可信网络中一种基于行为信任预测的博弈控制机制

田立勤 林 闯
（清华大学计算机科学与技术系 北京 100084）

摘 要 近年来，网络可信的研究已成为一个研究热点，其中用户的行为信任研究是网络可信研究的重要内容之一. 由于用户行为信任的评估是基于过去交往的行为证据之上，而我们需要的是未来的用户行为信任等级，因此科学地预测未来用户的行为信任等级是非常必要的，文中首先论述了如何利用贝叶斯网络对用户的行为信任进行预测，提供的机制不仅可以预测单属性条件下的行为信任等级，而且可以预测多属性条件下的行为信任等级. 由于信任和风险是并存的，单独依靠预测的信任等级进行决策是非常片面和危险的，因此该文的其余部分将行为信任预测结果和博弈分析相结合对双方的支付矩阵进行分析，计算出了基于用户安全行为属性的混合纳什均衡策略，证明了服务提供者进行控制的决策条件，得出了相关的一些重要性质，最后通过一个例子来说明论文的应用. 该文的结果对于量化分析用户行为信任具有重要的理论意义. 文章在分析过程和实例中结合了数字化电子资源的实际网络应用背景，因此该机制在实际的网络应用中同样具有重要的指导意义.

关键词 可信网络；行为信任；预测；博弈控制
中图法分类号 TP393

A Kind of Game-Theoretic Control Mechanism of User Behavior Trust Based on Prediction in Trustworthy Network

TIAN Li-Qin LIN Chuang
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract In recent years, the trustworthy network research has become a research focus. User trust study is one important branch of trustworthy network research field, and it includes not only user identity trust but also user behaviour trust. The traditional authorization and authentication security mechanism mainly solve user identity trust, it can't deal with user behaviour trust. User behaviour trust strengthens the dynamic state processing of the user, providing the strategy foundation for implementation of intelligent adaptive network security. Because the behaviour trust is based on the evidence of past transaction, but what we need is the future user behaviour trust, therefore scientifically predicting user future behaviour trust is very necessary. This paper first discusses a mechanism that how to use Bayesian network to forecast user behaviour trust. The mechanism not only can predict behaviour trust grade under the single trust attribute conditions, but also can predict trust grade under the multi-trust-attribute conditions. As trust coexists with risk, decision-making that only relay on forecasted trust grade is very one-sided and dangerous. Therefore we must also analyze risk in the decision-making of control. The rest of this paper analyzes payoff matrix of Game-theory combining foregoing forecasts results, figures out mixed Nash equilibrium strategy based on user secure attribute, puts forward the decision-making conditions of controlling for the service provider. Lastly the authors give an example to

收稿日期：2007-06-25. 本课题得到国家自然科学基金（60673184，60673187 和 90412012）、国家“九七三”重点基础研究发展规划项目基金（2006CB708301）和河北省科学技术研究与发展指导计划项目基金（07213570）资助. **田立勤**，男，1970 年生，博士研究生，副教授，研究方向为计算机网络、工作流模型和可信网络. E-mail：tianliqin@tsinghua.org.cn；chlin@tsinghua.edu.cn. **林 闯**，男，1948 年生，博士，教授，博士生导师，研究领域为系统性能评价、网络安全、随机 Petri 网、逻辑推理模型等.

illustrate how to use the result of the paper and analyze its advantage comparing existing user control strategy. The result of the paper not only has an important theoretical significance to quantitatively analyze user behavior trust, but also has a major guiding significance in the actual network application due to the authors consider the actual network application background of Providing of Digital Electronic Resources in the example and in all process of analysis.

Keywords　trustworthy network; behaviour trust; prediction; game-theoretic control

1　引　言

近年来，网络的可信研究已成为一个研究热点[1-5]，网络可信技术是在原有网络安全技术的基础上增加行为可信的安全新方法，强化了对网络状态的动态处理，为实施智能自适应的网络安全和服务质量控制提供策略基础. 可信网络的定义是：网络和用户的行为及其结果是可以预期与可管理的[2]. 网络的可信性表现在如下 3 个方面：(1) 网络用户的可信. 主要看网络用户的行为是否符合既定的规范，是否可预期可管理，对网络设备和数据是否会造成破坏或毁坏；(2) 网络服务的可信. 主要看网络服务器或服务程序向访问者提供的服务是否真实可靠、不带有欺骗性，对用户终端是否会带来病毒等. (3) 网络信息传输的可信性，主要看网络各结点在传输信息的过程中是否忠实，不删、不改、不夹带. 如果从可信网络的服务器、网络本身和网络用户 3 个组成信息系统层面上来看，现有的保护措施是逐层递减的[2]，这说明人们往往把过多的注意力放在对服务器和网络的保护上，而忽略了对用户端的保护，这显然是不合理的. 因为用户端不仅是创建和存放重要数据的源头，同时绝大多数的攻击事件也都是从用户端发起的，例如数据泄密和蠕虫病毒感染等都是因为用户终端的脆弱性引起的. 如果我们能够对用户行为进行预测和控制，将不安全因素从用户端源头开始控制，使其符合安全和行为规范，就可以更加完善地保证整个网络的安全. 因此加强用户端的可信是整个网络可信的重要内容之一.

网络用户信任不仅包括对用户的身份信任，也包括对用户的行为信任[6]. 传统的安全机制被用来提供用户的授权和认证，解决了用户的身份信任问题，但并不能处理用户的行为信任问题. 例如在数字化电子资源的订购方面，大学生通过可信的身份信任(一般是学校的 IP 地址)可以登陆到学校定购的数字资源服务器上，但他的行为却有可能是不可信的，例如，利用下载工具大量下载文章，私设代理服务器等不可信行为来谋求自己的利益.

由于用户的行为信任是基于过去交往的行为证据之上，而我们需要的是未来的用户行为信任等级，因此科学地预测未来用户的行为信任等级是非常必要的. 由于信任和风险是并存的，单独依靠预测的信任等级进行决策是非常片面和危险的，因此在控制决策中还必须对风险进行分析，如何将预测结果和博弈分析相结合找出纳什均衡策略，提供控制的决策条件是研究用户行为信任的重要内容之一. 本文的结果对于量化分析用户行为信任具有重要的理论意义. 论文在分析的过程和实例分析中结合了数字化电子资源的网络实际应用背景，因此在网络实际应用中也具有重要的指导意义.

本文第 2 节概述了基于行为信任预测的博弈控制的整体过程；第 3 节论述了用户行为信任的预测，包括贝叶斯网络模型的建立，相关先验概率的统计以及不同属性条件下的信任预测和相关性质分析；第 4 节对基于用户安全行属性的博弈进行了分析，并计算出了混合纳什均衡策略；第 5 节推导出了基于预测结果的博弈控制决策条件；第 6 节给出一个简单的应用例子；第 7 节给出了本文的结论.

2　基于用户行为信任预测的博弈控制的整体过程

基于行为信任预测的博弈控制的主要思想是在用户身份信任的基础上增加用户行为信任的控制和管理，包括行为信任的预测、风险分析和决策控制，强化对网络用户状态的动态处理，为实施智能自适应的网络安全机制提供策略基础. 它的整体模型如图 1 所示，服务提供者在接到用户的访问服务请求之后，首先对用户的身份信任进行确认，如果身份认证失败则拒绝访问，否则将继续对用户的行为信任进行预测和博弈控制决策，论文的主要内容见图 1 中椭圆圈住的部分，模型的步骤在图中用数字标出，每个数字的具体含义包括：

1 为用户访问服务；2 为服务提供者将用户的

身份信息提交给用户身份验证代理进行身份信任的确认；3 为验证代理将验证的结果返回服务提供者；4 为如果身份验证错误，则服务提供者拒绝访问；否则将用户行为信任的管理请求提交给基于用户行为信任的管理中心；5 为管理中心把用户行为信任的预测提交给行为信任预测代理；6 为行为信任预测代理访问用户行为信任数据统计数据库；7 为返回以往用户行为信任的统计数据；8A，8B 为行为信任预测代理将预测的结果同时递交行为信任决策代理和管理中心；9 为管理中心把用户行为的决策提交给基于行为信任的决策代理；10 为决策代理在预测的基础上进行博弈分析与决策，并将决策结果返回给管理中心；11 为管理中心将基于用户行为信任的决策结果返回给服务提供者；12 为服务提供者最终决定是否接受还是拒绝用户的请求.

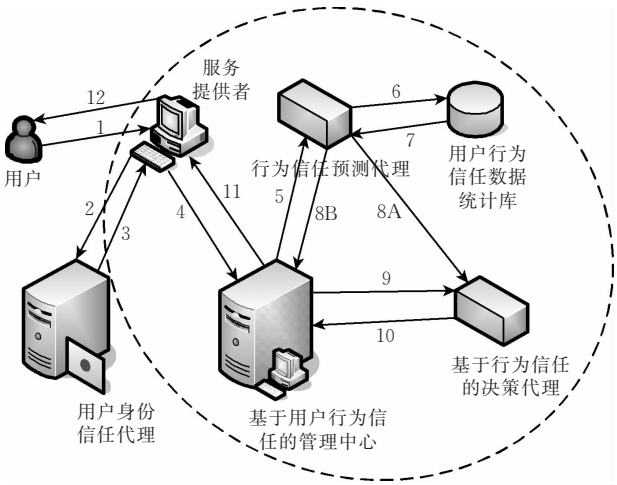

图 1 基于行为信任预测的博弈控制过程

3 基于贝叶斯网络的多条件下的用户行为信任的预测

3.1 用户行为信任的属性分解与贝叶斯网络模型

信任的概念最初是从社会学衍生出来的，因此具有主观性、笼统性等特性，这种社会学科的信任不利于量化自然学科的网络用户的行为信任. 为此，我们根据实际应用需求和功能特性将整体的用户行为信任进行逐层分解，将综合的、笼统的用户行为信任分解为若干行为信任属性，再将行为信任属性继续细化为可用软硬件直接测量的行为信任证据，这样可以有效解决可信网络中用户行为信任的笼统性和不确定性问题[6]. 例如将用户的行为信任划分为安全信任属性 S、性能信任属性 P 等，根据要求还可以继续划分，如消费信任属性、可靠性信任属性等.

安全信任属性主要描述用户行为是否符合规范，是否对访问的数据库造成破坏和进行攻击等，例如在数字化电子资源的订购方面，用户是否利用下载工具多线程大量下载文章，是否扫描重要端口，是否非法访问没有订购的数字资源等都属于安全行为信任证据. 性能信任属性主要描述用户性能方面的属性，例如在数字化电子资源的订购方面，用户下载文章的速率、用户对服务器的响应时间、用户使用完数据库后连接释放的时延等都属于性能行为信任证据，这些性能行为信任证据对于充分利用用户连接数这样有限的数据资源来说具有重要的意义，因为下载同样多的数据，性能行为信任属性低的用户将占用服务的时间多，其他的用户就可能因为用户连接数满而得不到服务，更详细的划分细节请读者参考文献[6].

贝叶斯网络模型的特色在于只要贝叶斯网络中任何一个节点状态确定，网络本身就可以利用贝叶斯公式进行正向或者逆向计算，从而得出网络中任意一个节点的概率. 它不但具有理论依据，而且将知识表示与知识推理结合起来，形成统一的整体. 一方面，它可以将用户行为信任预测的因果知识直接用有向图自然直观地表示出来，另一方面，也可以将以往用户行为的统计数据以条件概率的形式融入模型，这样贝叶斯网络就能将用户行为的先验知识和后验的数据无缝地结合在一起[7]. 一个用户行为信任预测的贝叶斯基本网络模型是一个有向无环图(见图 2)，它由代表变量节点及连接这些节点的有向边构成. 变量节点包括要预测的用户行为的总体信任 T 及其分解后的信任属性，如性能属性 P 及安全属性 S 等. 节点间的有向边代表了节点间的相互关系，由父节点指向其后代节点，父节点是用户行为总体信任 T，叶节点是用户行为信任的各种信任属性.

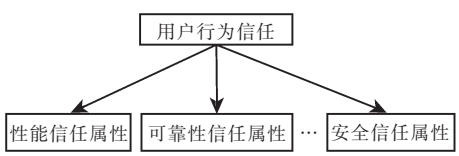

图 2 用户行为信任预测的贝叶斯网络基本模型

3.2 用户行为信任的等级划分和符号说明

为了能有效地对用户行为信任进行预测，将用户行为信任 T、性能属性 P 和安全属性 S 等各个节点划分为 L 个信任等级，并对这些信任等级从高到低进行顺序编号为整型变量 i，$i\in[1,L]$，它们所代表的信任区间范围从高到低的顺序分别是

$$\left[1-\frac{TH_1}{L-1},1\right],\left[1-2\times\frac{TH_1}{L-1},1-\frac{TH_1}{L-1}\right],\cdots,$$

$$\left[TH_0,1-(L-2)\times\frac{TH_1}{L-1}\right],[0,TH_0],$$

其中，TH_0是信任阈值，即当节点的行为信任值小于 TH_0时，服务提供者就不信任用户了，且 $TH_0+TH_1=1$. 每次交往后，交往的总次数 n 加 1，节点行为信任评估的值落在哪个范围内，则相应范围内所对应的次数加 1，其它保持不变. 为了满足各种不同要求的预测，我们还要保存两个和两个以上的不同节点值同时落在的不同范围的次数，这主要用来计算在多个信任属性条件下的用户行为信任的预测问题. 节点值同时落在两个不同节点范围内的次数用二维数组存储，节点值同时落在 3 个或 4 个不同节点范围内的次数分别用三维或四维数组存储. 数组的名字表示不同的节点，数组的下标表示不同的数值范围，因此我们用 T_i，P_i和 $S_i(1\leq i\leq L)$分别表示整体行为信任、性能属性和安全属性范围，用$|T_i|$，$|P_i|$和$|S_i|(1\leq i\leq L)$分别表示与所预测用户的交往历史中整体信任、性能属性和安全属性的值分别落在 T_i，P_i和 S_i范围内的次数，其值分别存储在数组 T_ia，P_ia 和 S_ia 中，节点值同时落在不同属性范围的次数用二维数组存储，如 T_iP_ja 储存信任 T 和属性 P 分别落在 T_i，P_i范围内的次数. 并用 $p(T_i)$，$p(P_i)$，$p(S_i)$分别表示它们的概率，这些符号的含义在后面的全文中均适用.

3.3　用户行为信任的预测

在利用贝叶斯网络对用户的行为信任进行预测之前，必须先计算出用户行为信任的先验概率、用户行为信任属性的先验概率及其条件概率. 先计算用户行为信任的先验概率：

$$p(T_i)=\frac{|T_i|}{n}(1\leq i\leq L)，并且\sum_{i=1}^{L}p(T_i)=1 \tag{1}$$

其中，n 表示与所预测用户交往的总次数. 计算用户行为属性的先验概率，其计算分法与计算用户行为信任先验概率的计算方法类似，以计算安全行为属性概率 $p(S_i)$为例，$p(S_i)=\frac{|S_i|}{n}(1\leq i\leq L)$，并且 $\sum_{i=1}^{L}p(S_i)=1$. 除了计算先验概率外，还必须计算各节点的条件概率，以计算 $p(S_i/T_j)$条件概率为例，它表示用户根节点在 T_j这个范围内的条件下安全属性节点在 S_i范围内的概率. 用式(2)计算

$$p(S_i/T_j)=\frac{p(S_i,T_j)}{p(T_j)}=\frac{|S_i\cap T_j|/n}{|T_j|/n}=\frac{|S_i\cap T_j|}{|T_j|} \tag{2}$$

有了所有节点的先验概率及所有叶节点的条件概率，就可以预测在某个特定行为信任属性条件下的用户行为信任等级的概率了. 首先看单信任属性(以安全信任属性为例，其他情况与此类似)条件下的用户行为信任的预测，利用贝叶斯公式计算

$$\begin{aligned}p(T_i/S_j)&=\frac{p(S_j/T_i)p(T_i)}{p(S_j)}\\&=\left(\frac{|S_j\cap T_i|}{|T_i|}\frac{|T_i|}{n}\right)\div\left(\frac{|S_j|}{n}\right)\\&=\frac{|S_j\cap T_i|}{|S_j|}\end{aligned} \tag{3}$$

3.4　行为信任预测的性质分析与计算的进一步扩展

从上面计算结论我们可以得到下面定理.

定理 1.　单个信任属性值的提高并不能提高该属性条件下的信任值，只有当各个信任属性值都相应增加时，该属性条件下的信任值才能增加.

证明.　首先证明单个信任属性值的提高并不能提高该属性条件下的信任值. 由式(3)知，在某个信任属性条件下的行为信任为$\frac{|A\cap T|}{|A|}$，其中 A 为某个行为信任属性. 我们假设在新的一次交往中，属性 A 的值提高到了预期的值，则$|A|$增加 1，即分母增加 1，这时如果整体信任没达到预期的值，即 $A\cap T$ 仍是原来的值，则分子不增加. 因此，交往前该属性条件下的行为信任值为$\frac{|A\cap T|}{|A|}$，交往后的该属性条件下的行为信任值为 $\frac{|A\cap T|}{|A|+1}$，由于 $\frac{|A\cap T|}{|A|}>\frac{|A\cap T|}{|A|+1}$，这就说明虽然信任属性 A 的值提高了，但该属性条件下的信任值并没有提高.

下面证明只有当各个信任属性值都相应增加，该属性条件下的信任值才能增加. 假设信任属性值至少增加 m 可以使信任属性值落在更高一级的信任范围内，即$|P|$和$|S|$增加 1，则新的信任 T 也至少增加 m，即$|T|$增加 1，这是因为 $T=\boldsymbol{A}\times\boldsymbol{W}=\sum_{i=1}^{N}a_iw_i$，其中 $\boldsymbol{A}$ 和 $\boldsymbol{W}$ 分别为信任属性向量和对应的权值向量，并且权值的和为 1，N 为属性的个数[6]，如果每个信任属性至少增加 m，则新的信任为

$$\begin{aligned}T'&=\sum_{i=1}^{N}(a_i+m)w_i=\sum_{i=1}^{N}a_iw_i+\sum_{i=1}^{N}mw_i\\&=\sum_{i=1}^{N}a_iw_i+m\sum_{i=1}^{N}w_i=T+m,\end{aligned}$$

由此知新信任至少增加 m. 由于各个信任属性也至少增加 m,则 $A\cap T$ 至少增加 m,即 $|A\cap T|$ 增加 1.

现在只要证明 $\frac{|A\cap T|}{|A|}\leq\frac{|A\cap T|+1}{|A|+1}$ 就能说明当各个信任属性值都相应增加时,该属性条件下的信任值也增加,即只要证明 $|A\cap T|\times(|A|+1)\leq(|A\cap T|+1)\times|A|$,化简得只要证明 $|A|\geq|A\cap T|$,由集合知识知 $|A|\geq|A\cap T|$ 是恒成立的,命题得证. 证毕.

利用贝叶斯公式,我们也可以预测在多信任属性条件下的用户行为信任等级概率,例如,我们假设 $L=5$,即行为信任等级分为 5 级,分别为非常信任(信任等级为 1)、信任(信任等级为 2)、比较信任(信任等级为 3)、基本信任(信任等级为 4)和不信任(信任等级为 5),那么我们用 $p(T_1/P_3,S_2)$ 可以求出关于性能信任属性为"比较信任"(信任等级是 3),安全信任属性为"信任"(信任等级是 2)的条件下,用户总体行为信任为"非常信任"(信任等级是 1)的概率. 双信任属性条件下的用户行为信任的计算见式(4):

$$\begin{aligned}p(T_i/P_j,S_k)&=\frac{p(P_j,S_k/T_i)p(T_i)}{p(P_j,S_k)}\\&=\frac{p(P_j,S_k,T_i)}{p(P_j,S_k)}\\&=\left(\frac{|P_j\cap S_k\cap T_i|}{n}\right)\div\left(\frac{|P_j\cap S_k|}{n}\right)\\&=\frac{|P_j\cap S_k\cap T_i|}{|P_j\cap S_k|}\end{aligned}\tag{4}$$

4 基于用户安全行为信任属性的博弈分析

4.1 文中符号说明和双方利益的得失分析

由于用户安全行为信任属性是用户行为信任中最重要的内容,因此本小节主要论述用户安全行为信任属性的博弈分析问题. 安全行为信任包括两个方面,即基本要求和高级要求,基本要求是指用户的行为是否规范,是否按契约的规定操作,例如,在学校的数字资源的使用方面,用户是否按规定使用资源,是否进行过量下载,私设对外代理服务器等;高级要求是指用户的行为是否具有攻击破坏行为,例如,有无攻击数字资源服务器企图,获取其他用户的帐号信息或商业竞争者以用户的名义进行拒绝服务(DOS)攻击等. 为了进行博弈分析,我们先介绍文中用到的符号所代表的意义,其中的实例和解释说明是以学校提供的数字资源为例的.

$Sloss_{acc}^{dec}>0$ 表示服务提供者在接受用户的欺骗访问时可能受到的平均损失量,如过量下载数字资源,私设对外代理服务器等,其他的欺骗也包括网络安全攻击导致服务器无法提供正常的服务或资源访问等.

$Sincome_{acc}^{n_dec}$ 表示服务提供者接受用户的不欺骗访问时,服务提供者可能得到正常的平均收益,如有偿数字资源服务下载,广告,帮助用户检索等获得的收益等.

$Sloss_{n_acc}^{n_dec}>0$ 表示服务提供者拒绝接受且用户不欺骗访问时服务提供者可能受到的平均损失,如数字资源服务因为拒绝正常的用户访问而使数字资源没有得到充分利用,以及双方由此引起的互不信任所造成的不合作损失等.

$Uincome_{acc}^{dec}$ 表示用户采取欺骗行为且服务提供者接受访问时用户得到的超额收益,如过量下载,私设对外代理服务器将数字资源转卖给第三方,获取其他用户的帐号信息,商业竞争者进行 DOS 攻击以提高自己的商业竞争力等获得的额外收益.

$Uincome_{acc}^{n_dec}$ 表示用户不欺骗且服务提供者接受访问时用户获得的平均收益,如下载相关的电子资源、浏览新闻和阅读专业资料等.

$Ucost>0$ 为用户采取欺骗行为所需要的成本. 如购买相应的软件、学习欺骗的方法和技巧所需要的时间和精力等.

$Upunish>0$ 表示用户采取欺骗行为所可能受到的惩罚, 如停止用户对数据库的使用权或受到法律起诉等.

4.2 基于用户安全行为信任属性的博弈分析

首先对用户和服务提供者双方利益的得失进行分析,如果服务提供者接受访问,用户不欺骗,那么服务提供者和用户都收益,他们的效用分别用 $Sincome_{acc}^{n_dec}$ 和 $Uincome_{acc}^{n_dec}$ 表示;如果服务提供者接受访问,用户欺骗,那么服务提供者得不到收益,只有损失 $Sloss_{acc}^{dec}$,用户的收益除了正常的平均收益 $Uincome_{acc}^{n_dec}$ 外,还可以得到因欺骗所获得的超额收益 $Uincome_{acc}^{dec}$,但用户欺骗也会有损失,一个是用户采取欺骗行为所需要的成本 $Ucost$,另一个是用户采取欺骗行为可能受到的惩罚 $Upunish$. 如果服务提供者拒绝访问,服务提供者既没有收益也不会有损失,但用户只要有欺骗的意图,它就需要为准备欺骗付出代价 $Ucost$,如果没有欺骗意图就没有这个代价. 用户之所以选择欺骗是因为用户认为欺骗所获得的收益大于不欺骗所获得的正常收益,也就是说我们假定用户欺骗所获得的收益大于用户正常访问

所获得的收益，即用户是理性的.

用户的信任等级不同，支付矩阵也不同. 前面我们已经把行为信任等级从高到低（即等级的值越小信任程度越大）分为 L 个等级，设用户行为信任等级为 $i(i=1,2,\cdots,L)$，则服务提供者和用户的支付矩阵分别为

$$\boldsymbol{A}_i=\begin{bmatrix}-Sloss_{acc}^{dec}\alpha_1^{i-1} & Sincome_{acc}^{n_dec}\alpha_2^{i-1}\\ 0 & -Sloss_{n_acc}^{n_dec}\alpha_6^{i-1}\end{bmatrix},$$

$$\boldsymbol{B}_i=\begin{bmatrix}Uincome_{acc}^{dec}\alpha_3^{i-1}+Uincome_{acc}^{n_dec}\alpha_4^{i-1}-Ucost-Upunish\alpha_5^{i-1} & -Ucost\\ Uincome_{acc}^{n_dec}\alpha_4^{i-1} & 0\end{bmatrix},$$

其中，$\alpha_K\in[0,1](K=1,2,\cdots,6)$ 是博弈分析的参数因子，主要取决信任划分的等级粒度和对安全要求的强度，可以根据决策者的要求进行调整. 注意这里 B_i 是在原支付矩阵的基础上进行了转置.

通过简单的画线法可以看到该博弈模型不存在纯策略均衡[8]，但我们可以求出混合策略的纳什均衡. 假定服务提供者以 x 的概率选择接受访问，以 $1-x$ 的概率选择拒绝访问，即服务提供者的混合策略为 $P_1=(x,1-x)$；假定用户以 y 的概率选择欺骗，以 $1-y$ 的概率选择不欺骗，即用户的混合策略为 $P_2=(y,1-y)$，那么用户的预期支付函数为

$$\begin{aligned}E_U(P_1,P_2)&=P_2B_iP_1^{\mathrm{T}}\\&=(y,1-y)\begin{bmatrix}Uincome_{acc}^{dec}\alpha_3^{i-1}+Uincome_{acc}^{n_dec}\alpha_4^{i-1}-Ucost-Upunish\alpha_5^{i-1} & -Ucost\\ Uincome_{acc}^{n_dec}\alpha_4^{i-1} & 0\end{bmatrix}\begin{pmatrix}x\\1-x\end{pmatrix}\\&=y(xUincome_{acc}^{dec}\alpha_3^{i-1}-xUpunish\alpha_5^{i-1}-Ucost)\end{aligned}\tag{5}$$

对上式关于 y 求偏导，可得服务提供者最优化的一阶条件为

$$\frac{\partial E_U(P_1,P_2)}{\partial y}=xUincome_{acc}^{dec}\alpha_3^{i-1}-xUpunish\alpha_5^{i-1}-Ucost=0,$$

解得

$$x^*=Ucost/(Uincome_{acc}^{dec}\alpha_3^{i-1}-Upunish\alpha_5^{i-1})\tag{6}$$

从这个公式可以看出，服务提供者的接受概率只与用户的支付有关，但并不是与用户的所有支付有关，而是只与用户欺骗相关的 3 个支付有关，因此，服务提供者要想提高自己的接受概率必须想办法加大用户欺骗时的成本，加大对用户欺骗的惩罚，减少用户欺骗成功所获得的收益.

可以看到混合纳什均衡策略的好处是给用户一个不确定的博弈结果，用户虽然知道服务提供者的支付矩阵和决策概率，但具体怎么决策并不能确定. 在这个博弈中，服务提供者以 x^* 的概率接受访问，以 $1-x^*$ 拒绝访问，此访问控制策略可以削减服务提供者的控制成本，因为即使拒绝访问是不确定的，足够高的被拒绝的可能性也将威胁住用户的欺骗，也就是说，如果拒绝的概率小于 $1-x^*$ 时，由于用户是理性的，我们从式(5)的一阶条件可知，用户的最优选择是欺骗，就好像没有拒绝访问一样. 相反，如果拒绝访问的概率大于 $1-x^*$，则用户的最优选择是不欺骗. 总之，服务提供者的拒绝率太低或太高，用户都有唯一的最优选择，只有服务提供者以混合纳什均衡策略 x^* 概率接受访问，以 $1-x^*$ 概率拒绝访问，用户对欺骗和不欺骗两种选择是无差异的（即有相同的支付），服务提供者没有给用户提供任何的投机机会. 下面给出一个信任等级与双方支付关系的一个性质.

性质 1.　服务提供者的得失、用户的收益与用户的信任等级成正比.

证明.　由 4.1 节知服务提供者的得失以及用户的正常收益，额外收益分别为 $Sloss_{acc}^{dec}\alpha_1^{i-1}$，$Sincome_{acc}^{n_dec}\alpha_2^{i-1}$，$Sloss_{n_acc}^{n_dec}\alpha_6^{i-1}$，$Uincome_{acc}^{dec}\alpha_3^{i-1}$ 和 $Uincome_{acc}^{n_dec}\alpha_4^{i-1}$，设两个用户 U_i 和 U_j 的行为信任等级分别为 i,j，并假设 $i<j$，因为信任等级越高，i,j 的值越小，因此用户 i 的信任等级大于用户 j 的信任等级，并设 $i-j=C<0$，则两用户的同一支付值的比为 $\alpha^{i-1}/\alpha^{j-1}=\alpha^{(i-1)-(j-1)}=\alpha^C$，由于 $\alpha\in[0,1]$，$C<0$，因此 $\alpha^C>1$，即用户 i 和用户 j 同一支付值的比是一个大于 1 的常量，因此它们的关系是成正比例的.　　证毕.

这个性质可以从实际网络应用中去理解，用户信任类型级别越高，服务提供者与用户可以合作的越深入，对用户开放的资源可以相对多一些，因此双方正常交往时所得到的平均收益会多一些，同时一旦高信任用户进行欺骗，欺骗的用户获得的额外收益也大，服务提供者受到的损失也大，因此服务提供者也会对高信任的用户进行更为严重的惩罚，可见这个性质是与实际网络应用相符合的.

5 基于用户行为信任预测的博弈控制策略

上面计算出了服务提供者的混合纳什均衡策略,即解决了以什么样的概率进行控制决策的问题,但具体的每次如何决策还不能确定,这还要结合用户的信任等级和对方用户的决策概率来决定,这是因为不同信任等级的用户其决策的策略是不同的,而且控制博弈策略取决于双方的博弈分析,不只是自己的单方面的推断,这也正是博弈论的内涵.下面我们以一个定理的形式给出基于用户行为信任预测的博弈控制条件.

定理 2. 已知用户行为的信任等级的预测概率 Pt 和服务提供者的支付矩阵,则服务提供者接受访问的控制条件是

$$\sum_{i=1}^{L} Pt_i[-y^* Sloss_{acc}^{dec}\alpha_1^{i-1} + (1-y^*)(Sincome_{acc}^{n_dec}\alpha_2^{i-1})] > 0,$$

其中 Pt_i 是信任等级为 i 的预测概率,y^* 和 $1-y^*$ 分别是用户欺骗和不欺骗的混合纳什均衡策略,L 是信任等级划分的级别. $Sloss_{acc}^{dec}>0$ 是服务提供者接受用户访问,用户如果欺骗时可能受到的平均损失量. $Sincome_{acc}^{n_dec}$ 是服务提供者接受用户访问,用户不欺骗时所获得的平均收益.

证明. 因为不同信任等级的用户其支付矩阵是不一样的,因此决策前先必须预测用户在各信任等级的概率 Pt_i,这个已经在 3.3 节计算出来了,这里不再赘述.

有了预测的用户信任等级概率,我们还要用博弈理论分析用户的决策概率,我们假定用户是理性的,即用户寻求以一种最大化自己支付的方式进行博弈,那么能达到这个要求并且双方可以持久保持稳定状态的就是混合策略的纳什均衡,因此先计算用户的混合纳什均衡策略.因为服务提供者的预期支付函数为

$$E_S(P_1,P_2)=P_1A_iP_2^{\mathrm{T}}=$$

$$(x,1-x)\begin{bmatrix}-Sloss_{acc}^{dec}\alpha_1^{i-1} & Sincome_{acc}^{n_dec}\alpha_2^{i-1}\\ 0 & -Sloss_{n_acc}^{n_dec}\alpha_6^{i-1}\end{bmatrix}\begin{pmatrix}y\\1-y\end{pmatrix}=$$

$$-xySloss_{acc}^{dec}\alpha_1^{i-1}+x(1-y)Sincome_{acc}^{n_dec}\alpha_2^{i-1}-(1-x)(1-y)Sloss_{n_acc}^{n_dec}\alpha_6^{i-1} \tag{7}$$

对式(7)求关于 x 求偏导,可得用户最优化的一阶条件为

$$\frac{\partial E_S(P_1,P_2)}{\partial x}=Sincome_{acc}^{n_dec}\alpha_2^{i-1}+Sloss_{n_acc}^{n_dec}\alpha_6^{i-1}-y(Sloss_{acc}^{dec}\alpha_1^{i-1}+Sincome_{acc}^{n_dec}\alpha_2^{i-1}+Sloss_{n_acc}^{n_dec}\alpha_6^{i-1})=0$$

解得

$$y^*=\frac{(Sincome_{acc}^{n_dec}\alpha_2^{i-1}+Sloss_{n_acc}^{n_dec}\alpha_6^{i-1})}{(Sloss_{acc}^{dec}\alpha_1^{i-1}+Sincome_{acc}^{n_dec}\alpha_2^{i-1}+Sloss_{n_acc}^{n_dec}\alpha_6^{i-1})} \tag{8}$$

即$(y^*,1-y^*)$是用户的混合纳什均衡策略.

由 4.2 节知,用户信任等级为 i 的服务提供者的支付矩阵为

$$\begin{bmatrix}-Sloss_{acc}^{dec}\alpha_1^{i-1} & Sincome_{acc}^{n_dec}\alpha_2^{i-1}\\ 0 & -Sloss_{n_acc}^{n_dec}\alpha_6^{i-1}\end{bmatrix},$$

现在求用户接受服务的决策条件,实际就是求服务提供者的接受概率为 1,用户选择欺骗和不欺骗的概率分别为 y^*,$1-y^*$ 时的服务提供者的利益得失情况,此矩阵的第一行表示接受用户访问,第一列表示用户欺骗,第二列表示不欺骗,因此服务提供者获得的利益为 $-y^*Sloss_{acc}^{dec}\alpha_1^{i-1}+(1-y^*)Sincome_{acc}^{n_dec}\alpha_2^{i-1}$. 上式只是用户信任等级为 i 时服务提供者获得的利益结果,要想得到该用户的全部获利情况,就必须对 L 个信任等级进行加权求和,即服务提供者总的获得的利益为

$$\sum_{i=1}^{L} Pt_i[-y^*Sloss_{acc}^{dec}\alpha_1^{i-1}+(1-y^*)(Sincome_{acc}^{n_dec}\alpha_2^{i-1})] \tag{9}$$

如果这个值大于零,则说明服务提供者的收益大于零,那么就接受访问,否则拒绝访问.命题得证.

证毕.

下面通过一个简单的应用实例来说明该结果的具体应用.

6 应用实例与对比分析

6.1 应用实例的背景

在学校订购的电子资源数据库服务中,服务提供者是电子数字资源提供商(数据库商),用户是指订购数据库资源的学校.用户身份信任的依据是用户的 IP 地址,即只要用户的 IP 地址在合法的范围内,用户就可以访问数据库.但只有身份信任还是不够的,因为一些学生在校内(身份信任是合法的)常常使用网络下载工具大批量下载学校购买的电子资源或者私设代理服务器牟取非法所得等,即用户的身份信任是可信的,但用户的行为信任不一定是可信的.数据库商为了制止这些不信任行为的发生,他们会根据用户不良行为的严重程度采取不同的惩罚措施,例如提出警告,暂停对数据库的访问等,如果停止的频率过多,则直接影响数据库商和学校之间

的合作，如果停止的频率过低，则达不到制止滥用数据库的目的，这时用户会更多选择欺骗，如果数据库商根据本文所得到的混合博弈均衡策略概率进行惩罚，那么用户的任何策略对用户来说都是无差异的，即具有相等的支付，数据库商没有给用户提供任何的投机机会，也就是说用户知道数据库商会因为他们“滥用”数据库而暂停他们使用数据库的权限，但对“滥用”的标准到底是什么不能确定，因此用户不敢随意欺骗.

表 1　实例参数的初值和计算的结果值

信任等级	*s_loss_acc_dec*	*s_loss_ nacc_ndec*	*s_income_ acc_ndec*	*u_income_ acc_ndec*	*u_income_ acc_dec*	*u_cost*	*u_pun*	*s_acc_p*	*u_dec_p*
1	1000.0	100.0	100.0	300.0	830.0	86.0	740.0	96	17
2	700.0	95.0	95.0	255.0	747.0	86.0	643.8	83	21
3	490.0	90.3	90.3	216.8	672.3	86.0	560.1	77	27
4	343.0	85.7	85.7	184.2	605.1	86.0	487.3	73	33
5	240.1	81.5	81.5	156.6	544.6	86.0	423.9	71	40

6.2　应用实例的数据假定与决策计算

为了简化例子并与实际应用相符合，设行为信任等级只有五级，分别为非常信任、信任、比较信任、基本信任和不信任，并设用户对应这五个信任等级的相应信任等级概率 Pt_i 分别为 0.1，0.7，0.12，0.04，0.04，即信任的概率比较大. 博弈分析的参数因子 α_i 分别为 0.7，0.95，0.9，0.85，0.87，0.95，其他参数的假定值见表 1 的第 2 列～第 8 列，其中 *s_loss_acc_dec* 表示务提供者接受用户的欺骗访问时可能受到的平均损失量；*s_loss_nacc_ndec* 表示服务提供者拒绝接受且用户不欺骗时服务提供者可能受到的平均损失；*s_income_acc_ndec* 表示服务提供者接受用户的不欺骗访问时，服务提供者可能得到正常的平均收益；*u_income_acc_ndec* 表示用户不欺骗且服务提供者接受访问时用户获得的平均收益；*u_income_acc_dec* 表示用户采取欺骗行为且服务提供者接受访问时用户得到的超额收益；*u_cost* 用户采取欺骗行为所需要的成本；*u_pun* 表示用户采取欺骗行为所可能受到的惩罚. 将上述参数代入式(6)可求出数据库商的混合纳什均衡的接受概率 *s_acc_p*，将上述参数代入式(8)可求出该用户的混合纳什均衡的欺骗概率 *u_dec_p*，具体结果见表 1 的第 9 列和第 10 列. 有了信任等级概率 Pt_i，博弈分析的参数因子 α_i，*s_loss_acc_dec*，*s_income_acc_ndec* 以及计算得到的用户欺骗概率 *u_dec_p* 就可以利用式(9)计算数据库商获得的效益并进行决策控制，如果计算的结果大于零就接受，否则就拒绝该用户的访问.

6.3　结果的比较与分析

目前大多数的访问控制主要是针对身份或角色的[9-10]，其他一些与信任相关的访问控制也主要是基于信任本身评估的[7,11]，都未将行为信任评估、预测与博弈控制三者结合起来进行控制，本文的用户行为的访问控制策略与其他基于身份、角色和信任本身评估的访问控制策略相比，优点主要有：(1)基于用户身份或角色的访问控制主要是以相对静态的身份和角色为基础的，而本文基于用户行为信任的控制是根据用户的行为进行动态控制决策的；(2)基于信任本身评估的控制决策只是基于过去的用户信任，不能说明未来用户行为的趋势，缺乏必要的信任预测；(3)预测是概率问题，在决策时不能仅仅取决于概率，必须明确是接受还是拒绝，因此要利用某种机制进行决策，由于用户行为是人参与的行为，因此利用博弈论进行得失分析是最恰当的. 因此论文的实例在应用中更切合实际.

上例的相关数据结果的统计见图 3. 从这个例子中可以看到用户因欺骗所获得的收益 *u_income_acc_dec* 和用户所受到的惩罚 *u_punish* 随着信任等级的降低而降低，在用户进行欺骗的成本固定不变的情况下，随着用户信任等级的降低，服务提供者的接受概率 *s_acc_p* 也在减少，用户的欺骗概率 *u_dec_p* 在增大，这与本文得出的结论是一致的. 注意：为了在同一张图看清楚计算结果的趋势，绘图时百分比的结果放大了 500 倍.

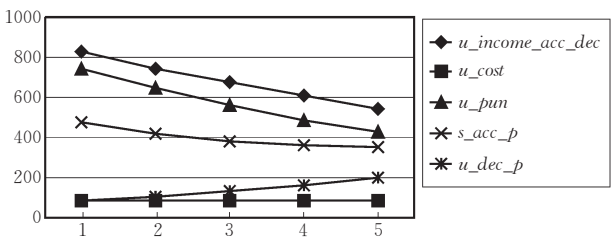

图 3　数据库商和用户信任等级的混合博弈概率趋势

7　结　论

本文论述了如何利用贝叶斯网络对用户行为信任进行多属性条件下的预测，并在预测的基础上对

服务提供者和用户的收益进行了博弈分析，推导出了混合纳什均衡策略，同时结合这两者的结果计算出了针对用户行为安全属性的决策控制条件. 本文的结果对于量化分析用户行为信任具有重要的理论意义，论文在分析的过程和实例中结合数字化电子资源的网络实际应用背景，因此在实际网络应用中也具有重要的指导意义.

参 考 文 献

[1] Ruohomaa S, Kutvonen L. Trust management survey//Proceedings of the iTrust 2005. Lecture Notes in Computer Science 3477. Berlin: Springer, 2005: 77-92

[2] Lin Chuang, Pen Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯，彭雪海. 可信网络研究. 计算机学报，2005，28(5)：751-758)

[3] Theodorakopoulos, George, Baras, John S. On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 318-328

[4] Pal P, Webber F, Atighetchi M, Combs N. Trust assessment from observed behavior: Toward and essential service for trusted network computing//Proceedings of the 5th IEEE International Symposium on Network Computing and Applications. Cambridge, MA, USA, 2006: 285-292

[5] Ciaran B, Karl K, Jean-Marc S, Vinny C. Towards an evaluation methodology for computational trust systems//Proceedings of the iTrust 2005. Lecture Notes in Computer Science 3477. Berlin: Springer, 2005: 289-304

[6] Tian Li-Qin, Lin Chuang, Ji Tie-Guo. Kind of quantitative evaluation of user behaviour trust using AHP. Journal of Computational Information Systems, 2007, 3(4): 1329-1334

[7] Lin Ai-Zhong, Vullings E, Dalziel J. A trust-based access control model for virtual organizations//Proceedings of the GCC Workshops. Changsha, China, 2006: 557-564

[8] Bell M. The use of game theory to measure the vulnerability of stochastic networks. IEEE Transactions on Reliability, 2003, 52(1): 63-68

[9] Bertino E, Squicciarini A C, Martino L, Paci F. An adaptive access control model for web services. International Journal of Web Services Research, 2006, 3(3): 27-60

[10] Hassan T, Morteza A, Rasool J. Trust-based user-role assignment in role-based access control//Proceedings of the AICCSA. Amman, Jordan, 2007: 807-814

[11] Adams William J, Davis I V, Nathaniel J. TMS: A trust management system for access control in dynamic collaborative environments//Proceedings of the IEEE International Performance, Computing, and Communications. Phoenix, Arizona, 2006: 143-150

[12] Azzedin F, Maheswaran M. Towards trust-aware resource management in grid computing Systems//Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID). Berlin, Germany, 2002: 452-457

[13] Liao Wen-Hui, Zhang Wei-Hong, Zhu Zhi-Wei, Ji Qiang. A real-time human stress monitoring system using dynamic Bayesian network//Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. San Diego, CA, USA, 2005: 70

TIAN Li-Qin, born in 1970, Ph. D. candidate, associate professor. His current research interests include computer networks, performance evaluation, network security and trustworthy networks.

LIN Chuang, born in 1948, Ph. D., professor, Ph. D. supervisor. His current research interests include computer networks, performance evaluation, network security, Petri net theory, trustworthy networks and trustworthy computing.

Background

This research is supported by the National Natural Science Foundation of China (Nos. 60673184, 60673187 and 90412012), the National Basic Research Program (973 Program) of China (No. 2006CB708301), and Science and Technology Project of Hebei Province (No. 07213570).

In recent years, the trustworthy network research has become a research focus. An important objective of above projects is to probe the user behaviour trust of trustworthy network, which strengthens the dynamic state processing of the user trust, providing the strategy foundation for the implementation of intelligent adaptive network security. Comparing current user access control strategy, which mainly based on user identity, role or trust self, it is relatively static, past and no considering both side profit, the authors consider user behaviour trust, predict trend of the behaviour trust and analyze both side payoff matrix. The authors first use Bayesian network to forecast user behaviour trust, then combine it with Game theory to decide if the service provider accept or deny user request. An framework of Game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network is provided.