博弈论隐私保护方法研究综述

周丹丹,李威伟,孙宇清

(山东大学 计算机科学与技术学院 数字媒体教育部研究中心,济南 250101)
E-mail:sun_yuqing@sdu.edu.cn

摘 要: 概述博弈论在隐私保护方面的理论、方法和应用,分别针对4种典型的隐私保护问题给出博弈论解决方案,分析隐私保护涉及的参与方、各方行动规则和策略选择、隐私量化方法、以及满足各方利益最大化的纳什均衡求解方法,在纳什均衡求解过程中,分析用户和敌手间策略和多用户间不同隐私保护策略对隐私保护方案的影响;总结对比了现有隐私保护问题所涉及的博弈论模型和相应的纳什均衡求解方法,以及博弈论在解决隐私保护问题时面临的挑战,最后讨论了移动应用和云存储等领域的博弈论隐私保护研究和应用方向.

关 键 词: 隐私保护;博弈模型;纳什均衡;策略
中图分类号: TP391 **文献标识码**:A **文 章 编 号**:1000-1220(2015)12-2696-05

Survey on Game Theory Based Privacy Protection

ZHOU Dan-dan,LI Wei-wei,SUN Yu-qing
(School of Computer Science and Technology,Shandong University,Jinan 250101,China)

Abstract:Game theory is emerging as an important method to tackle the privacy problems. This paper surveys the theories,methods and applications on how game theory is applied in privacy protection. Four representative types of problems are discussed and the game based solutions are presented. Facing each problem,we focus on how to determine game players,how to choose strategies and what action rules are set in each privacy problem. The methods of privacy quantification and Nash equilibrium calculation are also narrated. Specially,we discuss how the strategies of different users influence the protection solution,besides the traditional consideration of two sides,user and adversary. We analyze the innate characters of each type of problem and the relationship with the corresponding game model. Some detailed comparisons are also made about Nash Equilibrium solving in different privacy solutions. The challenges in applying game theory in privacy protection are presented,as well as some open problems. Finally,this paper discusses several future directions in some emerging application areas,such as mobile computing,big data analytics and cloud storage applications.

Key words:privacy protection;game model;nash equilibrium;strategy

1 引 言

隐私保护是近年来引起广泛关注的热点问题,它涉及诸多参与方,如用户、服务提供商、恶意隐私获取者等,他们既具有合作又具有竞争关系,每个参与方均具有最大化自我利益的动机. 例如基于手机定位的导航服务,用户必须提供自身地理位置信息来获得导航服务,而敌手却能够通过用户地理位置信息推测出用户隐私信息来获取利益. 用户和服务提供方、敌手之间的关系,客观上符合博弈论模型中参与者之间的博弈关系,采用博弈论方法解决隐私保护问题成为一种新的研究手段. 不同于传统的隐私保护方法,基于博弈论的隐私保护方法通过机制设计,描述参与方的收益和代价,模拟他们的理性选择过程,通过分析博弈均衡找到各方的最佳解决方案.

博弈模型有三个基本组成部分:参与者,策略和收益[3,4]. 参与者指参与博弈的理性决策主体,他们以最大化自身利益为目标,制定相关行动策略;每个参与者都有自己的策略集合,每一次博弈只能选择其中一个策略,所有参与者选择的策略构成策略组合;在特定策略组合下参与者所获得的利益称为收益,采用效用函数计算. 在博弈过程中,一个策略组合称为最优解的条件是没有一个参与者通过独自改变策略而增加收益,此策略组合称为纳什均衡. 博弈论主要研究具有竞争性质的参与主体之间的策略选择,对个体行为进行分析和预测. 基于博弈论的隐私保护方法的关键在于将用户隐私需求和环境因素描述成博弈论的对应因素,即分析具有竞争关系的参与方、各方策略、需求和收益;并通过结构化方法找到纳什均衡点.

博弈论在安全、隐私和无线网络等领域有许多应用[6-8,21-23],本文将综述这些成果,分析基于博弈理论的隐私问题建模方法,介绍面向竞争性目标的策略选择方案和纳什均衡求解过程,最后讨论博弈论解决隐私问题面临的挑战,论述研究发展方向.

2 基于斯塔克伯格博弈模型的隐私保护方法

在许多应用中,参与方的行为具有跟随关系,首先制定策略的一方为领导者,通过观察对方策略来制定对策的另一方为跟随者,双方以实现自身利益最大化为目的,即为斯塔克伯

收稿日期:2014-09-28 收修改稿日期:2014-11-25 基金项目:国家自然科学基金项目(61173140)资助;山东省科技发展计划项目(2014GGX101046)资助;山东省自主创新及成果转化专项(2014ZZCX03301)资助. 作者简介:**周丹丹**,女,1989 年生,硕士研究生,研究方向为隐私保护;**李威伟**,男,1990 年生,硕士研究生,研究方向为隐私保护;**孙宇清**(通信作者),女,1967 年生,博士,教授,研究方向为系统安全与隐私保护.

格博弈,如物理层安全[10]、隐私泄漏[1]和隐私投资[9]等. 下面通过位置隐私保护问题[24,25]和服务商在保护顾客隐私安全方面进行投资问题,给出基于斯塔克伯格博弈模型的隐私保护方案.

2.1 位置隐私保护问题

在基于地理信息的应用中,用户需要提交位置信息以获取服务,同时选择模糊化地理位置等方法保护位置隐私,但是模糊化会降低获得的服务质量,因此隐私保护和基于位置的服务的质量是矛盾关系;同时,敌手依据用户采用的隐私保护方法制定相应对策,通过观察用户的模糊地理位置猜测其真实位置.

Shokri 等人将零和贝叶斯斯塔克伯格博弈用于位置隐私保护[18],参与方为用户、服务提供商和敌手,整个隐私保护框架如图 1 所示. 用户首先制定隐私策略,目标是在确保一定服务质量前提下设定合理的隐私保护机制以降低敌手猜测的准确度;敌手随后执行攻击机制,目标是设定合适的猜测机制以提高攻击的准确度. 敌手获得的隐私信息即为用户损失,且敌手获得的用户位置信息是不确定的,所以此博弈模型属于零和贝叶斯博弈.

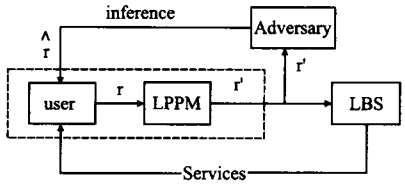

图 1　位置隐私保护框架

Fig. 1　Location privacy protection framework

用户使用位置隐私保护机制 LPPM(Location Privacy Protection Mechanism),以一定的概率分布 $\varphi(r)$ 选择不同的地理位置 r′以替代真实位置 r,或是将真实位置模糊化为 r′,表示成 fake $(r' \mid r)$,然后发给位置服务提供方以获得相关服务. 敌手则制定猜测机制,通过观察到的模糊化位置 r′来推测用户位置 $\hat{r}$,敌手的策略表示为 $hit(\hat{r} \mid r')$. 在此博弈中,用户的博弈效用函数为 $\text{Privacy}(\varphi, \text{false}, \text{hit}, d_p) = \sum_{\hat{r},r',r} \varphi(r) fake(r' \mid r) hit(\hat{r} \mid r) d_p(\hat{r}, r)$,其中 $d_p(\hat{r},r)$ 表示量化后的用户隐私需求. 用户隐私效用即为在用户策略和敌手策略已知的情况下,敌手推测用户位置对于用户真实位置隐私的影响.

用户的目标是最大化用户隐私,而敌手的目标是最小化用户隐私,纳什均衡求解就是在考虑对方最佳选择的基础上计算自身得益. 因此,用户的隐私期望得益为公式(1)所示.

$$\sum_{r'} \Pr(r') \min_{\hat{r}} \sum_{r} \Pr(r \mid r') d_p(\hat{r}, r) = \sum_{r'} \min_{\hat{r}} \sum_{r} \varphi(r) fake(r' \mid r) d_p(\hat{r}, r) \quad (1)$$

敌手在考虑用户的最佳策略后的期望得益为公式(2)所示:

$$\sum_{r} \varphi(r) \max_{\hat{r}} \sum_{\hat{r}} \text{hit}(\hat{r} \mid r') d_p(\hat{r}, r) \quad (2)$$

故博弈纳什均衡点为多约束条件下的最优解,求解过程可以将此问题规约到解线性规划问题,分别得到用户的最优隐私保护机制和敌手的最佳推测攻击[18].

2.2 服务提供商对保护顾客隐私信息的投资决策问题

在许多互联网应用中,服务提供方通常会向用户索取个人信息,作为回报,提供更好的个性化服务或者提供商品价格折扣. 如果服务提供方有意或者无意泄露用户数据,将会对用户带来损失,降低用户对服务商的信任. 虽然服务商可以在信息安全方面增加投资以降低用户隐私的泄漏风险,但是服务商在没有明确利益回报的前提下,没有动机进行投资. D'Acquisto 等人提出了损害共担策略,采用斯塔克伯格博弈模型进行解决[1],使得服务商明确一旦泄露用户隐私则需要承担一定损失. 博弈策略分别为:顾客控制提交的个人信息,服务提供商控制隐私安全投资. 博弈目标为:顾客提供最少量隐私以获得个性化服务,服务商最少投资 L^* 情况下承担最少损失,用户的损失表示为 L^*,博弈过程即为在同时最大化自身得益的策略下,寻找顾客与服务提供商的纳什均衡策略 (L^*, L^*).

起初顾客和服务提供商有对应的需求曲线,即 $\frac{q}{q^*} + \frac{p}{p^*} = 1$,其中 q 是商家实际提供的服务(量化值),p 是顾客购买价格,q^* 是商家可以提供服务的最大数量,p^* 是客户可以承受(愿意支付)的最高价格. 在顾客提供隐私后,服务提供商可以为顾客提供更多的服务,q^* 变为 $q^*(1+\alpha)$,需求曲线相应变为 $\frac{q}{q^*(1+\alpha)} + \frac{p}{p^*} = 1$,其中 α 是边际需求因素,并与商家获得的用户隐私信息量有关,α_{max} 是 α 的上限. 模型的关键是引入商家承担损失的比例参数 η,η 示隐私泄漏后服务提供商承担金钱损失的比率,$1-\eta$ 表示隐私泄漏后顾客承担的金钱损失的比率,所以顾客和提供商承担的损失分别为 $(1-\eta)LP_{db}$ 和 ηLP_{db},其中 L 指用户隐私信息泄漏带来的损失. P_{db} 表示数据泄漏的概率. 因此,顾客的博弈效用函数为公式(3)所示:

$$S_c = \frac{(p^* - \hat{p})^2}{2p^*} q^* \left[1 + \alpha_{max} \left(\frac{L}{L_{max}}\right)^{v}\right] - (1-\eta) LP_{db} \quad (3)$$

其中,L_{max} 是 L 的上限,$\hat{p}$ 是单位价格,v 为隐私参数,v 值越小顾客提供越少隐私就能获取更好服务. 公式的前一部分表示顾客因提供个人信息而获得的收益,后一部分表示用户承担的数据泄露带来的损失. 服务提供商的效用函数为公式(4)所示:

$$S_{sp} = \frac{p^* - \hat{p}}{p^*} q^* \left[1 + \alpha_{max} \left(\frac{L}{L_{max}}\right)^{v}\right] (\hat{p} - \hat{c}) - I - \eta LP_{db} \quad (4)$$

其中,$\hat{c}$ 是单位成本,I 为服务提供商投资隐私的成本. 因此公式的第一部分为服务提供商销售服务的收益,第二部分为安全投资,第三部分表示用户承担的数据泄露带来的损失. 通过对上述公式求偏导数,可以求解其纳什均衡 $(X^* = L^* / L_{max}, Y^* = I^* / I_{max})$.

3 基于扩展博弈模型的隐私保护方法

在许多应用中,参与者的行动存在先后次序和连续性,竞争双方的目的是实现自己利益的最大化,如短暂链接网络的结点撤销机制[12]和防止内部人员攻击的授权模型等[13]. 这类问题适合采用扩展博弈模型. 下面通过无线自组织网络中的信任和隐私权衡问题和普适计算环境下的身份暴露问题,给出详细解决方案.

3.1 无线自组织网络中的信任和隐私权衡问题

在无线自组织网络中,结点之间能够相互通信,依据其发送

信息的真假结点被分为两类:良性结点和恶意结点. Raya[19]等人采用动态贝叶斯博弈来解决无线自组织网络中的结点信任和隐私权衡问题. 通过对结点发出的消息进行投票,可将恶性结点移除. 为了对一个结点发送消息的可信性进行评估,其他结点需要参与投票,而在投票过程中会泄露自身的隐私如身份信息和位置信息,做出的投票贡献越大,结点隐私泄漏越多. 这里假设每个结点都是理性的,即期望以泄漏最少隐私信息换取相应的服务,则会出现搭便车问题,即不做贡献坐享渔利. 如果所有结点搭便车,那么无法判定消息可信性以去除恶意结点. 所以,在贡献和隐私方面,每个结点与其他结点进行博弈. 每一次投票称为一个阶段,每个结点有多次投票机会,此博弈具有连续性,并且在博弈过程中博弈参与方对其他参与方的信息不完全掌握,所以作者采用连续贝叶斯博弈模型来解决这个问题. 作者分别用宏观博弈 G_{AD} 和微观博弈 G_{TC} 对问题进行描述.

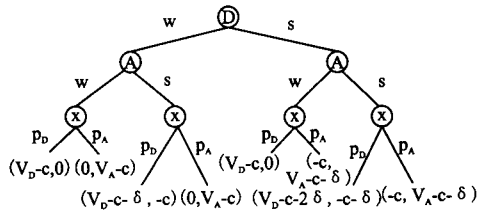

图 2 扩展博弈树

Fig. 2 Extended game tree

宏观博弈 G_{AD} 是指从全局角度考虑所有参与结点的行为,博弈参与者整体上分为攻击者 A 和防守者 D,即 P = {A, D}. 在每一轮投票中,他们具有相同的策略,投票 S(泄露隐私信息)或是等待 W,即 $S_A = S_D$ = {W,S}. 文中设定防守者首先决策,然后攻击者再决策,双方轮流做决定,直到达到博弈的截止时间. 博弈的目标是通过投票将恶意结点去除. v_A 和 v_D 分别表示当攻击者或者防守者赢得博弈时的收益. p_D、p_A 分别表示最后阶段博弈双方赢得博弈的概率(与每一方的结点数量相关),其中 $p_D + p_A = 1$. 扩展博弈树如图 2 所示,结点表示参与方,分支代表参与方的策略,叶子结点表示相应策略组合下博弈双方的效用,其中左边为首先决策的参与方效用,右边是第二个决策参与方的效用,c 表示达到信任等级所泄露的最小隐私信息量. 在博弈过程中,恶意结点也会参与投票以增加自己的信任值,良性结点为了超过恶意结点的信任等级,需要参与投票,δ 表示此博弈过程中增加的隐私泄露. 通过博弈树分析看出,攻击者的最佳策略总是 W,防守者其最佳反映策略总是 W,也就是双方一直等待直到博弈的最后阶段,并依靠他们获胜的概率来赢得博弈. 故只有在截止时间信息验证结点 V 才能决定,这并不是理想的结果. 为了鼓励参与方更早投票,作者引入回报 r,当 r≥c + δ 时,策略组合(S,S)即为新的纳什均衡.

微观博弈 G_{TC} 考虑多个良性结点的行为,最大化良性结点的整体利益. 设有 K 个良性结点. 每个参与者 k 的信任等级为 $t_k \leqslant 1$,通过贡献信息获得;ϕ 表示提供信息量到信任值的转换因子. 每个参与方的效用函数为公式(5)所示,即每个良性结点分得的共同收益减去其泄露的隐私信息.

$$\pi_k(t_1,t_2,\cdots,t_K) = \frac{v_\rho}{K} - \frac{t_k}{\phi} \tag{5}$$

通过分析 G_{TC} 的子博弈完美均衡得出每个参与个体的最佳策略为 $t_k^* = 0$. 由于这一结果并不理想,作者通过回报 r 鼓励参与方更早投票,每个结点得益为公式(6):

$$\pi_k(t_1,t_2,\cdots,t_K) = \frac{v_D}{K} + \frac{t_k}{\sum_{i=1}^{K} t_i} - \frac{t_k}{\phi} \tag{6}$$

此时,参与者的最佳策略为 $t_k^* = \dfrac{\phi r(K-1)}{K^2}$.

3.2 普适计算环境下的身份暴露问题

在普适计算环境下用户与服务提供商交易过程中容易泄漏隐私信息,用户可以使用分层身份模型更好的保护自身隐私. 基于层次的身份模型是将个人身份信息组织成一棵树,从根结点到叶结点,每项信息逐渐细化. 越靠近根结点,身份信息越泛化,代表的具有此信息的人数越多,泄露这些隐私信息对用户威胁较小;叶结点通常包含非常具体的身份信息,能够标识一个人或很少一组人,泄露这些隐私信息对用户威胁较大.

Zhu 等人[14]使用扩展博弈论方法研究普适计算环境下的身份暴露问题. 在此博弈中,博弈的参与方分别为提供个人信息的用户和索要信息的服务提供商. 用户的策略有三种,分别为不提供信息且终止服务、提供信息并接受服务和协商;服务提供商的策略也有三种,分别为索要信息、终止服务、接受信息并提供服务. 首先由用户根据服务提供商索取的个人信息做决定,只要博弈没有完成或者终止,双方依次轮流做决定,并且扩展博弈在有限轮次内结束. 例如当服务提供商向用户索取信息时,用户若选择协商信息提供策略,则根据分层身份模型寻找最一般化的身份信息集合给服务提供商提出建议. 若服务提供商选择继续协商,则会向用户索取更多信息. 博弈的目标为寻找同时满足用户和服务提供商需求的最优个人信息泄露. 对此扩展博弈树采用逆推法求出子博弈完美纳什均衡,从而得到同时满足用户和服务提供商需求的均衡结果.

4 基于拍卖博弈模型的隐私保护方法

拍卖博弈模型常常解决一对多的竞争服务,例如在互联网交易中一个需求对应多个提供商的情况. 提供商通常向用户索取必要的隐私信息以提供服务,进而处于商业目的,服务商可能索取额外的信息,以便提供进一步个性化服务或是恶意买卖用户信息. 用户处于自身利益考虑,在其他条件相同的情况下,希望选择索取个人信息少的服务商. Bonatti 等人采用拍卖博弈模型来解决这一问题[2],作者用离散化且有偏序关系的个人信息替代传统连续型支付方式(如金钱),通过维克里拍卖博弈模型来解决互联网中用户信息的隐私保护.

博弈参与者为一个用户和 N 个服务提供商. 用户策略 pol_0 是一组等价可替换的策略集合,例如 $pol_0 = \{r_1, r_2, r_3\}$,其中 $r_1 = \{c_1, c_{10}\}$ 代表用户愿意提供的最大个人信息集合,这相当于拍卖过程中拍卖者自身的估价. 商家策略也表示为用户信息项集合,如果信息请求满足用户策略,即用户愿意提供信息的子集,则该请求被用户接受. 例如商家 i 的策略是 $pol_i = \{c_1\}$,$pol_i \subseteq r_1$ 成立,则该请求满足用户要求,反之如果 $pol_i = \{c_1, c_2\}$,故不满足用户要求.

对于每个服务提供商,均有自己的信息需求策略 req_i,$1 \leqslant i \leqslant N$,即服务提供商为完成服务需要的最小信息集合,只有当用户满足基本需求策略 req_i 时,商家才能提供服务. 但是为了获得更多信息,实际索要信息策略为 pol_i,$1 \leqslant i \leqslant N$,相当

于竞拍者的出价,通常情况下 $req_i \subseteq pol_i$. 拍卖的目的:用户选择索取个人信息最少的服务提供商进行交易. 作者采用维克里拍卖求解索取信息最少的服务提供商,用户提供的个人信息量则满足索取次少的服务提供商的出价即可. 通过上述机制,可以使服务提供商之间形成竞争关系,最终促使服务提供商实际出价策略 req_i 跟其实际需求策略 pol_i 相等.

拍卖博弈在信息安全的其他方面也有应用,Reidt 等人利用荷式拍卖的思想解决移动网络中恶意结点的撤销问题[15],通过设计激励策略,使得诚实结点能够尽快移除恶意结点.

5　基于合作博弈模型的隐私保护方法

合作博弈用于解决具有竞争关系的利益相关方,通过策略合作达到利益最大化的过程. 例如在用户注册社交网络时,网站会对用户进行身份验证,并通过验证信息帮助用户推荐好友,但是,网站也可能泄漏用户隐私,因此用户和社交网站是合作竞争关系,同时双方遵守有约束力的协议. Anna 等人采用双人常和博弈模型解决用户在注册社交网络时的身份验证问题[11]. 合作博弈可分为两人讨价还价博弈和多人联盟博弈. 下面以数据发布中的隐私保护问题为例给出基于合作博弈模型的隐私保护解决方案.

在数据发布中经常使用 k-匿名技术来保护个人隐私信息. k-匿名是指在发布的数据中存在至少 k 个准标识符不可区分的记录,使攻击者不能判别出隐私信息所属的特定个体,k 为用户可承受的最大信息泄露风险. 传统的匿名方法事先定义 k,在匿名完成后才能得出信息损失量,如果损失的信息量超出可承受范围,则调整 k 值,重新计算匿名过程,因此造成很大浪费. Srinivasa 等人[16,17]将联盟博弈运用在基于 k-匿名的隐私保护数据发布问题. 其基本思想是,将待发布的数据表中的每一元组视为一个博弈参与方,数据表的划分就是求博弈联盟的过程,目标是使得各个参与方的损失在给定的信息损失门限内. 具体过程为,首先根据数据库中数据值域特征计算 k 的可能取值范围,根据联盟博弈的相关结论[17]得出关系 $2k \leqslant N \leqslant k\prod_{i=1}^{|QID|} L_i$,可得到 k 的取值范围

$$\lceil \frac{N}{\prod_{i=1}^{|QID|} L_i} \rceil \leqslant k \leqslant \lceil \frac{N}{2} \rceil .$$

其中,T 为数据表,QID 表示数据表中准标识符属性集合,如年龄和邮编,QID 中的每一个属性 i 都能用一个概念层次树来表示,L_i 表示属性 i 所对应的概念树的高度. 然后,根据敏感信息的概念树动态泛化,其中根节点为泛化程度越高的信息. 针对每一层对应的取值,计算元组对应的博弈参与方的得益,其效用函数为公式(7)所示:

$$\text{payoff}(t_j / QID) = \prod_{i=1}^{|QID|} \frac{r_{ij}}{L_i}, \forall t_j \in T \qquad (7)$$

r_{ij} 表示属性 j 对应的属性 i 概念树向上泛化的层数. 通过计算每个元组的得益,找出得益相同的元组组合成一个联盟,即为等价类 EQ_j,所有的等价类共同构成数据表的一个等价类划分.

如果当前划分后的信息损失没有达到给定的门限,则继续沿树根方向泛化,并计算每个元组的得益,直到满足门限要求为止. 由于一个元组被泛化到具有相同取值的联盟中,无法识别具体的个体身份,因此匿名后的发布表 T′满足隐私需求. 联盟的得益即为等价类中每个元组得益之和,联盟隐私定义为等价类中所有元组的最小收益. 最后,根据等价类划分结果,求出 k 值,k 即为每个等价类集合大小的最小值,并对数据集进行匿名化处理. 这种方法避免了匿名过程的多次计算.

6　总结与展望

采用博弈论方法解决隐私保护问题,能够综合考虑用户、敌手等多参与方的利益关系,寻求满足多方利益的解决方案,平衡隐私保护和服务质量间关系. 但是运用博弈论解决隐私问题也面临挑战,主要体现在博弈论模型的选取、对用户隐私的量化和纳什均衡点的求解.

量化隐私需求既是一个关键问题,又是一个挑战,其困难在于如何抽取参与方的实际偏好并选择合适模型和收益函数. 通过分析博弈参与方的行为策略,将具体隐私问题的解决形式化描述为博弈的目标. 现有工作对隐私的量化并没有统一的形式. 大部分工作对隐私仅从理论上进行抽象的概括,也有部分工作采用具体数值表示隐私[16-18].

表 1　隐私保护问题和博弈模型

Table 1　Privacy protection classification and game model

参与方数量	问题类型	博弈参与方	博弈模型	均衡求解方法
1:1	位置隐私保护问题[18]	用户 位置窃取者,	零和贝叶斯斯塔克伯格博弈	多约束条件下线性规划求解
	服务提供商隐私投资问题[1]		双人博弈	占优均衡
	普适计算环境下信息提供[14]	用户,服务提供方	扩展博弈	逆推法求子博弈完美均衡
	社交网站身份验证问题[11]		双人常和博弈讨价还价模型	重复剔除严格劣策略、约束最优化方法
1:n	面向网络服务的用户隐私保护[2]	用户,服务提供方	维克里拍卖模型	占优均衡
	数据发布中隐私保护[16,17]	数据表中的每个元组	联盟博弈	重复剔除严格劣策略、约束最优化方法
m:n	无线自组织网络中的信任和隐私[19]	参与结点	动态贝叶斯博弈	占优均衡

隐私保护中博弈参与方通常为用户和敌手,他们之间具有合作、对抗或者同时具备多种关系,博弈参与方的数量、相互关系以及博弈目的影响博弈模型的选择. 根据博弈策略空间的大小,可以将策略分为有限策略和无限策略. 有限策略通常表示为离散集合的形式,而无限策略用连续变量来表示. 博弈目标是指博弈参与方想要到达的期望,它与博弈策略密切相关. 为了达到博弈目标即纳什均衡,需要利用恰当的均衡分析方法求解隐私博弈,即使博弈中只有两个参与人,也很难在多项式时间求解纳什均衡. 虽然不同的博弈模型有不同的均衡求解方法,但是也有共性之处,如斯塔克伯格博弈模型通常

采用占优均衡和线性规划的方法,扩展博弈通常采用逆推法等.本文归纳了不同博弈模型的均衡求解方法见上页表 1,同时总结了博弈参与方和博弈模型的关系,旨在为面向不同隐私问题选择博弈模型和纳什均衡求解提供借鉴.这一工作尤其适合于具有利益冲突关系的隐私保护问题.下面给出两个代表性应用讨论.

在移动计算方面,无线网络运营商和无线应用提供商经常过多地索取用户的隐私信息,并且可能在服务过程中非法使用用户隐私.在这类问题中,用户和服务提供方具有多对多的合作竞争关系,因此适合使用博弈论模型进行隐私保护.例如:商家在提供免费 WIFI 的同时索要用户个人信息,用户也有不同的网络带宽需求,而且用户和商家之间具有多次连贯的服务关系.因此,可以采用序贯博弈模型来解决用户多次提供隐私换取带宽问题,用户也可以提供不同等级的隐私换取不同的带宽.

云服务是近来的热点研究领域,在日常生活中越来越普及如手机通信录的云存储.当用户在使用云服务时,用户数据在云端的存储方式和存储位置对用户透明;进而,服务提供方可能会使用蕴含在不同应用中特定用户的离散隐私信息,通过数据挖掘与整合技术推理出用户敏感信息.因此使用传统的隐私保护方法不能很好地进行保护隐私.由于用户和服务商存在合作竞争关系,博弈论为云计算中隐私保护问题提供了新的解决方案,将是今后的研究和应用方向.

本文综述了博弈论在各类隐私保护中的应用,并对斯塔克博格博弈、扩展博弈、拍卖博弈和合作博弈在隐私保护问题中的应用进行分类总结,指出采用博弈论解决隐私问题的一般规律、难点和挑战.通过分析问题特征,详述了如何选择博弈模型和问题求解,并讨论了未来研究和应用方向.

References:

[1] Giuseppe D'Acquisto, Marta Flamini, Maurizio Naldi. A game-theoretic formulation of security investment decisions under ex-ante regulation[C]. SEC 2012, IFIP AICT 376, 2012: 412-423.

[2] Piero A Bonatti, Marco Faella, Clemente Galdi, et al. Towards a mechanism for incentivating privacy[C]. ESORICS, LNCS, 2011, 6879: 472-488.

[3] Osborne M J, Rubinstein A. A course in game theory[M]. Cambridge, Massachusetts: MIT 1994.

[4] Fudenberg D, Tirole J. Game theory[M]. Cambrldge, Massachusetle: MIT Press Books, 1991.

[5] About RAND. History and mission[EB/OL]. http://www.rand.org/about/history/, 2007.

[6] Mohammad Hossein Manshaei, Zhu Quan-yan, Tansu Alpcan, et al. Game theory meets network security and privacy[R]. EPFL-REPORT-151965, Switzerland, April 2011.

[7] Gueye A. A game theoretical approach to communication security [D]. University of California, Berkeley, Electrical Engineering and Computer Sciences, March 2011.

[8] Allen B MacKenzie, Luiz A DaSilva. Game theory for wireless engineers[M]. Morgan & Claypool Publishers Press, 2006.

[9] Murat Kantarcioglu, Alain Bensoussan, SingRu (Celine) Hoe. Investment in privacy-preserving technologies under uncertainty[C]. Proceedings of GameSec 2011, LNCS 7037: 219-238.

[10] Han Z, Marina N, Debbah M, et al. Physical layer security game: how to date a girl with her boyfriend on the same table[C]. Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets), 2009: 287-294.

[11] Anna Cinzia Squicciarini, Christopher Griffin, Smitha Sundareswaran. Towards a game theoretical model for identity validation in social network sites[C]. Proceedings of 2011 IEEE International Conference on Privacy, Security, Risk, and Trust. 9-11 Oct. 2011: 1081-1088.

[12] Raya M, Manshaei M H, Felegyhazi M, et al. Revocation games in ephemeral networks[C]. Proceedings of ACM Conference on Computer and Communications Security (CCS), 2008: 199-210.

[13] Farzad Salim, Jason Reid, Uwe Dulleck, et al. Towards a game theoretic authorisation model[C]. Proceedings of GameSec, 2010: 208-219.

[14] Zhu Feng, Zhu Wei. A game theoretic approach to optimize identity exposure in pervasive computing[C]. Proceedings of 7th Annual IEEE International Conference on Pervasive Computing and Communications, 2009: 1-20.

[15] Reidt S, Srivatsa M, Balfe. The fable of the bees: incentivizing robust revocation decision making in Ad Hoc networks[C]. Proceedings of ACM Conference on Computer and Communications Security (CCS), 2009: 291-302.

[16] Srinivasa Chakravarthy L, Valli Kumari V. Preserving data privacy using coalitional game theory[C]. Proceedings of Greece, Athens European conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, Workshop on KD-HCM, 2011: 53-65.

[17] Srinivasa L Chakravarthy, Valli Kumari V Sarojini Ch. A coalitional game theoretic mechanism for privacy preserving publishing based on k-Anonymity[C]. Proceedings of 2nd International Conference on Communication, Computing&Security, 2012: 879-896.

[18] Reza Shokri, George Theodorakopoulos, Carmela Troncoso. Protecting location privacy: optimal strategy against localization attacks [C]. China Classification Society (CCS'12), 2012: 617-627.

[19] Maxim Raya, Reza Shokri, Jean-Prerre Hubaux. On the tradeoff between trust and privacy in wireless Ad Hoc Networks[J]. The Third ACM Conference on Wireless Network Security (WiSec' 10), March22-24, 2010, Hoboken, New Jersey, USA, 75-80.

[20] Das S K, Nita Rotaru C, Kantarcioglu M (Eds). Optimizing active cyber defense[C]. Proceedings of GameSec 2013, LNCS 8252, 2013: 206-225.

[21] Aron Laszka, Assane Gueye. Quantifying network topology robustness under budget constraints: general model and computational complexity [C]. Proceedings of GameSec 2013, LNCS 8252, 2013: 154-174.

[22] Aron Laszka, Benjamin Johnson, Jens Grossklags. Mitigation of targeted and non-targeted covert attacks as a timing game[C]. Proceedings of GameSec 2013, LNCS 8252, 2013: 175-191.

[23] Chen Yu-feng, Liu Xue-jun, Li Bin. The methods of user collaborate work location privacy protection based on game theory[J]. Computer Science, 2013, 40(10): 92-97.

[24] Xie Jie-rui, Bart Piet Knijnenburg, Jin Hong-xia. Location sharing privacy preference: analysis and personalized recommendation[C]. Proceedings of the 19th International Conference on Intelligent User Interfaces, 2014: 189-198.

[25] Knijnenburg B P, Kobsa A, Jin H. Preference-based location sharing: are more privacy options really better[C]. Proceedings of The First International Symposium of Chinese CHI (Chinese Chi 2013), 2013: 2667-2676.

附中文参考文献:

[23] 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.