基于博弈论与区块链融合的 *k*-匿名位置隐私保护方案 *

杨少杰[1]，郑 琨[1]，张 辉[1]，张光华[1,2†]

(1. 河北科技大学 信息科学与工程学院，石家庄 050000; 2. 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)

摘 要：基于移动用户的位置服务中，通常采用位置 *k*-匿名技术保护用户的隐私安全性。然而，用户协作构建 k-匿名组中难以保证请求用户和协作用户的诚信合作行为。针对以上问题，首先基于完全信息静态博弈理论分析请求用户和诚信用户的行为策略，计算请求用户的诚信阈值，协作用户根据请求阈值与协同阈值的比较决定是否参与匿名组构建；其次，构建信誉机制将用户的近期表现与收益结合，约束参与匿名组构建的请求用户及协作用户的不诚信行为；最后，使用区块链存储博弈过程和协作用户的位置信息，当发现请求用户和协作用户的不诚信行为时，对不诚信的用户进行信誉值和收益降低的处罚。安全分析表明，本方案能有效保护用户的位置隐私，促进请求用户与协作用户的诚信合作，同时激励更多的人参与匿名组的构建。

关键词：位置隐私保护；静态博弈；信誉机制；区块链

中图分类号：TP399 doi: 10.19734/j.issn.1001-3695.2019.10.0654

Anonymous location privacy protection scheme based on game theory and blockchain fusion

Yang Shaojie[1], Zheng Kun[1], Zhang Hui[1], Zhang Guanghua[1,2†]

(1. *College of Information Science & Engineering*, *Hebei University of Science & Technology*, *Shijiazhuang* 050000, *China*; 2. *State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Based on the location service of the mobile user, people use location k-anonymity technology to protect the privacy of users. However, it is difficult to ensure the honest cooperation behavior of the requesting user and the collaborative user in the user collaborative k-anonymous group. Aiming at the above problems, firstly, based on the complete information static game theory, this paper analyze the behavioral policies of requesting users and honest users, and calculate the requesting user's integrity threshold. The collaborative user decides whether to participate in the anonymous group construction according to the comparison between the request threshold and the cooperation threshold. Secondly, this paper build a reputation mechanism to combine users' recent performance with the benefits, restricting the untrustworthy behavior of the requesting users and the collaborative users who participate in the anonymous group construction; finally, using the blockchain to store the game process and the location information of the collaborative users. When this paper discover the dishonest behavior of requesting users and collaborating users, this paper will punish the dishonest users by reducing their reputation and profit. Security analysis shows that this solution can effectively protect the user's location privacy, promote the integrity cooperation between the requesting user and the collaborative user, and encourage more people to participate in the construction of the anonymous zone.

Key words: location privacy protection; static game; credibility mechanism; block chain

0 引言

随着无线通信技术与智能定位系统的发展,基于移动用户的位置服务[1]给用户的生活带来了极大的便利。然而,享受位置服务的同时面临着个人隐私泄露的风险。一方面,位置服务提供商可提供用户诸多服务(紧急事故处理、路线查询等);另一方面,用户的位置信息与查询内容易被位置服务提供商分析出个人敏感信息[2]。为此，学者们将现实场景中位置隐私保护技术归纳为三种结构：独立式结构、匿名服务器结构和分布式结构。独立式结构[3]较为简单,但要求终端用户具备一些存储和计算能力。匿名服务器结构[4]是在二者之间加入一个可信匿名服务器来解决客户端存储和计算能力不足的问题,但可信的匿名服务器遭受攻击时却难以保证用户的隐私安全。分布式结构[5] 是在独立式结构的基础上进行群组协作构建匿名组。然而,现实场景中匿名组的参与者互为不可信状态,即请求用户为获取额外收益会泄露协作用户的位置信息,协作用户提供虚假位置信息使得匿名组难以保护请求用户的位置隐私。因此，如何采取有效机制激励用户参与匿名组构建,遏制用户的行为,对用户的位置隐私保护具有重要意义。

位置隐私保护中,使用最广泛的模型便是 k 匿名模型。Gruteser 等[6]最早将 K-匿名应用至位置隐私保护,匿名组中有 k 个不可区分的位置信息使得服务提供商辨别出用户位置信息的概率为 1/k。随着研究的不断开展，位置 K-匿名通常由中心匿名服务器完成。文献[7]在完全可信中心匿名服务器的基础上，将用户的精确位置扩大至一个正方形的空间区域，并在匿名服务器中把地理空间划分若干匿名区域提高缓存利用率。然而，现实中难以保证匿名服务器的完全可信，且匿名服务器遭受攻击时会造成大量的用户隐私泄露。文献[8]基

收稿日期：2019-10-14；**修回日期：**2019-12-05 **基金项目：**国家重点研发计划项目(2016YFB0800703)；国家自然科学基金项目(61572255)；河北省高等学校科学技术研究项目(ZD2018236)

作者简介：杨少杰(1997-)，男，江苏宿迁人，硕士研究生，主要研究方向为位置隐私保护；郑琨(1981-)，女，河北石家庄，讲师，主要研究方向为计算机应用；张辉(1973-)，男，河北石家庄，工程师，主要研究方向为网络与信息安全；张光华(1979-)，男(通信作者)，河北石家庄，副教授，博士，主要研究方向为网络与信息安全(xian_software@163.com).

于半可信匿名服务器的结构，提出了一种基于假位置和Stackelberg 博弈的匿名算法。引入假名服务器将用户隐私分开存储，有效避免了匿名服务器遭受攻击时用户的完整隐私信息被泄露的问题。

为了避免中心服务器带来的通信瓶颈和并非完全可信的问题，学者们提出了群组协作构建 k 匿名组的方法。Chow[9]等提出了一种用户合作点对点空间伪装算法。用户通过单跳或多跳通信与周围用户构成点对点组，然后将位置区域扩充为点对点匿名组。以匿名组代替用户真实位置进行位置服务查询，保护用户的隐私。文献[10]为了提高用户的服务质量，提高匿名系统性能提出了一种用户协作无匿名区域的位置隐私保护方法。通过用户协作构建匿名组，并以匿名组中心代替用户真实位置发起增量查询，提高了服务质量。但是，上述方案均假设协作用户是可信的，未考虑现实环境的不可信状态。

文献[11]在文献[10]的基础上，通过安全求和的方法解决协作用户的不诚信问题。然而复杂的密码学技术使得锚点计算算法较低，当不诚信的协作用户较多时，多次重新计算容易导致死循环。此外，考虑协作用户的不可信行为，文献[12]提出一种基于查询分片用户协作的位置隐私保护方法，根据安全等级将请求信息分成若干片段，再随机分发给组内其他用户。仅当组内所有用户的请求片段被集齐后才发给服务提供商，保护用户的隐私安全。然而，上述均未考虑请求用户泄露协作用户位置信息的行为。为此，Liu[13]等提出了一种基于信誉激励机制的位置隐私保护方案。为用户设定阈值,仅当用户信誉达到阈值时,才能获得周围人的帮助。该方案考虑了请求用户和协作用户的诚信行为，缺点是信誉激励机制存于云服务器上，并假设第三方云服务器是半可信的。区块链具有去中心化、难窜改和激励机制等特点，已有学者将区块链技术和分布式 k-匿名位置隐私保护相结合进行研究。文献[14]结合区块链技术，对 k-匿名激励机制进行了改进。设计了保证金制度，一定程度上遏制了恶意用户的加入，提高匿名区的成功率。文献[15]首次利用区块链技术将请求用户与协作用户的匿名区生成过程视作交易,保存在区块链中。对泄露协作用户位置的请求用户和提供虚假位置的协作用户一旦发现其存在欺诈行为,便对其进行多轮禁止构造匿名区的惩罚。

可见，尚无将博弈论和区块链结合研究位置隐私保护工作的出现。结合了上述位置隐私保护研究的优缺点，提出了一种基于博弈论与区块链融合的 k-匿名位置隐私保护方案。考虑了请求用户的不诚信行为，通过博弈论计算请求用户的诚信阈值,协作用户根据协同阈值决定是否参与匿名组构建。使用区块链存储请求用户与协作用户的博弈过程及协作用户的位置信息，并构建信誉机制。一旦发现请求用户泄露协作用户的位置信息和协作用户提供虚假位置信息参与匿名组构建，则对不诚信的用户进行惩罚，从而保证匿名组的真实可用，保护用户的位置隐私。

1　预备知识

1.1　博弈论

博弈论(Game Theory)又称对策论,应用在经济学、社会交际学及信息工程学等诸多领域。一个完整的博弈可分为以下四个方面：博弈参与者、多方博弈策略、博弈次序和博弈收益[16]。1951 年,Nash[17]给出了博弈论一个重要概念—纳什均衡,从合作博弈拓展到非合作博弈领域。

完全信息静态博弈[18]为博弈参与者同时作出策略选择且对各参与者收益有完全了解的博弈。每个博弈参与者的策略相对其他博弈参与者的策略或策略组合皆为最佳对策，该解的概念定义为纳什均衡。纳什均衡可定义如下：

定义 1　纳什均衡。有 n 个博弈参与者进行博弈,每个博弈参与者的策略空间为 $S_1,S_2,\cdots,S_n$ 。各个博弈方皆有多个策略选择 $S_{1j},S_{2j},\cdots,S_{nj}$，其中 $S_{ij}\in S_i$ 表示第 i 个博弈参与者的第 j 个策略。用 $U_1,U_2,\cdots,U_n$ 表示各博弈参与方策略的多元函数。则在博弈 $G=\{S_1,S_2,\cdots,S_n;U_1,U_2,\cdots,U_n\}$ 中，各博弈参与方组成的策略集合为 $(S_1^*,S_2^*\cdots S_n^*)$，若任一博弈参与方所选的策略 S_i^* 都是对其他参与者的策略集合 $(S_1^*,S_2^*,\cdots S_{i-1}^*,S_{i+1}^*,\cdots,S_n^*)$ 的最佳对策，则称 $(S_1^*,S_2^*\cdots S_n^*)$ 为博弈 G 的一个纳什均衡。

由于某些博弈不存在纳什均衡或纳什均衡不唯一，故而纳什均衡可解决诸多博弈问题，但并不能彻底解决完全信息静态博弈的问题。解决此类问题的方法是把纯策略分配不等的概率扩展为混合策略。混合策略的正式定义如下：

定义 2　混合策略。有 n 个博弈参与者进行博弈,每个博弈参与者的策略空间为 $S_1,S_2,\cdots,S_n$ 。各个博弈参与者皆有多个策略选择 $S_{1j},S_{2j},\cdots,S_{nj}$，其中 $S_{ij}\in S_i$ 表示第 i 个博弈参与者的第 j 个策略。若博弈方 i 以概率 $P=(P_{i1},P_{i2},\cdots,P_{ik})$ 选择策略 $S=(S_{i1},S_{i2},\cdots,S_{ik})$，且 $P_{i1}+P_{i2}+\cdots+P_{ik}=1$，则称此策略为混合策略。

1.2　区块链

区块链系统囊括了众多计算机研究成果：计算机密码学、点对点通信技术及分布式存储等。为了解决分布式存储一致性问题,用户可用智能合约执行预先编写的一组程序规则来保证数据的一致性。区块链技术具有匿名、去中心化、去信任化、不可窜改和防伪溯源等特点,使其在隐私保护、多方合作和可信计算中广泛应用[19]。区块链的分类有很多种，通常按应用场景划分为公有链、私有链和联盟链[20]。

2　基于博弈论与区块链融合的 k-匿名位置隐私保护方案

本节提出了基于博弈论与区块链融合的k-匿名位置隐私保护方案。首先，对该方案的系统架构进行描述；其次，基于博弈理论计算出请求用户的诚信阈值并设计了信誉机制解决了匿名组构建存在的问题；最后，设计了记账权竞争机制选出用户进行区块的发布并将用户的博弈以交易账单形式存储于区块链中作为日后不可抵赖的证据，约束用户的不诚信行为。

2.1　系统架构

为了对用户的位置隐私实施保护，本方案采用分布式 k-匿名结构，并基于博弈论与区块链技术约束了用户的自私行为，确保了匿名组的真实可用性。不同于传统的中心匿名服务器结构，分布式 k-匿名结构由用户联盟构建匿名组，没有可信第三方参与匿名组的构建。如图 1 所示，该系统架构由三个部分组成：位置服务请求用户、匿名组构建协作用户和位置服务提供商。

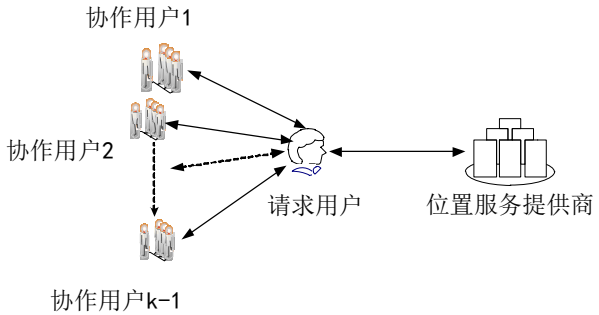

图 1　系统结构

Fig. 1　System structure

请求用户基于自身地理位置进行服务查询时，首先向周围用户广播匿名组构建请求，获取到不少于 k-1 个参与匿名组构建的协作用户真实位置信息。其次，将自身位置和协作

用户的位置混合构建匿名组，向服务提供商发起服务查询。最后，服务提供商依据请求用户提供的位置信息和查询内容返回对应需求的查询结果，请求用户在查询结果中筛选出自己所需的结果，从而获得服务的同时保护了隐私安全。

为了确保匿名组的真实可用，约束请求用户泄露协作用户的真实位置信息获取额外收益的行为，每个用户依据对自身位置隐私泄露的忍耐程度设定了协同阈值，通过博弈理论分析计算出请求用户的诚信阈值，当诚信阈值小于协同阈值时，该协作用户不参与此请求用户的匿名组构建。协同阈值的取值范围为[0,1]，协同阈值越低，对隐私泄露的忍耐程度越高，能够参与更多的匿名组构建；协同阈值越高，则对隐私泄露的忍耐程度越低，对发起匿名组请求的用户诚信阈值要求越高。若协作用户未设置过协同阈值，则可采取默认值0.5，日后依据现实复杂情况调整协同阈值。协作用户对位置隐私泄露的忍耐程度和协同阈值的对应关系如表 1 所示。

表 1　忍耐度和协作阈值关系表

Tab. 1　Tolerance and collaboration threshold relationship

忍耐度	协作阈值
高	[0,0.2]
较高	(0.2,0.4]
中	(0.4,0.6]
较低	(0.6,0.8]
低	(0.8,1]

当请求用户的诚信阈值高于协作用户的协同阈值时，协作用户将帮助请求用户构建匿名组，但仍存在两个问题：第一，协作用户参与匿名组的构建，却不想提供所处位置真实信息，于是虚假生成一个位置信息导致匿名组难以满足请求用户的位置隐私安全。第二，请求用户完成匿名组构建后泄露协作用户的位置信息以获取额外收益。针对上述问题，本方案为用户建立信誉机制，将用户收益与近期表现结合，使得不诚信合作的用户在若干轮有限次的匿名组构建总收益小于诚信合作的总收益，从而约束二者的不诚信行为。

2.2　基于博弈论的诚信阈值分析

本节计算请求用户的诚信阈值。请求用户广播匿名组构建请求，协作用户依据协同阈值决定是否参与匿名组构建的过程可看做双方的博弈。虽然博弈方的策略选择有先后顺序，但博弈双方并不知晓对方所采取的策略，可看做同时决策，属于静态博弈范畴。博弈方为请求用户和协作用户，请求用户的策略集合为诚信请求和不诚信请求，协作用户的策略集合为提供位置和不提供位置。基于博弈理论分析博弈双方的决策时，还需定义不同策略下的收益。

为了充分衡量请求用户的诚信行为，本方案将结合用户的历史行为在基础得益上使用贴现系数作为本次得益。例如协作用户多次参与同一请求用户的匿名组构建会对协作用户的隐私安全性造成影响。其中：

α：请求用户采取的策略对协作用户日后收益影响的贴现系数。

β：请求用户采取的策略对自身日后收益影响的贴现系数。

基础得益：根据请求用户的历史行为，计算出本次博弈中请求用户和协作用户采取不同策略所获得的收益。

通过上述分析，请求用户和协作用户不同策略下的收益定义如下：

U_{C-P}^{++}：请求用户采取诚信请求策略且协作用户提供位置信息时，协作用户的收益。假设双方在此策略组合下协作用户的基础得益为$b_u_{c-p}^{++}$，则协作用户第 n 次响应同一请求用户的请求时，协作用户的收益为

$$\begin{aligned} U_{C-P}^{++} &= b\_u_{c-p}^{++} + b\_u_{c-p}^{++} \times \alpha + \\ &\quad b\_u_{c-p}^{++} \times \alpha^2 + \cdots + b\_u_{c-p}^{++} \times \alpha^n \\ &= b\_u_{c-p}^{++} \times \frac{1-\alpha^n}{1-\alpha} \end{aligned} \tag{1}$$

U_{C-P}^{-}：请求用户采取不诚信请求策略且协作用户提供位置信息时，协作用户的收益(负)。假设双方在此策略组合下协作用户的基础得益为$b_u_{c-p}^{-}$，则协作用户第 n 次响应同一请求用户的请求时，协作用户的收益为

$$\begin{aligned} U_{C-P}^{-} &= b\_u_{c-p}^{-} + b\_u_{c-p}^{-} \times \alpha + \\ &\quad b\_u_{c-p}^{-} \times \alpha^2 + \cdots + b\_u_{c-p}^{-} \times \alpha^n \\ &= b\_u_{c-p}^{-} \times \frac{1-\alpha^n}{1-\alpha} \end{aligned} \tag{2}$$

U_{C-NP}^{-}：请求用户采取诚信请求策略且协作用户不提供位置信息时，协作用户的收益(负)。假设双方在此策略组合下协作用户的基础得益为$b_u_{c-np}^{-}$，则协作用户第 n 次响应同一请求用户的请求时，协作用户的收益为

$$\begin{aligned} U_{C-NP}^{-} &= b\_u_{c-np}^{-} + b\_u_{c-np}^{-} \times \alpha + \\ &\quad b\_u_{c-np}^{-} \times \alpha^2 + \cdots + b\_u_{c-np}^{-} \times \alpha^n \\ &= b\_u_{c-np}^{-} \times \frac{1-\alpha^n}{1-\alpha} \end{aligned} \tag{3}$$

U_{C-NP}^{+}：请求用户采取不诚信请求策略且协作用户不提供位置信息时，协作用户的收益。此处可理解为协作用户成功保护了位置隐私所获得的收益。假设双方在此策略组合下协作用户的基础得益为$b_u_{c-np}^{+}$，则协作用户第 n 次响应同一请求用户的请求时，协作用户的收益为

$$\begin{aligned} U_{C-NP}^{+} &= b\_u_{c-np}^{+} + b\_u_{c-np}^{+} \times \alpha + \\ &\quad b\_u_{c-np}^{+} \times \alpha^2 + \cdots + b\_u_{c-np}^{+} \times \alpha^n \\ &= b\_u_{c-np}^{+} \times \frac{1-\alpha^n}{1-\alpha} \end{aligned} \tag{4}$$

U_{R-H}^{+}：请求用户采取诚信请求策略且协作用户提供位置信息时，请求用户的收益。假设双方在此策略组合下请求用户的基础得益为$b_u_{r-h}^{+}$，则协作用户第 n 次响应同一请求用户的请求时，请求用户的收益为

$$\begin{aligned} U_{R-H}^{+} &= b\_u_{r-h}^{+} + b\_u_{r-h}^{+} \times \beta + \\ &\quad b\_u_{r-h}^{+} \times \beta^2 + \cdots + b\_u_{r-h}^{+} \times \beta^n \\ &= b\_u_{r-h}^{+} \times \frac{1-\beta^n}{1-\beta} \end{aligned} \tag{5}$$

U_{R-NH}^{++}：请求用户采取不诚信请求策略且协作用户提供位置信息时，请求用户的收益。假设双方在此策略组合下请求用户的基础得益为$b_u_{r-nh}^{++}$，则协作用户第 n 次响应同一请求用户的请求时，请求用户的收益为

$$\begin{aligned} U_{R-NH}^{++} &= b\_u_{r-nh}^{++} + b\_u_{r-nh}^{++} \times \beta + \\ &\quad b\_u_{r-nh}^{++} \times \beta^2 + \cdots + b\_u_{r-nh}^{++} \times \beta^n \\ &= b\_u_{r-nh}^{++} \times \frac{1-\beta^n}{1-\beta} \end{aligned} \tag{6}$$

U_{R-NH}^{-}：请求用户采取不诚信请求策略且协作用户不提供位置信息时，请求用户的收益(负)。假设双方在此策略组合下请求用户的基础得益为$b_u_{r-nh}^{-}$，则协作用户第 n 次响应同一请求用户的请求时，请求用户的收益为

$$\begin{aligned} U_{R-NH}^{-} &= b\_u_{r-nh}^{-} + b\_u_{r-nh}^{-} \times \beta + \\ &\quad b\_u_{r-nh}^{-} \times \beta^2 + \cdots + b\_u_{r-nh}^{-} \times \beta^n \\ &= b\_u_{r-nh}^{-} \times \frac{1-\beta^n}{1-\beta} \end{aligned} \tag{7}$$

依据上述分析，该博弈的博弈矩阵如表 2 所示。

表 2　请求用户和协作用户的博弈矩阵

Tab. 2　Game matrix for requesting users and cooperating users

协作用户	请求用户	
	诚信	不诚信
提供	U_{C-P}^{++}，U_{R-H}^{+}	U_{C-P}^{-}，U_{R-NH}^{++}
不提供	U_{C-NP}^{-}，0	U_{C-NP}^{+}，U_{R-NH}^{-}

利用博弈论分析表 2 中博弈矩阵的纳什均衡，从协作用户角度而言，当请求用户采取诚信请求策略时，协作用户选择提供位置策略的收益最大；当请求用户采取不诚信请求策略时，协作用户选择不提供位置策略的收益最大。从请求用户角度而言，当协作用户采取提供位置的策略时，请求用户选择不诚信请求的策略收益最大；当协作用户采取不提供位置的策略时，请求用户选择诚信请求的策略收益最大。根据以上分析，该博弈矩阵并不存在纯策略纳什均衡，需在混合策略下计算混合策略纳什均衡。

假设请求用户采取诚信请求策略的概率为θ，则请求用户采取不诚信请求策略的概率为$1-\theta$；协作用户采取提供位置信息策略的概率为ρ，则协作用户采取不提供位置信息策略的概率为$1-\rho$。请求用户的策略概率分布为P_R=(θ,1-θ)，协作用户的策略概率分布为P_C=(ρ,1-ρ)。

根据表 2 及上述假设，可计算出请求用户的收益函数E_R：

$$\begin{aligned} E_R = {} & \theta[\rho U_{R-H}^{+} + (1-\rho)\times 0] + \\ & (1-\theta)[\rho U_{R-NH}^{++} + (1-\rho)\times U_{R-NH}^{-}] \end{aligned} \tag{8}$$

将E_R对θ进行求导并令导数为 0 得:

$$\begin{aligned} \frac{\partial E_R}{\partial \theta} &= \rho U_{R-H}^{+} - \rho U_{R-NH}^{++} - (1-\rho)\times U_{R-NH}^{-} \\ &= \rho(U_{R-H}^{+} - U_{R-NH}^{++} + U_{R-NH}^{-}) - U_{R-NH}^{-} \\ &= 0 \end{aligned} \tag{9}$$

解出：

$$\rho = \frac{U_{R-NH}^{-}}{U_{R-H}^{+} - U_{R-NH}^{++} + U_{R-NH}^{-}} \tag{10}$$

同理，可计算出协作用户的收益函数E_C：

$$\begin{aligned} E_C = {} & \rho[\theta U_{C-P}^{++} + (1-\theta)\times U_{C-P}^{-}] + \\ & (1-\rho)[\theta U_{C-NP}^{-} + (1-\theta)\times U_{C-NP}^{+}] \end{aligned} \tag{11}$$

将E_C对ρ进行求导并令导数为 0 得:

$$\begin{aligned} \frac{\partial E_C}{\partial \rho} &= \theta U_{C-P}^{++} + (1-\theta)\times U_{C-P}^{-} - \theta U_{C-NP}^{-} - (1-\theta)\times U_{C-NP}^{+} \\ &= \theta(U_{C-P}^{++} - U_{C-P}^{-} - U_{C-NP}^{-} + U_{C-NP}^{+}) + U_{C-P}^{-} - U_{C-NP}^{+} \\ &= 0 \end{aligned} \tag{12}$$

解出：

$$\theta = \frac{U_{C-NP}^{+} - U_{C-P}^{-}}{U_{C-P}^{++} - U_{C-P}^{-} - U_{C-NP}^{-} + U_{C-NP}^{+}} \tag{13}$$

上述运用熵概念计算出请求用户和协作用户的收益，并基于混合策略下的纳什均衡求解出了请求用户采取诚信请求策略的概率θ，即请求用户的诚信阈值。协作用户将θ与自身的协同阈值进行比较，若θ大于协同阈值，则提供位置信息，否则不提供位置信息。

2.3　基于博弈论的信誉机制

当用户的诚信阈值大于协作用户的协同阈值时，协作用户将提供位置信息参与匿名组的构建。假设请求用户和协作用户均为理性用户，其决策均为以自身利益最大化为目标的理性决策。博弈方为请求用户和协作用户，请求用户的策略集合为泄露协作用户位置信息和不泄露协作用户位置信息，协作用户的策略集合为提供虚假位置信息和提供真实位置信息。基于博弈理论分析博弈双方的决策时，还需定义不同策略下的收益：

本方案假设请求用户是以构造匿名组为主要目的的理性请求用户，因此成功构造匿名组的收益大于泄露协作用户位置信息的收益。请求用户对应策略下的收益由高到低为

U_R^{++}：请求用户完成匿名组构建后，泄露协作用户位置信息的收益；

U_R^{+}：请求用户完成匿名组构建后，未泄露协作用户位置信息的收益；

U_R^{-}：请求用户未完成匿名组构建，但泄漏了协作用户位置信息的收益；

U_R^{--}：请求用户未完成匿名组构建，且未泄漏协作用户位置信息的收益；

同样，对于理性的协作用户而言，首要工作是保护自身位置隐私安全。在此基础上与请求用户合作构建匿名组。故而协作用户对应策略下的收益由高到低为

U_C^{++}：协作用户以虚假生成的位置信息参与匿名组构建并成功构建匿名组，且未被请求用户识别的收益；

U_C^{+}：协作用户以真实位置信息参与匿名组构建并成功构建匿名组，且未被请求用户泄露的收益；

U_C^{-}：协作用户以虚假生成的位置信息参与匿名组构建，但被请求用户识别被惩罚的收益；

U_C^{--}：协作用户以真实位置信息参与匿名组构建，但被请求用户泄露的收益；

此外，构建了信誉机制为每个用户设计了信誉值，仅当用户P_i信誉值为$C_u(x_0)$时方可作为请求用户，否则只能以协作用户身份被惩罚参与匿名组构建，牺牲作为协作用户的收益获取信誉值，此处的收益可理解为请求用户未完成匿名组的构建，且未泄漏协作用户位置信息的收益。

若用户P_i作为请求用户在本次匿名组构建中被察觉泄露了协作用户位置信息，则信誉分降低 p 分，且不能作为请求用户参与匿名组构建。仅当P_i作为协作用户诚信参与 p 轮匿名组构建后，再次作为请求用户发起匿名组构建请求时才可能得到协作用户的响应。同理，若用户P_C作为协作用户在本次匿名组构建中提供了虚假位置信息，则信誉分降低 p 分，仅当P_C作为协作用户诚信参与 p 轮匿名组构建后，信誉分为$C_u(x_0)$时作为请求用户发起匿名组构建请求才可能得到协作用户的响应。

综上，本方案信誉机制如下：

用户的信誉值$C_u(X_k)$由初始信誉值$C_u(x_0)$和调节参数$\delta(x_i)$共同确定,且满足：

$$C_u(x_k) = C_u(x_{k-1}) + \delta(x_{k-1}) = C_u(x_0) + \sum_{i=0}^{k-1}\delta(x_i) \tag{14}$$

其中,$\delta(x_i)\in\{-p,+1\}$表示对用户信誉值的调节。若发现请求用户或协作用户存在不诚信行为时,则对不诚信用户的信誉值降低 p 分；若用户作为协作用户提供真实位置参与匿名组构建时,对其信誉值上升 1 分。本方案规定只有用户的信誉值$C_u(x_k)=C_u(x_0)$时，作为请求用户发起匿名组构建请求才可能够得到协作用户的响应。当协作用户多次诚信参与匿名组构建后,信誉值较高,可能导致下次进行不诚信行为,故将初始信誉值设为最大信誉值,满足$C_u(x_k)\le C_u(x_0)$。作为补偿，本方案将记录协作用户参与匿名组构建的次数并以此为基础设计区块链记账权竞争机制。

基于博弈论与区块链融合的k-匿名位置隐私保护方案中，使用区块链存储博弈过程和协作用户的位置信息，由于数据的不可窜改，区块链存储的交易账单将作为证据对不诚信的用户进行惩罚。而完善的密码学理论保证了参与匿名组构建

协作用户的位置安全性，使得网络中的协作用户积极参与匿名组构建。同时，区块的更新，将由记账权竞争机制选出一个节点打包并发布下一区块。为了激励用户参与记账权的竞争,区块链系统将对获得记账权的用户进行奖励。

2.4 记账权竞争机制

假设有 K 个用户 $P_1,P_2,\cdots,P_K$ 参与记账权竞争，用户 $P_1,P_2,\cdots,P_K$ 作为协作用户参与匿名组构建的次数为 $x_1,x_2,\cdots,x_K$，获得记账权的用户 P_i 生成新区块的收益 $income$ 为

$$income = x_i + 1, x_i = \arg\max f(x_i) \tag{15}$$

其中 $f(x_i) = |\sin x_i|$，$x_i \in \{x_1,x_2,\cdots,x_K\}$。记账权竞争机制主要作用是选择用户进行区块的更新，设计的原理为作为协作用户参与匿名组构建次数越多，获得记账权概率越大。考虑到参与记账权竞争的用户作为协作用户时参与匿名组构建次数较大始终占据记账权使得区块链存在风险，本方案引入函数 $\arg\max f(x_i)$ 来确定记账权的选择。此外，P_i 作为协作用户参与匿名组构建次数越多，基于博弈论计算请求用户和协作用户的收益越大，从而 P_i 的诚信阈值越高，当 P_i 发起匿名组构建请求时，会有更多的协作用户参与匿名组构建。

2.5 交易过程

a) 用户 P_i 向网络中的用户广播匿名组构建请求：

$$request = \{TS_{U\to C}, ID_U, C_u(x_0), x_i, Sign_{SK-ID_U}(C_u(x_0), TS_{U\to C})\} \tag{16}$$

其中 $TS_{U\to C}$ 为用户 P_i 发送 $request$ 的时间戳；ID_U 为用户 P_i 在区块链系统中的唯一标志,用于代替用户的真实身份；$C_u(x_0)$ 表示请求用户 P_i 的信誉值；x_i 为用户 P_i 作为协作用户参与匿名组构建次数；$Sign_{SK-ID_U}(C_u(x_k), TS_{u\to M})$ 为用户 P_i 用自己的私钥 $SK-ID_U$ 对信誉值和时间戳的签名。

b) 协作用户收到 P_i 广播的 $request$ 后，去区块链系统中查找记录请求用户 P_i 的交易账单，得到请求用户 P_i 的信誉值 $C_u(x_k)$ 和作为协作用户参与匿名组构建次数 $x_i^{\wedge}$ 并分别与 $C_u(x_0)$ 和 x_i 比较，如若不一致，进行步骤 c) ；如若一致，转到步骤 d) 。

c) 若 $C_u(x_k) \neq C_u(x_0)$ 或 $x_i \neq x_i^{\wedge}$，则用户 P_i 虚假构造信誉值或协作次数发起匿名组构建请求，协作用户不参与匿名组构建并广播惩罚账单：

$$\begin{aligned} punishment = \{&TS_{C\to U}, ID_C, pun, sign_{SK-ID_C}(TS_{C\to U}, pun),\\ &TS_{U\to C}, x_i, C_u(x_0), Sign_{SK-ID_U}(C_u(x_0), TS_{u\to M})\} \end{aligned} \tag{17}$$

其中 $TS_{C\to U}$ 为惩罚账单生成的时间戳；ID_C 为协作用户 P_C 在区块链系统中的唯一标志；pun 为惩罚账单的标志符；$sign_{SK-ID_C}(TS_{C\to U}, pun)$ 为协作用户 P_C 用自己的私钥 $SK-ID_C$ 对惩罚标志和时间戳进行签名。

d) 协作用户 P_C 计算 P_i 的诚信阈值并与自身的协同阈值进行比较。若小于协作阈值，不响应 P_i 广播的匿名组构建请求；若大于等于协作阈值，则向 P_i 发送协作账单：

$$\begin{aligned} Bill = \{&TS_{C\to U}, ID_U, Enc_{PK-ID_U}(LOC_C, TS_{C\to U}),\\ &sign_{SK-ID_C}(Enc_{PK-ID_U}(LOC_C, TS_{C\to U}))\} \end{aligned} \tag{18}$$

其中 $Enc_{PK-ID_U}(LOC_C, TS_{C\to U})$ 为协作用户 P_C 用请求用户 P_i 的公钥 $PK-ID_U$ 对提供的位置信息和时间戳进行的加密密文，P_i 可用自己的私钥进行解密，获取 P_C 提供的位置信息。$sign_{SK-ID_C}(Enc_{PK-ID_U}(LOC_C, TS_{C\to U}))$ 为协作用户 P_C 用自己的私钥 $SK-ID_C$ 对密文的签名。

e) 请求用户 P_i 收到协作账单后，用协作用户的公钥 $PK-ID_C$ 验证 $sign_{SK-ID_C}(Enc_{PK-ID_U}(LOC_C, TS_{C\to U}))$。如若验证成功，将私钥 $SK-ID_U$ 对密文 $Enc_{PK-ID_U}(LOC_C, TS_{C\to U})$ 进行解密，获取协作用户 P_C 提供的位置信息。然后将用协助用户公钥对提供的位置信息和时间戳进行加密的密文 $Enc_{PK-ID_C}(LOC_C, TS_{C\to U})$ 和用请求用户私钥对密文 $Enc_{PK-ID_C}(LOC_C, TS_{C\to U})$ 进行的签名 $sign_{SK-ID_U}(Enc_{PK-ID_C}(LOC_C, TS_{C\to U}))$ 写入协作账单并广播。

f) 网络中的所有用户收到广播的交易账单后进行验证。通过后，保存交易账单并当区块链更新时，由记账权竞争机制选出用户进行区块更新。

3 安全分析

本节对基于博弈论与区块链融合的k-匿名位置隐私保护方案进行安全分析。首先从匿名组真实可用和k-匿名位置隐私安全角度对方案的隐私安全进行分析；其次分析了信誉值的合理性，并通过证明得出结论：当 $p \geq \max\{\frac{U_R^{++}-U_R^{+}}{\delta(U_R^{+}-U_R^{--})}, \frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}\}$ 时，本方案能有效阻止请求用户和协作用户的不诚信行为；最后论述了区块链于本方案的优势。

3.1 隐私安全性分析

定理 1 假设 P_R 为请求用户，至少有 K-1 个协作用户 P_1, P_2,…, P_{k-1} 提供位置信息参与匿名组构建。当且仅当下述条件：

$$\begin{cases} U_R = U_R^{+} \\ U_i = U_C^{+} \\ P \leq 1/K \end{cases}$$

满足时，本方案是安全有效的。其中 U_R 表示请求用户的收益，U_i 表示协作用户的收益。$1 \leq i \leq K-1$ 且 i 为整数，P 为位置服务提供商正确识别请求用户真实位置信息的概率。

证明：本方案采取用户合作构建 k-匿名组的方式保护用户的位置隐私安全性。$U_R = U_R^{+}$ 表示请求用户完成匿名组构建后未泄露协作用户位置信息的收益，保护了参与匿名组构建的协作用户的位置隐私安全；$U_i = U_C^{+}$ 表示协作用户提供真实位置信息帮助请求用户构建匿名组，保护了匿名组内位置信息的真实性；上述两个条件保证了匿名组的真实可用性，可高效构建匿名组。在以上两个条件下，$P \leq 1/K$ 表示请求用户将 k-匿名组代替自身位置向位置服务提供商发起服务查询，位置服务提供商正确分析出请求用户位置信息的概率为 1/K。故从匿名组真实可用性和 k-匿名位置隐私安全性而言，基于博弈论与区块链融合的k-匿名位置隐私保护方案是安全有效的。

3.2 信誉值分析

定理 2 假设协作用户发现请求用户泄露其位置信息的概率为 δ，请求用户发现协作用户提供虚假位置信息的概率为 ω。若存在 K-1 个协作用户 P_1, P_2,…, P_{k-1} 提供位置信息参与匿名组构建，当

$$p \geq \max\{\frac{U_R^{++}-U_R^{+}}{\delta(U_R^{+}-U_R^{--})}, \frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}\}$$

时，本方案能有效阻止请求用户和协作用户的不诚信行为，保证匿名组的真实可用。

证明：在第 n 次参与匿名组构建博弈中，若请求用户 P_i 采取完成匿名组构建后，泄露协作用户位置的策略，则其在第 n 次匿名组构建博弈中所获收益为：$n\_E_R = U_R^{++}$。

不妨设协作用户在 m 时刻发现请求用户 P_i 泄露其位置信息的不诚信行为，则 P_i 信誉分降为 $C_u(x_0)-p$，且只能以协作用户的身份被惩罚参与匿名组构建获取信誉值，此处用户的收益可看做 P_i 作为请求用户未完成匿名组的构建，且未泄漏协作用户位置信息的收益。当用户的信誉值为 $C_u(x_0)$ 时再次作为请求用户发起匿名组构建请求才可能得到协作用户的响应。设 $1 \leq i \leq p$，从收益的角度而言，P_i 在第 n+i 次匿名组构建博弈中的收益为 $n+i\_E_R = U_R^{--}$。综上，P_i 在 p+1 轮匿名组

构建中获得的总收益为

$$E_{R1}^{total}=\delta\times[U_R^{++}+p\times U_R^{--}]+(1-\delta)\times[U_R^{++}+pU_R^{+}] \quad (19)$$

同理，在第 n 次参与匿名组构建博弈中，若请求用户 P_i 采取完成匿名组构建后，未泄露协作用户位置的策略，则其在第 n 次匿名组构建博弈中所获收益为：$n\_E_R=U_R^{+}$。双方的诚信行为能建立良好的合作关系，设$1\le i\le p$，从收益的角度而言，P_i作为请求用户在第 n+i 次匿名组构建博弈中的收益为$n+i_E_R=U_R^{+}$。综上，P_i在 p+1 轮匿名组构建中获得的总收益为

$$E_{R2}^{total}=(p+1)U_R^{+} \quad (20)$$

从博弈理论而言，当$E_{R1}^{total}\le E_{R2}^{total}$时，$P_i$会采取完成匿名组构建后，未泄露协作用户位置的策略。从而：

$$E_{R1}^{total}=\delta\times[U_R^{++}+p\times U_R^{--}]+(1-\delta)\times[U_R^{++}+pU_R^{+}]$$

$$\le E_{R2}^{total}=(p+1)U_R^{+} \quad (21)$$

化简得：

$$p\ge\frac{U_R^{++}-U_R^{+}}{\delta(U_R^{+}-U_R^{--})} \quad (22)$$

综上所述，当 $p\ge\frac{U_R^{++}-U_R^{+}}{\delta(U_R^{+}-U_R^{--})}$时，请求用户能够诚信的构建匿名组。

在第 n 次参与匿名组构建博弈中，若信誉值为$C_u(x_0)$的协作用户 P_C 采取以虚假生成的位置信息参与匿名组构建的策略，且未被请求用户识别，则其在第 n 次匿名组构建博弈中所获收益为：$n\_E_{C1}=U_C^{++}$。P_C其后作为请求用户诚信参与匿名组构建时所获收益为U_R^{+}；若被请求用户识别，则其在第 n 次匿名组构建博弈中所获收益为：$n\_E_{C2}=U_C^{-}$。P_C信誉分降为$C_u(x_0)-p$，且只能以协作用户的身份被惩罚参与匿名组构建获取信誉值，此处用户的收益可看做P_C作为请求用户未完成匿名组的构建，且未泄漏协作用户位置信息的收益。当用户的信誉值为$C_u(x_0)$时再次作为请求用户发起匿名组构建请求才可能得到协作用户的响应。设$1\le i\le p$，从收益的角度而言，P_C在第 n+i 次匿名组构建博弈中的收益为$n+i_E_R=U_R^{--}$。综上，P_C在 p+1 轮匿名组构建中获得的总收益为

$$E_{C1}^{total}=\omega\times[U_C^{-}+pU_R^{--}]+(1-\omega)[U_C^{++}+pU_R^{+}] \quad (23)$$

同理，在第 n 次参与匿名组构建博弈中，若信誉值为$C_u(x_0)$的协作用户 P_C 采取以真实位置信息参与匿名组构建的策略，且未被请求用户泄露，则其在第 n 次匿名组构建博弈中所获收益为：$n\_E_{C3}=U_C^{+}$。双方的诚信行为能建立良好的合作关系，设$1\le i\le p$，从收益的角度而言，P_C作为请求用户在第 n+i 次匿名组构建博弈中的收益为$n+i_E_R=U_R^{+}$。综上，P_i在 p+1 轮匿名组构建中获得的总收益为

$$E_{C2}^{total}=U_C^{+}+pU_R^{+} \quad (24)$$

从博弈理论而言，当$E_{C1}^{total}\le E_{C2}^{total}$时，信誉值为$C_u(x_0)$的协作用户 P_C 会采取以真实位置信息参与匿名组构建的策略。从而：

$$\omega\times[U_C^{-}+pU_R^{--}]+(1-\omega)[U_C^{++}+pU_R^{+}]\le U_C^{+}+pU_R^{+} \quad (25)$$

化简得：

$$p\ge\frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}-\frac{U_C^{+}-U_C^{-}}{U_R^{+}-U_R^{--}} \quad (26)$$

不妨取 $p\ge\frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}$，显然满足上式。即当 $p\ge\frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}$时，协作用户能够诚信的参与匿名组构建。

综上所述，当

$$p\ge\max\{\frac{U_R^{++}-U_R^{+}}{\delta(U_R^{+}-U_R^{--})},\frac{(1-\omega)(U_C^{++}-U_C^{+})}{\omega\times(U_R^{+}-U_R^{--})}\}$$

时，本方案能有效阻止请求用户和协作用户的不诚信行为，保证匿名组的真实可用。

3.3 区块链分析

基于博弈论与区块链融合的 k-匿名位置隐私保护方案，采用区块链存储博弈过程和协作用户的位置信息，无须第三方机构。而分布式存储、点对点的通信避免了第三方的计算力不足和被攻击造成隐私泄露等问题。其次，区块链系统中用户使用的都是假名，避免了恶意节点获取用户的真实身份。而使用非对称密钥对数据进行加密，极大的保障了数据的安全性。此外，区块链存储的博弈过程和协作用户的位置信息难窜改，一旦发现请求用户和协作用户的自私自利行为，可依据区块链所存储的交易账单作为证据对不诚信的用户进行惩罚。最后，区块链的激励机制使得网络中的用户积极参与匿名组构建，保护用户隐私的同时提高了匿名组生成效率。

4 讨论

本方案包含加解密及签名运算，故在满足安全性的基础上，仍需对计算复杂度，实际应用的网络开销等问题进行分析。本节首先对方案的计算复杂度进行分析求解；其次，分析了本方案中影响网络开销的因素；最后将本方案与同类研究工作进行比较彰显本方案的优势。

4.1 计算复杂度分析

交易过程中包含公钥和私钥的加解密及签名运算，其计算复杂度不妨用 O(enc)表示。首先，当请求用户 P_i 发起匿名组构建请求时，用私钥对信誉值和签名加密，计算复杂度为 O(enc)。其次，协作用户 P_C 向 P_i 发送协作账单，P_i用协作用户的公钥 $PK-ID_C$ 验证 $sign_{SK-ID_C}(Enc_{PK-ID_U}(LOC_C,TS_{C\to U}))$。成功后，用自己的私钥 $SK-ID_U$ 对密文 $Enc_{PK-ID_U}(LOC_C,TS_{C\to U})$进行解密，此时计算复杂度为 O(enc)。最后，当区块更新时，参与区块生成的用户此时的计算复杂度为 O(enc)。若用户收到 L≥K-1 个协作账单，其计算复杂度最大为 $\mathrm{O(enc)+L*O(enc)+O(enc)=O(enc)}$。

同理，当协作用户 P_C 收到 P_i 广播的 *request* 后验证签名 $Sign_{SK-ID_U}(C_u(x_k),TS_{u\to M})$ 的正确性，计算复杂度为 O(enc)。确认为 P_i 广播的 *request* 后，P_C 去区块链系统(假设有 M 个区块)中查找记录请求用户 P_i 的交易账单，得到请求用户 P_i 的信誉值 $C_u(x_k)$ 和作为协作用户参与匿名组构建次数 x_i^{A} 并分别与 $C_u(x_0)$和 x_i 比较，若不一致则广播惩罚账单，此时计算复杂度为 $\mathrm{O}(M)+\mathrm{O(enc)=O(enc)}$。若一致，则 P_C 根据阈值比较是否响应 P_i 的请求，若不响应则此刻计算复杂度为 O(1)；若响应则发送协作账单给 P_i，其中涉及计算密文 $Enc_{PK-ID_U}(LOC_C,TS_{C\to U})$ 和对密文的签名 $sign_{SK-ID_C}(Enc_{PK-ID_U}(LOC_C,TS_{C\to U}))$，所需的计算复杂度为 $O(1)+O(enc)+O(enc)=O(enc)$。综上，不提供位置信息的协作用户计算复杂度最高为：$\mathrm{O(enc)+O(1)+O(enc)=O(enc)}$。提供位置信息的协作用户计算复杂度最高为：$O(enc)+O(enc)+O(enc)=O(enc)$。

4.2 网络开销分析

用户采取位置 K 匿名隐私保护方法，因此隐私需求 K 的数值是影响网络开销的因素之一。对请求用户而言，K 值越

大，需要更多的协作用户，从而进行加解密和签名的次数越多，计算时延和通信开销越大；对协作用户而言，其计算时延和通信开销在于和请求用户的点对点通信，故而 K 值的改变并不影响协作用户的计算时延和通信开销。此外，区块的长度和交易账单的数目也是是影响网络开销的因素之一。当区块的长度或交易账单的数目增加时，根节点的计算时延将会增加，从而产生新区块的时延增加，使得网络中的节点通信开销和计算时延增大。该因素对协作用户的计算时延和通信开销影响尤为明显。因为协作用户需在区块链系统中查找记录请求用户的交易账单，故区块的长度和交易账单的数目的增加使得协作用户的计算时延和通信开销进一步增大。

4.3 方案对比

文献[9, 10]方案中用户通过单跳或多跳通信与周围用户构成点对点匿名组，以此保护自己的位置隐私。其中并未考虑匿名组构建中用户的不可信行为，且周围用户较少时，需较大的通信时延获取满足隐私需求的用户。文献[10]方案采用安全求和的方法解决协作用户的不诚信行为，却存在多次求和计算造成死循环的问题。与文献[9~11]方案比较，本方案考虑了用户间的不可信行为并基于博弈论确保匿名组的真实可用。文献[13]方案基于信誉激励机制为用户设置阈值，并将证书存储于半可信第三方云服务器。与文献[13]方案比较，本方案基于区块链存储博弈过程，无须第三方，且基于博弈论和信誉机制约束了用户的不诚信行为。文献[15]方案是首次利用区块链研究 LBS 位置隐私保护的方案，其以帮助用户构建匿名区的次数作为请求用户的阈值并通过交互记录机制约束用户的自利行为，并通过实验得到方案的网络开销较小、有较好的可用性。然而，此方案的阈值机制和信任评估模型并不完善。本方案借鉴了文献[15]方案中利用区块链存储博弈过程的思想，设计了阈值机制，并考虑了协作用户多次帮助请求用户造成的迭代隐私问题。其次，基于博弈论分析了请求用户的诚信阈值，解决了协作用户多次帮助请求用户造成的隐私安全问题。最后，基于信誉机制约束了请求用户和协作用户的自利行为。此外，通过分析得到本方案的网络开销影响因素与文献[15]方案大致相同，未来的的研究将通过实验计算网络开销并与相关工作对比优化，进一步提高方案的实用性。

5 结束语

针对 k-匿名位置隐私保护中用户协作构建匿名组的方式难以保证请求用户和协作用户的诚信合作行为，提出了一种基于博弈论与区块链融合的 k-匿名位置隐私保护方案。协作用户根据对隐私泄露的容忍程度设定协同阈值，并基于静态博弈下的混合策略纳什均衡计算请求用户的诚信阈值。当诚信阈值大于协同阈值时，帮助请求用户构建匿名组。针对匿名组构建中请求用户泄露协作用户的位置信息和协作用户提供虚假位置信息行为，设计信誉机制并通过区块链存储博弈过程和协作用户的位置信息，一旦发现其不诚信行为，对其作出信誉分降低 p 分，且只能以协作用户的身份被惩罚参与匿名组构建获取信誉值的处分。安全分析表明，所设计的方案能遏制请求用户和协作用户的不诚信行为，激励用户参与匿名组的构建，保护请求用户和协作用户的位置隐私安全。本方案尚有不足，在理论证明后仍需通过实验数据对网络开销进行量化分析验证方案的实用性。故下一步的研究工作主要为通过实验对网络开销进行量化分析增强方案的实用性。

参考文献：

[1] 刘树栋, 孟祥武. 一种基于移动用户位置的网络服务推荐方法 [J]. 软件学报, 2014, 25 (11): 2556-2574. (Liu Shudong, Meng Xiangwu. Approach to Network Services Recommendation Based on Mobile Users'Location [J]. Journal of Software, 2014, 25 (11): 2556-2574.)

[2] 李志鹏, 孙名松, 宋增林. 移动智能终端的位置隐私保护技术 [J]. 哈尔滨理工大学学报, 2018, 23 (02): 58-64. (Li Zhipeng, Sun Mingsong, Song Zenglin. The Location Privacy Protection Technology of Mobile Intelligent Terminal [J]. Journal of Harbin University of Science and Technology, 2018, 23 (02): 58-64.)

[3] 王宇航, 张宏莉, 余翔湛. 移动互联网中的位置隐私保护研究 [J]. 通信学报, 2015, 36 (09): 230-243. (Wang Yuhang, Zhang Hongli, Yu Xiangzhan. Research on location privacy in mobile internet [J]. Journal on Communications, 2015, 36 (09): 230-243.)

[4] Sun Gang, Liao Dan, Li Hui, *et al.* L2P2: A location-label based approach for privacy preserving in LBS [J]. Future Generation Computer Systems, 2017, 74 (09): 375-384.

[5] 万盛, 李凤华, 牛犇, 等. 位置隐私保护技术研究进展 [J]. 通信学报, 2016, 37 (12): 124-141. (Wan Sheng, Li Fenghua, Niu Ben, *et al.* Research progress on location privacy-preserving techniques [J]. Journal on Communications, 2016, 37 (12): 124-141.)

[6] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking [C]// Proceedings of the International Conference on Mobile Systems, Applications, and Services, San Francisco California, USA, 2003: 163-168

[7] 李树全, 李锐, 朱大勇, 等. 基于用户网格和两级缓存的 LBS 位置隐私保护方案 [J/OL]. 计算机应用研究, 2019, 37 (8) . (2019-02-12) [2019-10-13]. https://doi. org/10. 19734/j. issn. 1001-3695. 2019. 02. 0074. (Li Shuquan, Li Rui, Zhu Dayong, *et al.* Two-level cache location privacy protection scheme based on user grid [J/OL]. Application Research of Computers, 2019, 37 (8) . (2019-02-12) [2019-10-13]. https://doi. org/10. 19734/j. issn. 1001-3695. 2019. 02. 0074.)

[8] 夏兴有, 白志宏, 李婕, 等. 基于假位置和 Stackelberg 博弈的位置匿名算法 [J/OL]. 计算机学报, 2018, 41 (7) . (2018-11-28) [2019-10-01]. http://kns. cnki. net/kcms/detail/11. 1826. TP. 20181127. 1348. 004. html. (Xia Xingyou, Bai Zhihong, Li Jie, *et al.* A Location Cloaking Algorithm Based on Dummy and Stackelberg Game. [J/OL]. Chinese Journal of Computers, 2018, 41 (7) . (2018-11-28) [2019-10-01]. http://kns. cnki. net/kcms/detail/11. 1826. TP. 20181127. 1348. 004. html)

[9] Chow C Y, Mokbel M F, Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service [C]. Proceedings of the 14th annual ACM international symposium on advances in geographic information systems, 2006: 171-178

[10] 黄毅, 霍峥, 孟小峰. CoPrivacy: 一种用户协作无匿名区域的位置隐私保护方法 [J]. 计算机学报, 2011, 34 (10): 1976-1985. (Huang Yi, Huo Zheng, Meng Xiaofeng. CoPrivacy: A Collaborative Location Privacy-Preserving Method without Cloaking Region. Chinese Journal of Computers, 2011, 34 (10): 1976-1985)

[11] 陈玉凤, 刘学军, 李斌. 基于博弈论的用户相互协作的位置隐私保护方法 [J]. 计算机科学, 2013, 40 (10): 92-97. (Chen Yufeng, Liu Xuejun, Li Bin. Collaborative Position Privacy Protection Method Based on Game Theory [J]. Computer Science, 2013, 40 (10): 92-97.)

[12] 江颉, 傅超仪. 基于查询分片用户协作的位置隐私保护方法 [J]. 小型微型计算机系统, 2019, 40 (05): 935-940. (Jiang Jie, Fu Chaoyi. Location Privacy Protection Method Based on Query Fragment and User Collaboration [J]. Journal of Chinese Mini-Micro Computer Systems, 2019, 40 (05): 935-940.)

[13] Li Xinghua, Miao Meixia, Liu Hai, *et al.* An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism [J]. Soft Computing, 2017, 21 (14): 3907-3917.

[14] 徐健, 温蜜, 张凯. 结合区块链技术的改进 K-匿名激励机制方案

[J/OL]. 计算机工程与应用, 2019 (2019-08-22) [2019-10-13]. http://kns. cnki. net/kcms/detail/11. 2127. TP. 20190822. 1349. 006. html. (Xu Jian, Wen Mi, Zhang Kai. An Improved K-Anonymous Incentive Mechanism Scheme Combined with Blockchain Technology [J/OL]. Computer Engineering and Application, 2019 (2019-08-22) [2019-10-13]. http://kns. cnki. net/kcms/detail/11. 2127. TP. 20190822. 1349. 006. html.)

[15] 刘海, 李兴华, 雒彬, 等. 基于区块链的分布式K匿名位置隐私保护方案 [J]. 计算机学报, 2019, 42 (05): 942-960. (Liu Hai, Li Xinghua, Luo Bin, *et al.* Distributed K-Anonymity Location Privacy Protection Scheme Based on Blockchain. Chinese Journal of Computers, 2019, 42 (05): 942-960)

[16] 马蓉, 冯盛源, 熊金波, 等. 基于安全博弈模型的隐私保护方法 [J]. 武汉大学学报: 理学版, 2018, 64 (02): 165-174. (Ma Rong Feng Shengyuan Xiong Jinbo, *et al.* Privacy Protection Method Based on Security Game Model [J]. Journal of Wuhan University: Natural Science Edition, 2018, 64 (02): 165-174.)

[17] Nash J F. Equilibrium Points in n-Person Games [J]. Proceedings of the National Academy of Sciences of the United States of America, 1950, 36 (1): 48-49

[18] Bonanno, Giacomo. Behavior and deliberation in perfect-information games: Nash equilibrium and backward induction [J]. International Journal of Game Theory, 2017, 47 (3): 1001-1032

[19] Zyskind Guy, Nathan Oz, Pentland Alex. Decentralizing Privacy: Using Blockchain to Protect Personal Data [C]// 2015 IEEE Security and Privacy Workshops (SPW) , 2015: 180-184

[20] 任彦冰, 李兴华, 刘海, 等. 基于区块链的分布式物联网信任管理方法研究 [J]. 计算机研究与发展, 2018, 55 (7): 1462-1478. (Ren Yanbing, Li Xinghua, Liu Hai, *et al.* Blockchain-Based Trust Management Framework for Distributed Internet of Things. Journal of Computer Research and Development, 2018, 55 (7): 1462-1478)