社交网络用户隐私保护的博弈模型

黄启发 朱建明 宋 彪 章 宁
(中央财经大学信息学院 北京 100081)

摘 要 基于不完全信息的动态博弈,分别通过攻防博弈、共同防御博弈、联合攻击博弈研究了社交网络用户隐私的攻防博弈过程,并重点探讨了用户关系层次对博弈结果的影响。结论表明,非完全自私的防御者可以优化整体的防御水平,优化的程度取决于用户隐私价值大小和关系层次的综合作用;攻击者之间共谋可以获得更高的攻击效用,关系层次对不同的攻击者具有不同的影响。研究结果对社交网络用户更好地保护隐私具有一定指导作用。

关键词 社交网络,隐私,攻防博弈,共同防御博弈,联合攻击博弈

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.10.041

Game Model of User's Privacy-preserving in Social Networks

HUANG Qi-fa ZHU Jian-ming SONG Biao ZHANG Ning
(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract Based on incomplete information dynamic game, this paper analyzed three kinds of game between attackers and defenders of social networks: offensive-defensive game, mutual defense game, joint attacking game, and further discussed the effects of relationship levels on game process. The result tells us that incomplete selfish defenders can optimize their overall defense and the degree of optimization is depended on their privacy value and relationship levels, and collusion between attackers can obtain higher attack utility, but relationship levels have different effects to different attackers. The result of this study has a certain guiding role to social networks user's privacy-preserving.

Keywords Social networks, Privacy, Offensive-defensive game, Mutual defense game, Joint attacking game

1 引言

近年来社交网络已经成为人们交流的重要平台。人们已经习惯于借助社交网络发布各种信息,社交网络逐渐成为互联网的重要入口,并汇聚了用户的海量信息,因此常常成为犯罪分子的攻击目标,随着针对社交网络的安全事件频发,用户隐私保护问题越来越受到全社会的广泛关注。

造成社交网络用户隐私泄露的两大主要因素是技术缺陷和经济利益,因此,社交网络用户隐私保护也应从这两方面着手。目前的研究主要集中于通过技术手段和方法保护用户隐私,如对用户的主要属性及关系进行匿名,或者对用户账户设置访问权限等。但是,对于隐私的保护者和攻击者来说,他们的行为都不是无代价的,都需要在成本与收益间进行权衡,讲究行为的策略性。基于此,本研究将社交网络用户隐私的保护者和攻击者视为博弈的双方,以"理性人"假设为基础,探讨社交网络用户隐私保护的博弈过程。

本文第2节首先介绍了目前社交网络用户隐私保护的研究进展,及博弈论在信息安全领域的应用情况;第3节研究了不完全信息动态博弈下社交网络用户隐私的保护模型,分为攻防博弈、共同防御博弈和联合攻击博弈3种情形进行分析,并将用户之间的关系层次作为重要变量引入模型,深入分析关系层次对博弈结果的影响;最后得出结论。

2 社交网络用户隐私保护的相关研究分析

目前,对于社交网络用户隐私保护的研究主要集中于匿名和访问控制两个方面,前者是从外部视角即分析人员的视角来研究的,后者采用的是内部视角即社交网络成员自身的视角。

2.1 匿名

匿名是目前社交网络用户隐私保护最主要的方法,根据匿名的对象不同,主要分为节点匿名(node anonymization)和边扰动(edge perturbation)两种方式。前者的目的在于掩盖社交网络成员的真实身份,后者旨在保证网络图可用性的同时通过随机加边和删边阻止攻击者根据已有的关系推断网络节点的身份[1],两种方式经常结合使用,从而达到更好的匿名效果。

社交网络用户由于与众多属性相关联,因此可用于识别相应的用户,Sweeney[2]提出K-匿名(K-anonymity)方法,该

到稿日期:2013-10-29 返修日期:2014-03-21 本文受国家自然科学基金项目:基于博弈论的信息安全理论与方法研究(61272398),国家社会科学基金重点项目:大数据时代网络媒介生态环境下个人信息保护体系的构建研究(13AXW010),中央财经大学博士生重点选题支持计划项目:社交网络平台信息安全综合评价模型研究资助。

黄启发(1979—),男,博士生,主要研究方向为网络经济与安全,E-mail:qifa-h007@63.com;朱建明(1965—),男,教授,博士生导师,主要研究方向为信息安全;宋 彪(1983—),男,博士生,讲师,主要研究方向为经济信息分析;章 宁(1975—),女,教授,博士生导师,主要研究方向为信息系统服务外包。

方法由于没有对敏感属性做任何约束，因此容易受到同质性攻击和背景知识攻击。观察到社交网络图中节点的结构相似性决定了单个节点区别与其他节点的程度，Hay 等人[3]提出了 K-候选人匿名(K-candidate anonymity)，即将网络节点聚类到不同分区，公开每个分区节点的数量、每个分区内部和分区之间的边的密度，用这个匿名的图研究原始图的宏观特征。Liu 和 Terzi[4]指出节点的度序列是高度偏的?，攻击者常常很容易收集到目标个体的度的信息，因此提出一种 K-度匿名(K-degree anonymity)方法，在匿名图中每个节点都与其他至少K－1个节点具有相同的度，K-度匿名图能够阻止背景知识攻击。Zhou 和 Pei[5]假设攻击者知道由目标节点的直接邻域组成的子图，提出 K-邻域匿名(K-neighborhood anonymity)方法，通过泛化节点标签和加边对原图进行修改，直到每个邻域与其他至少 K－1 个其他邻域相比不能被分辨出来，作者证明满足条件的 K-邻域匿名图是一个 NP 难题。Zou 等人[6]假设攻击者知道一个确定用户周围的所有子图，如果在匿名图中子图能够以很高的概率被识别，则用户将面临较高的身份泄露风险。因此，他们提出 K-自同构匿名(K-automorphism anonymity)方法，图中的任何子图都与其他至少 $K-1$ 个子图是同构的。Cormode 等人[7]提出一种 $(K,1)$-聚类 $((K,1)$-groupings)，通过匿名从网络实体到图中节点的映射，可以完美地保护基础网络图结构，利用真实双向图数据进行实验，表明 $(K,1)$-聚类匿名图可以很好地平衡隐私和可用性问题。

随机化匿名(anonymizaiton by randomization)是在保持边的总数不变的情况下，在社交网络图中，通过随机地删除边和增加边来改变图的结构。Hay 等人[8]通过实验证明当随机扰动边的比例在 5%～10%范围内时，确实可以起到匿名的效果，但是，随机扰动边的比例超过了 10%，就会导致信息的大量丢失。Ying 和 Wu[9]提出一种光谱保护随机化(spectrum-preserving randomization)方法，用于引导选择在社交网络图中增加的边和删除的边。Wu 等人[10]用一种低级近似(low rank approximation)方法重建随机化的社交网络结构，以便保留精确的网络拓扑特征，他们的研究表明，实践中重建比随机化引致更小的隐私威胁，因为与重建的网络相比，随机化的网络与原始网络更相似。Vuokko 和 Terzi[11]研究了结构和属性都已经被随机化的社交网络的重建机制，认为重建可以在多项式时间内实现。

网络泛化(network generalization)是一种通过公开网络节点结构特征的汇总信息来缓解结构化背景知识攻击的方法。Zheleva 和 Getoor[12]提出一种两步骤泛化数据的匿名方法：第一步，将节点看作数据表中的记录，匿名它们的属性；第二步，将总的结构信息保留在等价类内部或等价类之间，部分地保护社交网络的结构。Campan 和 Truta[13]提出同时使用属性信息和结构信息最优化效用函数，这种匿名算法经过调整后能够更好地保护社交网络的结构信息和节点的属性值。韦伟等人[14]提出了一种基于 GSNPP(greedy for social network privacy-preserving)算法的社交网络隐私保护方法，该方法首先对原始社交网络图中的节点进行聚类，产生多个节点簇，再通过簇内泛化和簇间泛化的方式对社交网络进行匿名，并量化了匿名过程中的信息丢失。

差分隐私(differential privacy)是指个人隐私泄露的风险不会因为其加入到某个数据库中而显著增加[15]，它看待隐私的视角从数据公开前、后比较关于个体的先验、后验的信念，转移到评估由于个人隐私加入到数据库中而产生的风险上来，它将保护施加于数据释放过程而非数据本身上。因此，其保护的目标是数据的统计信息而不是在数据中保护用户的隐私。一种差分隐私的算法是在计数查询(如：社交网络中多少人年龄超过 22 岁?)中加入拉普拉斯噪声(Laplacian noise)[16]，那么输出范围就是$\{1,\cdots,n\}$，其中 n 是社交网络的大小。Dwork 等人[17]提出一种弱条件下的差分隐私：(ε,δ)-差分隐私((ε,δ)-differential privacy)，用于产生非常不可能的输出结果。

2.2 访问控制

传统的访问控制方法主要是指授权，即信息资源仅对那些被资源所有人授权的用户开放，资源所有人对不同的用户赋予不同的访问权利。但是这种方法对于动态的和处于分布环境下的社交网络不再适用，社交网络更倾向于制定访问者必须满足的详细要求，并用这些要求频繁地标识被授权的人员，当社交网络的结构状态发生变化时，被授权的人员随之变化，而已经存在的授权无须修改[1]。目前对社交网络用户隐私访问控制的研究主要有 4 个方面：

(1)基于规则的访问控制。由于社交网络的特殊性，为了很好地标识被授权人员，制定明确和详细的访问规则对于用户、网络管理者都是至关重要的。Carminati[18]在 2006 年提出了一种基于规则的详细的访问政策，其包含了一系列的访问条件，指明了被授权用户为了获得信息资源所必须具备的关系类型、关系深度和关系的信任水平。后来，针对这种政策的可执行问题，作者[19]又补充了解决方案，即将每个关系与一套分布式规则(distribution rules)相关联以表达他们的隐私偏好，分布式规则包含了一系列分布式条件(distribution conditions)，这些条件会根据被授权用户为了获得访问权必须拥有的关系特征，确定他们访问到一个给定的关系中。

(2)基于访问权的访问控制。“关系传递”是社交网络的重要特征之一，在关系传递的过程中，关系中伴随的信任水平也被同时传递，基于“朋友的朋友也是朋友”的思想，Kruk 等[20]提出一种访问权委派(access rights delegation)模型：D-FOAF(distributed-friend of a friend)，访问权委派的基础是社交网络信息和信任水平，当请求者与信息资源所有人的距离和友谊水平满足要求时，他会获得访问授权，这种访问权能够进一步委派给其他请求者，当且仅当其他请求者符合给定的距离和友谊水平条件时。

(3)基于安全水平的访问控制。安全水平是衡量社交网络中人与人之间信任程度的重要变量，用户隐私的保护就是要隔离不安全的他人，若能为社交网络中每个用户及信息建立安全档案，则隐私保护会变得相当容易和方便。据此，Ali 等[21]提出了一种多层访问控制(multi-level access control)模型，即在信任水平的基础上详细确定用户和资源的安全水平，每个用户的安全水平根据社交网络中其他用户对他的信任评价进行平均计算得到，资源的安全水平与其所有人的安全水平相关联，用户只能访问那些与自身安全水平相等或较低的信息资源。这种方式的最大问题在于，社交网络始终是动态变化的，管理用户和资源的安全水平(如：计算、更新安全水平)会成为一项非常复杂的任务。

(4)基于本体的访问控制。本体是概念化的规范说明，具

有明确、形式化、共享和概念模型的特征[22]，基于本体论(ontology)的信息安全模型是信息安全研究的重要分支。Masoumzadeh 等[23]提出一种基于本体论的访问控制模型(ontology-based access control model)，精炼地表达了社交网络知识的访问控制政策，并用证据-概念原型(proof-of-concept prototype)展示了方法的适用性。

2.3 博弈论在网络安全中的应用

作为应用数学的一个分支，博弈论主要研究游戏中个体的预测行为与实际行为，并分析他们的优化策略，在经济学、计算机科学、军事战略等很多学科都有广泛的应用。近年来，博弈论与信息安全的研究引起了广泛关注，已经取得一些研究成果，如王元卓等[24]利用随机博弈方法对网络攻防进行量化分析；姜伟等[25]利用博弈模型对主动防御的网络安全测评进行建模，并提出了最优选取算法；George 等[26]分析了非结构化网络中恶意用户的均衡策略，并指出网络拓扑的重要作用；Dominic 等[27]分析了社交网络中用户注重邻居安全程度的保护策略，认为注重邻居的安全状况比完全自私能够获得更好的收益；Manshaei 等[28]将博弈论在网络安全方面的研究总结成 6 个方面：物理层和 MAC 层的安全、自组织网络的安全、入侵检测系统、匿名性和隐私、网络安全经济学和密码学。

3 社交网络用户隐私保护的博弈分析

社交网络用户隐私保护的博弈分 3 种情形进行讨论：1)攻防博弈：假设参与博弈的攻防双方都是完全理性和自私的，只从自身的角度出发，根据自身的成本、收益选择采取的策略；2)共同防御博弈：假设防守的社交网络用户之间并不是完全自私的，在考虑自身成本收益的同时，也会关注社交圈内其他关联用户的安全状况和防护水平；3)联合攻击博弈：假设攻击者并不是单独行动，他们也会通过社交网络进行共谋，实施联合攻击，获得更高的攻击效用。

3.1 社交网络用户隐私保护的攻防博弈模型

假设 1：攻击者的策略集为{弱攻击，强攻击}，社交网络用户的防御策略集为{弱防御，强防御}，攻击者选择强攻击时，可以成功攻击所有防御程度的用户；攻击者选择弱攻击时，只能成功攻击弱防御的用户。

假设 2：博弈发生前，每个社交网络用户都会选择适合自己的防御策略，防御策略在博弈过程中不会改变，即用户的防御策略是确定的。但是在不同博弈模型之间，用户可以改变防御策略。

假设 3：攻击者一旦对某用户攻击成功，就会借助此用户对其他关联用户发动攻击，后续攻击成本会减少，减少的程度与两个用户之间的关系层次呈正比，即关系越紧密的关联用户，攻击成功的成本越小。

假设 4：攻击者与社交网络用户之间信息是不对称的，即攻击者不清楚每个社交网络用户具体的防御策略，但清楚社交网络中部分用户采用弱防御策略，部分用户采用强防御策略。

定义 1(攻击成本，Cost of attack)　表示攻击者成功发动一次攻击所发生的成本，包括硬件、软件、专业知识及相应的法律后果等。并假设攻击者对社交网络发动弱攻击时成本为 C_a，发动强攻击时成本为 $2C_a$；对单个用户发动弱攻击时成本为 C_b，发动强攻击时成本为 $2C_b$，且 $C_a>C_b$。攻击成本可以自主增加。

定义 2(防御成本，Cost of defense)　表示社交网络用户为保护自己的隐私所发生的成本，包括硬件投入、安全软件、培训和专业知识等。并假设用户选择弱防御时成本为 C_d，选择强防御时成本为 $2C_d$，防御成本可以自主增加。

定义 3(攻击收益，Value)　表示攻击者攻击成功后获得的收益，即社交网络用户隐私的价值。并假设弱防御用户隐私的价值为 V，且 $V>C_d$，$V>C_a$，$V>C_b$，强防御用户隐私的价值为 $2V$，且 $2V>2C_d$，$2V>2C_a$，$2V>2C_b$，同时认为社交网络用户的防御收益与攻击者的攻击收益在数量上相等。

定义 4(攻击效用，Utility)　表示攻击者获得的攻击收益与攻击成本的比值，即攻击效用 $U=$攻击收益/攻击成本，$U>0$，不同的攻击方式会有不同的攻击效用，并假设攻击者偏好攻击效用大的攻击方式。

定义 5(关系层次 L，Level)　表示两个社交网络用户之间的关系紧密程度，且 $0<L<1$，L 越大表示两者之间的关系越紧密。当攻击者借助攻击成功的用户攻击其他关联用户时，成本是单独攻击这个关联用户的$(1-L)$倍。

为简便起见，假设社交网络中仅有 2 位用户，分别选择弱防御和强防御的策略，攻击者在发动攻击时，由于不清楚每个网络用户具体的防御策略，会有以下 4 种可能的攻击方式(如图 1 所示)。

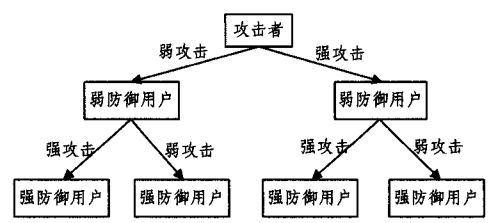

图 1　攻击者的博弈树

1. 先以弱攻击方式攻击社交网络，成本为 C_a，弱防御的用户会被攻击成功，然后借助这个弱防御用户以强攻击方式攻击强防御用户，攻击成功，成本为$(1-L)2C_b$。则总攻击成本为 $C_a+(1-L)2C_b$，获得总攻击收益为 $3V$，攻击效用 $U_1=(3V)/(C_a+(1-L)2C_b)$。

2. 先以弱攻击方式攻击社交网络，成本为 C_a，弱防御用户被攻击成功，然后借助这个弱防御用户以弱攻击方式攻击强防御用户，攻击失败，成本为$(1-L)C_b$。则总攻击成本为 $C_a+(1-L)C_b$，获得总攻击收益为 V，攻击效用 $U_2=(V)/(C_a+(1-L)C_b)$。

3. 先以强攻击方式攻击社交网络，成本为 $2C_a$，弱防御用户先被攻击成功，然后借助这个弱防御用户以强攻击方式攻击强防御用户，攻击成功，成本为$(1-L)2C_b$。则总攻击成本为 $2C_a+(1-L)2C_b$，获得总攻击收益为 $3V$，攻击效用 $U_3=(3V)/(2C_a+(1-L)2C_b)$。

4. 先以强攻击方式攻击社交网络，成本为 $2C_a$，弱防御用户先被攻击成功，然后借助这个弱防御用户以弱攻击方式攻击强防御的网络用户，攻击失败，成本为$(1-L)C_b$。则总攻击成本为 $2C_a+(1-L)C_b$，获得总攻击收益为 V，攻击效用 $U_4=(V)/(2C_a+(1-L)C_b)$。

以上 4 种方式中 $U_1>U_3>U_2>U_4$，因此第 1 种方式为攻击者的最佳策略，即攻击者应先以弱攻击方式对社交网络

发起攻击，部分防御能力低的用户会先被成功攻击，然后借助这些用户对其他关联用户发动强攻击。

在攻防博弈模型中，由于假设社交网络用户是完全理性和自私的，而且防御策略是预先确定的，因此每个用户会根据自身隐私的价值独自选择合适的防御策略，即隐私价值为 V 的用户选择弱防御策略，防御成本为 C_d，隐私价值为 $2V$ 的用户选择强防御策略，防御成本为 $2C_d$。则总防御成本为 $3C_d$，所保护的隐私的总价值为 $3V$。

讨论：根据攻击效用 U_1 的计算公式可以看出，攻击成本 C_a、C_b 越大，攻击效用越小，关系层次 L 越大，攻击效用越大，因此攻击者在发动攻击时，应先发动成本较小的攻击，再发动成本较大的攻击，在将部分用户成功攻击以后，应先对其联系紧密的好友发动攻击，然后再攻击关系松散的好友。

更一般地，假设社交网络中有 3 位用户：P_1，P_2，P_3，他们之间两两相连，$L_{12}=L_{21}$，$L_{23}=L_{32}$，$L_{13}=L_{31}$，且 $L_{12}>L_{13}>L_{23}$，$L_{12}>L_{23}$。他们的防御有两种情形：

第一种情形：有两个用户的隐私价值为 V，都采用弱防御策略（假设为 P_1，P_2），一个用户的隐私价值为 $2V$，采用强防御策略（假设为 P_3）。

此时攻击者的攻击策略为：先以弱攻击方式攻击网络，其中一个弱防御用户先被攻击成功（假设为 P_1），攻击成本为 C_a。对其余两个用户，攻击者由于并不了解他们的防御情况，因此有两种选择：

A：先发动弱攻击，后发动强攻击，若弱攻击成功，则转向下一个用户，若不成功，则发动强攻击。由于 $L_{12}>L_{13}$，因此借助 P_1 先对 P_2 发动弱攻击，攻击成功，成本为 $(1-L_{12})C_b$；由于 $L_{13}>L_{23}$，攻击者会再借助 P_1 对 P_3 发动弱攻击，攻击失败，成本为 $(1-L_{13})C_b$；再对 P_3 发动强攻击，攻击成功，成本为 $(1-L_{13})2C_b$，则总攻击成本为

$$TC_A=C_a+(1-L_{12})C_b+(1-L_{13})3C_b$$

获得隐私的总价值为 $4V$，社交网络用户的总防御成本为 $4C_d$。

B：直接对两个用户分别发动强攻击。借助 P_1 先对 P_2 发动强攻击，攻击成功，成本为 $(1-L_{12})2C_b$；再借助 P_1 对 P_3 发动强攻击，攻击成功，攻击成本为 $(1-L_{13})2C_b$，则总攻击成本为

$$TC_B=C_a+(1-L_{12})2C_b+(1-L_{13})2C_b$$

获得隐私的总价值为 $4V$，社交网络用户的总防御成本为 $4C_d$。

$TC_B-TC_A=(L_{13}-L_{12})C_b<0$，B 方式为最佳选择。

第二种情形：一个用户的隐私价值为 V，采用弱防御策略（假设为 P_1），两个用户的隐私价值为 $2V$，都采用强防御策略（假设为 P_2，P_3）。此时攻击者采取 A、B 两种攻击方式的总攻击成本分别为

$$TC_A'=C_a+(1-L_{12})3C_b+(1-L_{13})3C_b$$

$$TC_B'=C_a+(1-L_{12})2C_b+(1-L_{13})2C_b$$

对于任何 L_{13}、L_{12} 都有 $TC_B'-TC_A'<0$，B 方式为最佳选择，但获得隐私的总价值为 $5V$。社交网络用户的总防御成本为 $5C_d$。

假设社交网络中有 N_1+1+N_2 个用户时，其中 N_1+1 个用户隐私的价值为 V，采用弱防御策略，N_2 个用户隐私的价值为 $2V$，采用强防御策略。则总防御成本为 $(N_1+1+2N_2)C_d$，隐私的总价值为 $(N_1+1+2N_2)V$。

攻击者采取 A 中攻击方式时，总攻击成本为

$$TC_A''=C_a+\sum_{i=1}^{N_1}(1-l_i)C_b+\sum_{j=1}^{N_2}(1-l_i)3C_b$$

攻击者采取 B 种攻击方式时，总攻击成本为

$$TC_B''=C_a+\sum_{i=1}^{N_1}(1-l_i)2C_b+\sum_{j=1}^{N_2}(1-l_j)2C_b$$

$$TC_B''-TC_A''=\sum_{i=1}^{N_1}(1-l_i)C_b-\sum_{j=1}^{N_2}(1-l_j)C_b$$

当 $\sum_{i=1}^{N_1}(1-l_i)C_b>\sum_{j=1}^{N_2}(1-l_j)C_b$ 时，$TC_B''-TC_A''>0$，A 种方式为最佳选择；

当 $\sum_{i=1}^{N_1}(1-l_i)C_b<\sum_{j=1}^{N_2}(1-l_j)C_b$ 时，$TC_B''-TC_A''<0$，B 种方式为最佳选择。

3.2 社交网络用户隐私保护的共同防御博弈模型

在共同防御博弈中，假设社交网络用户之间并不是完全自私的，每个用户都清楚一旦自身被攻击成功，就会给好友带来很大的安全风险，而好友被攻击成功也会给自身安全带来潜在威胁。因此，在保护隐私的过程中，他们除了关心自己的安全成本和安全收益外，还要关注社交网络中其他好友的安全状况和防御水平，追求整体防御水平的最优化。

假设 5：社交网络中，所有用户都采用强防御策略。其他假设和定义与 3.1 节模型相同。

为简便起见，仍先假设社交网络中仅有 2 位用户，其隐私的价值分别为 V 和 $2V$，但都采用强防御策略，因此总防御成本为 $4C_d$，所保护的隐私的总价值仍为 $3V$。对攻击者而言，由于社交网络用户防御水平的提高，弱攻击策略将不再发挥作用，攻击者的最佳选择为 3.1 节模型中的第 3 种攻击方式，即以强攻击方式攻击两位用户，总攻击成本为 $2C_a+(1-L)2C_b$，获得总攻击收益为 $3V$。

讨论：由于假设社交网络用户是理性的，因此在他们都选择强防御策略从而提高整体防御水平时必须要考虑“这种行为是不是合算的?”他们不可能不计后果或不计成本地提高防御水平。因此本文给出以下定理：

定理 1 方案 2 与方案 1 相比，若总攻击成本增加的比例大于总防御成本增加的比例，则认为方案 2 优于方案 1。

其中，方案 1：社交网络用户独自选择适合自身的防御策略。

方案 2：社交网络用户都选择强防御策略。

当社交网络仅有 2 位用户时，方案 1 中攻击者的最佳策略为 3.1 节模型的分析结果，总攻击成本为 $C_a+(1-L)2C_b$，社交网络用户的总防御成本为 $3C_d$；方案 2 中总攻击成本为 $2C_a+(1-L)2C_b$，总防御成本为 $4C_d$，两个方案的攻击收益相同。方案 2 与方案 1 相比：

总攻击成本增加的比例为

$$R_1=[(2C_a+(1-L)2C_b)-(C_a+(1-L)2C_b)]/(C_a+(1-L)2C_b)$$
$$=C_a/(C_a+(1-L)2C_b)$$

总防御成本增加的比例为

$$R_2=(4C_d-3C_d)/(3C_d)=1/3$$

$$R=R_1-R_2=[2C_a-2(1-L)C_b]/[3C_a+6(1-L)C_b]>[2C_b-2(1-L)C_b]/[3C_a+6(1-L)C_b]\text{（因为 }C_a>C_b\text{）}$$
$$=(2LC_b)/[3C_a+6(1-L)C_b]>0$$

因此，若社交网络用户不是完全自私的，在都采用强防御策略后，会使攻击者总攻击成本增加的比例大于用户总防御成本增加的比例，用户的整体防御水平会得到优化。而且 R_1、R 都与 L 成正比，L 越大，R_1、R 越大，即用户之间关系越紧密，都采用强防御策略后，攻击者的总攻击成本增加的比例就越高，总攻击成本增加比例与总防御成本增加比例之间的差距就越大，整体防御水平优化的效果就越好。

更进一步，当社交网络中有 3 位用户且都加强防御时，攻击者只能以强攻击方式攻击所有用户，在 3.1 节模型所示的两种情形下，发生的总攻击成本都为 $2C_a+(1-L_{12})2C_b+(1-L_{13})2C_b$，则方案 2 与方案 1 相比：

第一种情形：采取 B 种方式时总攻击成本增加的比例为

$R_1'=C_a/[C_a+(1-L_{12})2C_b+(1-L_{13})2C_b]$

总防御成本增加的比例为

$R_2'=(6C_d-4C_d)/(4C_d)=1/2$

$R'=R_1'-R_2'=[C_a-2C_b(2-L_{12}-L_{13})]/[2C_a+4C_b(2-L_{12}-L_{13})]$

当 $L_{12}+L_{13}>2-C_a/2C_b$ 时，$R'>0$。

第二种情形：总攻击成本增加的比例为

$R_1''=C_a/[C_a+(1-L_{12})2C_b+(1-L_{13})2C_b]$

总防御成本增加的比例为

$R_2''=(6C_d-5C_d)/(5C_d)=1/5$

$R''=R_1''-R_2''=[4C_a-2C_b(2-L_{12}-L_{13})]/[2C_a+4C_b(2-L_{12}-L_{13})]>[4C_a-4C_b]/[2C_a+4C_b(2-L_{12}-L_{13})]$

对于所有 $0<L_{12}<1$、$0<L_{13}<1$，都有 $R''>0$。

因此，当社交网络中整体用户的隐私价值较低时，只有关系满足一定条件的朋友之间提高防御强度，整体防御水平才能得到优化，否则可能会有些“不合算”。而当整体用户的隐私价值较高时，无论关系程度如何，都应该提高防御强度，整体防御效果都会得到优化。

假设社交网络中有 N_1+1+N_2 个用户且都采用强防御策略，攻击者只能对所有用户采取强攻击方式，总攻击成本为

$$TC_{总}''=2C_a+\sum_{i=1}^{N_1}(1-l_i)2C_b+\sum_{j=1}^{N_2}(1-l_i)2C_b$$

总防御成本增加的比例为

$R_{防}=(N_1+1)/(N_1+1+2N_2)$

攻击者采取 A 种方式攻击时，总攻击成本增加的比例为

$R_A=(TC_{总}''-TC_A'')/TC_A''$

当 $C_a+\sum_{i=1}^{N_1}(1-l_i)C_b>\frac{N_2+2N_1+2}{2N_2}\sum_{j=1}^{N_2}(1-l_j)2C_b$ 时，$R_A-R_{防}>0$，即攻击者对社交网络和弱防御用户发动弱攻击的成本之和大于对强防御用户发动强攻击成本的 $\frac{N_2+2N_1+2}{2N_1}$ 倍时，社交网络用户提高防御强度可以改善整体防御水平。

攻击者采取 B 种方式攻击时，总攻击成本增加的比例为

$R_B=(TC_{总}''-TC_B'')/TC_B''$

当 $\sum_{i=1}^{N_1}(1-l_i)C_b+\sum_{i=1}^{N_2}(1-l_j)C_b<(N_2C_a)/[(N_1+1)]$ 时，$R_B-R_{防}>0$，即攻击者对社交网络中的所有用户发动弱攻击的成本之和小于对社交网络发动弱攻击成本的 $\frac{N_2}{N_2+1}$ 倍时，社交网络用户提高防御强度可以改善整体防御水平。

因此，当社交网络中的用户较多时，无论攻击者选择 A 种攻击方式还是 B 种攻击方式，都需满足一定的条件才能通过提高防御强度改善整体的防御水平。

3.3 社交网络用户隐私保护的联合攻击博弈模型

以上 3.1 节和 3.2 节的分析中，都假设攻击者只有一个，且此攻击者的攻击能力可弱可强，而现实中可能并非如此：有些攻击者可能只具备弱攻击的能力，另一些攻击者具备强攻击的能力。为了使分析更加贴近现实，在联合攻击博弈模型中作如下假设：

假设 6：攻击者分为两类：弱攻击者 WA(Weak Attacker)和强攻击者 SA(Strong Attacker)，他们的攻击能力在博弈前是确定的，博弈过程中不发生改变。弱攻击者只能发动弱攻击，强攻击者可以发动弱攻击，也可以发动强攻击。同时，假设社交网络用户分别采用适合自身的防御策略，而非都采用强防御策略。

由于社交网络是个公开的网络平台，并不能阻止攻击者通过社交网络建立社交圈子，因此，攻击者可能会通过社交网络进行共谋，对用户发动联合攻击。

定理 2 若与非联合攻击相比，联合攻击能够提高攻击者的攻击效用，则联合攻击优于非联合攻击。

为简便起见，假设社交网络中攻击者和用户都为 2 位，攻击者分别为弱攻击者 WA 和强攻击者 SA，他们对社交网络发动弱攻击的成本都为 C_a，发动强攻击的成本为 $2C_a$，对单个用户发动弱攻击时成本为 C_b，发动强攻击时成本为 $2C_b$，且 $C_a>C_b$。用户的防御策略分别为弱防御和强防御，隐私的价值分别为 V 和 $2V$。当两个攻击者分别独自对网络用户发动攻击时：

弱攻击者 WA：最佳攻击方式同 3.1 节模型中的第二种方式，先对社交网络发动弱攻击，成本为 C_a，弱防御的用户被攻击成功，然后借助弱防御用户对强防御用户发动弱攻击，攻击失败，成本为 $(1-L)C_b$，总攻击成本为 $C_a+(1-L)C_b$，获得总攻击收益为 V，攻击效用 $U_{wa}=(V)/(C_a+(1-L)C_b)$。

强攻击者 SA：最佳攻击方式同 3.1 节模型中的第 1 种方式，先对社交网络发动弱攻击，成本为 C_a，弱防御的用户被攻击成功，然后借助弱防御用户对强防御用户发动强攻击，攻击成功，成本为 $(1-L)2C_b$，总攻击成本为 $C_a+(1-L)2C_b$，获得总攻击收益为 $3V$，攻击效用 $U_{sa}=(3V)/(C_a+(1-L)2C_b)$。

当两个攻击者共谋时，对网络用户发动联合攻击，即首先由弱攻击者 WA 对社交网络发动弱攻击，成功攻击弱防御的用户，然后由强攻击者 SA 借助弱防御用户对其他用户发动强攻击。则：

弱攻击者 WA：攻击成本为 C_a，攻击收益为 V，攻击效用 $U'_{wa}=(V)/(C_a)$。

强攻击者 SA：攻击成本为 $(1-L)2C_b$，攻击收益为 $2V$，攻击效用 $U'_{sa}=(2V)/((1-L)2C_b)$。

联合攻击与非联合攻击相比：

$\Delta U_{wa}=U'_{wa}-U_{wa}=(V)/(C_a)-(V)/(C_a+(1-L)C_b)>0$

$\Delta U_{sa}=U'_{sa}-U_{sa}=(2V)/((1-L)2C_b)-(3V)/(C_a+(1-L)2C_b)>0$

因此，若攻击者借助社交网络进行共谋，对网络用户发动联合攻击，则都可以获得更好的攻击效用。

讨论：根据 ΔU_{wa}、ΔU_{sa} 的计算公式可以得出，ΔU_{wa} 与 L 成反比，ΔU_{sa} 与 L 成正比，即用户之间的关系越紧密，攻击者通过共谋发动联合攻击时，弱攻击者攻击效用的增加值越小，强攻击者攻击效用的增加值越大。因此，强攻击者比弱攻击者更倾向于发动联合攻击。

假设社交网络中有 N_1+1+N_2 个用户，其中 N_1+1 个用户隐私的价值为 V，采用弱防御策略，N_2 个用户隐私的价值为 $2V$，采用强防御策略。当两个攻击者分别独自对社交网络发动攻击时：

弱攻击者 WA：最佳攻击方式同 3.1 节模型中的第 2 种方式，始终对社交网络及网络中的用户发动弱攻击，对社交网络及弱防御用户攻击成功，对强防御用户攻击失败，则总的攻击成本为

$$TC_{WA}=C_a+\sum_{i=1}^{N_1}(1-l_i)C_b+\sum_{j=1}^{N_2}(1-l_j)C_b$$

获得的总收益为 $(N_1+1)V$，攻击效用为

$$U_{wa}^{*}=(N_1+1)V/TC_{WA}$$

强攻击者 SA：先对社交网络发动弱攻击，成本为 C_a，然后可以分别采取 A、B 两种攻击方式对网络中的用户发动攻击，都可以攻击成功，则总的攻击成本分别为

$$TC_{SA}^{A}=C_a+\sum_{i=1}^{N_1}(1-l_i)C_b+\sum_{j=1}^{N_2}(1-l_j)3C_b$$

$$TC_{SA}^{B}=C_a+\sum_{i=1}^{N_1}(1-l_i)2C_b+\sum_{j=1}^{N_2}(1-l_j)2C_b$$

获得的总收益为 $(N_1+1+2N_2)V$，总攻击效用分别为

$$U_{Sa}^{A}=(N_1+1+2N_2)V/TC_{SA}^{A}$$

$$U_{Sa}^{B}=(N_1+1+2N_2)V/TC_{SA}^{B}$$

当两个攻击者共谋时，对社交网络及用户发动联合攻击，即弱攻击者 WA 对社交网络发动弱攻击，攻击成功，面对社交网络中巨大用户隐私价值的诱惑，弱攻击者 WA 不可能此时将攻击权转交给强攻击者 SA，他会再对网络中的所有用户发动弱攻击，可以成功攻击弱防御用户，强防御用户攻击失败；然后由强攻击者 SA 借助弱防御用户对其他用户发动强攻击。为了后面计算的方便，提出一个较为合理的假设：

假设 7：对社交网络中的弱防御用户发动弱攻击获得的效用与对强防御用户发动强攻击获得的效用相同。

则联合攻击时：

弱防御用户 WA：攻击成本、攻击收益和攻击效用与非联合攻击时相同。

强防御用户 SA：攻击成本为

$$TC_{SA}=\sum_{j=1}^{N_2}(1-l_j)2C_b$$

获得的攻击收益为 $2N_2V$，攻击效用为

$$U_{Sa}^{*}=2N_2V/TC_{SA}$$

联合攻击与非联合攻击相比：

弱防御用户 WA 的攻击效用没有变化；

强防御用户 SA：

$$\Delta U_{sa}^{A}=U_{Sa}^{*}-U_{Sa}^{A}$$

$$\Delta U_{sa}^{B}=U_{Sa}^{*}-U_{Sa}^{B}$$

根据假设 7 可证明：$\Delta U_{sa}^{A}>0$，$\Delta U_{sa}^{B}>0$。

讨论：联合攻击时，弱攻击者的攻击效用没有变化，而强攻击者的攻击效用增加，因此，为了共谋能顺利进行，需要在两个攻击者之间建立效用再分配机制，由强攻击者将多获得的效用转让一部分给弱攻击者，从而提高弱攻击者共谋的积极性。

结束语 在社交网络用户隐私保护的过程中，将恶意的攻击者和网络用户视为攻防的双方，分析他们的成本收益及最佳策略，具有很好的现实意义。通过本文的分析我们认为，社交网络用户在保护隐私的过程中，完全理性和自私并不是最佳策略；他们不仅仅要注重自身安全防御状况，也要关注好友的隐私保护水平，这样才能更好地保护整体的隐私；整体防御水平优化的效果，要综合考虑用户隐私价值的大小和用户之间关系层次的紧密程度；而对于攻击者来说，相互协作发动联合攻击，虽然获得的总收益不会增加，但效用水平会得到提高。

参 考 文 献

[1] Carminati B, Frrari E, Petego A. Security and privacy in social networks[J]. Encyclopedia of Information Science and Technology, 2009, 7: 3369-3376

[2] Sweeney L. K-anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5): 557-570

[3] Hay M, Milau G, Jensen D, et al. Resisting structural reidentification in anonymized social networks[J]. Proceedings of the VLDB Endowment, 2008, 1(1): 102-114

[4] Liu Kun, Terzi E. Towards identity anony- mization on graphs [C]// Proceedings of the ACM SIGMOD Conference. Vancouver, Canada, 2008: 93-106

[5] Zhou Bin, Pei Jian. Preserving privacy in social networks against neighborhood attack[C]// IEEE 24th International Conference on Data Engineering. 2008: 506-515

[6] Zou Lei, Chen Lei, Ozsu M T. K-automorphism: A general framework for privacy preserving network publication[J]. Proceedings of 35th International Conference on Very Large Data Base, 2009, 2(1): 946-957

[7] Cormode G, Srivastava D, Yu Ting, et al. Anonymizing bipartite graph data using safe groupings[J]. Proceedings of the VLDB Endowment, 2008, 1(1): 833-844

[8] Hay M, Milau G, Jensen D, et al. Anonymizing social networks [J]. Computer Science Department Faculty Publication Series, 2007: 180-197

[9] Ying Xiao-wei, Wu Xin-tao. Randomizing social networks: a spectrum preserving approach [C]// SDM. 2008, 8: 739-750

[10] Wu Le-ting, Ying Xiao-ei, Wu Xin-tao. Reconstruction of randomized graph via low rank approximation[C]// SDM. 2010: 60-71

[11] Vuokko N, Terzi E. Reconstructing rando- mized social networks[C]// SDM. 2010: 49-59

[12] Zheleva E, Getoor L. Preserving the privacy of sensitive relationships in graph data [M]// Privacy, security, and trust in KDD. Springer Berlin Heidelberg, 2008: 153-171

[13] Campan A, Truta T M. A clustering approach for data and structural anonymity in social networks [M]// Privacy, Securi-

ty, and Trust in KDD. Springer Berlin Heidelberg, 2009: 33-54

[14] 韦伟，李杨，张为群. 一种基于 GSNPP 算法的社交网络隐私保护方法研究[J]. 计算机科学，2012，39(3)：104-106

[15] Dwork C. Differential privacy[C]// ICALP. 2006: 1-12

[16] Dwork C, McSherry F, Nissim K, et al. Calibrating noise to sensitively in privacy data analysis[M]// Theory of Cryptography. Springer Berlin Heidelberg, 2006: 265-284

[17] Dwork C, Kenthapadi K, McSherry F, et al. Our data, ourselves: privacy via distributed noise genetation [M] // Advances in Cryptology-EUROCRYPT 2006. Springer Berlin Heidelberg, 2006: 486-503

[18] Carminati B, Ferrari E, Pergo A. Rule-based access control for social networks[C]// Proceedings of OTM Workshop. Montpellier, France, 2006: 1734-1744

[19] Carminati B, Ferrari E, Pergo A. Private relationship in social networks[C]// Proceedings of ICDE Workshops. Istanbul, Turkey, 2007: 163-171

[20] Kruk S R, Grzonkowski S, Gzella A, et al. D-FOAF: Distributed identity management with access right delegation[C]// R Mizoguchi, Shi Z Z, Giunchiglia F, eds. ASWC, Volume4185 of Lecture Notes in Computer Science. Springer, 2006: 140-154

[21] Ali B, Villegas W, Maheswaran M. A trust based approach for protecting user data in social networks [C] // Proceedings of Conference on the Center for Advanced Studies on Collaborative Research. Richmond Hill, Ontario, Canada, 2007: 288-293

[22] Gruber T. Towards principles for the design of ontologies used for knowledge sharing[J]. International Journal of Human-Computer Studies, 1995, 43(5/6): 907- 928

[23] Masoumzadeh A, Joshi J. OSNAC: an ontology-based access control model for social networking systems[C]// IEEE Second International Conference on Social Computing. 2010: 751-759

[24] 王元卓，林闯，程学旗，等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报，2010(9)：1748-1762

[25] 姜伟，方滨兴，田志宏，等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报，2009(4)：817-887

[26] George T, John S. Malicious users in unstructured networks [C]// 26th IEEE International Conference on Computer Communications. 2007: 884-891

[27] Meier D, Oswald Y A, Schmid S, et al. On the windfall of friendship inoculation strategies on social networks[C]// Proceedings of the 9th ACM Conference on Electronic Commerce. 2008: 294-301

[28] Manshaei M, Zhu Quan-yan, Alpcan T, et al. Game theory meets network security and privacy [J]. ACM Computing Surveys, 2013, 45(3): 25-69

（上接第 159 页）

参 考 文 献

[1] 王意洁，孙伟东，周松，等. 云计算环境下的分布存储关键技术[J]. 软件学报，2012，23(4)：926-986

[2] 张亚勤. 未来计算在“云-端”[OL]. http://blog.sina.com.cn/s/blog_596ccc870100apsl.html

[3] Furht B, Escalante A. Handbook of Cloud Computing [M]. Springer Science Business Media, LLC 2010

[4] Wang L, Luo J, Shen J, et al. Cost and time aware ant colony algorithm for data replica in alpha magnetic spectrometer experiment[C]// 2013 IEEE International Congress on Big Data (BigData Congress). IEEE, 2013: 247-254

[5] Dong F, Luo J, Song A, et al. An effective data aggregation based adaptive long term CPU load prediction mechanism on computational grid[J]. Future Generation Computer Systems, 2012, 28(7): 1030-1044

[6] Moore R, Prince TA, Ellisman M. Data-Intensive computing and digital libraries[J]. Communications of the ACM, 1998, 41(11): 56-62

[7] Bell W H, Cameron D G, Carvajal-Schiaffino R, et al. Evaluation of an economy-based file replication strategy for a data grid[C]// Proceedings CCGrid 2003 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2003. IEEE, 2003: 661-668

[8] Ghemawat S, Gobioff H, Leung S T. The Google file system [J]. ACM SIGOPS Operating Systems Review, ACM, 2003, 37(5): 29-43

[9] Shvachko K, Kuang H, Radia S, et al. The hadoop distributed file system, Mass Storage Systems and Technologies (MSST) [C]// 2010 IEEE 26th Symposium on. IEEE, 2010: 1-10

[10] 侯孟书，王晓斌，卢显良，等. 一种新的动态副本管理机制[J]. 计算机科学，2006，33(9)：50-51

[11] Foster R K. Identifying Dynamic Replication Strategies for a High Performance Data Grid[C]// Proceeding of the Second International workshop on Grid Computing. Denver, November 2003: 75-86

[12] 李静，陈蜀宇，吴长泽. 一种基于安全的网格数据副本策略模型[J]. 计算机应用，2006，26(10)：2282-2284

[13] Yuan Dong, Yang Yun, Liu Xiao, et al. A Highly Practical Approach toward Achieving Minimum Data Sets Storage Cost in the Cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1234-1244

[14] S Shao-zhong, K Fan-Sen, W Li-fang. Application of Baumol-Wolfe method on planning location selecting of automotive components manufacturing distribution center, Transportation, Mechanical, and Electrical Engineering (TMEE)[C]// 2011 International Conference on. IEEE, 2011: 132-136

[15] Winter P. Steiner problem in networks: a survey[J]. Networks, 1987, 17(2): 129-167

[16] 李镇坚，朱洪. 一种点边带权最小生成树的近似算法[J]. 计算机应用与软件，2008，25(1)：12-13

[17] Yang Y, Liu K, Chen J, et al. An algorithm in SwinDeW-C for scheduling transaction-intensive cost-constrained cloud workflows[C]// IEEE Fourth International Conference on e-Science. IEEE, 2008: 374-375