一个基于博弈理论的隐私保护模型

张伊璇[1)] 何泾沙[1)] 赵 斌[1)] 朱娜斐[2)]

[1)](北京工业大学软件学院 北京市物联网软件与系统工程技术研究中心 北京 100124)

[2)](中国科学院软件研究所 北京 100190)

摘 要 作为计算机网络用户十分关注的问题之一,隐私保护是信息安全领域当前的一个研究热点.目前的隐私保护方案主要分为匿名和访问控制两大类,它们通过使用不同的技术手段防止用户重要隐私信息的泄露,各有优缺点.然而,运用博弈理论分析这些隐私保护模型,可以发现访问者与隐私信息拥有者之间存在着囚徒困境.因此,为了更有效地解决隐私保护问题,该文从获取收益的角度研究隐私保护,建立一个基于博弈理论的隐私保护模型,在允许访问者对隐私相关信息进行访问的同时,能有效阻止访问者试图获取被访问者不希望泄露的隐私信息的行为.该模型以历史访问数据作为基础,结合访问场景,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,计算出访问者进行善意访问的概率,通过将该概率与隐私信息拥有者对隐私泄露的容忍程度相比较,最终决定是否允许访问者提出的访问请求.该文重点介绍该模型的实现流程、博弈过程及具体架构,并且通过实验与传统模型进行比较,验证提出的隐私保护模型能够对用户的隐私信息提供更加有效的个性化保护.

关键词 隐私保护;博弈论;纳什均衡;阈值;囚徒困境

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2016.00615

A Privacy Protection Model Base on Game Theory

ZHANG Yi-Xuan[1)] HE Jing-Sha[1)] ZHAO Bin[1)] ZHU Na-Fei[2)]

[1)](*School of Software Engineering, Beijing Engineering Research Center for IoT Software and Systems, Beijing University of Technology, Beijing* 100124)

[2)](*Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

Abstract As a very important issue that network users are concerned about, privacy protection is an active research topic. Current solutions on privacy protection can be classified primarily into two categories: anonymity and access control, each following a different approach and relies on different technical means in the prevention of the disclosure of user privacy information and thus has some advantages and disadvantages. Meanwhile, by applying game theory to analyzing traditional privacy models, we can derive the prisoner's dilemma between the two sides of the access. To deal with the privacy protection issue more effectively, in this paper, we propose a privacy protection model based on game theory from the point of view of realizing benefits from the access with the goal of allowing access to a certain extent while denying further access when disclosure of privacy is about to happen. By making use of information about historical access and considering current access scenario, our proposed model would perform analysis on the benefits that both sides of the access could realize and thus derive the probability that the access is an honest one. Access control decision can then be made by comparing the probability with the tolerance level on privacy disclosure stated in the access control policy. We will describe the procedure in our model

收稿日期:2015-01-31;最终修改稿收到日期:2015-10-31.本课题得到国家自然科学基金(61272500)、国家"八六三"高技术研究发展计划项目基金(2015AA017204)和北京市自然科学基金(4142008)资助.**张伊璇**,女,1988 年生,博士研究生,主要研究方向为信息安全、访问控制、隐私保护、博弈论等.E-mail:s201125006@emails.bjut.edu.cn.**何泾沙**(通信作者),男,1961 年生,博士,教授,博士生导师,主要研究领域为计算机与网络安全、网络测试技术、无线通信技术、数字取证.E-mail:jhe@bjut.edu.cn.**赵 斌**,男,1979 年生,博士研究生,讲师,主要研究方向为网络安全、信任管理.**朱娜斐**,女,1983 年生,博士后,主要研究方向为网络安全、隐私保护、互联网测试.

and the game play scenario and present the general framework of the model. We will also show some experiment results to demonstrate the effectiveness of our model as well as its superiority over traditional access control models through comparison analysis.

Keywords privacy protection; game theory; Nash equilibrium; threshold; prisoner's dilemma

1 引 言

当前,随着计算机技术以及信息基础设施的高速发展,网络成为人与人之间通信所必不可少的媒介之一,越来越多的个人隐私信息在网络中存储和传播.因此,网络已经成为犯罪分子窃取用户个人隐私信息的首要途径,带来了很多隐私保护方面的问题,严重威胁着网络社会与网络经济的快速和健康发展[1-2].根据调查显示,随着大数据时代的到来,85%的网络用户普遍担心自身资料被他人获取与扩散,这会给个人隐私带来严重威胁[3].

当前造成网络中用户隐私信息泄露的原因主要有两个:技术缺陷和利益诱惑.而目前关于隐私保护的研究主要集中于通过技术手段防止用户隐私信息的泄露,针对隐私保护的技术手段的研究主要集中在两个方面:匿名和访问控制.两者在实现保护的方式上有所不同,匿名是从外部视角来达到隐私保护的目的,而访问控制则是从内部视角来实现隐私保护的.

匿名是当前常用的隐私保护方法之一,它的主要原理是在获取或使用用户的隐私信息时,不使用用户的真实身份信息,而是使用匿名的方式,使他人无法将采集到的信息与用户的真实身份进行关联,以此来达到保护用户隐私的目的.根据对象的不同,匿名主要包括节点匿名[4-6]和边匿名[7-8],而将两者结合使用可以达到更好的隐私保护效果.节点 K-匿名的主要思想是访问攻击者选定攻击目标后,在匿名化的社交网络中进行匹配识别时,使隐私泄露的概率小于 $1/K$,主要手段是将社会网络中所有节点聚类成若干超节点,其中每个超节点至少包含 K 个节点,并且做到超节点中的节点之间相互不可区分.节点 K-匿名的缺点是执行效率较低,不适用于大型网络.边 K-匿名与节点 K-匿名的主要思想相似,其主要手段是由一些边组成子图,当访问攻击者将目标所在的特定子图作为背景知识进行隐私攻击时,社会网络中至少有 K 个子图可作为候选项,从而使目标子图导致隐私泄露的概率低于 $1/K$[9].自从 Sweeney[10]在 2002 年提出 K-anonymity(K-匿名)技术用于保护用户隐私信息后,专家和学者们对匿名方法进行了深入的研究.朱青等人[11]在总结前人研究的 K-匿名算法中准标识符对敏感属性的影响的基础上,为了解决个性化条件下 Web 查询服务的数据隐私保护问题,提出了一种面向查询服务的数据隐私保护算法,直接通过匿名化数据计算准标识符对敏感属性的效用以及改进效用矩阵,以达到更好的保护数据隐私安全的目的.黄毅等人[12]针对基于位置服务的广泛应用给用户带来的隐私泄露问题,在基于中心服务器的位置 K-匿名方法的基础上,提出了一种用户协作无匿名区域的隐私保护方法 CoPrivacy,在不使用匿名区域的情况下达到 K-匿名的效果,并且提高了匿名系统的整体性能,简化了服务提供商的查询处理过程.霍峥等人[13]针对无线网络签到服务中假名用户的轨迹隐私泄露问题,提出了一种轨迹隐私保护方法 PrivateCheckIn,设计了一种签到序列缓存机制,通过为缓存的签到序列建立前缀树,对前缀树进行剪枝及重构形成 K-匿名前缀树,遍历 K-匿名前缀树得到 K-匿名签到序列,以达到轨迹 K-匿名的隐私保护效果.然而,基于匿名的隐私保护方法存在许多不完善之处.在本质上,匿名保护方法中的保护对象不是隐私信息本身,而是隐私信息拥有者的真实身份,实现隐私信息保护是通过隐藏隐私信息拥有者的真实身份信息而达到.因此,一旦隐私信息拥有者的身份信息通过其他渠道或方式泄露出去,其所有的隐私信息就会被泄露.此外,由于可以对获取到的背景信息实施分析等攻击手段,匿名保护无法有效抵御一致性攻击和背景知识攻击,造成匿名比较容易遭到破解.

隐私保护的第 2 种主要技术手段是基于访问控制的隐私保护.该类方法主要是对传统的面向信息安全的访问控制方法进行适当扩展,以满足保护用户隐私信息的要求.Sun 等人[14]通过研究访问控制在医疗领域中的应用,提出了一个保护数字化隐私信息的方法,以提高医疗领域数字化信息的安全性.在普适计算环境中,用户的隐私保护意愿可以通过

允许用户自己制定面向隐私信息的访问控制策略(隐私策略)而得到实现,研究隐私策略的统一表示及其执行机制可以有效地解决隐私策略的多样性问题[15]. Tan[16]提出了一个适用于普适计算环境的轻量级有条件的隐私保护认证和访问控制方案,用以解决在普适计算环境中只能为合法用户提供服务与用户希望在获取隐私相关服务过程中保证自身隐私信息的匿名性二者之间产生的矛盾. Lu 等人[17]提出了一个适用于移动医疗急救的安全和隐私保护的计算框架 SPOC,在基于属性的访问控制和一个新的隐私保护度量及计算技术的基础上,引入了以用户为中心的隐私访问控制技术,用以解决目前因为智能手机和无线传感器网络的普遍应用而得到蓬勃发展的移动医疗急救系统中信息安全和隐私保护的诸多问题. Fotiou 等人[18]提出了一个访问控制实施委托方案,在该方案中,信息的提供者可以根据访问控制策略评估访问者提交的访问请求,无需考虑访问者的凭证或者是访问策略的实际定义,该方案可以保护用户身份,为隐私保护设置基础. 然而,以上这些基于访问控制的隐私保护模型或方法也存在着诸多的不完善之处,这是由于这些基于访问控制的隐私保护模型采取的技术路线基本上是在传统的面向信息安全的访问控制模型中加入隐私保护的相关策略,从而对已有模型进行一定的扩展,使访问控制策略在保护信息安全的同时反映隐私保护的需求. 但是,这样的解决方案无法从根本上根据隐私保护的特点,使隐私信息拥有者能够实时动态地控制访问者的访问请求,使访问者获得的信息无法超过隐私信息拥有者对于隐私信息泄露的容忍程度,也没有考虑访问者可以通过多次得到允许的访问所产生的叠加效应而获得隐私信息这一问题. 此外,目前所提出的模型或方法一般也缺乏广泛的适用性,大多针对的是具体应用环境中的隐私保护问题,因此无法满足普遍情况下的隐私保护需求.

综上所述,目前对用户的隐私信息进行保护的两种主要技术各自存在着不足. 在本文中,我们另辟蹊径,从利益的角度去研究隐私保护问题,建立隐私保护模型,在访问者对被访问者的隐私信息进行访问的过程中,假设隐私信息的保护者和访问者双方都要为可能采取的行为付出一定的代价,而将付出的代价和获得的收益作为双方决策时要考虑和权衡的因素. 基于以上观点,本文将隐私信息访问者和拥有者(被访问者)视为相互博弈的双方,通过博弈理论对善意访问或恶意访问(对访问者而言)和允许访问(泄露)或拒绝访问(不泄露)(对被访问者而言)这个过程中双方所采取的策略以及获得的相应收益进行分析,从而建立一个博弈模型,作为实现用户隐私信息保护的基础,最终达到有效保护用户隐私信息的目的.

在访问及获取隐私信息的过程中,访问者提出访问请求后,被访问者会根据隐私保护策略决定是否允许访问者的访问请求. 在这里,我们遵循以下两个原则:第一,不同的被访问者对泄露个人隐私信息的容忍程度存在差异,反映出个人喜好或对隐私信息保护的敏感程度;第二,我们假设访问者对同一被访问者进行访问的次数具有叠加效应,即随着访问次数的增加,访问者获取被访问者隐私的可能性或概率也会越大. 因此,随着访问次数的增加,被访问者的隐私保护意识也应随即提高. 为此,在隐私保护模型中,我们将访问者没有超过被访问者对隐私泄露容忍程度的访问请求视为善意访问,而将超过被访问者容忍程度的访问请求视为恶意访问. 在访问控制系统中就可以根据以上两个原则设定隐私保护策略,使访问控制系统能够根据被访问者设定的隐私保护策略去接受访问者的善意请求,同时拒绝恶意请求. 以上的隐私保护模型设计思路与传统的隐私保护模型的不同之处在于,传统的隐私保护模型通常忽略了隐私保护的这些重要特点,仅仅判断访问者当前的访问请求属于善意还是恶意. 虽然访问者每次的访问请求都可能是善意的,但是通过将多次访问得到的不同信息叠加结合起来,则可能会超过被访问者对隐私泄露的容忍程度,最终造成隐私泄露. 被访问者对隐私信息泄露的容忍程度以及对隐私信息进行访问的叠加效应是本文提出的隐私保护模型中的研究重点.

本文运用博弈论对隐私保护问题进行分析,提出了一个隐私保护模型. 其中,隐私信息的访问者和拥有者(被访问者)是博弈的双方,并且双方所采取的博弈策略都是自然存在的. 对于被访问者来说,能够采取的策略是“允许访问隐私信息”或“拒绝访问隐私信息”;对于访问者来说,能够采取的博弈策略是“善意访问隐私信息”或“恶意访问隐私信息”,用是否超过被访问者对隐私泄露的容忍程度作为判断的依据. 博弈双方采取不同的博弈策略将会带来不同的收益,而对于隐私信息之间的关联性问题,则在计算双方收益时还要考虑访问者过去已经获得的隐私信息对本次访问带来的影响,博弈论中的重复博弈能够很好地应用于描述这一过程. 以收益作为基

础,访问双方进行博弈可能存在纳什均衡,而又通过纳什均衡得到访问者善意访问的概率.而被访问者可以根据自己对隐私泄露的容忍程度在隐私保护策略中设定一个阈值,只有访问者善意访问的概率高于该阈值时才允许访问者的访问请求.在每一次访问结束后,被访问者将该次访问所涉及的隐私信息进行记录,作为后续博弈中对同一访问者的请求进行收益计算的一个因素.访问者访问的次数越多,根据叠加效应,获得的隐私信息的内容可能会越来越多,造成泄露用户隐私的概率就会越来越大.因此,同一访问者在先后不同次访问中所对应的收益是不同的,其善意访问的概率也应该在下降,直到低于被访问者设置的阈值,此时访问者将不再被允许访问被访问者的隐私信息.本模型假设博弈双方均是理性的,访问者与被访问者的决策有先后顺序,但是先进行决策的访问者采取的策略并不能被被访问者观察到,因此可以视为二者同时进行决策,因而该博弈属于静态博弈.

本文第 2 节对博弈理论的一些预备知识进行简介;第 3 节介绍传统隐私保护模型中访问者与被访问者的策略博弈过程,从而得到博弈双方所面对的囚徒困境问题;第 4 节详细介绍本文所提出的基于博弈理论的隐私保护模型的实现流程、博弈过程、具体架构等主要内容;第 5 节通过对比实验与分析验证所提出的模型保护用户隐私的有效性及优越性;第 6 节总结本文的研究工作,并对未来的研究工作进行展望.

2 博弈论预备知识介绍

博弈理论源于1944年 von Neumann 和 Morgenstern[19] 合著的 Game Theory and Economic Behaviors(《博弈论与经济行为》)一书,该书首次完整而清晰地表述了博弈论的研究框架,并且阐述了博弈论的基本公理.在之后的很长一段时间里,对博弈论的研究仅仅停留在双人零和博弈上,直到 20 世纪 50 年代初,博弈论大师 Nash[20] 提出了博弈论中最重要的理论——Nash 均衡,确定了非合作博弈的形式和理论基础,将博弈论的研究领域扩展到非合作博弈以及非零和博弈中.根据博弈双方之间是否存在一个具有约束性的协议,博弈论可以分为合作博弈及非合作博弈;根据博弈双方利益之和是否为零,博弈论可以分为零和博弈及非零和博弈;根据博弈方在博弈时的决策顺序,博弈论可以分为静态博弈及动态博弈.博弈论中的基本要素包括博弈者、博弈策略、博弈收益、博弈顺序.其中,博弈者指的是参与博弈活动的主体,他们以自己获得最大收益作为主要目的进行理性决策.博弈策略是指博弈者在轮到自己采取行动时可以选择的策略集合.博弈收益是指博弈者在采取不同博弈策略时的所得,是博弈过程中博弈者首要关心的问题.博弈顺序是指博弈者进行决策的先后顺序,也是能够被其他博弈参与者观察到的博弈者的行动顺序,如果在进行博弈时博弈者虽有先后顺序,但是其他博弈者不能观察到先行博弈者采取的策略,则视为博弈者同时进行决策.

3 传统隐私保护模型的博弈分析

在传统的隐私保护模型中,博弈双方依然是隐私信息的访问者与被访问者,双方的策略分别是“善意访问隐私信息”或“恶意访问隐私信息”以及“允许访问隐私信息”或“拒绝访问隐私信息”.下面我们通过博弈论对博弈双方的策略选择进行分析.

首先定义博弈双方采取不同策略时所对应的收益:

$B\_income_{wel}^{acp}$:当访问者采取“善意访问隐私信息”策略,而被访问者采取“允许访问隐私信息”策略时,被访问者获得的收益.该收益也是当访问者采取“善意访问隐私信息”策略,而被访问者采取“拒绝访问隐私信息”策略时,被访问者的损失.该收益可以被视为被访问者通过允许访问者对其隐私信息进行访问而实现了提供某些服务或扩大影响范围的目的.

$F\_income_{wel}^{acp}$:当访问者采取“善意访问隐私信息”策略,而被访问者采取“允许访问隐私信息”策略时,访问者获得的收益.该收益可以被视为访问者通过善意访问获取用户的隐私信息而获得了某些服务或加深了对被访问者的了解,使双方的进一步交流能够继续下去.

$B\_loss_{mal}^{acp}$:当访问者采取“恶意访问隐私信息”策略,而被访问者采取“允许访问隐私信息”策略时,被访问者遭受的损失.该损失可以被视为被访问者泄露了超过自己对隐私泄露容忍程度的隐私信息,给自己带来经济、声望、事业或其他方面的伤害.

$F\_income_{mal}^{acp}$:当访问者采取“恶意访问隐私信息”策略,而被访问者采取“允许访问隐私信息”策略时,访问者获得的收益.该收益有别于访问者通过善意访问获得的收益,可以被视为访问者获得自己所希望得到,但是超过被访问者隐私泄露容忍程度而

带来的额外收益. 通常，恶意访问要承担更大的风险，与此同时，收益也要大于访问者通过善意访问而获得的收益.

$B\_income_{\mathrm{mal}}^{\mathrm{den}}$：当访问者采取“恶意访问隐私信息”策略，而被访问者采取“拒绝访问隐私信息”策略时，被访问者获得的收益. 该收益可以被视为被访问者成功地保护了自己的隐私信息，只将自己认为可以提供的隐私信息提供给了访问者，成功地抵御了自己不希望访问者通过恶意访问而获取隐私信息所带来的收益.

显然，当博弈双方分别采取“善意访问隐私信息”策略和“允许访问隐私信息”策略时，博弈双方可以建立起良好、持久的信息共享关系，有助于双方的了解和合作，为博弈双方都带来收益. 当博弈双方分别采取“恶意访问隐私信息”策略和“允许访问隐私信息”策略时，来自被访问者单方面的信任为访问者恶意获取超过被访问者容忍程度的隐私信息提供了便利条件，会给被访问者带来损失，同时给访问者带来额外收益. 当博弈双方分别采取“善意访问隐私信息”策略和“拒绝访问隐私信息”策略时，被访问者的拒绝使得访问者无法获得任何收益，同时被访问者也由于自己的拒绝策略丧失了提供服务或扩大影响的机会，也是被访问者的损失. 当博弈双方分别采取“恶意访问隐私信息”策略和“拒绝访问隐私信息”策略时，被访问者成功保护了自己的隐私信息，而访问者没有获得被访问者的隐私信息，因此被访问者获得了一定的收益，而访问者没有获得任何收益. 遗憾的是，在开放式网络中，被访问者无法对访问者的恶意访问行为采取任何惩罚措施.

根据上述分析，传统隐私保护模型中博弈双方的博弈矩阵可以使用表 1 进行表达. 上述分析及表 1 反映出，传统的隐私保护模型仅仅考虑到访问者本次访问隐私信息可能带来的影响，忽略了多次访问获得的隐私信息具有关联性和叠加性这个特点，即使是多次善意的访问所带来的结果也可能会造成被访问者泄露的隐私信息超过了自己的容忍程度. 同时，缺乏惩罚手段也使被访问者缺少保护自己隐私信息的方法，造成访问者可以毫无顾虑地进行恶意访问，而不用担心承担任何对自己不利的后果.

表 1　传统隐私保护模型中的博弈矩阵

被访问者	访问者	
	善意	恶意
允许	$B\_income_{\mathrm{wel}}^{\mathrm{acp}}, F\_income_{\mathrm{wel}}^{\mathrm{acp}}$	$-B\_loss_{\mathrm{mal}}^{\mathrm{acp}}, F\_income_{\mathrm{mal}}^{\mathrm{acp}}$
拒绝	$-B\_income_{\mathrm{wel}}^{\mathrm{acp}}, 0$	$B\_income_{\mathrm{mal}}^{\mathrm{den}}, 0$

利用画线法对表 1 中的博弈矩阵进行分析，从访问者的角度来看，当被访问者选择“允许访问隐私信息”策略时，对于访问者来说，“恶意访问隐私信息”策略将给自己带来更大的收益，即 $F\_income_{\mathrm{mal}}^{\mathrm{acp}} > F\_income_{\mathrm{wel}}^{\mathrm{acp}}$；当被访问者选择“拒绝访问隐私信息”策略时，对于访问者来说，“恶意访问隐私信息”策略与“善意访问隐私信息”策略所带来的收益相同，均为 0. 从被访问者的角度来分析，当访问者选择“善意访问隐私信息”策略时，对于被访问者来说，“允许访问隐私信息”策略可以给自己带来更大的收益，即 $B\_income_{\mathrm{wel}}^{\mathrm{acp}} > -B\_income_{\mathrm{wel}}^{\mathrm{acp}}$；当访问者选择“恶意访问隐私信息”策略时，对于被访问者来说，“拒绝访问隐私信息”策略可以给自己带来更大的收益，即 $B\_income_{\mathrm{mal}}^{\mathrm{den}} > -B\_loss_{\mathrm{mal}}^{\mathrm{acp}}$. 以上分析表明，该博弈矩阵存在一个纯策略纳什均衡（$B\_income_{\mathrm{mal}}^{\mathrm{den}}, 0$），所对应的博弈策略为（拒绝，恶意）. 显然，该纳什均衡与网络中倡导的信息交流与共享这一基本原则相矛盾，即使是涉及到用户个人隐私的信息也不是绝对不能允许任何泄露，而是不能超过用户个人隐私策略中表达的容忍程度. 因此，大多数网络用户也不可能始终选择这一均衡策略. 最优选择与博弈双方的初衷相违背，这就是传统隐私保护模型中访问者与被访问者之间存在的囚徒困境.

4　基于博弈论的隐私保护模型的博弈分析

为了解决传统隐私保护模型中存在的囚徒困境问题，在本文中，我们以博弈论为基础提出一个隐私保护模型. 该模型建立在重复博弈的相关理论之上，通过一个反馈机制记录访问者对隐私信息进行过的访问，当访问者再一次进行访问时，提出的模型将结合访问者过去的访问记录计算不同访问策略所对应的收益，以这些收益作为基础进行博弈，得到纳什均衡，再通过纳什均衡求得访问者此次进行善意访问的概率. 同时，被访问者会根据自身对于隐私泄露的容忍程度，通过隐私保护策略设置一个阈值，与访问者进行善意访问的概率相比较，目的是仅当善意访问的概率高于设置的阈值时，被访问者才会采取“允许访问隐私信息”策略，否则将采取“拒绝访问隐私信息”策略.

隐私保护阈值是决定访问者的访问请求是否被允许的一个关键参数，可以由被访问者根据自身对隐私泄露的要求或敏感程度而设定，取值范围一般

为[0,1].该阈值反映被访问者对隐私泄露的容忍程度,基本原则为容忍程度越高,则阈值设置的越低;容忍程度越低,则阈值设置的越高.在未设置时,阈值可以默认设置为取值范围的中间值0.5,被访问者可以根据网络环境的动态状况以及对隐私泄露的容忍程度实时动态地设置此阈值,表2是阈值与容忍程度的一种对应关系.

表2 隐私泄露容忍程度与阈值关系表

容忍程度	阈值
极高	[0, 0.2]
高	(0.2, 0.4]
中	(0.4, 0.6]
低	(0.6, 0.8]
极低	(0.8, 1]

在访问者进行访问的过程中,当访问者善意访问的概率高于该阈值时,访问者的请求将被允许;反之,当访问者善意访问的概率低于该阈值时,访问者的请求将被拒绝.

4.1 基于博弈论的隐私保护模型流程

基于博弈论的隐私保护流程图具体如图1所示,步骤如下:

1.访问者发起访问请求,请求访问被访问者的隐私信息.

2.系统获知访问者请求访问的隐私信息,并从历史数据库中获取该访问者已经访问过的隐私信息.

3.系统通过将步2中的隐私信息进行结合得到访问者通过此次访问能够获得的隐私信息集合,即计算对隐私信息访问的叠加效应.

4.根据访问者通过历次访问得到的隐私信息集合,计算此次访问中,访问者与被访问者采取不同策略时所对应的收益.

5.根据不同策略以及计算出的收益,模拟双方采取不同的博弈策略.

6.从双方博弈获得纳什均衡,从该纳什均衡中可以得出双方的收益期望值以及选择各个博弈策略的概率.

7.根据纳什均衡可以得到访问者选择"善意访问隐私信息"策略的概率.

8.系统将以上概率,即访问者采取"善意访问隐私信息"策略的概率与被访问者通过隐私保护策略设置的访问阈值进行比较,若前者不小于后者,则采取"允许访问隐私信息"策略,表明访问者通过此次访问所获得的隐私信息与历史访问所获得的隐私信息相结合没有超过被访问者对于隐私泄露的容忍程度;否则采取"拒绝访问隐私信息"策略,访问者只能够得到历史访问记录中的隐私信息.

9.将此次访问的最终结果记录到对隐私信息进行访问的历史数据库中,应用在后续访问决策中.当访问者再次提出访问请求时,步9中记录的历史数据会通过步2～4对博弈双方的收益产生影响,进而影响被访问者决定采取"允许访问隐私信息"策略或"拒绝访问隐私信息"策略.

图1中的流程表明,通过访问反馈机制记录的历史数据以及阈值的设置,如果被访问者得出访问者通过此次访问所获得的隐私信息以及从前已经得到的历史信息相结合会造成不希望泄露的隐私信息的泄露,则认为访问者采取"恶意访问隐私信息"策略,被访问者不仅会拒绝访问者进行此次超出隐私泄露容忍程度的访问,还会根据访问者访问隐私信息的历史记录这个反馈机制,对访问者施以惩罚.因

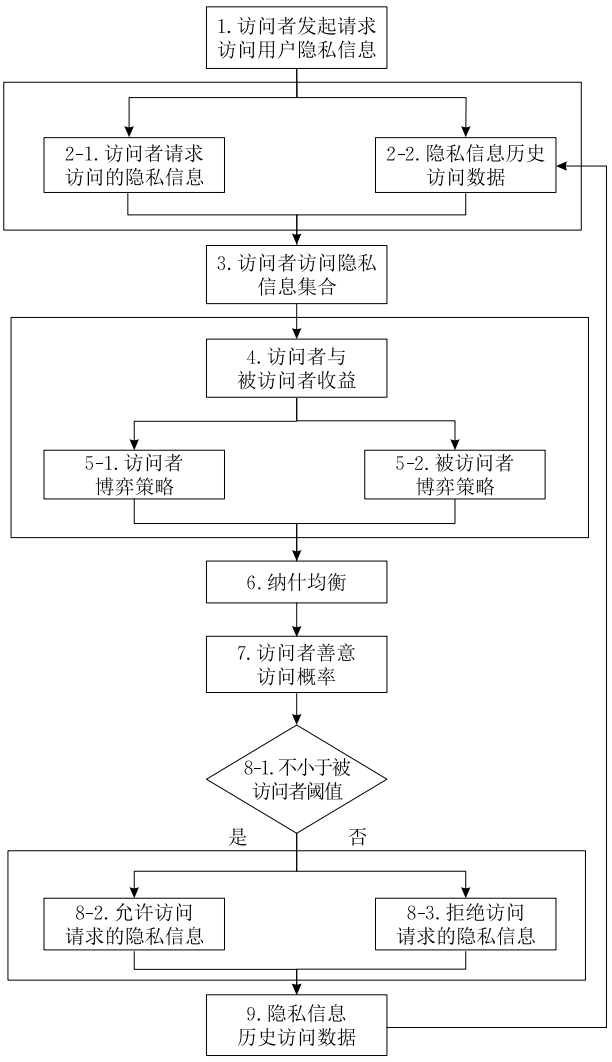


图1 基于博弈论的隐私保护模型流程图

此，当博弈双发分别将“恶意访问隐私信息”和“拒绝访问隐私信息”作为各自的博弈策略时，被访问者因为成功保护自己的隐私信息而获得收益，访问者也由于被访问者实施的惩罚而得到损失.

下面让我们具体描述访问者与被访问者的博弈过程.

4.2　访问者与被访问者的博弈过程

在讨论之前，我们首先对该博弈中纳什均衡的存在性进行证明. 在基于博弈论的隐私保护模型中，博弈双方的策略集合都是有限集，因此这是一个有限战略式博弈. 根据纳什均衡的存在性定理，即每一个有限战略式博弈至少存在一个纳什均衡[21]，可以得出该隐私保护模型的博弈过程至少存在一个纳什均衡.

接下来，我们需要重新定义双方在不同博弈策略下的收益.

δ：访问者此次请求访问的隐私信息对被访问者今后收益影响的贴现值.

ζ：访问者此次请求访问的隐私信息对访问者今后收益影响的贴现值.

$B'\_income_{\mathrm{wel}}^{\mathrm{acp}}$：当访问者采取“善意访问隐私信息”策略，而被访问者采取“允许访问隐私信息”策略时，被访问者的收益. 该收益也是当访问者采取“善意访问隐私信息”策略，而被访问者采取“拒绝访问隐私信息”策略时，被访问者的损失. 假设访问者每次请求访问被访问者的隐私信息时，被访问者的收益为 $b\_income_{\mathrm{wel}}^{\mathrm{acp}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}B'\_income_{\mathrm{wel}}^{\mathrm{acp}} &= b\_income_{\mathrm{wel}}^{\mathrm{acp}} + b\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \delta + \\ & b\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \delta^2 + \cdots + b\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \delta^n \\ &= b\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \frac{1-\delta^n}{1-\delta}.\end{aligned}$$

$F'\_income_{\mathrm{wel}}^{\mathrm{acp}}$：当访问者采取“善意访问隐私信息”策略，而被访问者采取“允许访问隐私信息”策略时，访问者的收益. 假设访问者每次请求访问被访问者的隐私信息时，访问者的收益为 $f\_income_{\mathrm{wel}}^{\mathrm{acp}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}F'\_income_{\mathrm{wel}}^{\mathrm{acp}} &= f\_income_{\mathrm{wel}}^{\mathrm{acp}} + f\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \xi + \\ & f\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \xi^2 + \cdots + f\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \xi^n \\ &= f\_income_{\mathrm{wel}}^{\mathrm{acp}} \times \frac{1-\xi^n}{1-\xi}.\end{aligned}$$

$B'\_loss_{\mathrm{mal}}^{\mathrm{acp}}$：当访问者采取“恶意访问隐私信息”策略，而被访问者采取“允许访问隐私信息”策略时，被访问者的收益. 假设访问者每次请求访问被访问者的隐私信息时，被访问者的收益为 $b\_loss_{\mathrm{mal}}^{\mathrm{acp}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}B'\_loss_{\mathrm{mal}}^{\mathrm{acp}} &= b\_loss_{\mathrm{mal}}^{\mathrm{acp}} + b\_loss_{\mathrm{mal}}^{\mathrm{acp}} \times \delta + \\ & b\_loss_{\mathrm{mal}}^{\mathrm{acp}} \times \delta^2 + \cdots + b\_loss_{\mathrm{mal}}^{\mathrm{acp}} \times \delta^n \\ &= b\_loss_{\mathrm{mal}}^{\mathrm{acp}} \times \frac{1-\delta^n}{1-\delta}.\end{aligned}$$

$F'\_income_{\mathrm{mal}}^{\mathrm{acp}}$：当访问者采取“恶意访问隐私信息”策略，而被访问者采取“允许访问隐私信息”策略时，访问者的收益. 假设访问者每次请求访问被访问者的隐私信息时，访问者的收益为 $f\_income_{\mathrm{mal}}^{\mathrm{acp}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}F'\_income_{\mathrm{mal}}^{\mathrm{acp}} &= f\_income_{\mathrm{mal}}^{\mathrm{acp}} + f\_income_{\mathrm{mal}}^{\mathrm{acp}} \times \xi + \\ & f\_income_{\mathrm{mal}}^{\mathrm{acp}} \times \xi^2 + \cdots + f\_income_{\mathrm{mal}}^{\mathrm{acp}} \times \xi^n \\ &= f\_income_{\mathrm{mal}}^{\mathrm{acp}} \times \frac{1-\xi^n}{1-\xi}.\end{aligned}$$

$B'\_income_{\mathrm{mal}}^{\mathrm{den}}$：当访问者采取“恶意访问隐私信息”策略，而被访问者采取“拒绝访问隐私信息”策略时，被访问者的收益. 假设访问者每次请求访问被访问者的隐私信息时，被访问者的收益为 $b\_income_{\mathrm{mal}}^{\mathrm{den}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}B'\_income_{\mathrm{mal}}^{\mathrm{den}} &= b\_income_{\mathrm{mal}}^{\mathrm{den}} + b\_income_{\mathrm{mal}}^{\mathrm{den}} \times \delta + \\ & b\_income_{\mathrm{mal}}^{\mathrm{den}} \times \delta^2 + \cdots + b\_income_{\mathrm{mal}}^{\mathrm{den}} \times \delta^n \\ &= b\_income_{\mathrm{mal}}^{\mathrm{den}} \times \frac{1-\delta^n}{1-\delta}.\end{aligned}$$

$F'\_loss_{\mathrm{mal}}^{\mathrm{den}}$：当访问者采取“恶意访问隐私信息”策略，而被访问者采取“拒绝访问隐私信息”策略时，访问者的损失. 假设访问者每次请求访问被访问者的隐私信息时，访问者的收益为 $f\_loss_{\mathrm{mal}}^{\mathrm{den}}$，则访问者第 n 次请求访问被访问者的隐私信息时

$$\begin{aligned}F'\_loss_{\mathrm{mal}}^{\mathrm{den}} &= f\_loss_{\mathrm{mal}}^{\mathrm{den}} + f\_loss_{\mathrm{mal}}^{\mathrm{den}} \times \xi + \\ & f\_loss_{\mathrm{mal}}^{\mathrm{den}} \times \xi^2 + \cdots + f\_loss_{\mathrm{mal}}^{\mathrm{den}} \times \xi^n \\ &= f\_loss_{\mathrm{mal}}^{\mathrm{den}} \times \frac{1-\xi^n}{1-\xi}.\end{aligned}$$

基于以上的收益和损失表示，博弈双方的博弈矩阵如表 3 所示.

表 3　基于博弈论的隐私保护模型中的博弈矩阵

被访问者	访问者	
	善意	恶意
允许	$B'\_income_{\mathrm{wel}}^{\mathrm{acp}}, F'\_income_{\mathrm{wel}}^{\mathrm{acp}}$	$-B'\_loss_{\mathrm{mal}}^{\mathrm{acp}}, F'\_income_{\mathrm{mal}}^{\mathrm{acp}}$
拒绝	$-B'\_income_{\mathrm{wel}}^{\mathrm{acp}}, 0$	$B'\_income_{\mathrm{mal}}^{\mathrm{den}}, -F'\_loss_{\mathrm{mal}}^{\mathrm{den}}$

通过画线法对表 3 中的博弈矩阵进行分析，从访问者的角度来分析，当被访问者选择“允许访问隐私信息”策略时，对于访问者来说，采取“恶意访问隐私信息”策略可以给自己带来更大的收益，即

$F'\_income_{mal}^{acp} > F'\_income_{wel}^{acp}$；当被访问者选择“拒绝访问隐私信息”策略时，对于访问者来说，采取“恶意访问隐私信息”策略带来的收益小于采取“善意访问隐私信息”策略带来的收益，即 $-F'\_loss_{mal}^{den} < 0$. 从被访问者的角度来分析，当访问者选择“善意访问隐私信息”策略时，对于被访问者来说，采取“允许访问隐私信息”策略可以给自己带来更大的收益，即 $B'\_income_{wel}^{acp} > -B'\_income_{wel}^{acp}$；当访问者选择“恶意访问隐私信息”策略时，对于被访问者来说，采取“拒绝访问隐私信息”策略可以给自己带来更大的收益，即 $B'\_income_{mal}^{den} > -B'\_loss_{mal}^{acp}$. 通过以上分析，我们发现在该博弈矩阵中不存在纯策略纳什均衡，因此我们需要计算其混合策略纳什均衡.

我们分别用 P_F 和 P_B 来表示表 3 中访问者和被访问者的收益矩阵. 假设被访问者选择“允许访问隐私信息”策略的概率为 x，则被访问者选择“拒绝访问隐私信息”策略的概率为 $1-x$，被访问者的混合策略概率为 $P_b=(x,1-x)$. 同样，假设访问者选择“善意访问隐私信息”策略的概率为 y，则访问者选择“恶意访问隐私信息”策略的概率为 $1-y$，访问者的混合策略概率为 $P_f=(y,1-y)$. 被访问者的收益函数 E_B 可以通过式(1)进行计算：

$$\begin{aligned}E_B &= P_b \times P_B \times \boldsymbol{P}_f^{\mathrm{T}}\\ &= \begin{bmatrix} x & 1-x \end{bmatrix} \begin{bmatrix} B'\_income_{wel}^{acp} & -B'\_loss_{mal}^{acp} \\ -B'\_income_{wel}^{acp} & B'\_income_{mal}^{den} \end{bmatrix} \begin{bmatrix} y \\ 1-y \end{bmatrix}\\ &= (2x-1)\times y \times B'\_income_{wel}^{acp} + x\times(-B'\_loss_{mal}^{acp})\times(1-y) + (1-x)\times(1-y)\times B'\_income_{mal}^{den} \end{aligned} \tag{1}$$

E_B 对 x 求导，可以得到式(2)：

$$\frac{\partial E_B}{\partial x} = 2\times y \times B'\_income_{wel}^{acp} - (B'\_loss_{mal}^{acp} + B'\_income_{mal}^{den})\times(1-y) \tag{2}$$

令式(2)等于 0，可以求得 y 的值，用式(3)表示：

$$\begin{aligned} y &= \frac{B'\_loss_{mal}^{acp} + B'\_income_{mal}^{den}}{2\times B'\_income_{wel}^{acp} + B'\_loss_{mal}^{acp} + B'\_income_{mal}^{den}}\\ &= \left(b\_loss_{mal}^{acp}\times\frac{1-\delta^n}{1-\delta} + b\_income_{mal}^{den}\times\frac{1-\delta^n}{1-\delta}\right)\Big/ \left(2\times b\_income_{wel}^{acp}\times\frac{1-\delta^n}{1-\delta} + b\_loss_{mal}^{acp}\times\frac{1-\delta^n}{1-\delta} + b\_income_{mal}^{den}\times\frac{1-\delta^n}{1-\delta}\right)\\ &= \frac{b\_loss_{mal}^{acp} + b\_income_{mal}^{den}}{2\times b\_income_{wel}^{acp} + b\_loss_{mal}^{acp} + b\_income_{mal}^{den}} \end{aligned} \tag{3}$$

同样，访问者的收益 E_F 可以通过式(4)进行计算：

$$\begin{aligned} E_F &= P_b \times P_F \times \boldsymbol{P}_f^{\mathrm{T}}\\ &= \begin{bmatrix} x & 1-x \end{bmatrix} \begin{bmatrix} F'\_income_{wel}^{acp} & F'\_income_{mal}^{acp} \\ 0 & -F'\_loss_{mal}^{den} \end{bmatrix} \begin{bmatrix} y \\ 1-y \end{bmatrix}\\ &= x\times F'\_income_{wel}^{acp}\times y + x\times F'\_income_{mal}^{acp}\times(1-y) + (1-x)\times(-F'\_loss_{mal}^{den})\times(1-y) \end{aligned} \tag{4}$$

E_F 对 y 求导，可以得到式(5)：

$$\frac{\partial E_F}{\partial y} = x\times(F'\_income_{wel}^{acp} - F'\_income_{mal}^{acp} - F'\_loss_{mal}^{den}) + F'\_loss_{mal}^{den} \tag{5}$$

令式(4)等于 0，可以求得 x 的值，用式(6)表示：

$$\begin{aligned} x &= \frac{F'\_loss_{mal}^{den}}{F'\_income_{mal}^{acp} + F'\_loss_{mal}^{den} - F'\_income_{wel}^{acp}}\\ &= \left(f\_loss_{mal}^{den}\times\frac{1-\xi^n}{1-\xi}\right)\Big/ \left(f\_income_{mal}^{acp}\times\frac{1-\xi^n}{1-\xi} + f\_loss_{mal}^{den}\times\frac{1-\xi^n}{1-\xi} - f\_income_{wel}^{acp}\times\frac{1-\xi^n}{1-\xi}\right)\\ &= \frac{f\_loss_{mal}^{den}}{f\_income_{mal}^{acp} + f\_loss_{mal}^{den} - f\_income_{wel}^{acp}} \end{aligned} \tag{6}$$

由此得到的混合策略纳什均衡如式(7)所示：

$$\begin{aligned} \begin{bmatrix} x & 1-x \end{bmatrix} &= \left[\frac{f\_loss_{mal}^{den}}{f\_income_{mal}^{acp} + f\_loss_{mal}^{den} - f\_income_{wel}^{acp}} \quad 1 - \frac{f\_loss_{mal}^{den}}{f\_income_{mal}^{acp} + f\_loss_{mal}^{den} - f\_income_{wel}^{acp}} \right],\\ \begin{bmatrix} y & 1-y \end{bmatrix} &= \left[\frac{b\_loss_{mal}^{acp} + b\_income_{mal}^{den}}{2\times b\_income_{wel}^{acp} + b\_loss_{mal}^{acp} + b\_income_{mal}^{den}} \quad \frac{2\times b\_income_{wel}^{acp}}{2\times b\_income_{wel}^{acp} + b\_loss_{mal}^{acp} + b\_income_{mal}^{den}} \right] \end{aligned} \tag{7}$$

通过以上的混合策略纳什均衡，隐私保护模型可以得到被访问者选择“允许访问隐私信息”策略的概率以及访问者选择“善意访问隐私信息”策略的概率. 由于被访问者会根据自身对隐私泄露的容忍程度在隐私保护策略中设定一个访问阈值，将访问者“善意访问隐私信息”策略的概率与该访问阈值相比较，若该概率不小于该阈值，则被访问者允许访问者的访问请求，否则被访问者拒绝访问者的访问请求.

4.3 基于博弈论的隐私保护模型的架构设计

在分析了基于博弈论的隐私保护模型的流程和博弈过程后，图 2 是对该模型的一个具体架构设计. 该设计主要分为三部分：执行部分、决策部分和隐私信息历史访问数据库. 执行部分主要包括采集访问者的基础访问信息以及执行访问控制决策. 决策部

分主要包括接收执行部分采集的基础访问信息，通过一系列相关算法计算访问控制决策结果，并将结果提交给执行部分，同时将访问者此次访问获得的隐私信息记录到隐私信息历史数据库中. 隐私信息历史访问数据库主要负责存储记录访问者访问过的用户隐私信息数据，供决策部分进行访问控制决策计算时使用.

在图 2 的架构设计中，执行部分包括两个模块：隐私信息获取模块和决策执行模块. 其中，隐私信息获取模块负责采集访问者此次请求访问的被访问者的隐私信息，并将该信息提供给决策部分. 决策执行模块负责接收决策部分反馈的最终决策结果，并执行.

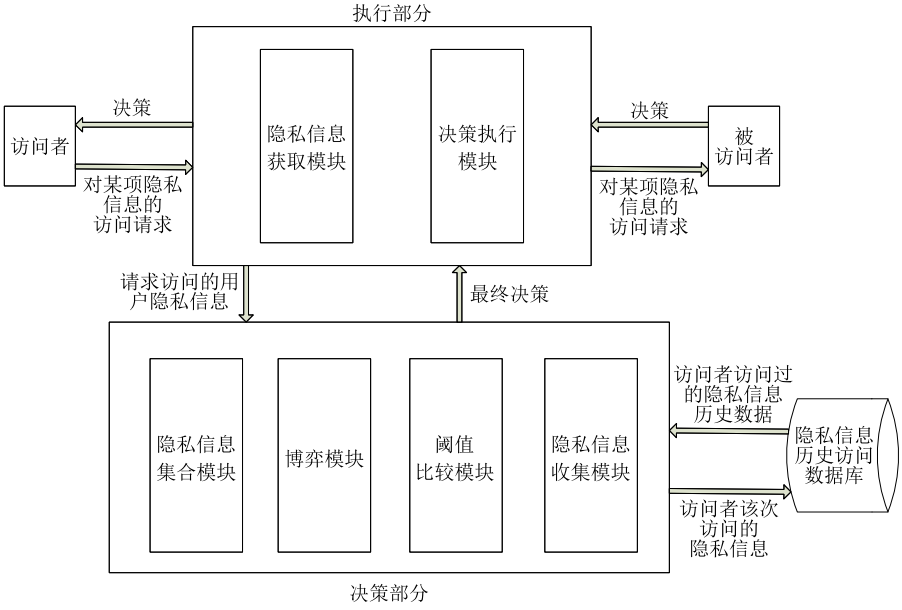


图 2　基于博弈论的隐私保护模型架构设计图

决策部分包括 4 个模块：隐私信息集合模块、博弈模块、阈值比较模块以及隐私信息收集模块. 隐私信息集合模块负责接收来自执行部分提供的访问者此次请求访问的隐私数据和来自历史访问数据库中该访问者访问过的隐私信息历史数据，将两者结合计算出访问者通过此次访问可以获得的隐私信息的集合. 博弈模块负责计算访问者和被访问者博弈过程中的混合策略纳什均衡，再通过混合策略纳什均衡计算出访问者采取“善意访问隐私信息”策略的概率. 阈值比较模块负责将博弈模块得到的访问者采取“善意访问隐私信息”策略概率与被访问者事先设置的阈值相比较得到最终决策，如果前者不小于后者，则采取“允许访问隐私信息”策略，否则采取“拒绝访问隐私信息”策略，并将该决策提供给执行模块. 最后，隐私信息收集模块负责收集本次访问者获取的隐私信息，并将其存储在隐私信息历史访问数据库中.

5　实验与分析

通过访问控制对隐私进行保护是逐渐得到广泛关注的一项重要的隐私保护技术. 然而，目前基于访问控制进行隐私保护模型或方法[14-18,22-25]（在本文中统称为传统模型）的主要设计思路是在已有的面向信息安全的访问控制模型中加入相应的隐私保护策略，通过增加策略的方式对已有模型进行适当扩展，使访问控制策略同时反映信息安全和隐私保护的要求，将隐私信息（隐私保护）与机密信息（信息安全）同等对待加以保护，再使用基于身份、角色、属性、上下文等传统的访问控制机制根据制定的访问控制策略对访问请求进行授权，做出允许访问或拒绝访问的决策. 对访问请求进行授权的具体流程依然为当访问者提出访问隐私信息的请求后，被访问者根据包含隐私保护的访问控制策略对此请求进行授权. 因此，这些传统的基于访问控制的隐私保护模型自然地继承了对每一个访问请求独立进行授权这一特点，无法根据隐私保护的特点来支持隐私保护的核心要求，即阻止访问者通过将多次访问的信息叠加而最终获取隐私信息；以及隐私信息拥有者实时动态制定隐私保护策略，以确保访问者获得的信息不会超过隐私信息拥有者对于隐私信息泄露的容忍程度.

我们通过实验对本文中提出的基于博弈理论的隐私保护模型进行分析并与传统隐私保护模型进行比较.在实验设置中,我们假设有 100 个访问者和 20 个被访问者.实验中的被访问者随机标记 1 个或 1 组信息作为不希望泄露的隐私信息.在第 1 个实验中,访问者分别使用这两种隐私保护模型访问被访问者的隐私信息.如果访问者能够成功访问超过被访问者容忍程度(即不希望泄露)的隐私泄露,则造成隐私泄露.我们通过实验来观察传统隐私保护模型与基于博弈论的隐私保护模型中隐私泄露的概率,以及这两种模型对于隐私保护的有效性.隐私泄露的概率是指在某个访问者对某个被访问者的某次访问中,获得的综合隐私信息超过被访问者对于隐私泄露容忍程度的概率.隐私保护有效性是指在某个访问者对某个被访问者的某次访问中,被访问者成功保护了自己隐私信息的概率,它与隐私泄露概率密切相关,可以通过隐私泄露概率计算得出.

需要指出的是,对于每一个访问者个体来说,访问次数的叠加并不意味着请求访问的隐私内容的叠加,如果他每次请求访问的都是同一个在被访问者容忍程度内的隐私信息,则永远不会超过被访问者的容忍程度,而如果他一开始请求访问的隐私信息就已经是超过被访问者容忍程度的隐私信息,则会立即被拒绝.然而,对于广义上的访问者与被访问者来说,访问次数的叠加通常意味着访问隐私信息内容的叠加.因此,为了获得客观的实验结果,我们设置访问者连续 100 次随机访问被访问者,而我们从这 100 个结果中任意抽取连续的 30 次访问,观察被访问者对应的某个或某组隐私信息被成功阻止访问的概率.为了进一步确保实验结果的客观性和准确性,我们重复此实验 50 次,然后取这 50 次实验结果的平均值作为最终的实验结果.实验中访问次数与用户隐私泄露概率的关系如表 4 所示.

表 4 访问次数与隐私泄露概率关系表

访问次数	隐私泄露概率	
	传统模型	基于博弈论的模型
1	0.03	0.01
2	0.05	0.03
3	0.05	0.04
4	0.08	0.06
5	0.14	0.08
⋮	⋮	⋮
26	0.78	0.40
27	0.82	0.43
28	0.80	0.45
29	0.84	0.50
30	0.85	0.48

我们通过式(8)来计算隐私保护的有效性,其中,p 为隐私泄露的概率,e 为隐私保护的有效性

$$e=\left(\frac{1}{2}\right)^{p-1}-1 \tag{8}$$

同时,为了观察基于博弈论的隐私保护模型中被访问者设置的阈值与访问次数的关系,我们的实验仍然假设有 100 个访问者和 20 个被访问者,设置访问者连续 100 次随机访问被访问者,而我们从这 100 个结果中随机抽取连续的 70 次访问,观察对于不同的阈值,隐私保护模型统计访问者超过被访问者对于隐私泄露的容忍程度的访问次数.其中,阈值是指被访问者根据自己对隐私泄露的容忍程度设定的一个值,不同的用户可以根据自己对于不同隐私信息的不同敏感度设置不同的阈值,而隐私保护模型只有在访问者采取"善意访问隐私信息"策略的概率高于该阈值时才采取"允许访问隐私信息"策略.我们再一次重复此实验 50 次,并取这 50 次实验结果的平均值作为最终的实验结果.表 5 是被访问者设置的阈值与访问次数关系的实验结果.

通过以上实验得到的结果和比较结果分别在图 3～图 5 中显示.

表 5 被访问者阈值与访问次数关系表

阈值	访问次数
0.1	52
0.2	40
0.3	33
0.4	28
0.5	20
0.6	15
0.7	10
0.8	6
0.9	3
1.0	0

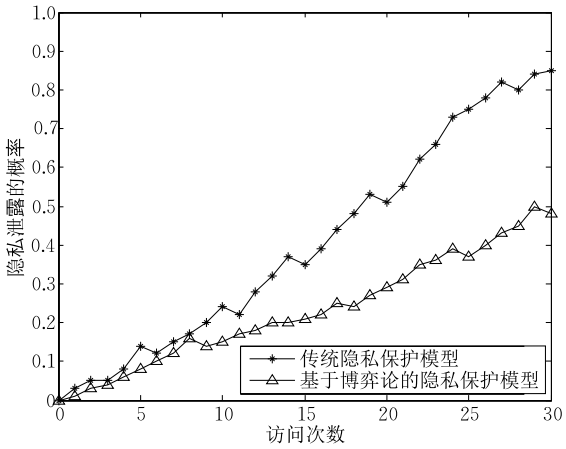


图 3 传统隐私保护模型与基于博弈论的隐私保护模型的隐私泄露概率比较

图 3 的结果表明，随着访问次数的增加，传统隐私保护模型以及基于博弈论的隐私保护模型的隐私泄露概率都在增大. 这是由于重复访问次数的增加造成隐私信息内容的叠加效应，即随着访问次数的增加，被访问者隐私信息泄露的也越来越多，即使某些隐私信息本身并没有超过被访问者对于隐私泄露的容忍程度，但将它们组合起来所透露的隐私信息也可能超过了被访问者的容忍程度. 然而，相比之下，本文提出的基于博弈论的隐私保护模型的隐私泄露概率始终低于传统的隐私保护模型. 从图 3 可以看出，传统隐私保护模型中隐私泄露的概率始终大于基于博弈论的隐私保护模型，该概率在传统隐私保护模型中由 0 上升到 0.85，在基于博弈论的隐私保护模型中只由 0 上升到 0.5.

图 4 的结果表明，随着访问次数的增多，传统隐私保护模型与基于博弈论的隐私保护模型的隐私保护有效性均呈下降趋势. 这也是由于重复访问的叠加效应造成的必然结果，即随着访问者访问次数的增加，获取的被访问者的隐私信息也会越来越多. 同样，从图 4 可以看出，传统隐私保护模型对于被访问者隐私信息保护的有效性从 1.0 降到 0.1 附近，而基于博弈论的隐私保护模型对于被访问者隐私信息保护的有效性只从 1.0 降到 0.5 附近，并且前者始终低于后者.

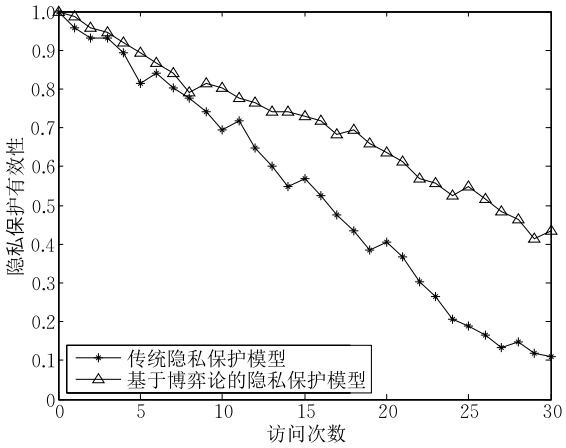


图 4　传统隐私保护模型与基于博弈论的隐私保护模型的隐私保护有效性比较

此外，基于博弈论的隐私保护模型的另外一个特点是被访问者隐私保护阈值的灵活设置，由被访问者根据自身对于隐私信息保护的敏感度或要求进行设置，用来决定是否允许访问者进行访问. 该阈值用于与访问者采取“善意访问隐私信息”策略的概率相比较，只有当善意访问的概率不小于阈值时，才采取“允许访问隐私信息”策略，否则采取“拒绝访问隐私信息”策略. 阈值的设定机制确保了隐私保护模型可以更好地反映被访问者的隐私信息保护个性化需求，做到更加有效地降低隐私信息泄露的概率，提高隐私保护的自适应性.

图 5 表明，在基于博弈论的隐私保护模型中，随着阈值的提高，达到被访问者对于隐私泄露的容忍程度的访问次数在减少，即被访问者对隐私泄露容忍程度越低. 反之，阈值越低，访问者不超过被访问者对隐私保护容忍程度的访问次数也就越多，即被访问者对隐私泄露容忍程度越高.

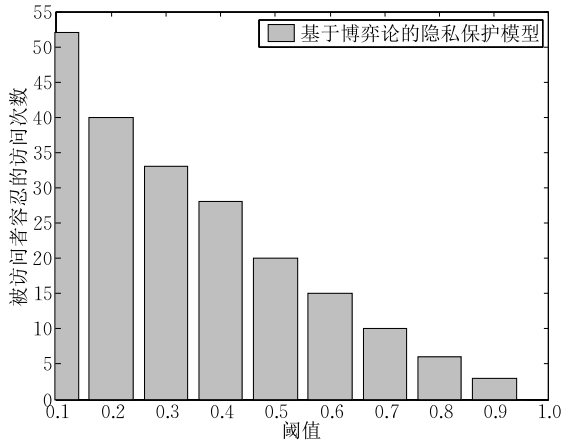


图 5　基于博弈论的隐私保护模型的阈值与容忍程度关系

6　总结与展望

本文首先介绍了当前的隐私保护模型的技术手段，并且分析了它们的特点和不足. 之后，从收益的角度出发，通过博弈论分析了传统隐私保护模型的缺点. 在此基础上，本文提出了一种基于博弈论的隐私保护模型，通过对访问者隐私信息历史访问数据的收集、访问者与被访问者之间的策略博弈以及被访问者阈值的设置，可以更有效地保护用户的隐私信息. 本文分别介绍了所提出的基于博弈论的隐私保护模型的实现流程、博弈过程以及具体架构设计，最后通过实验验证了所提出的隐私保护模型相对于传统隐私保护模型能够更有效地保护用户隐私.

未来，我们将进一步扩展与完善基于博弈理论的隐私保护模型，包括考虑访问隐私信息叠加效应的动态与非一致性，即访问不同的隐私信息会产生不同的叠加效果，以及面向并行访问的保护机制. 我们还将研究如何将该模型应用在诸如购物网站、社交平台等实际系统中，使用商业数据对模型进行性能评价及进一步完善.

参 考 文 献

[1] Bettini C, Riboni D. Privacy protection in pervasive systems: State of the art and technical challenges. Pervasive and Mobile Computing, 2015, 17(PB): 159-174

[2] Zhang Wei, Wang Wei, Zhang Xin-Chang, Shi Hui-Ling. Research on privacy protection of WHOIS information in DNS//Proceedings of the 6th FTRA International Conference on Computer Science and its Applications. Guam, USA, 2015, 330: 71-76

[3] Yu Zhi-Xin, Huang Tian-Shu, Yang Nai-Kuo, Wang Yang. Novel privacy-protecting distributed computation model and its applications. Journal of Xi'an Jiaotong University, 2007, 41(8): 954-958(in Chinese)
(余智欣，黄天戍，杨乃扩，汪阳. 一种新型的分布式隐私保护计算模型及其应用. 西安交通大学学报，2007，41(8)：954-958)

[4] Bhagat S, Cormode G, Krishnamurthy B, Srivastava D. Prediction promotes privacy in dynamic social networks// Proceedings of the 3rd Conference on Online Social Networks. Berkeley, USA, 2010: 6

[5] Tripathy B K, Mitra A. An algorithm to achieve *k*-anonymity and *l*-diversity anonymisation in social networks//Proceedings of the 2012 4th International Conference on Computational Aspects of Social Networks. Sao Carlos, Brazil, 2012: 126-131

[6] Hao Yi-Fan, Cao Hui-Ping, Bhattatai K, Misra S. STK-anonymity: *K*-anonymity of social networks containing both structural and textual information//Proceedings of the ACM SIGMOD Workshop on Databases and Social Networks. New York, USA, 2013: 19-24

[7] Liu Xiang-Yu, Yang Xiao-Chun. A generalization based approach for anonymizing weighted social network graphs// Proceedings of the 12th International Conference on Web-Age Information Management. Wuhan, China, 2011: 118-130

[8] Wang Ya-Zhe, Xie Long, Zheng Bai-Hua, Lee K C K. Utility-oriented *K*-anonymization on social networks//Proceedings of the 16th International Conference on Database Systems for Advanced Applications. Hong Kong, China, 2011: 78-92

[9] Liu Xiang-Yu, Wang Bin, Yang Xiao-Chun. Survey on privacy preserving techniques for publishing social network data. Journal of Software, 2014, 25(3): 576-590(in Chinese)
(刘向宇，王斌，杨晓春. 社会网络数据发布隐私保护技术综述. 软件学报，2014，25(3)：576-590)

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

[11] Zhu Qing, Zhao Tong, Wang Shan. Privacy preservation algorithm for service-oriented information search. Chinese Journal of Computers, 2010, 33(8): 1315-1323(in Chinese)
(朱青，赵桐，王珊. 面向查询服务的数据隐私保护算法. 计算机学报，2010，33(8)：1315-1323)

[12] Huang Yi, Huo Zheng, Meng Xiao-Feng. CoPrivacy: A collaborative location privacy-preserving method without cloaking region. Chinese Journal of Computers, 2011, 34(10): 1976-1985(in Chinese)
(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. 计算机学报，2011，34(10)：1976-1985)

[13] Huo Zheng, Meng Xiao-Feng, Huang Yi. PrivateChekIn: Trajectory privacy-preserving for check-in services in MSNS. Chinese Journal of Computers, 2013, 36(4): 716-726 (in Chinese)
(霍峥，孟小峰，黄毅. PrivateChekIn：一种移动社交网络中的轨迹隐私保护方法. 计算机学报，2013，36(4)：716-726)

[14] Sun Li-Li, Wang Hua, Soar J, Rong Chun-Ming. Purpose based access control for privacy protection in E-Healthcare services. Journal of Software, 2012, 7(11): 2443-2449

[15] Wei Zhi-Qiang, Kang Mi-Jun, Jia Dong-Ning, et al. Research on privacy-protection policy for pervasive computing. Chinese Journal of Computers, 2010, 33(1): 128-138(in Chinese)
(魏志强，康密军，贾东宁等. 普适计算隐私保护策略研究. 计算机学报，2010，33(1)：128-138)

[16] Tan Zuo-Wen. A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. Journal of Network and Computer Applications, 2012, 35(6): 1839-1846

[17] Lu Rong-Xing, Lin Xiao-Dong, Shen Xue-Min. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(3): 614-624

[18] Fotiou N, Marias G F, Polyzos G C. Access control enforcement delegation for information-centric networking architectures. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 497-502

[19] von Neumann J, Morgenstern O. Game Theory and Economic Behaviors. USA, Princeton: Princeton University Press, 1944

[20] Nash F J. Equilibrium points in *N*-Person games. Proceedings of the National Academy of Science of the United States of America, 1950, 36(1): 48-49

[21] Luo Yun-Feng. Game Theory Tutorial. Beijing: Tsinghua University Press, Beijing Jiaotong University Press, 2007(in Chinese)
(罗云峰. 博弈论教程. 北京：清华大学出版社，北京交通大学出版社，2007)

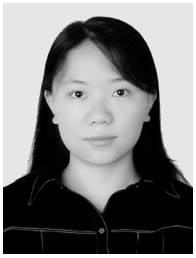
[22] Omran E, Grandison T, Nelson D, Bokma A. A comparative analysis of chain-based access control and role-based access control in the healthcare domain. International Journal of Information Security and Privacy, 2013, 7(3): 36-52

[23] Jana S, Narayanan A, Shmatikov V. A scanner darkly: Protecting user privacy from perceptual applications//

Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2013: 349-363

[24] Pappas V, Krell F, Vo B, et al. Blind seer: A scalable private DBMS//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2014: 359-374

[25] Tan Jia-Qi, Drolia U, Martins R, et al. Short paper: CHIPS: Content-based heuristics for improving photo privacy for smartphones//Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks. Oxford, UK, 2014: 213-218



ZHANG Yi-Xuan, born in 1988, Ph. D. candidate. Her research interests include network security, access control, game theory and distributed network technology.

HE Jing-Sha, born in 1961, Ph. D., professor, Ph. D. supervisor. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

ZHAO Bin, born in 1979, Ph. D. candidate, lecturer. His research focuses on network security, cloud computing and information forensics.

ZHU Na-Fei, born in 1981, Ph. D., post doctoral fellow. Her research focuses on network security, privacy protection and Internet measurement.

Background

In this paper, we focus on privacy protection in computer networks. Privacy protection is one of the most important research topics and is an issue that network users are concerned about. Researchers have proposed many solutions to protect user privacy, which can be categorized primarily into two types—anonymity and access control. These solutions rely on technical means to prevent the disclosure of user privacy information via different approaches, and thus have advantages and limitations. Meanwhile, through analyzing traditional access control based privacy protection methods using game theory, we can derive the situation of the prisoner's dilemma between the two sides of access.

To deal more effectively with the privacy issue, in this paper, we propose a privacy protection model based on game theory to better reflect the intrinsic nature of privacy protection, i. e., to allow access to a certain extent and deny access at the point that is right before the disclosure of privacy is about to happen. By collecting information about historical access, analyzing the benefits that both sides of the access could realize and considering privacy protection policy, our proposed model could provide more effective privacy protection. In the paper, we illustrate the procedure involved in the model, the scenario of the game play between the requester and the protector as well as a framework design of the model. We also perform some experiments to demonstrate the effectiveness of our model as well as its advantages over tradition privacy protection models.

The work in this paper has been supported by the National Natural Science Foundation of China (61272500): models and methods for dynamic access control based on game theory in open networks. The work has also been supported by the National High Technology Research and Development Program (863 Program) of China (2015AA017204): research and field trial of key digital forensics technologies for intelligent mobile terminals, and the Beijing Natural Science Foundation (4142008): dynamic and adaptive secure clock synchronous models and methods in wireless sensor networks based on mobile reference nodes. This paper studies a key security problem, i. e., privacy protection, and proposes a privacy protection model based on game theory to deal with privacy protection problem in information processing, storage and communication, which is a focus in the research supported by the above funds.