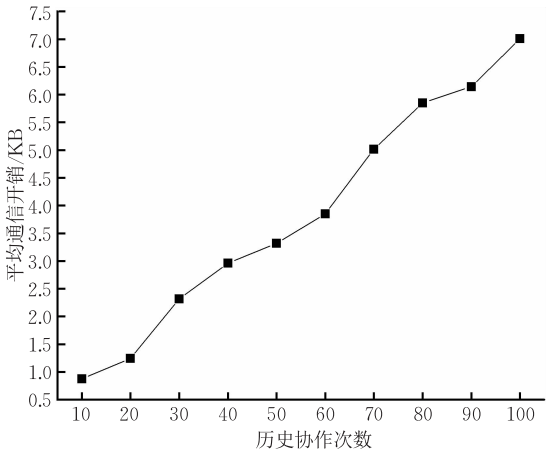


图 9　历史协作次数对请求用户所需通信开销的影响

次数并不影响协作用户在匿名区构造过程中的计算时延.

5.6　网络中用户数量对本方案的影响

下面简要分析网络中用户数量对使用本方案构造匿名区成功率的影响. 在该部分实验中,通过生成随机数的方式分别为请求用户生成其历史帮助其他用户构造匿名区的次数以及协作用户的判断阈值. 设定请求用户的隐私保护需求 $K=5,10,15$ 和 20,针对不同的 K 值分别重复执行 50 次实验,具体结果如图 10 所示.

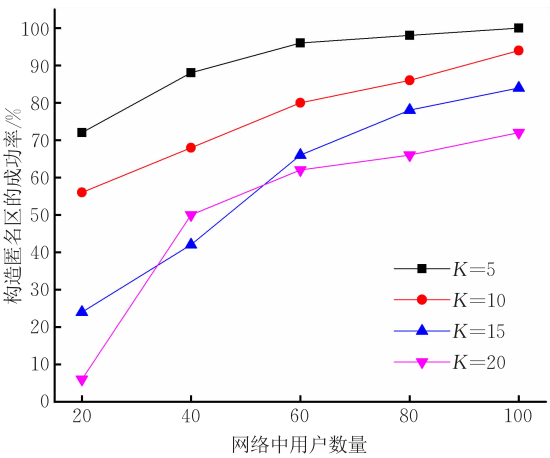


图 10　网络中用户数量对匿名区构造成功率的影响

实验表明,随着网络中用户数量的不断增加,网络中决定给请求用户提供帮助的协作用户数量也不断增多,即判断阈值 δ_i 满足 $\lambda_0 \geq \delta_i$ 的协作用户 P_i 的数量也不断变大,从而导致请求用户使用本方案构造匿名区的成功率也不断增大.

5.7　方案对比

最后,通过与现有分布式 K 匿名位置隐私保护方案[21,35]进行对比,说明本方案的实用性. 其中,方案[21]是经典的分布式 K 匿名位置隐私保护方案,它利用树形结构存储请求用户和协作用户的位置信息,从而避免请求用户位于构造出的匿名区域中心;而作为目前最好的一个分布式 K 匿名位置隐私保护方案,方案[35]通过设计信誉机制来促使协作用户参与匿名区构造,并引入半可信的第三方使得请求用户可对协作用户提供的信誉证书进行批验证,从而极大地降低了请求用户的计算时延.

如图 11 和图 12 所示,与方案[35]相比,本方案不仅在无需第三方参与且能有效防止匿名区构造过程中出现位置泄露和位置欺骗行为的同时,还降低了请求用户和协作用户的计算时延和通信开销. 此外,与方案[21]相比,本方案在未显著增加请求用户和协作用户计算时延和通信开销的同时,有效约束匿名区构造过程中请求用户和协作用户的行为. 这就说明本方案具有较好的实用性.

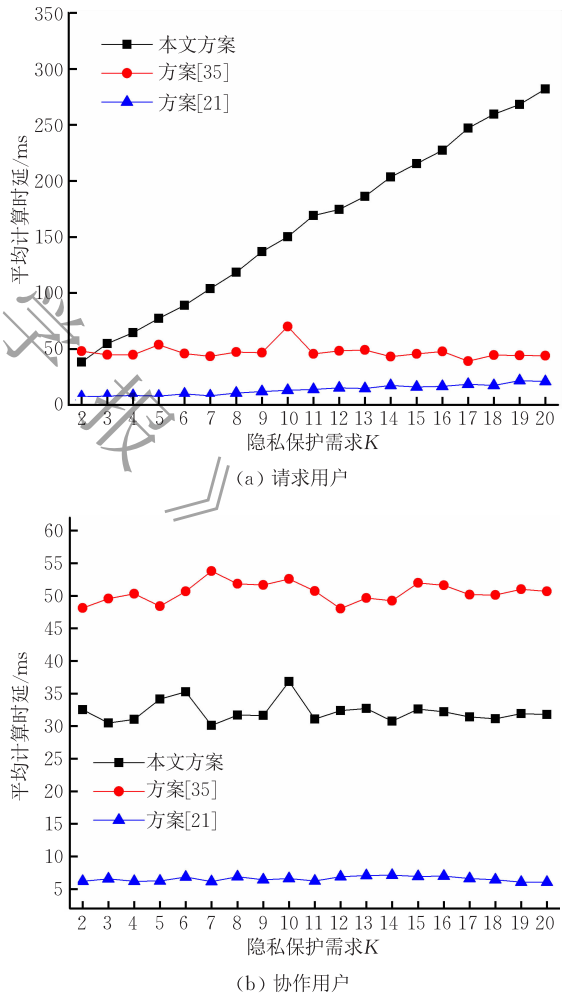
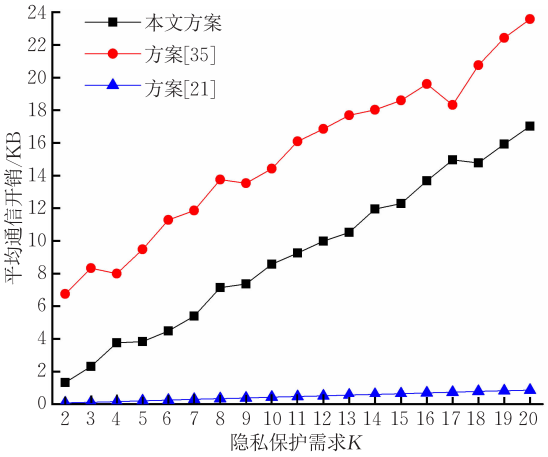
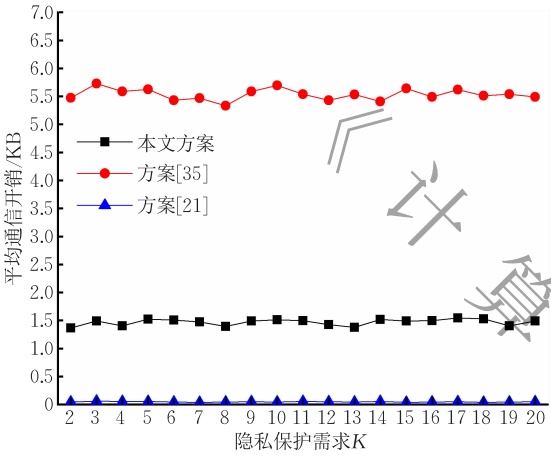


图 11　平均计算时延

综上所述,当请求用户采用本方案保护其 LBS 查询时的位置隐私时,他和网络中协作用户所需的计算时延、通信开销和存储开销都极为有限. 这就证明



(a) 请求用户



(b) 协作用户

图 12 平均通信开销

了本方案能高效地生成匿名区,具有较好的实用性.

6 总结与展望

现有分布式 K 匿名隐私保护方案并不能有效保护用户的位置隐私.造成这一问题的原因是这些方案并未考虑匿名区构造过程中的隐私泄露和欺骗行为,使得自利的请求用户在收到协作用户的真实位置后会将其泄露给第三方以获取额外收益;而自利的协作用户则会向请求用户提供虚假位置,导致构造出的匿名区不能满足请求用户的位置隐私保护需求.为了解决该问题,本文首先形式化描述分布式匿名区构造过程博弈,并通过分析请求用户和协作用户的策略选择和收益,给出分布式 K 匿名位置隐私保护的安全性定义.随后,利用区块链分布式存储参与博弈的请求用户和协作用户以及协作用户提供的位置信息作为证据,通过惩罚具有位置泄露和欺骗行为的用户在未来发送匿名区协同构造请求时不能成功地构造匿名区,来约束请求用户和协作用户的自利性行为.本文基于上述讨论提出了一个基于区块链的分布式 K 匿名位置隐私保护方案.安全性分析及实验表明本方案不仅能有效防止请求用户泄露协作用户的位置信息,还能促使协作用户提供真实的位置,从而高效地构造出匿名区.此外,本方案不仅能保护人群稀疏场景中请求用户的位置隐私,还能保护其连续查询时的位置隐私.

在分布式 K 匿名位置隐私保护方法中,请求用户的位置隐私保护需求与所享受的服务质量是相互矛盾的.为了兼顾用户对这两方面的需求,在未来的工作中,作者将分析影响请求用户位置隐私保护和所享受的服务质量的因素,在博弈论指导下,建立两者之间的博弈模型,指导分布式 K 匿名位置隐私保护方案的设计,使得所提方案能够兼顾位置隐私保护和服务质量.此外,在分布式匿名区构造过程中,准确地度量请求用户和协作用户的信誉值,不仅能协助请求用户选择可信的协作用户提供的位置信息来构造匿名区,还能帮助协作用户确定是否参与匿名区构造.因此,未来的另一个工作是利用可信计算的方法与理论,设计适用于分布式匿名区构造的信任评估模型.

参 考 文 献

[1] Krumm J. A survey of computational location privacy. Personal and Ubiquitous Computing, 2009, 13(6): 391-399

[2] Damiani M L. Location privacy models in mobile applications: Conceptual view and research directions. GeoInformatica, 2014, 18(4): 819-842

[3] Zhu H, Lu R, Huang C, et al. An efficient privacy-preserving location-based services query scheme in outsourced cloud. IEEE Transactions on Vehicular Technology, 2016, 65(9): 7729-7739

[4] Wang X, Mu Y, Chen R. One-round privacy-preserving meeting location determination for smartphone applications. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1712-1721

[5] Yu R, Kang J, Huang X, et al. MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. IEEE Transactions on Dependable Secure Computing, 2016, 13(1): 93-105

[6] Wang X, Pande A, Zhu J, et al. STAMP: Enabling privacy-preserving location proofs for mobile users. IEEE/ACM Transactions on Networking, 2016, 24(6): 3276-3289

[7] Olteanu A M, Huguenin K, Shokri R, et al. Quantifying interdependent privacy risks with location data. IEEE Transactions on Mobile Computing, 2017, 16(3): 829-842

[8] De Montjoye Y A, Hidalgo C A, Verleysen M, et al. Unique in the crowd: the privacy bounds of human mobility. Scientific Reports, 2013, 3(6), Article No. 1376

[9] De Montjoye Y A, Radaelli L, Singh V K, et al. Unique in the shopping mall: on the identifiability of credit card metadata. Science, 2015, 347(6221): 536-539

[10] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking//Proceedings of the 1st International Conference on Mobile System, Applications, and Services (MobiSys 2003). San Francisco, USA, 2003: 1-12

[11] Liu X, Liu K, Guo L, et al. A game-theoretic approach for achieving K-anonymity in location based services//Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013). Turin, Italy, 2013: 2985-2993

[12] Xiao Y, Xiong L. Protecting locations with differential privacy under temporal correlations//Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2015). Denver, USA, 2015: 1298-1309

[13] Wu Y C, Chen H, Zhao S Y, et al. Differentially private trajectory protection based on spatial and temporal correlation. Chinese Journal of Computers, 2018, 41(2): 309-322 (in Chinese)
(吴云乘，陈红，赵素云等. 一种基于时空相关性的差分隐私轨迹保护机制. 计算机学报，2018，41(2)：309-322)

[14] Duckham M, Kulik L. A formal model of obfuscation and negotiation for location privacy//Proceedings of the 3rd International Conference on Pervasive Computing (Pervasive 2005). Munich, Germany, 2005: 152-170

[15] Li M, Salinas S, Thapa A, et al. n-CD: A geometric approach to preserving location privacy in location-based services//Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013). Turin, Italy, 2013: 3012-3020

[16] Mascetti S, Freni D, Bettini C, et al. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. VLDB Journal, 2011, 20(4): 541-566

[17] Schlegel R, Chow C Y, Huang Q, et al. User-defined privacy grid system for continuous location-based services. IEEE Transactions on Mobile Computing, 2015, 14(10): 2158-2172

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

[19] Vu K, Zheng R, Gao J. Efficient algorithm for k-anonymous location privacy in participatory sensing//Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM 2012). Orlando, USA, 2012: 2399-2407

[20] Chow C Y, Mokbel M F, Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service//Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems (GIS 2006). Arlington, USA, 2006: 171-178

[21] Ghinita G, Kalnis P, Skiadopoulos S. PRIVÉ: Anonymous location-based queries in distributed mobile systems//Proceedings of the 16th International Conference on World Wide Web (WWW 2007). Banff, Canada, 2007: 371-380

[22] Ghinita G, Kalnis P, Skiadopoulos S. MOBIHIDE: A mobilea peer-to-peer system for anonymous location-based queries//Proceedings of the 10th International Symposium on Spatial and Temporal Databases (SSTD 2007). Boston, USA, 2007: 221-238

[23] Chow C Y, Mokbel M F, Bao J, et al. Query-aware location anonymization for road networks. Geoinformatica, 2011, 15(3): 571-607

[24] Sun G, Liao D, Li H, et al. L2P2: A location-label based approach for privacy preserving in LBS. Future Generation Computer Systems, 2017, 74: 375-384

[25] Chow C Y, Mokbel M F, Liu X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. Geoinformatica, 2011, 15(2): 351-380

[26] Kim H I, Shin Y S, Chang J W. A grid-based cloaking scheme for continuous queries in distributed systems//Proceedings of the 11th International Conference on Computer and Information Technology (CIT 2011). Pafos, Cyprus, 2011: 75-82

[27] Peng T, Liu Q, Meng D, et al. Collaborative trajectory privacy preserving scheme in location-based services. Information Sciences, 2017, 387(C): 165-179

[28] Zhong G, Hengartner U. A distributed k-anonymity protocol for location privacy//Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2009). Galveston, USA, 2009: 1-10

[29] Takabi H J, Joshi B D, Karimi H A. A collaborative k-anonymity approach for location privacy in location-based services//Proceedings of the 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2009). Washington, USA, 2009: 1-9

[30] Che Y, Yang Q, Hong X. A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks//Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC 2012). Shanghai, China, 2012: 2098-2102

[31] Hwang R H, Huang F H. SocialCloaking: A distributed architecture for K-anonymity location privacy protection//Proceedings of the 2014 International Conference on Computing, Networking and Communications (ICNC 2014). Honolulu, USA, 2014: 247-251

[32] Hwang R H, Hsueh Y L, Wu J J, et al. SocialHide: A generic distributed framework for location privacy protection. Journal of Network and Computer Applications, 2016, 76: 87-100

[33] Yang D, Fang X, Xue G. Truthful incentive mechanisms for K-anonymity location privacy//Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013). Turin, Italy, 2013: 2994-3002

[34] Zhang Y, Tong W, Zhong S. On designing satisfaction-ratio-aware truthful incentive mechanisms for K-anonymity location privacy. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2528-2541

[35] Li X, Miao M, Liu H, et al. An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism. Soft Computing, 2017, 21(14): 3907-3917

[36] Chow C Y, Mokbel M F. Enabling private continuous queries for reveal user locations//Proceedings of the 10th International Symposium on Spatial and Temporal Databases (SSTD 2007). Boston, USA, 2007: 258-275

[37] Gong X, Chen X, Xing K, et al. Personalized location privacy in mobile networks: A social group utility approach//Proceedings of the 34th IEEE International Conference on Computer Communications (INFOCOM'15). Hong Kong, China, 2015: 1008-1016

[38] Gong X, Chen X, Xing K, et al. From social group utility maximization to personalized location privacy in mobile networks. IEEE/ACM Transactions on Networking, 2017, 25(3): 1703-1716

[39] Shao Q F, Jin C Q, Zhao Z, et al. Blockchain: Architecture and research progress. Chinese Journal of Computers, 2017, 40(1): 1-21(in Chinese)
(邵奇峰, 金澈清, 张召等. 区块链技术: 架构及进展. 计算机学报, 2017, 40(1): 1-21)

LIU Hai, Ph. D. His research interests include location privacy protection and security protocol design.

LI Xing-Hua, Ph. D., professor, Ph. D. supervisor. His research interests include network and information security, privacy protection and cryptography.

LUO Bin, Ph. D. candidate. Her research interests include location privacy protection and trust evaluation.

WANG Yun-Wei, Ph. D. candidate. His research interests include blockchain and privacy protection.

REN Yan-Bing, M. S. candidate. His research interests include location privacy protection and blockchain.

MA Jian-Feng, Ph. D., yangtze river scholar professor, Ph. D. supervisor. His research interests include network and information security, coding theory and cryptography.

DING Hong-Fa, Ph. D. candidate, lecturer. His research interests include data privacy protection and security protocol design.

Background

With the development of wireless communication and positioning technologies, location-based service (LBS) has become a part of our daily life. However, since LBS always requires the users to submit their locations, an unprecedented threat about location privacy of mobile users comes with the convenience of widely used technique. Therefore, LBS location privacy protection has attracted substantial attention.

Distributed K-anonymity is one of the most common and classic solutions for LBS location privacy protection. In this technique, the request user can acquire the cooperative users' locations by himself/herself to construct an anonymous cloaking region and submit the anonymous cloaking region to location-based service provider (LSP) instead of his/her real location. Compared with other location privacy protection methods, such as differential privacy, obfuscation or cryptography-based methods, distributed K-anonymity can provide precise query results without any requirement for a third party or complicated cryptographic technologies.

Unfortunately, the existing distributed K-anonymity location privacy protection schemes do not consider location leaking or cheating behaviors during the construction of anonymous cloaking region. This can lead to, for example, a selfish request user that discloses the cooperative users' locations to gain illegal benefits. Alternatively, a selfish cooperative user could provide a fake location, in which case the constructed anonymous cloaking region cannot ensure the privacy protection requirement of the request user and, more seriously, LSP could be used to identify the request user's location.

To address this problem, this paper proposes a novel distributed K-anonymity location privacy protection scheme based on blockchain. In the proposed scheme, we utilize blockchain to record the users involved in the construction of the anonymous cloaking region and the provided locations as evidences. If location leaking or cheating behaviors occur, the corresponding users cannot successfully construct the anonymous cloaking region when they initiate queries. This punishment technique ensures that no users can deviate from the prescribed scheme. The presented security analysis demonstrates that the proposed scheme not only prevents the request user from disclosing the locations but also incentivizes the cooperative users to provide their real locations, thereby protecting the privacy of the users' locations effectively. Extensive experiments indicate that the proposed method can construct the anonymous cloaking region efficiently.

This work was sponsored in party by the National Natural Science Foundation of China (Nos. U1708262, U1736203, and U1405255); the National Key Research and Development Program of China (No. 2017YFB0801805); the talent introduction program of Guizhou University of Finance and Economics (No. 2018YJ16).