一种基于隐私偏好的隐私保护模型及其量化方法

张盼盼[1,2,4] 彭长根[2,3,4,5] 郝晨艳[1,2,4]

(贵州大学数学与统计学院 贵阳 550025)[1] (贵州大学贵州省公共大数据重点实验室 贵阳 550025)[2]
(贵州大学计算机科学与技术学院 贵阳 550025)[3] (贵州大学密码学与数据安全研究所 贵阳 550025)[4]
(广东省信息安全技术重点实验室 广州 510006)[5]

摘 要 针对隐私保护与服务质量之间的均衡问题,提出了一种基于隐私偏好的博弈度量模型。首先,对用户的隐私偏好进行形式化定义,根据用户的隐私偏好度提出隐私偏好的量化方法;在此基础上,分析服务提供者基于用户隐私偏好的策略选择并提出基于博弈的隐私度量模型,在混合策略下运用策略熵度量用户隐私的泄露情况,能够全面地考虑用户的隐私偏好对服务提供者博弈策略的影响,并对用户的隐私泄露进行有效的度量;最后,用一个案例来说明所提方案的可行性。

关键词 隐私保护,纳什均衡,隐私偏好,策略熵

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.06.022

Privacy Protection Model and Privacy Metric Methods Based on Privacy Preference

ZHANG Pan-pan[1,2,4] PENG Chang-gen[2,3,4,5] HAO Chen-yan[1,2,4]

(College of Mathematics and Statistics, Guizhou University, Guiyang 550025, China)[1]
(Guizhou Provincial Key Laboratory of Big Data, Guizhou University, Guiyang 550025, China)[2]
(College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)[3]
(Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China)[4]
(Guangzhou Provincial Key Laboratory of Information Security, Guangzhou 510006, China)[5]

Abstract The balance between privacy protection and service quality is an issue remained to be solved. This paper proposed a game metric model based on privacy preference. Firstly, the formal definition of the user's privacy preference was proposed, and a method of quantifying privacy preference was proposed. On the basis of this, the service provider's strategy selection based on privacy preference was analyzed and the privacy metric model based on game theory was put forward, the strategy entropy was used to measure the user privacy disclosure under the mixed strategy, which can comprehensively consider user's privacy preferences on the service provider's game strategy and effectively measure user's privacy leak. Finally, the feasibility was demonstrated through a case.

Keywords Privacy protection, Nash equilibrium, Privacy preference, Strategy entropy

1 引言

计算机技术以及信息基础设施的快速发展在给人们带来极大便利的同时,也直接或间接地泄露了人们的隐私,严重威胁到了网络用户的经济安全和人身安全。隐私保护因此受到了人们极大的关注,相关方法被相继提出,它们能够在一定程度上防止隐私泄露,从而达到隐私保护的目的,因此隐私保护方法中隐私度量的研究具有重要的意义。

Shannon提出的信息熵理论[1]成为了信息量化和通信的理论基础。Diáz等[2]于2002年最早将信息熵应用于隐私保护,提出用信息熵来度量匿名通信系统的匿名性。假定攻击者的目的是确定消息发送者(或接收者)的真实身份,系统中的每位用户都以一定的概率被认为是消息的真实发送者或接收者,将攻击者猜测某用户是真实发送者或接收者的事件看作一个随机变量,用信息熵来量化系统的隐私水平。Ma等[3]于2009年考虑了攻击者的累积信息对系统隐私的影响,并提出了在V2X车联网系统中对信息熵进行隐私度量的方法。Chen等[4]于2012年针对LBS查询隐私进行度量,对攻击者在无背景知识和有背景知识两种情况下判断用户是查询信息的真实发送者的条件概率,并利用互信息度量系统的隐

到稿日期:2017-05-21 返修日期:2017-08-23 本文受国家自然科学基金(61662009,61363068,61262073),国家密码发展基金(MMJJ20170129),广东省信息安全技术重点实验室(GDXXAQ2016-04),贵州省教育厅青年科技人才成长项目(黔教合KY字[2016]169),贵州省科技基金计划项目(黔科合基础[2016]1023),贵州大学研究生创新基金(研理工2017071,研理工2017068)资助。

张盼盼(1991-),女,硕士生,主要研究方向为可信计算与信息安全;彭长根(1963-),男,博士,教授,博士生导师,主要研究方向为密码学与信息安全,E-mail:peng_stud@163.com(通信作者);郝晨艳(1990-),女,硕士生,主要研究方向为可信计算与信息安全。

私水平。Yang 等[5]于 2012 年总结了社交网络中的风险，并利用信息熵和互信息度量系统的隐私水平。张学军等[6]于 2014 年针对查询隐私度量机制存在过高评价用户隐私水平的问题，提出了一个泛化的查询隐私度量框架，其形式化定义了隐私度量指标，并提供了一种融合攻击者背景知识和推理能力的系统以及基于信息熵的隐私度量方法。彭长根等[7]于 2016 年基于 Shannon 信息论的通信框架提出了隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型，并在模型中引入了信息熵、平均互信息量、条件熵及条件互信息等描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量。同年，Liu 等[8]在竞标拍卖中运用信息熵度量增价竞标中竞标人的隐私。微软研究院的 Dwork 等[9]于 2006 年提出一种新型的隐私即差分隐私方法，该方法通过添加噪声机制使数据失真来保护数据的隐私性，与传统的隐私保护方法相比，它定义了一个极为严格的攻击模型，并对隐私泄露风险给出了严谨、定量化的表示和证明，在大大降低隐私泄露风险的同时，极大地保证了数据的可用性。Vadhan 等[10]于 2017 年对差分隐私进行了介绍和概述，将其与计算复杂性、密码学和理论计算机科学等其他学科进行了深层联系。Chatzikolakis 等[11]于 2015 年提出一种新颖的弹性可辨性度量方法，该方法通过扭曲几何距离来捕获每个区域的不同程度的密度，获得机制适应噪声水平，同时在任何地方都能达到相同的隐私程度。

随着信息论与博弈论在密码学中的应用，两者的交叉研究引起了关注。Liu 等[12]于 2008 年提出了一种用户隐私泄露量可达到最优 Pareto-Nash 均衡的基于位置社交网络的隐私保护方法。Humbert 等[13]于 2010 年建立了手机网络中用户与攻击者双方关于隐私的博弈模型。Chorppath 等[14]于 2013 年对基于位置服务中的服务提供方和用户建立完全信息博弈。周丹丹等[15]于 2015 年分析了隐私保护涉及的参与方、各方行动规则和策略选择、隐私度量方法以及满足各方利益最大化的纳什均衡求解方法。同年，Xu 等[16]针对在收集、开放、挖掘个人资料过程中出现的隐私问题，将数据提供者、收藏者、用户之间的交互作为博弈进行建模，并提出一种查找博弈的纳什均衡的方法。张伊璇等[17]于 2016 年从获取收益的角度来研究隐私保护，建立了一个基于博弈理论的隐私保护模型，该模型分析访问者与被访问者之间不同的博弈策略所对应的收益。同年，Panaousis 等[18]在位置隐私中分析用户所体验的服务水平与公司利润之间的平衡，在用户与公司之间制定了斯坦伯格贝叶斯博弈。Wu 等[19]于 2017 年构建了多人博弈模型，并分析了博弈模型中纳什均衡的存在性和唯一性。近年来，针对个人隐私保护技术的多个敏感属性的研究越来越多，Yuan 等[20]于 2010 年根据用户的隐私保护要求和具有相同背景知识的攻击不符合个性化隐私的要求，提出一种基于用户个人隐私请求提供隐私保护服务的框架。Guo 等[21]于 2016 年提出了一种基于多敏感度属性的个性化隐私保护模型，其利用多维度分组技术的个性化匿名模型来实现个性化保存。

在上述研究的基础上，为了进一步解决隐私传播模型中隐私保护与隐私服务质量间的均衡问题，本文构建了隐私保护的博弈模型。首先量化用户的隐私偏好，分析服务提供者根据用户的隐私偏好进行的策略选择；然后详细分析了服务提供者与攻击者的博弈过程；最后运用策略熵对博弈过程中用户的隐私信息泄露量进行度量，实现了隐私与服务之间的平衡，并有效地度量了模型的隐私泄露水平。

2　基础知识

首先介绍博弈论[22]中的一些相关概念。

定义 1(纳什均衡)　有 n 个参与人的策略式表述博弈 $G=(s_1,\cdots,s_n;u_1,\cdots,u_n)$，策略组合 $s^*=(s_1^*,\cdots,s_i^*,\cdots,s_n^*)$ 是一个纳什均衡，如果对于每一个 i，s_i^* 是给定其他参与人选择 $s_{-i}^*=(s_1^*,\cdots,s_{i-1}^*,s_{i+1}^*,\cdots,s_n^*)$ 的情况下第 i 个参与人的最优策略，即 $u_i(s_1^*,s_{i-1}^*)\geqslant u_i(s_i,s_{i-1}^*)$，$\forall i,s_i\in S_i$。

定义 2(混合策略纳什均衡)　在 n 个参与人博弈的策略式表述 $G=(s_1,\cdots,s_n;u_1,\cdots,u_n)$ 中，假定参与人 i 有 k 个纯策略 $s_i=\{s_{i1},\cdots,s_{ik}\}$，则概率分布 $\sigma_i=(\sigma_{i1},\cdots,\sigma_{ik})$ 称为 i 的一个混合策略，$\sigma_{ik}=\sigma(s_{ik})$ 是 i 选择 s_{ik} 的概率。对于所有的 $k=1,2,\cdots,K$，$0\leqslant\sigma_{ik}\leqslant1$，其中 $\sum\sigma_{ik}=1$，混合策略组合 $\sigma^*=(\sigma_1^*,\cdots,\sigma_i^*,\cdots,\sigma_n^i)$ 是一个纳什均衡，如果对于所有的博弈参与者 $i(i=1,2,\cdots,n)$ 下式成立：

$$v_i(\sigma_i^*,\sigma_{-i}^*)\geqslant v_i(\sigma_i,\sigma_{-i}^*),\ \forall\sigma_i\in\sum_i$$

3　基于博弈论的隐私保护度量模型

为了解决隐私传播模型中隐私保护与服务质量间的均衡问题，本文基于完全信息静态博弈的相关理论，构建了以博弈论为基础的一个隐私保护的博弈模型。假设博弈双方都是理性的，通过分析用户的隐私偏好及其对博弈策略的影响，使得用户选择合适的博弈策略；通过分析隐私服务提供者与隐私攻击者之间的博弈策略，分析博弈双方的效用函数，得出博弈双方的最优策略。

3.1　隐私偏好的量化

用户在享受隐私服务带来便利的同时，也面临着隐私服务提供者滥用用户隐私信息的风险。因此，为了在隐私保护的过程中定量地分析隐私泄露，本文考虑了用户对自身数据的隐私暴露需求，形式化定义并运用数学方法量化用户的隐私偏好，以有效地帮助用户定量地表达自身的隐私偏好。

定义 3(隐私偏好)　隐私偏好指用户对隐私信息的重视程度，即同意暴露哪些隐私信息，禁止暴露哪些隐私信息，亦即用户根据自己主观意向的要求对其提供的隐私数据进行保护的倾向。

假设 $PP=(x_1,\cdots,x_i,\cdots,x_n)$ 是用户的隐私偏好，$i(i=1,2,\cdots,n)$ 表示用户的隐私信息，$x_i(x_i\in X)$ 表示用户根据自身对隐私信息的保护需求而对隐私信息的主观评价值。

为了清晰地阐述用户隐私信息的主观评价，本文以一个病例表为例进行解释，如表 1 所列。假定病例中的 5 组属性分别为姓名、性别、身份证号、地址、病症，根据患者的信息保护需求对不同的信息有不同的评价值。

表 1 患者的隐私偏好

Table 1 Privacy preference of patients

ID	姓名	性别	身份证号	地址	病症
1	3	2	5	3	3
2	8	6	8	8	8
3	5	3	4	4	5

定义 4(隐私偏好度) 为了便于在隐私保护过程中定量地分析用户隐私信息的偏好,需要对用户的隐私偏好进行量化,用于表示用户对隐私信息的重视程度,称为隐私偏好度,记为 DPP。对于用户的任意隐私信息 $\forall i\in I$,隐私偏好可函数化表示为 $r:I\times X\rightarrow R^{+}$,$r(i,x_i)=w_i$,$w_i$ 表示用户对隐私信息 i 的重视程度。

$W_{DPP}=(w_1,\cdots,w_2,\cdots,w_n)(i=1,2,\cdots,n)$表示隐私偏好度的集合,其中 w_i 为[0,1]区间中的一个数值。

根据用户的自身需要设置对隐私信息的评价,本文通过统计标准差标准化方法对用户的隐私信息偏好进行标准化处理,具体的隐私偏好标准化表达式如下:

$$r(i,x_i)=\frac{x_i-(x_j)\min}{(x_j)_{\max}-(x_j)_{\min}},w_i\in[0,1] \tag{1}$$

隐私偏好度反映了数据拥有者基于自身的主观意向要求对其隐私数据进行保护的倾向程度,是决定服务提供者博弈策略的一个关键参数,可以由用户根据自身对隐私泄露的要求或敏感程度而设定,取值范围为[0,1]。隐私偏好度越大,表示用户对该数据的隐私保护需求越高;隐私偏好度越小,表示用户对该数据的隐私保护需求越低。根据用户对自身隐私数据进行保护的倾向程度,本文将用户的隐私偏好分为 3 个等级:高、中、低。等级的划分可以根据用户对隐私数据保护的主观要求进行实时动态的设置,等级划分的关系如下:

$$DPP=\begin{cases}(0,0.3)\in R\\ [0.3,0.7]\in Z\\ (0.7,1)\in Q\end{cases} \tag{2}$$

其中,R 表示弱隐私偏好,Z 表示中隐私偏好,Q 表示强隐私偏好。不同等级的隐私偏好代表用户对隐私数据保护强度的需求,隐私偏好度越大,用户对自身的隐私信息的保护需求就越高。当 $DPP=0$ 时,说明用户对自身信息的泄露并无需求,即信息的泄露对用户并未产生影响;当 $DPP=1$ 时,说明用户对自身信息的保护需求最大,即用户不希望信息被泄露。

3.2 博弈模型的建立

根据用户对自身隐私信息的保护倾向,可以了解不同的用户对隐私信息有着不同的隐私偏好,并且不同的隐私偏好表示用户对隐私保护的需求不同,因此博弈策略的选择会受隐私偏好的影响。本文基于用户的偏好来构建隐私保护的博弈模型。

隐私保护的博弈模型是一个五元组$[P,I_S,I_A,U_S,U_A]$。

1)P 是参加博弈的局中人集合,文中博弈的参与者为隐私服务的提供者 S 与隐私服务的攻击者 A,即 $P=\{S,A\}$。本文假设参与者都是理性的,并且其都在追求各自利益的最大化。

2)I_S 是服务提供者的策略集合,隐私服务提供者的策略分别是隐私服务提供者的“提供服务”或“不提供服务”,表示为$\{O,NO\}$;用户的隐私偏好影响着隐私服务提供者的策略选择,用户的隐私偏好度越高,在攻击者发起攻击时,隐私服务提供者提供服务的等级可能就越低。本文将服务提供者提供服务的策略详细划分为高级服务、中等服务、低级服务,分别表示为 QO,ZO 和 RO。

3)I_A 是隐私攻击者的策略集合,攻击者的策略分别为“善意攻击”或“恶意攻击”。隐私攻击者的策略表示为$\{W,M\}$。

4)U_S 是服务提供者根据用户的隐私偏好与攻击者进行博弈时选择不同策略所对应的收益集合。

5)U_A 是攻击者与服务提供者博弈时在不同策略下所对应的收益集合。

图 1 给出了本文基于隐私偏好的隐私保护博弈模型的框架。

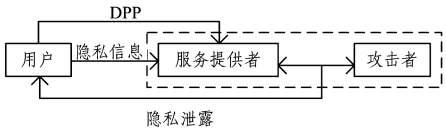

图 1 基于隐私偏好的隐私保护博弈模型

Fig. 1 Game model of privacy protection based on privacy preference

3.3 基于博弈论的隐私保护模型的博弈分析

根据用户隐私偏好的分析以及隐私服务提供者与攻击者的博弈模型,本文对博弈的过程进行具体的分析。

表 2 列出了服务提供者与攻击者的效用。服务提供者的策略是根据用户的隐私偏好而进行偏向选择的,用户根据自身隐私保护需求设置不同的隐私偏好,隐私偏好度比较大,说明用户的隐私保护需求比较高,从而在攻击者访问期间,服务提供者选择提供低级服务的可能性就越大。

表 2 服务提供者与攻击者的效用矩阵

Table 2 Utility matrix of service providers and attackers

	服务提供者	
攻击者	$QO/ZO/RO$	NO
W	$(a_1,b_1)/(a_2,c_1)/(a_3,d_1)$	$(-e,0)$
M	$(f_1,b_2)/(f_2,c_2)/(f_3,d_2)$	$(-g,0)$

$\{W,QO/ZO/RO\}$表示攻击者选择善意攻击而服务提供者选择提供高级服务、中等服务或者低级服务时的策略组合。$(a_1,b_1)/(a_2,c_1)/(a_3,d_1)$是服务提供者在选择不同策略时与攻击者的收益,其中 $a_1\geqslant a_2\geqslant a_3$。

$\{W,NO\}$表示攻击者选择善意攻击而服务提供者选择不提供服务时的策略组合。$(-e,0)$是在该策略组合下两者的收益,$-e$ 是攻击者受到的损失,服务提供者在不提供服务的情况下没有获利也没有损失。

$\{M,QO/ZO/RO\}$表示攻击者选择恶意攻击而服务提供者提供高级服务、中等服务或者低级服务时的策略组合。$(f_1,b_2)/(f_2,c_2)/(f_3,d_2)$是服务提供者在选择不同策略时与攻击者的收益,其中 $f_1\geqslant f_2\geqslant f_3$。由于善意攻击比恶意攻击的强度弱,并且能够带来的收益多于损失,因此 $b_1\geqslant 0\geqslant b_2$,$c_1\geqslant 0\geqslant c_2$,$d_1\geqslant 0\geqslant d_2$。

$\{M,NO\}$表示攻击者选择恶意攻击而服务提供者选择不提供服务时的策略组合。$(-g,0)$是在这个组合下两者的收

益，$-g$ 是攻击者受到的损失，而服务提供者在不提供服务的情况下没有获利也没有损失。

根据博弈双方的效用矩阵，可以计算双方的混合策略纳什均衡。假设服务提供者选择提供服务与不提供服务的概率分别为 p 和 $1-p$，攻击者选择善意攻击与恶意攻击的概率分别为 q 和 $1-q$。

当用户的隐私偏好为 Q 时，服务提供者提供的策略为 RO 或者 NO，那么攻击者选择善意攻击的期望效用为：

$$U_{A_1}=a_3p_R+(-e)(1-p_R) \tag{3}$$

攻击者选择恶意攻击的期望效用为：

$$U_{A_2}=f_3p_R+(-g)(1-p_R) \tag{4}$$

如果混合战略是攻击者的最优选择，则意味着攻击者在善意攻击与恶意攻击之间是无差异的，即：

$$U_{A_1}=U_{A_2} \tag{5}$$

$$a_3p_R+(-e)(1-p_R)=f_3p_R+(-g)(1-p_R) \tag{6}$$

通过计算可得：

$$p_R=\frac{e-g}{a_3-f_3+e-g} \tag{7}$$

同理，可以得到用户的隐私偏好为 Z 和 R 时，服务提供者提供服务的概率分别为：

$$p_Z=\frac{e-g}{a_2-f_2+e-g},p_Q=\frac{e-g}{a_1-f_1+e-g} \tag{8}$$

根据用户的隐私偏好，当攻击者进行恶意攻击与善意攻击时，若用户的隐私偏好为 Q 等级，则服务提供者提供服务和不提供服务的期望效用分别为：

$$U_{S_1}=d_1q_R+d_2(1-q_R) \tag{9}$$

$$U_{S_2}=0 \tag{10}$$

通过计算可得：

$$q_R=\frac{-d_2}{d_1-d_2} \tag{11}$$

同理，可以得到用户的隐私偏好为 Z 和 R 时，攻击者进行善意攻击的概率分别为：

$$q_Z=\frac{-c_2}{c_1-c_2},q_Q=\frac{-b_1}{b_1-b_2} \tag{12}$$

因此，根据用户的隐私偏好，可以得到在不同偏好下，服务提供者与攻击者的混合策略纳什均衡分别为：

$$\begin{aligned}&p_R=\frac{e-g}{a_3-f_3+e-g},q_R=\frac{-d_2}{d_1-d_2}\\&p_Z=\frac{e-g}{a_2-f_2+e-g},q_Z=\frac{-c_2}{c_1-c_2}\\&p_Q=\frac{e-g}{a_1-f_1+e-g},q_Q=\frac{-b_1}{b_1-b_2}\end{aligned} \tag{13}$$

3.4　隐私度量

用户根据自身的需要设置隐私信息的偏好，服务提供者将根据用户的隐私偏好为攻击者提供服务。在博弈的过程中，双方都在争取各自利益的最大化，根据两者的效用矩阵虽然可以计算得到混合策略纳什均衡，但是并不能得知此时用户的隐私泄露情况。本文基于提供者与攻击者博弈，运用策略熵来度量用户的隐私泄露量。

$$H=-P_i\log P_i-(1-P_i)\log(1-P_i) \tag{14}$$

其中，i 表示用户的隐私偏好等级为 Q，Z 或者 R 的情况；p 表示混合策略纳什均衡中服务提供者提供服务的概率，$1-p$ 是其不提供服务的概率；H 表示在混合策略纳什均衡中服务提供者的隐私泄露量。

本文分析的是一次博弈模型；如果攻击者进行多次攻击并在有限次之后停止，那么服务提供者与攻击者进行 $T=1,2,\cdots,n$ 次有限重复博弈时，服务提供者与攻击者的每次博弈都将根据混合策略纳什均衡选择最优策略，因此有限博弈与一次博弈相同。但是，由于攻击者需要的隐私信息不同，用户的隐私偏好不同，最后求得的混合策略纳什均衡也不同，因此有限重复博弈下用户的隐私泄露量为：

$$H=-\sum_T(P_i^T\log P_i^T+(1-P_i^T)\log(1-P_i^T)) \tag{15}$$

4　实例分析

个人隐私保护中，医疗数据的隐私泄露尤为严重，因此在本文隐私保护博弈模型的基础上提出一个在访问控制中攻击者访问医疗数据的实例。实例中，博弈双方为医生和医疗数据的隐私保护平台，攻击者用符号 A 表示；医疗数据的隐私保护平台即为隐私服务提供者，用符号 S 表示；攻击者的策略为善意访问和恶意访问，用符号 W 和 M 表示；隐私服务提供者的策略为允许访问和拒绝访问，用符号 O 和 NO 表示。

病人将自己的信息存储到隐私保护平台，并根据自身对隐私数据的保护需求对隐私数据设置隐私偏好，攻击者在对数据进行访问时，服务提供者会根据病人的隐私偏好对攻击者分配访问权限，即攻击者也可以进行不同等级的访问。

通过对医院 50 名病人的调查，实验选取了其中 3 名患者对隐私信息的偏好数据，病人对自身的隐私偏好如表 3 所列。

表 3　患者的隐私偏好度

Table 3　Privacy preference grade of patients

ID	姓名	性别	身份证号	地址	病症
1	0	1	0.5	0.5	0.5
2	0.5	0	1	0.5	0
3	0.67	0	0.5	0	1

攻击者对用户的信息拥有访问权限，服务提供者的策略分为提供服务和不提供服务。当攻击者访问 $ID=1$ 的用户的姓名时，由于被访问的数据是弱隐私偏好，服务提供方在允许提供服务的情况下将为攻击者提供强隐私服务；当攻击者访问 $ID=2$ 的用户的身份证号时，由于被访问的数据是强隐私偏好，服务提供方在允许提供服务的情况下将为攻击者提供弱隐私服务；当攻击者访问 $ID=3$ 的用户的姓名时，服务提供方在允许提供服务的情况下将为攻击者提供中等隐私服务。

当攻击者访问的数据是强隐私偏好时，可以得到服务提供者与攻击者的博弈效用矩阵，如表 4 所列。

表 4　服务提供者与攻击者的博弈效用矩阵

Table 4　Game utility matrix of service providers and attackers

	服务提供者	
攻击者	*RO*	*NO*
W	(5,2)	(−2,0)
M	(7,−2)	(−3,0)

由于攻击者访问的是用户的强隐私偏好数据，服务提供者的策略为选择提供服务或者不提供服务，如果服务提供者选择提供服务时，将为攻击者提供弱隐私服务。因此，根据博弈双方的效用矩阵，可以计算得到 $p=33\%$，$q=50\%$，即服务提供者有 0.33 的概率选择提供弱隐私服务，攻击者有 0.5 的概率选择善意攻击的策略。那么，最终服务提供者通过服务策略泄露的隐私量为 0.636。

在服务提供者与攻击者进行有限次的博弈时，每次博弈过程双方都会选择基于混合策略的最优策略，若攻击者每次要访问的信息不同，则用户的隐私偏好将不同，产生的混合策略也不同，从而每次博弈的隐私泄露量也是不同的。

结束语 本文提出了一种基于隐私偏好的隐私保护博弈模型，对用户的隐私偏好进行定义并提出量化方法，基于用户的隐私偏好分析服务提供者在博弈过程中对策略的选择，并运用策略熵度量在博弈过程中用户的隐私泄露量。本文首先基于完全静态博弈构建隐私保护的博弈模型，实现隐私与服务之间的平衡，有效地保护了用户的隐私信息；其次，考虑了用户的隐私偏好对隐私信息泄露的影响，并采用标准化方法量化用户的隐私偏好，以有效地帮助用户精确地表达用户的隐私偏好；最后，根据博弈模型求得在用户隐私偏好的影响下博弈双方的混合策略纳什均衡以及度量用户的隐私泄露量，能够全面地考虑用户的主观感受对隐私泄露的影响。因此，在下一步研究中，通过构建隐私保护的贝叶斯博弈模型，将考虑攻击者的背景知识对隐私信息泄露的影响，并对攻击者的背景知识进行量化，基于信息熵对隐私泄露进行度量。

参 考 文 献

[1] SHANNON C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1948, 27(3): 379-423.

[2] DÍAZ C, SEYS S, CLAESSENS J, et al. Towards Measuring Anonymity[C]// International Conference on Privacy Enhancing Technologies. Springer-Verlag, 2002: 54-68.

[3] MA Z, KARGL F, WEBER M. Measuring location privacy in V2X communication systems with accumulated information[C]// IEEE International Conference on Mobile Adhoc and Sensor Systems. IEEE, 2009: 322-331.

[4] CHEN X, PANG J. Measuring query privacy in location-based services[C]// ACM Conference on Data and Application Security and Privacy. ACM, 2012: 49-60.

[5] YANG Y, LUTES J, LI F, et al. Stalking online: On user privacy in social networks[C]// ACM Conference on Data and Application Security and Privacy. ACM, 2012: 37-48.

[6] ZHANG X J, GUI X L, FENG Z C, et al. A Quantifying Framework of Query Privacy in Location-Based Service[J]. Journal of Xi'an Jiaotong University, 2014, 48(2): 8-13. (in Chinese)
张学军，桂小林，冯志超，等. 位置服务中的查询隐私度量框架研究[J]. 西安交通大学学报，2014，48(2)：8-13.

[7] PENG C G, DING H F, ZHU Y J, et al. Information Entropy Models and Privacy Metrics for Privacy Protection[J]. Journal of Software, 2016, 27(8): 1891-1903. (in Chinese)
彭长根，丁红发，朱义杰，等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报，2016，27(8)：1891-1903.

[8] LIU D, BAGH A. New Privacy-Preserving Ascending Auction for Assignment Problems[J/OL]. http://dx.doi.org/10.2139/ssrn.2883867.

[9] DWORK C. Differential privacy[J]. Lecture Notes in Computer Science, 2006, 26(2): 1-12.

[10] VADHAN S. The Complexity of Differential Privacy[J/OL]. http://doi.org/10.1007/978-3-319-57048-8-7.

[11] CHATZIKOKOLAKIS K, PALAMIDESSI C, STRONATI M. Constructing elastic distinguish ability metrics for location privacy[J]. Proceedings on Privacy Enhancing Technologies, 2015, 2015(2): 156-170.

[12] LIU H, KRISHNAMACHARI B, ANNAVARAM M. Game theoretic approach to location sharing with privacy in a community-based mobile safety application[C]// Proceedings of the 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems. ACM, 2008: 229-238.

[13] HUMBERT M, MANSHAEI M H, FREUDIGER J, et al. Tracking Games in Mobile Networks[C]// International Conference on Decision & Game Theory for Security. Springer-Verlag, 2010: 595-599.

[14] CHORPPATH A K, ALPCAN T. Trading privacy with incentives in mobile commerce: A game theoretic approach[J]. Pervasive & Mobile Computing, 2013, 9(4): 598-612.

[15] ZHOU D D, LI W W, SUN Y Q. Survey on Game Theory Based Privacy Protection[J]. Journal of Chinese Computer Systems, 2015, 36(12): 2696-2700. (in Chinese)
周丹丹，李威伟，孙宇清. 博弈论隐私保护方法研究综述[J]. 小型微型计算机系统，2015，36(12)：2696-2700.

[16] XU L, JIANG C, WANG J, et al. Game theoretic data privacy preservation: Equilibrium and pricing[C]// IEEE International Conference on Communications. IEEE, 2015: 7071-7076.

[17] ZHANG Y X, HE J S, ZHAO B, et al. A Privacy Protection Model Base on Game Theory[J]. Chinese Journal of Computers, 2016, 39(3): 615-627. (in Chinese)
张伊璇，何泾沙，赵斌，等. 一个基于博弈理论的隐私保护模型[J]. 计算机学报，2016，39(3)：615-627.

[18] PANAOUSIS E, LASZKA A, POHL J, et al. Game-Theoretic Model of Incentivizing Privacy-Aware Users to Consent to Location Tracking[C]// IEEE Computer Society. 2016: 1006-1013.

[19] WU X, DOU W, NI Q. Game theory based privacy preserving analysis in correlated data publication[C]// Australasian Computer Science Week Multiconference. ACM, 2017: 73.

[20] YUAN M, CHEN L, YU P S. Personalized privacy protection in social networks[J]. Proceedings of the Vldb Endowment, 2010, 4(2): 141-150.

[21] GUO M, LIU Z, WANG H B. Personalized Privacy Preserving Approaches for Multiple Sensitive Attributes in Data Publishing [J/OL]. https://doi.org/10.12783/dtetr/ssme-ist2016/3965.

[22] FUDENBERG D, TIROLE J. Game Theory[J]. Mit Press Books, 2010, 1(7): 841-846.