基于博弈论的隐私保护分布式数据挖掘

葛新景 朱建明
(中央财经大学信息学院 北京 100081)

摘 要 隐私保护的分布式数据挖掘问题是数据挖掘领域的一个研究热点,而基于经济视角,利用博弈论的方法对隐私保护分布式数据挖掘进行研究只是处于初始阶段。基于收益最大化,研究了完全信息静态博弈下分布式数据挖掘中参与者(两方或多方)的策略决策问题,得出了如下结论:数据挖掘在满足一定的条件下,参与者(两方或多方)的准诚信攻击策略是一个帕累托最优的纳什均衡策略;在准诚信攻击的假设下,参与者(多方)的非共谋策略并不是一个纳什均衡策略。同时给出了该博弈的混合战略纳什均衡,它对隐私保护分布式数据挖掘中参与者的决策具有一定的理论和指导意义。

关键词 博弈论,隐私保护,分布式数据挖掘
中图法分类号 TP311 **文献标识码** A

Privacy Preserving Distributed Data Mining Based on Game Theory

GE Xin-jing ZHU Jian-ming
(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract Privacy preserving distributed data mining has become an important issue in the data mining. Based on economic perspectives, game theory has been applied to privacy preserving data mining, which is a relatively new area of research. This paper studied the strategies of parties (two-party or multi-party) by using a complete information static game theory framework for the privacy preserving distributed data mining, where each party tries to maximize its own utility. Research results show that the semi-honest adversary strategy of parties (two-party or multi-party) is Pareto dominance and Nash equilibrium under certain conditions in distributed data mining; and non-collusion strategy of parties (multi-party) is not a Nash equilibrium under the assumption of semi-honest adversary behavior, then the mixed strategy Nash equilibrium was given. So this paper has some theoretical and practical implication for the strategy of parties in privacy preserving distributed data mining.

Keywords Game theory, Privacy-preserving, Distributed data mining

1 引言

在数据挖掘领域,随着越来越强大的数据挖掘工具的开发和应用,数据挖掘对个人隐私和数据安全的可能威胁也越来越备受关注,基于隐私保护的数据挖掘(privacy preserving data mining, PPDM)问题已成为该领域的一个研究热点。根据数据的分布情况,PPDM技术可以分为集中式和分布式的隐私保护数据挖掘技术。然而在现实和电子商务环境中,绝大多数数据库都是以分布式的形式存在的,即数据在两个或多个组织之间分布。为了共同的利益,数据的拥有者欲进行合作数据挖掘,但是由于隐私问题,数据挖掘的参与者并不想与其它参与者共享自己的数据。例如在商业部门,顾客的个人信息被要求很好地保存,而且不能被公开泄露,然而为了某些活动比如交叉销售,跨部门的顾客信息分析有时是必需的。因此,在分布式环境下,如何进行隐私保护的数据挖掘问题引起了许多学者的关注。

安全多方计算技术是分布式环境下隐私保护数据挖掘中常用的一种技术。在基于安全多方计算技术的隐私保护数据挖掘算法或协议中,主要防御两种类型的攻击行为[2]:准诚信攻击(semi-honest adversary)和恶意攻击(malicious adversary)。然而,在现有大多数研究中,通常假定数据挖掘参与者是准诚信攻击的,虽然假设参与者是准诚信攻击具有一定的现实意义[2],但是其理论依据是什么?同时需要注意的是准诚信攻击是否能阻止参与者之间的共谋行为?因为准诚信攻击只是假设参与者能够正确地执行算法或协议的内容,并没有假定参与者之间不允许共谋,那么在准诚信攻击的假设下,参与者的最优策略是共谋还是非共谋策略呢?

本文针对上述问题,基于收益最大化,利用博弈论的方法进行了研究,并得出了如下结论:数据挖掘在满足一定的条件下,参与者采取准诚信攻击策略是一个帕累托最优的纳什均

到稿日期:2010-12-15 返修日期:2011-03-25 本文受教育部科学技术研究重点项目(109016),北京市自然科学基金项目(4112053),国家自然科学基金项目(60970143)资助。

葛新景(1976-),女,博士生,讲师,主要研究方向为电子商务、数据挖掘,E-mail:xjge@163.com;朱建明(1965-),男,教授,博士生导师,主要研究方向为电子商务、信息安全。

衡策略；进一步在准诚信攻击的假设下，参与者的非共谋策略并不是一个纳什均衡策略。同时给出了该博弈的混合战略纳什均衡，从而本文对隐私保护分布式数据挖掘中参与者的决策具有一定的理论和指导意义。

2 相关研究现状

分布式环境下的隐私保护数据挖掘问题已经引起了许多学者的关注并取得一定的成果。基于隐私保护的分布式数据挖掘技术主要有随机化技术[3]、安全多方计算技术等。而基于经济视角，利用博弈论的方法对隐私保护分布式数据挖掘进行研究只是处于初始阶段。

分布式隐私保护问题与基于加密的安全多方计算有着许多共同之处，基于加密的安全多方计算技术已成为分布式环境下隐私保护数据挖掘的一个非常重要的隐私保护技术[2]。常用的加密技术有不经意传输、同态加密、不经意多项式计算等[4]。同时，密码学中许多基本的安全运算，如标量内积(Scalar Product)、安全求和(Secure Sum)、集合并的安全运算(Secure Set Union)、集合交集大小的安全运算(Secure Size of Set Intersection)等也被应用到隐私保护的分布式数据挖掘中[5]。需要注意的是，基于安全多方计算的思想，设计具有隐私保护的分布式数据挖掘算法或协议时，准诚信攻击模型并不能阻止参与者之间的共谋行为[4]。

在分布式数据挖掘过程中，数据挖掘参与者之间需要相互合作，而合作中又存在着冲突，这正是博弈论研究的范畴[6]。文献[7]首次基于微观经济的视角，利用两人博弈模型分析了数据挖掘中的聚类问题。文献[8]也证明了分布式计算满足博弈论。文献[9,10]将分布式数据挖掘模型转化为完全信息下的静态博弈，基于收益最大化原理以安全求和算法为例，利用博弈论研究了隐私保护数据挖掘中安全多方计算中的共谋问题。研究表明，在准诚信攻击模型假设下，参与者之间的非共谋行为并不是纳什均衡解。如在3个及以上参与者参加的隐私保护分布式数据挖掘中，几个参与者可以通过共谋来获得其它数据挖掘参与者的隐私数据，从而获得除数据挖掘结果外的额外利益。需要注意的是，在准诚信攻击的假设下，参与者的非共谋策略不是一个纳什均衡策略，那么该博弈是否存在纳什均衡？如果存在，那么它的纳什均衡策略是什么？同时准诚信攻击假设是否具有理论依据？本文正是在文献[9,10]的研究基础之上，研究了分布式数据挖掘中参与者的策略决策问题，不仅指出在准诚信攻击的假设下，参与者的非共谋策略不是一个纳什均衡策略，而且给出了该博弈的混合战略纳什均衡，并进行了案例分析；同时本文给出了分布式数据挖掘中参与者选择准诚信攻击策略的理论依据，因为准诚信攻击策略是一个帕累托最优的纳什均衡策略。

3 博弈基础

博弈论作为微观经济学的重要组成部分已经被广泛应用于许多领域，如经济、金融等。完全信息静态博弈是博弈论中一种最简单的博弈，这里“完全信息”指每个参与人对所有其他参与人的特征(包括战略空间、支付函数等)有完全的了解，“静态”指的是所有参与人同时选择行动且只选择一次。

纳什均衡是完全信息静态博弈解的一般概念，其正式定义如下[6]：

定义1(纳什均衡) 有 n 个参与人的战略式表述博弈 $G=\{S_1,\cdots,S_n;u_1,\cdots,u_n\}$，战略组合 $s^*=(s_1^*,\cdots,s_i^*,\cdots,s_n^*)$ 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 个参与人的最优战略，即

$$u_i(s_i^*,s_{-i}^*)\geqslant u_i(s_i,s_{-i}^*),\ \forall s_i\in S_i,\ \forall i$$

或者用另一种表达方式，s_i^* 是下述最大化问题的解 $s_i^*\in \underset{s_i\in S_i}{\operatorname{argmax}} u_i(s_1^*,\cdots,s_{i-1}^*,s_i,s_{i+1}^*,\cdots,s_n^*)$，其中 $i=1,2,\cdots,n$。

在博弈中，如果一个战略规定参与人在每一个给定的信息情况下只选择一种特定的行动，则称该战略是纯战略。相反，如果一个战略规定参与人在给定信息情况下以某种概率分布随机地选择不同的行动，则称该战略是混合战略。下面给出混合战略纳什均衡的定义[6]。

定义2(混合战略纳什均衡) 在 n 个参与人博弈的战略式表述 $G=\{S_1,\cdots,S_n;u_1,\cdots,u_n\}$ 中，假定参与人 i 有 k 个纯战略：$S_i=\{s_{i1},\cdots,s_{iK}\}$，则概率分布 $\sigma_i=(\sigma_{i1},\cdots,\sigma_{iK})$ 称为 i 的一个混合战略，这里 $\sigma_{ik}=\sigma(s_{ik})$ 是 i 选择 s_{ik} 的概率，对于所有的 $k=1,\cdots,k$，$0\leqslant\sigma_{ik}\leqslant 1$，$\sum_{1}^{K}\sigma_{ik}=1$，混合战略组合 $\sigma^*=(\sigma_1^*,\cdots,\sigma_i^*,\cdots,\sigma_n^*)$ 是一个纳什均衡，如果对于所有的 $i=1,2,\cdots,n$，下式成立：$v_i(s_{ik},\sigma_{-i})\geqslant v_i(s_{ik}',\sigma_{-i})$，$\forall s_{ik}'\in S_i$。

4 分布式隐私保护数据挖掘的博弈分析

在基于隐私保护的分布式数据挖掘中，面对的攻击行为主要有两种类型[2]：准诚信攻击和恶意攻击。因此，在设计具有隐私保护的分布式数据挖掘算法或协议中，通常假设数据挖掘参与者是准诚信攻击者或恶意攻击者。准诚信攻击是假设参与者能够正确地执行算法或协议的内容，但在协议或算法的执行过程中，企图通过分析从其它参与者那里得到的数据而得到额外的信息。恶意攻击假设参与者在数据挖掘过程中，随意背离而不能够正确地执行协议或算法。因此，数据挖掘中每个参与者的策略为准诚信攻击或恶意攻击。

同时，对于数据挖掘中参与者的准诚信攻击和恶意攻击行为的假设，数据挖掘参与者之间还可选择共谋或非共谋行为。因为在协议的执行过程中，通过参与者之间的共谋行为，可以获得除挖掘结果外的额外利益，如非共谋参与者的隐私数据。

因为这两种情况属于不同的阶段，为便于表达，可以分为两个不同的博弈过程。即第一阶段数据挖掘参与者首先决定自己的最优策略是准诚信攻击还是恶意攻击，第二阶段在假设自己是准诚信攻击者还是恶意攻击者的前提下，再决定自己的最优策略是共谋或非共谋。同时假设每个数据挖掘参与者都是风险中性的，且决策准则都一样，都是以自身期望效用最大化为依据的。

4.1 第一阶段数据挖掘参与者的博弈分析

在完全信息静态博弈下，数据挖掘参与者在第一阶段首

先决定自己的最优策略是准诚信攻击还是恶意攻击，博弈的战略式表述如下：

博弈的参与人集合：

数据挖掘所有参与者 $P_1, P_2, \cdots, P_n$。

每个参与人的战略空间：

S_i＝{准诚信攻击，恶意攻击}

收益：如果所有数据挖掘参与者都是准诚信攻击者，则每个参与者均得到正确的数据挖掘结果，从而得到相同的利益 u；若数据挖掘过程中只有一个参与者 $P_i(i=1,2,\cdots,n)$ 是恶意攻击者，而其它参与者都是准诚信的，则参与者 P_i 得到收益 $\theta_i(\theta_i \geqslant 0)$，其它参与者的收益是 $-\theta_i$；若数据挖掘过程中至少有两个参与者是恶意攻击者，则每个参与者均不能得到正确的数据挖掘结果，从而利益为 0。同时，假设每个参与者执行数据挖掘算法的成本是相同的，为了简单起见，不妨设为 0，这并不影响我们对数据挖掘参与者策略的博弈分析。

在具有隐私保护的数据挖掘中，数据挖掘的参与者有两种情况：两个参与者(Two-Party)和多个参与者(Multiparty)。下面分别对有两个和多个参与者的数据挖掘中参与者的策略进行博弈分析。

4.1.1 隐私保护分布式数据挖掘的博弈分析

若在隐私保护的分布式数据挖掘中有多个参与者 $P_1, P_2, \cdots, P_n$，这里 $n \geqslant 2$。为简单起见，假设 $n=2$，即只有两个参与者 P_1, P_2，其博弈的战略式表述可以用矩阵表直观地给出，如表 1 所列，其中 $u \geqslant 0, \theta_1, \theta_2 \geqslant 0$。表中左列是参与者 P_1 的战略空间，上行是参与者 P_2 的战略空间，每一个数字格是对应战略组合下的支付(收益)。其中第一个数字是参与者 P_1 的收益，第二个数字是参与者 P_2 的收益。

表 1 两个参与者的隐私保护数据挖掘博弈分析

		参与者 P_2	
		准诚信攻击	恶意攻击
参与者 P_1	准诚信攻击	u,u	$-\theta_2, \theta_2$
	恶意攻击	$\theta_1, -\theta_1$	0,0

在该博弈中，①若假设 $\theta_1, \theta_2 \geqslant u$(即在数据挖掘算法执行过程中，若只有一个参与者是恶意攻击的，虽然不能得到正确的数据挖掘结果，但该恶意攻击参与者可以获得某些额外的利益，而且该利益大于正确得到数据挖掘结果的利益)，此时博弈的纳什均衡是(恶意攻击，恶意攻击)，则由于博弈双方互相不信任，所有参与者均是恶意攻击者，从而无法得到正确的数据挖掘结果，却浪费了大量的数据挖掘成本，合作无法进行。

②若假设 $0 \leqslant \theta_1 \leqslant u, 0 \leqslant \theta_2 \leqslant u$(即在数据挖掘算法执行过程中，若只有一个参与者是恶意攻击的，虽然不能得到正确的数据挖掘结果，但该恶意攻击参与者可以获得某些额外的利益，但该额外利益小于得到正确数据挖掘结果的利益，这种假设也是符合实际的，因为大多数情况下，合作进行数据挖掘的目的是为了得到正确的数据挖掘结果而非额外的其它利益)，则该博弈存在两个纯战略纳什均衡：(准诚信攻击，准诚信攻击)、(恶意攻击，恶意攻击)。即给定参与者 P_1 是准诚信攻击的，参与者 P_2 的最优战略是准诚信攻击；给定参与者 P_1 是恶意攻击的，参与者 P_2 的最优战略是恶意攻击；给定参与者 P_2 是准诚信攻击的，参与者 P_1 的最优战略是准诚信攻击；给定参与者 P_2 是恶意攻击的，参与者 P_1 的最优战略是恶意攻击。这里纳什均衡战略(准诚信攻击，准诚信攻击)是帕累托最优的。

在该博弈中，若假设参与者 P_1 以 $\alpha(0 \leqslant \alpha \leqslant 1)$ 的概率选择准诚信攻击，以 $1-\alpha$ 的概率选择恶意攻击，参与者 P_2 以 $\beta(0 \leqslant \beta \leqslant 1)$ 的概率选择准诚信攻击，以 $1-\beta$ 的概率选择恶意攻击，则参与者 P_1 的期望效用函数为

$$E_1 = \alpha[\beta u + (1-\beta)(-\theta_2)] + (1-\alpha)[\beta\theta_1 + (1-\beta)\cdot 0]$$

最优化的一阶条件为

$$\frac{\partial E_1}{\partial \alpha} = \beta u + (1-\beta)(-\theta_2) - \beta\theta_1 = \beta u + \beta\theta_2 - \beta\theta_1 - \theta_2 = 0$$

上式意味着 $\beta^* = \frac{\theta_2}{u+\theta_2-\theta_1}$。即如果 $\beta > \beta^*$，参与者 P_1 的最优选择是准诚信攻击；如果 $\beta < \beta^*$，参与者 P_1 的最优选择是恶意攻击；当 $\beta = \beta^*$ 时，参与者 P_1 随机地选择准诚信攻击或恶意攻击。

同理可得参与者 P_2 的期望效用函数并求得最优化的一阶条件为

$$\frac{\partial E_2}{\partial \beta} = \alpha u + (1-\alpha)(-\theta_1) - \alpha\theta_2 = \alpha u + \alpha\theta_1 - \alpha\theta_2 - \theta_1 = 0$$

上式意味着 $\alpha^* = \frac{\theta_1}{u+\theta_1-\theta_2}$。即如果 $\alpha > \alpha^*$，参与者 P_2 的最优选择是准诚信攻击；如果 $\alpha < \alpha^*$，参与者 P_2 的最优选择是恶意攻击；当 $\alpha = \alpha^*$ 时，参与者 P_2 随机地选择准诚信攻击或恶意攻击。

因此，博弈的混合战略纳什均衡是 $\alpha^* = \frac{\theta_1}{u+\theta_1-\theta_2}, \beta^* = \frac{\theta_2}{u+\theta_2-\theta_1}$。即参与者 P_1 以 $\alpha^* = \frac{\theta_1}{u+\theta_1-\theta_2}$ 的概率选择准诚信攻击，参与者 P_2 以 $\beta^* = \frac{\theta_2}{u+\theta_2-\theta_1}$ 的概率选择准诚信攻击。

混合战略纳什均衡似乎是一个难以令人满意的概念。海萨尼(Harsanyi)[6]证明，混合战略均衡等价于不完全信息下的纯战略纳什均衡。因为完全信息只是一个理想状态，现实中每个人对其他人的目标函数总不可能是完全了解的。在不完全信息下，每个参与人在选择自己的战略时，似乎面对的是一个选择混合战略的对手，尽管每个参与人事实上选择的都是纯战略。如在该隐私保护的数据挖掘博弈中，混合战略纳什均衡的本质特征不在于参与人随机的选择行动，而在于参与者 P_1 不知道参与者 P_2 将选择什么纯战略，参与者 P_2 不知道参与者 P_1 将选择什么纯战略。

同时需要说明的是，对于 $n \geqslant 3$ 个数据挖掘参与者的隐私保护分布式数据挖掘，可得到与 $n=2$ 时类似的结论。

4.1.2 讨论

根据上述分析可知，对于多方(两方)参与的隐私保护分布式数据挖掘博弈，当 $\theta_i \geqslant u \geqslant 0 (1 \leqslant i \leqslant n)$ 时，博弈纳什均衡中所有参与者的最优策略均为恶意攻击。然而此时无法得到正确的数据挖掘结果，却浪费了大量的数据挖掘成本，合作无法进行。如何解决不可能合作的问题？现在已经提出很多方

法。方法之一是存在强制执行的协议，要求每一个合作方必须按照协议的要求执行，否则将受到法律的惩罚。另一方面，从技术上杜绝合作数据挖掘者的恶意攻击行为（如不诚实提供数据）来解决合作无法进行的问题。如文献[10]以多方安全求和为例，通过多次求和后比较结果的方法增加数据挖掘者的成本，减少收益来防止怀有恶意的参与者提供不准确数据，从而使安全求和顺利进行。文献[11]提出了具有激励相容特性的隐私保护数据挖掘，在数据挖掘参与者"理性人"的假设下，数据挖掘参与者基于收益最大化在数据挖掘过程中愿意提供自己的真实数据。

然而，对于多方（两方）参与的隐私保护分布式数据挖掘博弈，当 $0\leqslant\theta_i\leqslant u,(1\leqslant i\leqslant n)$ 时，存在两个完全信息静态博弈下的纯战略纳什均衡，即（准诚信攻击，准诚信攻击，…，准诚信攻击）和（恶意攻击，恶意攻击，…，恶意攻击）。其中（准诚信攻击，准诚信攻击，…，准诚信攻击）帕累托优于（恶意攻击，恶意攻击，…，恶意攻击）。在该博弈中，如果每个参与者都是准诚信的，则可以得到正确的数据挖掘结果，这是大家所希望的，也是帕累托最优的纳什均衡策略。在现实中，如何实现帕累托最优的纳什均衡而避免其它非帕累托最优纳什均衡出现呢？一种方法是数据挖掘参与者在博弈开始之前进行不花什么成本的"廉价磋商"（cheap talk）[6]。尽管无法保证磋商会达成一个协议，即使达成协议也不一定会被遵守，但事前磋商确实可以使某些纳什均衡在实际中出现。例如数据挖掘参与者在数据挖掘前进行提前的磋商，所有数据挖掘参与者都提前告诉其它参与者自己将选择准诚信攻击策略，同时考虑到实践中数据挖掘成本的巨大性，则我们有很大的把握说纯战略纳什均衡（准诚信攻击，准诚信攻击，…，准诚信攻击）将会出现。

对于完全信息静态博弈下的混合战略纳什均衡，由于其等价于不完全信息静态博弈下的纯战略纳什均衡，数据挖掘的收益 u 越大，$\theta_i\geqslant 0,(1\leqslant i\leqslant n)$ 越小，则数据挖掘参与者在挖掘过程中选择准诚信策略的概率越大。在极端情况下，如果 $u\to\infty$ 或 $\theta_i=0$，即数据挖掘的收益 u 趋于无穷大，或者是通过恶意攻击不能获得任何收益，基于收益最大化的考虑，则数据挖掘参与者选择恶意攻击策略的概率为 0，选择准诚信攻击的概率为 1。

通过上述分析可知，在隐私保护的分布式数据挖掘研究中，考虑到数据挖掘成本的巨大性和正确数据挖掘结果收益的巨大性，或者进行不花什么成本的"廉价磋商"，或者设计具有激励相容特性的隐私保护数据挖掘算法或协议，则理性的数据挖掘参与者基于自己收益的最大化，选择准诚信攻击策略即帕累托最优的策略的概率是非常大的。因此在如上述假设条件下，假设数据挖掘参与者是准诚信的攻击者是符合实际和具有现实意义的。而在现有关于隐私保护的分布式挖掘中，许多学者也都是在假设参与者是准诚信攻击的模型下，设计具有隐私保护的数据挖掘协议或算法，从而该博弈分析给出了准诚信攻击假设的理论基础。

4.1.3 案例分析

由于完全信息下的混合战略纳什均衡等价于不完全信息下的纯战略纳什均衡，而现实中，每个人对其他人的目标函数总不可能是完全了解的，因此完全信息只是一个理想状态，而不完全信息更符合实际情况。下面，将对完全信息静态博弈下的混合战略策略即不完全信息静态博弈下的纯战略纳什均衡策略进行案例分析。

案例 1　关联规则挖掘是数据挖掘中一项重要的研究课题，在商业等领域有着成功的应用。在隐私保护分布式关联规则数据挖掘的研究中，文献[1]基于数量积运算在两方参与的垂直划分的数据集上设计了具有隐私保护水平的、在布尔型关联规则挖掘中找到频繁项目集的算法，详细的计算过程有兴趣的读者可参看文献[1]。其中，数量积 $c.\ count=\vec{X}\times\vec{Y}=\sum_{i=1}^{n}x_i * y_i$ 的安全计算是算法的关键。

下面讨论在该算法的执行过程中，数据挖掘参与者的策略选择，即选择准诚信还是恶意攻击策略。

对于二维非零向量的数量积函数，有如下定理[11]。

定理 1　令二维数量积函数

$$f(v_1,v_2)=\sum_{j=1}^{k}v_1^j\cdot v_2^j$$

式中，v_i 是非 0 向量，v_i^j 是向量 v_i 第 j 行的值，则 f 是 DNCC (deterministically non-cooperatively computable model)[11]。

证明：略，参见文献[11]。

由定理 1 可知，由于数量积函数 f 是 DNCC，从而可以推断文献[1]给出的隐私保护垂直分布关联规则数据挖掘算法是 DNCC。

如果一个函数是 DNCC，则该函数是激励相容的。如果一个函数是激励相容的，则在函数算法的执行过程中，数据输入者将会输入自己的真实数据[11]。将该性质反映到文献[1]基于标量积给出的隐私保护垂直分布关联规则数据挖掘算法中，则在算法的执行过程中，数据挖掘参与者基于自己收益的最大化，将会如实输入自己的真实隐私数据。因为数据挖掘参与者如果选择恶意攻击策略，在算法执行过程中输入修正后的数据，不仅其它数据挖掘参与者不能得到正确的数据挖掘结果，自己根据自己的真实数据和算法也不能推算出正确的数据挖掘结果，从而选择恶意攻击策略的收益将会很小，即 $\theta_i\geqslant 0,(1\leqslant i\leqslant n)$ 很小。因此在该案例中，对于理性的数据挖掘参与者，基于收益的最大化，其更倾向于选择准诚信攻击策略，即选择准诚信攻击策略的概率更大。

案例 2　集合的安全运算已经被广泛应用于隐私保护数据挖掘问题中[5]，并且文献[11]已经证明集合的并集和交集运算都不是 DNCC。具体表述如下：

定理 2　令 $f(S_1,S_2,\cdots,S_n)=S\cup S_2\cup\cdots\cup S_n$ 是集合 $S_1,S_2,\cdots,S_n$ 的并集，则 f 不是 DNCC。

证明：略，参见文献[11]。

定理 3　令 $f(S_1,S_2,\cdots,S_n)=S\cap S_2\cap\cdots\cap S_n$ 是集合 $S_1,S_2,\cdots,S_n$ 的交集，则 f 不是 DNCC。

证明：略，参见文献[11]。

由定理 2 和定理 3 可知，集合的并集和交集运算都不是 DNCC，这意味着集合的并集和交集运算不是激励相容的，则在算法的执行过程中，参与者基于自己收益的最大化，没有动

力输入自己的真实数据。因为如果参与者输入修正后的数据，在假设其他数据参与者提供真实数据的前提下，则该参与者基于自己的真实数据和函数运算的结果该参与者可以推算出正确的函数运算结果，但其他数据参与者却不能得到正确的运算结果，使竞争处于劣势，从而可以认为该参与者获得了比得到正确函数运算结果更大的收益，即 $\theta_i \geqslant u$。因此在该种情况下，对于理性的数据参与者，基于收益的最大化，其更倾向于选择恶意攻击策略，即选择准恶意攻击策略的概率更大。

4.2 第二阶段数据挖掘参与者的博弈分析

在前面第一阶段的数据挖掘的博弈分析中，我们已得出结论：在隐私保护的分布式数据挖掘中，假设数据挖掘者是理性人，基于收益最大化的要求，数据挖掘参与者的帕累托最优纳什均衡策略是准诚信攻击策略，而且它是符合实际和具有现实意义的。但需要注意的是，准诚信攻击只是假设数据挖掘参与者必须遵守协议，按照协议的要求进行准确的计算和数据的传输，却不能阻止参与者之间的共谋行为[4]。通过参与者之间的共谋行为，共谋的参与者有时可以获得除数据挖掘结果之外的利益，如非共谋参与者的隐私数据。那么，在假设数据挖掘参与者在准诚信攻击策略的条件下，在利益的驱使下，参与者是采取共谋策略还是非共谋策略呢？在目前关于隐私保护的数据挖掘协议或算法中，许多研究者假设参与者是准诚信的且参与者之间没有共谋行为，这是一个非常强的假设，是否与现实情况相一致呢？下面将基于数据挖掘参与者收益最大化的假设前提，对此进行博弈分析。

4.2.1 准诚信攻击假设下数据挖掘参与者的共谋行为分析

在基于隐私保护的分布式数据挖掘中，如果数据挖掘的参与者只有两方，则不存在参与者之间的共谋问题。如果数据挖掘的参与者有三方或者更多，则有可能存在参与者之间的共谋行为。为了简单且不失一般性，我们假设数据挖掘的参与者有三方，即有 3 个参与者 P_1, P_2, P_3。对于多于三方的隐私保护数据挖掘参与者的最优策略完全可以由基于三方参与的隐私保护数据挖掘类推。

在完全信息静态博弈下，假设数据挖掘参与者 P_1, P_2, P_3 在第一阶段首先决策自己的最优策略是准诚信攻击(如数据挖掘参与者在博弈开始之前首先进行“廉价磋商(cheap talk)”)，则第二阶段博弈的战略式可以表述如下：

博弈的参与人集合：数据挖掘所有参与者 P_1, P_2, P_3

每个参与人的战略空间：$S_i = \{$共谋，非共谋$\}$

收益：如果所有数据挖掘参与者都是准诚信攻击者且采取非共谋策略，则每个参与者均得到正确的数据挖掘结果从而得到相同的利益 u；若在假设所有数据挖掘者是准诚信的数据挖掘过程中，如果参与者 P_1 与参与者 P_2 共谋，则可得到参与者 P_3 的隐私数据。假设参与者 P_1 与参与者 P_2 得到除数据挖掘结果外的额外收益 υ_3，则参与者 P_3 损失额外收益 υ_3；如果参与者 P_1 与参与者 P_3 共谋，则可得到参与者 P_2 的隐私数据，假设参与者 P_1 与参与者 P_3 得到除数据挖掘结果外的额外收益 υ_2，则参与者 P_2 损失额外收益 υ_2；如果参与者 P_2 与参与者 P_3 共谋，则可得到参与者 P_1 的隐私数据，假设参与者 P_2 与参与者 P_3 得到除数据挖掘结果外的额外收益 υ_1，则参与者 P_1 损失额外收益 υ_1。如果 3 个参与者同时共谋，则合作无法进行，收益为 0。如果只有一个参与者采取共谋策略，而其它两个参与者均是非共谋的，则参与者之间的共谋行为无效。

因此，上述 3 个参与者 P_1, P_2, P_3 的隐私保护分布式数据挖掘博弈的战略式表述可以用矩阵表直观地给出，如表 2 所列。其中 $u \geqslant 0, \upsilon_1, \upsilon_2, \upsilon_3 \geqslant 0$，每一个数字格是对应战略组合下的支付(收益)，其中第一个数字是参与者 P_1 的收益，第二个数字是参与者 P_2 的收益，第三个数字是参与者 P_3 的收益。

表 2 多个参与者的隐私保护数据挖掘博弈分析

(a)参与者 P_3：非共谋

		参与者 P_2	
		非共谋	共谋
参与者 P_1	非共谋	u,u,u	u,u,u
	共谋	u,u,u	$u+\upsilon_3, u+\upsilon_3, u-\upsilon_3$

(b)参与者 P_3：共谋

		参与者 P_2	
		非共谋	共谋
参与者 P_1	非共谋	u,u,u	$u-\upsilon_1, u+\upsilon_1, u+\upsilon_1$
	共谋	$u+\upsilon_2, u-\upsilon_2, u+\upsilon_2$	0,0,0

在该博弈中，① 若假设 $\upsilon_1, \upsilon_2, \upsilon_3 \geqslant u$，即参与者隐私数据的价值不小于数据挖掘结果给参与者带来的收益，此时博弈的纳什均衡是(共谋，共谋，共谋)。因此，由于互相不信任，所有参与者均担心自己的隐私信息被侵犯，而且在其他站点诚实时，共谋有可能得到更高的收益，所有参与者选择了共谋，合作无法进行。

② 若假设 $0 \leqslant \upsilon_1, \upsilon_2, \upsilon_3 \leqslant u$，则博弈不存在纯战略纳什均衡。下面求博弈的混合战略纳什均衡。假设参与者 P_1 以概率 ρ_1 选择共谋策略，参与者 P_2 以概率 ρ_2 选择共谋策略，参与者 P_3 以概率 ρ_3 选择共谋策略，其中 $0 \leqslant \rho_1, \rho_2, \rho_3 \leqslant 1$。则参与者 P_1 的期望效用函数为

$$\begin{aligned}\pi_1 = {} & (1-\rho_1)[(1-\rho_2)(1-\rho_3)u+\rho_2(1-\rho_3)u+(1-\rho_2)(\rho_3)u+\rho_2\rho_3(u-\upsilon_1)]+\rho_1[(1-\rho_2)(1-\rho_3)u+\\ & \rho_2(1-\rho_3)(u+\upsilon_3)+(1-\rho_2)\rho_3(u+\upsilon_2)+0]\end{aligned}$$

最优化的一阶条件为

$$\begin{aligned}\frac{\partial \pi_1}{\partial \rho_1} = {} & -[(1-\rho_2)(1-\rho_3)u+\rho_2(1-\rho_3)u+(1-\rho_2)(\rho_3)u+\rho_2\rho_3(u-\upsilon_1)]+[(1-\rho_2)(1-\rho_3)u+\rho_2(1-\rho_3)(u+\upsilon_3)+(1-\rho_2)\rho_3(u+\upsilon_2)+0]\\ = {} & \rho_2(1-\rho_3)\upsilon_3+(1-\rho_2)\rho_3\upsilon_2+\rho_2\rho_3\upsilon_1-\rho_2\rho_3 u=0 \quad (1)\end{aligned}$$

同理可得参与者 P_2 的期望效用函数并求得最优化的一阶条件为

$$\begin{aligned}\frac{\partial \pi_2}{\partial \rho_2} = {} & -[(1-\rho_1)(1-\rho_3)u+\rho_1(1-\rho_3)u+(1-\rho_1)\rho_3 u+\rho_1\rho_3(u-\upsilon_2)]+[(1-\rho_1)(1-\rho_3)u+\rho_1(1-\rho_3)(u+\upsilon_3)+(1-\rho_1)\rho_3(u+\upsilon_1)+0]\\ = {} & \rho_1(1-\rho_3)\upsilon_3+(1-\rho_1)\rho_3\upsilon_1+\rho_1\rho_3\upsilon_2-\rho_1\rho_3 u=0 \quad (2)\end{aligned}$$

同理可得参与者 P_3 的期望效用函数并求得最优化的一阶条件为

$$\begin{aligned}\frac{\partial \pi_3}{\partial \rho_3} = {} & -[(1-\rho_1)(1-\rho_2)u+\rho_1(1-\rho_2)u+(1-\rho_1)\rho_2 u+\rho_1\rho_2(u-\upsilon_3)]+[(1-\rho_1)(1-\rho_2)u+\rho_1(1-\rho_2)(u+\upsilon_2)+(1-\rho_1)\rho_2(u+\upsilon_1)+0]\end{aligned}$$

$$=\rho_1(1-\rho_2)v_2+(1-\rho_1)\rho_2 v_1+\rho_1\rho_2 v_3-\rho_1\rho_2 u=0 \quad (3)$$

求解由式(1)、式(2)、式(3)构成的方程组，可得该博弈的混合战略纳什均衡是

$$\rho_1^*=\frac{2v_1}{u+3v_1-v_2-v_3},\rho_2^*=\frac{2v_2}{u+3v_2-v_1-v_3},$$
$$\rho_3^*=\frac{2v_3}{u+3v_3-v_1-v_2} \quad (4)$$

即在隐私保护分布式数据挖掘中假设参与者是准诚信攻击的前提下，参与者 P_1 以 $\rho_1^*=\frac{2v_1}{u+3v_1-v_2-v_3}$ 的概率选择共谋，参与者 P_2 以 $\rho_2^*=\frac{2v_2}{u+3v_2-v_1-v_3}$ 的概率选择共谋，参与者 P_3 以 $\rho_3^*=\frac{2v_3}{u+3v_3-v_1-v_2}$ 的概率选择共谋。

根据海萨尼(Harsanyi)[6]定理，该混合战略均衡等价于不完全信息下的纯战略纳什均衡，即在不完全信息下，所有参与者均为准诚信攻击的前提下，上述均衡式(4)给出了每个参与者选择共谋行为的概率。

4.2.2 讨论

根据上述分析可知，对于多方参与的隐私保护分布式数据挖掘博弈，如果假设所有的数据挖掘参与者都是准诚信攻击的，基于收益的最大化，参与者采取非共谋行为并不是最优纳什均衡策略。特别当参与者的隐私信息价值大时，如 v_1，v_2，$v_3\geqslant u$，共谋有可能得到更高的收益，所有参与者的纳什均衡策略是共谋，而使得合作无法进行下去。文献[9,10]均以安全求和为例，对隐私保护数据挖掘中参与者的共谋行为进行了博弈分析，指出非共谋行为并不是最优纳什均衡策略。我们的结论与文献[9,10]是一致的，而且本文给出了该博弈分析的混合战略均衡，其等价于不完全信息下的纯战略纳什均衡，更符合实际情况。因为在实际中，完全信息只是一个理想的情形，现实中所有参与者面对的更多的是采取混合策略的合作者。

结束语 隐私保护的分布式数据挖掘问题是数据挖掘领域的一个研究热点。本文基于收益最大化，在完全信息静态博弈下研究了数据挖掘中参与者的策略决策问题，得出了如下结论：数据挖掘在满足一定的条件下(如当 $0\leqslant\theta_i\leqslant u$，$(1\leqslant i\leqslant n)$时)，参与者的准诚信攻击策略是一个帕累托最优的纳什均衡策略；当 $\theta_i\geqslant u\geqslant 0$，$(1\leqslant i\leqslant n)$时，博弈纳什均衡中所有参与者的最优策略均为恶意攻击策略；进一步，在准诚信攻击的假设下，参与者的非共谋策略并不是一个纳什均衡策略，而且给出了该博弈的混合战略纳什均衡，同时对上述问题进行了案例分析，从而对隐私保护的分布式数据挖掘中参与者的决策具有一定的理论和指导意义。

需要指出的是，本文只是在完全信息静态博弈下对隐私保护的分布式数据挖掘进行了研究。而现实的合作数据挖掘中，信息往往是不完全的，完全信息只是一个理想的情形，而且数据挖掘也具有动态的特性。本文主要是基于静态(Static)共谋的策略分析，而自适应(Adaptive)共谋也许更符合实际情况，这些都是今后需进一步研究的。

参 考 文 献

[1] Vaidya J S, Clifton C. Privacy preserving association rule mining in vertically partitioned data[C]// Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2002:639-644

[2] Lindell Y, Pinkas B. Privacy preserving data mining [J]. Journal of Cryptology, 2002, 15(3):177-206

[3] Agrawal R, Srikant R. Privacy-preserving data mining[C]// Proceedings of the SIGMOD Conference on Management of Data. ACM Press, 2000:439-450

[4] Lindell Y, Pinkas B. Secure Multiparty Computation for Privacy-preserving Data Mining [J]. Journal of Privacy and Confidentiality, 2009, 1(1):59-98

[5] Clifton C, Kantarcioglu M, Vaidya J, et al. Tools for Privacy Preserving Distributed Data Mining [J]. ACM SIGKDD Explorations, 2002, 4(2):28-34

[6] 张维迎. 博弈论与信息经济学[M]. 上海：上海人民出版社，2004

[7] Kleinberg J, Papadimitriou C, Raghavan P. A microeconomic view of data mining [J]. Data Mining and Knowledge Discovery, 1998, 2(4):311-324

[8] Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation[C]// Proceedings of the Twenty-fifth Annual ACM Symposium on Principles of Distributed Computing. New York, USA: ACM Press, 2006:53-62

[9] Kargupta H, Das K, Liu K. Multi-party, privacy-preserving distributed data mining using a game theoretic framework [J]. PKDD, 2007, 4702:523-531

[10] 张国荣，印鉴. 基于博弈论的安全多方求和方法[J]. 计算机应用研究，2009, 26(4):1497-1499

[11] Kantarcioglu M, Jiang Wei. Incentive Compatible Privacy-preserving Data Analysis[R]. UTDCS-29-08. UT Dallas Computer Science Department, 2008

(上接第 139 页)

[6] http://whoshouldifollow.com/

[7] http://wefollow.com/

[8] 李文波，孙乐，张大鲵. 基于 Labeled-LDA 模型的文本分类新算法[J]. 计算机学报，2008，31：620-627

[9] http://www.ranks.nl/resources/stopwords.html

[10] Celli F, Lascio F M L D, Magnani M, et al. Social network data and practices: the case of friendfeed[C]// International Conference on Social Computing, Behavioral Modeling and Prediction. Lecture Notes in Computer Science. Springer, Berlin, 2010

[11] 曹娟，张勇东，李锦涛，等. 一种基于密度的自适应最优 LDA 模型选择方法[J]. 计算机学报，2008，31(10)：1780-1787

[12] Grosseck G, Holotescu C. Can we use twitter for educational activities? [C]// the 4th International Sscientific Conference on elearning and software for education. Bucharest, Rumania, April 2008:17-18

[13] Sakaki T, Okazaki M, Matsuo Y. Earthquake Shakes Twitter Users: Real-time Event Detection by Social Sensors[C]// the 19th International World Wide Web Conference. Raleigh, North Carolina, USA, April 26-30