网络环境下一种基于概率密度的信任博弈模型

陈 晶,杜瑞颖,王丽娜,田在荣
(武汉大学计算机学院,湖北武汉 430072)

摘 要: 随着可信计算的飞速发展,网络可信受到越来越多研究者的关注,信任模型的研究是其中主要研究内容之一.本文提出一种网络环境下基于概率密度的信任博弈模型,将信任模型的研究和网络环境相结合,把整个信任系统分为证据收集、基于概率密度的信任度量以及服务博弈三部分.证据收集模块利用数据挖掘和关联规则匹配进行信任证据的判断与评估.信任度量模块将信任细分为信任度和确定度,并按照熵原理使用概率密度函数来表现.虽然信任度量的目的是为了指导服务,单纯依靠信任度量并不可靠,服务博弈模块将度量结果结合支付矩阵进行博弈分析,计算出服务提供者行为的混合合纳什均衡策略.在三部分的分析过程中,与网络环境紧密结合,因此该方法对于网络可信的研究具有重要指导意义.

关键词: 信任模型; 概率密度函数; 博弈论
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2010) 02-0427-07

A Trust Game Method Basing on Probability Model in Networks

CHEN Jing, DU Rui-ying, WANG Li-na, Tian Zai-rong
(*School of Computer, Wuhan University, Wuhan, Hubei* 430072, *China*)

Abstract: With the trust computing rapid developing, the trust model becomes an important research area of the network trust which attracts more and more researchers. In this paper, we propose a trust game method basing on probability density in networks. Our trust model includes three parts which are evidence collection, trust estimation basing on probability density and game service where the application background is networks. In evidence collection part, we use data mining technology to collect evidences. In order to estimate trust neatly, we divided trust into credit and certainty, and use probability density function to express according to entropy theory. Though the trust estimation aims to guide service, but if we only depend on it, it is not reliable. We utilize game payment matrix to compute the nash equilibrium of the service provider. The analysis process of three parts fuses with network environment, hence, the method has significance to research network trust.

Key words: trust model; probability density function; game theory

1 引言

现阶段,可信这个概念被越来越多的研究者所关注.通过不同的信任模型表示方法和各类推荐信息的处理方法,产生了很多不同的信任模型[1].

Marsh 在此方面做出了前期工作[2],提出了基于社会关系的信任模型.在计算模型中引入了事件重要性和有效性两个概念,在考虑信任与风险的同时,设置门限值来做出决策.该模型的主要缺点是该模型是一个一维的信任模型,主要关注的是由直接经验所产生的信任值,而没有考虑其它实体的参考意见.TidalTrust[3] 和 EigenTrust[4] 在产生信任等级的时候,综合了本地和其它实体的信息.但也是一维的信任模型.一维模型中信任都是由单一的信任值表示的,很可能通过一条证据和多条证据得出的信任值是一样的,这样信任值并不能表现出这些取值的确定性和可靠性.当其它实体的推荐都聚合到一个单一值的时候,将导致信任信息的丢失.另外,也不易体现出推荐的作用.例如,在 TidalTrust 中,如果实体接收到的推荐全部来自低信任值的推荐者,那么聚合后的信任值无法反映出真实的情况.或者当高信任等级的推荐者提供了关于某个观点或者实体的低推荐值,也无法通过最后的信任值有效的反映出来.文献[5~7]中提出了二维或者三维的信任模型,也称为信仰模型.这些信任模型基于贝叶斯定理,使用belief(b),disbelief(d)和 uncertainty(u)来表示信任.这些模型的缺点在于三个参数不能独立进行赋值,例如,文献[7]中,规定 $b+d+u=1$.因此,u 的大小将会影响 b 和 d 的大小,使得信任的表示受到限制.同样,这三个模型也都没有能表现信任等级确定性的参数.另外,上面提到的信任模型,只是单纯意义上的信任评估方法,而缺乏对证据收集过程的研究.信任是基于实

收稿日期:2008-08-07;修回日期:2009-05-28
基金项目:国家自然科学基金重大研究计划项目(No.90718006);国际合作项目(No.2007DFA11000);国家青年自然科学基金(No.60903196);湖北省自然科学基金(No.2009CDB379)

体的历史行为对未来行为的预期判断,所以单纯的依赖信任度量结果并不能非常有效的判断或者驱使实体的行为合法化.

本文提出一种网络环境下基于概率密度的信任博弈模型,为更加系统完整的阐述,将该方法分为证据收集、基于概率密度的信任度量及服务博弈这三部分.

在证据收集阶段,证据主要通过信任实体自身获得,同时需要把这些证据进行分类,判断是恶意的还是合法的,为下一步的信任度量提供必要的支持.这个过程是上述信任模型中忽略或者介绍较简单的.本文将数据挖掘引入到证据收集中,采用基于关联规则的评估方案,利用它在处理海量数据方面的优势,从大量的实体事件和行为中挖掘出正常和恶意行为模式,省去了人工区分合法与非法证据的过程,并且解决了证据收集的自适应性问题与可扩展性问题.基于概率密度的信任度量将信任分为信任度和确定度这两个相互独立的概念,综合邻近实体意见进行度量,通过概率密度计算信任度,利用证据收集的结果计算确定度,并根据信任度量结果寻找实体之间的可信路径.

基于度量结果的服务博弈中,以一定概率接受服务,使得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,没有给用户提供任何的投机机会,使用户更倾向于诚信.与基于自身评估的访问控制策略相比,优点主要有:(1)访问控制策略对于用户都是信任的,而在复杂网络的环境下,这是难以达到的;(2)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,而本文基于用户信任度量进行动态控制决策的;(3)用户行为是人参与的行为,人会在决策过程中权衡收益,因此利用博弈论进行得失分析是最恰当的.

2 前提假设

(1)现阶段,已经有些安全路由协议研究实体之间报文的安全传递,如 Ariadne[8],SAR[9],SEAD[10],而文章主要研究信任模型,所以不对报文做相应安全性的设计,可以将一些现有的安全路由方案和信任模型相互融合[11].

(2)信任度量时,各观点之间相互独立.

(3)博弈服务时,假设用户都是理性的,即用户行为决策时,尽量保证收益最大化.

3 信任证据收集

在信任度量系统中可通过数据挖掘技术,提取实体的行为特征,总结恶意行为的规律,从而建立起比较完备的信任规则库来进行恶意行为辨别.主要过程分为数据采集、数据预处理以及数据挖掘 3 个步骤:

(1)数据采集 在网络环境中,当实体 A 和实体 B 需要进行交互通信的时候,系统首先需要收集报文信息.主要收集的报文为:报文源 IP 地址(SIP)、源物理地址(SMAC)、报文目的 IP 地址(DIP)、目的物理地址(DMAC)、报文到达时间(RTime)、通信持续时间(CTime)、流量(Flux)和吞吐量(Throughout),则收集的数据集合为 $C_{set}=\{\text{SIP, SMAC, DIP, DMAC, RTime, CTime, Flux, Throughout}\}$.在实体交互过程中,每个实体都将网卡设置成混杂模式,以完成信息收集.

(2)数据预处理 原始数据项集并不能直接反映网络中的攻击行为,网络中很多攻击并非是发送一些不合法报文,而是将其修改成合法但会导致异常结果的报文,如黑洞攻击、虫洞攻击等.因此,需要将原始数据进行预处理,使得数据可以更加直接反映出网络特点;另外,就是需要反映出时间相关性,如果单纯对上述数据进行挖掘,只能找到在某个时间点上的规则,而不能反映一段时间内报文的相关性.根据上述分析,预处理可分为两步:

首先,对数据进行属性划分,按需求不同可以设置不同的属性作为划分的标准.为了能准确的判断各实体发送的报文是否可信,本文按地址进行划分.针对实体 i,将报文分为:①源 IP 地址不是节点 i,但源 MAC 地址为节点 i 的报文,设为 S_1,表示节点 i 发送的为转发的报文;②源 IP 地址是节点 i 且源 MAC 地址为节点 i 的报文,设为 S_2,这表示节点 i 自己发送的报文;③目的 IP 地址与 MAC 地址都为节点 i 的报文,设为 S_3,这表示节点 i 自己需要处理的报文;④目的 IP 地址不是节点 i,但 MAC 地址为节点 i 的报文,设为 S_4,这表示节点 i 接收的是需要转发的报文;

第二步,将数值属性划分为几个区间.本文首先将数值属性分类转换,再采用布尔型关联规则进行挖掘.为避免产生过多规则,可按报文数量划分为高、中、低三个区间,以 m 作为参数,把 n 个对象分为 m 个簇,使簇内具有较高的相似度,而簇间的相似度较低.采用的簇准则函数是簇集中的每个样本点(数据或对象)到该类中心的距离平方之和,并使它最小.

本文将原始数据中的数值分类转化为使用 H, M, L 来代替,计算这三个类的中心点,并对各个报文统计数值字段进行相同的处理,将原有的包含数值属性的字段全部替换为布尔型,然后采用经典的关联规则挖掘方法来进行知识发现.算法的流程如下:

(a)选 3 个初始簇中心:$cluster_1(y)$, $cluster_2(y)$, $cluster_3(y)$.括号内的序号 y 为寻找簇中心的迭代运算的次序号.簇中心的向量值可以任意设定,一般可用开始 3 样本点作为初始簇中心.

(b)逐个将需分类的样本$\{x\}$按最小距离原则分配

给簇中心的某一个 $cluster_j(y)$.假如 $i=j$ 时,$Dst_j(y)=\min\{\|x-cluster_i(y)\|,i=1,2,3\}$,则 $x\in C_j(y)$,其中 y 为迭代运算次序号,第一次迭代则 $y=1$,C_j 表示第 j 个簇,其簇中心为 $cluster_j$.

(c)计算各个簇中心新的向量值,即求各簇域中包含样本的均值向量 $cluster_j(y+1)=\sum_{x\in C_j(y)} x/N_j, j=1,2,3$,其中 N_j 是第 j 个簇域 C_j 中所包含的样本数.以均值向量为新的簇中心,可以使簇准则函数 $J_j=\sum_{x\in C_j(y)}\|x-cluster_j(y+1)\|$ 最小,其中 $j=1,2,3$.

(d)如果 $cluster_j(y+1)\neq cluster_j(y)$,其中 $j=1,2,3$,则 $y=y+1$,回到步骤 2,将样本逐个重新分类,重复迭代计算.如果 $cluster_j(y+1)=cluster_j(y), j=1,2,3$,则算法收敛,计算完毕.

(3)关联规则挖掘　数据预处理完成后,采用 Apriori 算法进行关联规则挖掘[12].Apriori 算法于 1993 年由 Agrawal 提出,其核心是基于两阶段频集思想的递推算法.基本思想是:首先,由较小的频繁项目集 L_k 产生较大的候选频繁集 L_{k+1},如此反复,找出所有的频集.这些项集出现的频繁性至少和预定义的最小支持度一样,然后由频集产生关联规则,这些规则必须满足最小的支持度和最小的可信度.

经过上述几个步骤,可形成初始化的信任度量准则,主机定时进行流量分析与关联规则匹配,对不符合关联规则的网络流量,即可认为是恶意行为,作为一次恶意行为处理,负面证据数增加 1,否则认为是正常行为,正面证据数增加 1.

4　基于概率密度的信任度量

4.1　用户信任接口

表 1　符号定义表

符号	含义
$scene_i$	表示第 i 个场景,$i\in\{1,2,\cdots,n\}$
a,b	小写字母表示实体
X,Y	大写字母表示观点
$X_a(scene_i)$	实体 a 在场景 $scene_i$ 中的观点 X
$REC_a^b(scene_i)$	实体 a 对于 b 在场景 $scene_i$ 中的推荐度
$Max\_pro(scene_i)$	证据数最大期望值

用户信任接口(User Trust Interface,UTI)是为用户反映信任等级的接口,主要表现对某一观点的信任程度和确定程度.UTI 中,观点 X 是由二元组表示,$X=(TS,AS)\in[0,1]\times[0,1]$.而推荐度 $REC_a^b(scene_i)$ 表示为 $REC_a^b(scene_i)=(TS_a^b(scene_i),AS_a^b(scene_i))$,即在场景 $scene_i$ 的情况下,实体 a 对 b 的信任推荐度.$TS_a^b(scene_i)$ 表示实体 a 对实体 b 的信任程度,而 $AS_a^b(scene_i)$ 则表示实体 a 对提供的推荐值的确定程度.如果 $AS_a^b(scene_i)$ 较低,则说明实体 a 对实体 b 的 $TS_a^b(scene_i)$ 容易改变,反之,则实体 a 对实体 b 的 $TS_a^b(scene_i)$ 不易改变.X_a 和 $X_a(scene_i)$ 的解释与此类似.信任值和确定值各自独立.例如,$REC_a^b(scene_i)=(1,0.1)$ 表示实体 a 认为 b 当前是可信的,但是由于收集的证据数量较少,所以并不确定.同样,也可能实体 a 不相信实体 b,但实体 a 对该观点非常确定.推荐的传播如图 1 的推荐链所示,表现了信任的整合和分散过程.

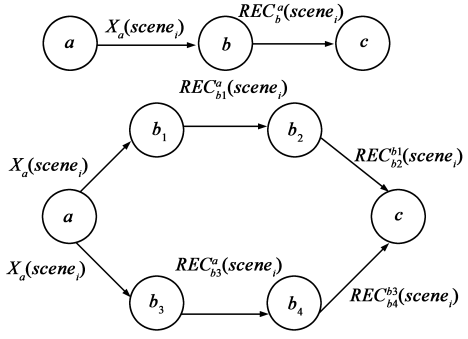


图1　信任链

4.2　信任接口的概率表示

信任接口的表现方式上,组成论使我们有了新视角:由于信任等级高的实体可能出现异常行为,而信任等级低的实体却不一定出现异常行为,所以信任实体的行为本身具有随机性,有随机性的研究对象(广义集合)都应当遵守最复杂原理(熵原理).即自动使自己内部状态的复杂程度在限制条件下达到最大值.本文通过熵原理来研究信任,以概率密度函数(probability density function,pdf)来表现信任接口.假设信任值 x 是一个 $x\in[0,1]$ 的随机变量,而且 x 与 $(1-x)$ 具有对称性,假设其概率分布函数为 $f(x)$.

定理 1　信任值 x 的概率分布函数可以写为

$$f(x)=\frac{(m+n+1)!}{m!\ n!}x^m(1-x)^n$$

其中 $m=p-1$,$n=q-1$,$0\leqslant x\leqslant 1$,$p>0$,$q>0$,p 和 q 分别表示正面证据数和负面证据数,收集到的证据总数为 $p+q$.

证明　考虑从熵原理加适当的约束条件推求这个概率密度分布函数,可以看出它是下面三个约束条件与熵原理的应用结果.

(1)变量 x 的对数平均值为固定值(等价于几何平均值为常数):

$$u=\int_0^1(\ln x)f(x)\,dx \tag{1}$$

(2)$(1-x)$ 的对数平均值也是固定之值:

$$v=\int_0^1\ln(1-x)f(x)\,dx \tag{2}$$

(3)作为概率密度,当然还有

$$1=\int_0^1 f(x)\,\mathrm{d}x \tag{3}$$

根据上面的三个约束公式和熵原理,利用拉格朗日方法,构造的 F 函数是

$$\begin{aligned}F=&\int_0^1 -f(x)\ln f(x)\mathrm{d}x+C_1[(\int_0^1 f(x)\mathrm{d}x)-1]\\&+C_2[(\int_0^1 \ln x f(x)\mathrm{d}x)-u]\\&+C_3[(\int_0^1 \ln(1-x)f(x)\mathrm{d}x)-v]\end{aligned} \tag{4}$$

求 F 对未知的概率密度 $f(x)$ 的偏微分,并且令它等于0(利用熵原理),我们得到

$$f(x)=e^{C_1-1}x^{C_2}(1-x)^{C_3} \tag{5}$$

通过等式(5)和等式(3),可得

$$e^{C_1-1}=1/B(C_2+1,C_3+1) \tag{6}$$

将等式(6)代入等式(5),可得

$$f(x)=\frac{1}{B(C_2+1,C_3+1)}x^{C_2}(1-x)^{C_3} \tag{7}$$

通过 u,v 的约束公式即等式(1)和(2)可以求出 C_2 和 C_3,最后可以得到概率密度分布函数

$$f(x)=\frac{1}{B(p,q)}x^{p-1}(1-x)^{q-1},0\leqslant x\leqslant 1,p>0,q>0 \tag{8}$$

$B(p,q)$的含义是 $B(p,q)=\int_0^1 x^{p-1}(1-x)^{q-1}\mathrm{d}x$.并且 $B(p,q)=\frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}$.其中 $\Gamma(x)$为 Gamma 分布,所以概率分布函数可以写为 $f(x)=\frac{(m+n+1)!}{m!\ n!}x^m(1-x)^n$,其中 $m=p-1,n=q-1,0\leqslant x\leqslant 1,p>0,q>0$,$p$ 和 q 分别表示正面证据数和负面证据数,收集到的证据总数为 $p+q$.

在用户信任接口中,观点 $X_a(scene_i)$可以用 p,q 通过概率密度表示 $X_a(scene_i)=(TS_a(p,q),AS(p,q))$.实体 a 对观点 X 的可信应该是在某个范围之内的,当信任值在范围 $TS\in[\theta,1]$之内的概率超过门限 ϕ 时,即当 $TS_a(p,q)=\int_\theta^1\frac{(m+n+1)}{m!\ n!}x^m(1-x)^n\mathrm{d}x\geqslant\phi$,实体 a 认为观点 X 是可信的.图2是 p 和 q 分别为3和6时候的概率密度函数图.信任值则是由曲线和坐标轴 x 轴以及变量 x 的变化区间所围成的面积.

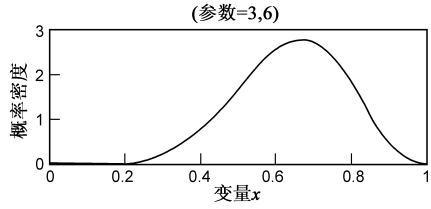


图2 概率密度函数图

在场景 $scene_i$ 中,观点 $X_a(p,q)$的确定值 $AS_a(p,q)$表示为:

$$\begin{cases}AS_a(p,q)=\left(\dfrac{p+q}{Max\_pro(scene_i)}\right)^{\frac{1}{2}}, & p+q\leqslant Max\_pro(scene_i)\\1, & p+q>p_{\max}+q_{\max}\end{cases}$$

确定值的计算公式反映了:

(1)正面和负面的证据数都影响最终的确定值,收集到的证据数越多,那么确定值将越高,反之,确定值越低.

(2)在收集证据的时候,前面收集到的证据对确定值的影响将比后面收集到的证据的影响大,尽量避免由于获得证据过少而使得确定值过小的情况.

(3)当缺乏相关信息的时候,即 $p+q=0$,那么确定值 $AS_a(p,q)=0$.当收集到的证据数超过最大证据数的期望值时,确定值也不会再随之增大,还是为1.

$X_a(scene_i)=(TS_a(p,q),AS_a(p,q))$反映了某个观点由正面和负面证据所产生的信任值和确定值,通过信任值和确定值,用户可以估计事件发生正面和负面频率,为信任判断提供依据.

4.3 推荐度和信任传递

定义1 推荐度:在场景 $scene_i$ 中,如果实体 $a_1,a_2\cdots,a_n$ 对于命题 X 的观点分别为 $X_{a_1}(scene_i)$、$X_{a_2}(scene_i),\cdots,X_{a_n}(scene_i)$,实体 b 对实体 a_i 的观点推荐度用 $REC_b^{a_i}(scene_i)$表示,那么在场景 $scene_i$ 中,实体 b 对于命题 X 的推荐度为

$$REC_b(scene_i)=(TS_b^{REC},AS_b^{REC})=\left(\frac{\sum_{i=1}^n(\eta_1\cdot TS_{a_i}+(1-\eta_1)\cdot TS_b^{a_i})}{n},\frac{\sum_{i=1}^n(\eta_2\cdot AS_{a_i}+(1-\eta_2)\cdot AS_b^{a_i})}{n}\right)$$

其中 η_1 和 η_2 为信任值和确定值的影响因子,$0<\eta_1<1$ 且 $0<\eta_2<1$.

说明 在场景 $scene_i$ 中,实体 a_i 对于命题 X 的观点 $X_{a_i}(scene_i)$可以表示为 $X_{a_i}(TS_{a_i},AS_{a_i})$,对于不同的实体 a_i,实体 b 存在不同的推荐度 $REC_b^{a_i}(TS_b^{a_i},AS_b^{a_i})$,实体 b 将聚合所有可联系的实体的观点,计算出其它实体共同产生的推荐度.首先,任一实体 $a_i(\forall\, i\in n)$对观点的信任程度为 TS_{a_i},当实体 a_i 的消息传送到实体 b 后,实体 b 将会通过实体 a_i 的历史表现对实体 a_i 提供的信任值进行加权聚合,即 $\eta_1\cdot TS_{a_i}+(1-\eta_1)\cdot TS_b^{a_i}$,信任值影响因子决定 TS_{a_i}的影响大小.然后,实体 b 将依次聚合 n 个可联系实体提供的信任值,并对每次所得结果求代数平均值$(\sum_{i=1}^n\eta_1\cdot TS_{a_i}+(1-\eta_1)\cdot TS_b^{a_i})/n$.同理,依次聚合 n 个可联系实体提供的确定值后,最终推荐度确定值为$(\sum_{i=1}^n\eta_2\cdot AS_{a_i}+(1-\eta_2)\cdot AS_b^{a_i})/n$.

其中,在实体 b 的邻居中,并不是所有的实体都可以推荐的,而必须是满足一定要求的实体.具体要求如下所示(推荐者搜索算法):

```
Input:
  int AS_threshold;—成为推荐者的 AS 门限值
  int Max_dis;      —最大距离
  int Num_node;     —总节点数
  int X[Num_node];—Num_node 的观点矩阵
  int ID_local;     —本地节点标识
Output:
  int recommender_ID[];
procedure select_recommender() {
  int NodeID[],dis[];
  int Num_rec = 0;
  for (int j = 0;j < Num_node;j ++ )
    dis[j] = Distance(ID_local,j);
  for (int j = 0;j < Num_node;j ++ ) {
    if (X[j].AS > = AS_threshold &&
      dis[j]! = 0&&dis[j] < Max_dis) {
      NodeID[Num_rec] = j;
      Num_rec ++ ;
    }
  }
  For (int j = 0;j < Num_rec;j ++ )
    recommender_ID[j] = NodeID[j];
  return recommender_ID[];
}
```

定义 2　在场景 $scene_i$ 中,如果实体 b 的所有可联系实体对命题 X 的推荐度为 $REC_b(scene_i) = (TS_b^{rec}, AS_b^{rec})$,而实体 b 通过自身观察对命题 X 的判断为 $OB_b(scene_i) = (TS_b^{ob}, AS_b^{ob})$,那么实体 b 对命题 X 在场景 $scene_i$ 的观点为

$$X_b(scene_i) = (\eta_3 \cdot TS_b^{ob} + (1-\eta_3)TS_b^{rec}, \eta_4 \cdot AS_b^{ob} + (1-\eta_4)AS_b^{rec}) = (TS_b, AS_b)$$

其中 η_3 和 η_4 为信任值和确定值的影响因子,$0 < \eta_3 < 1$ 且 $0 < \eta_4 < 1$.

说明　$X_b(scene_i)$的计算公式与其它实体信任值和确定值的计算公式非常相似,主要区别于 η_3、η_4 和 η_1、η_2 的取值不同.一般情况下,$\eta_3 > \eta_1$,$\eta_4 > \eta_2$.这是因为(TS_b^{ob}, AS_b^{ob})是由实体 b 自身观察到的结果,所以更具有可信性,也就分配了更大的权值.当 $\eta_3 = \eta_1$ 且 $\eta_4 = \eta_2$ 的时候,$REC_b(scene_i) = (TS_b^{REC}, AS_b^{REC})$的求值公式中,如果 i 的取值范围从 $i \in \{i \mid 1,2,\cdots,n \wedge i \neq b\}$ 扩充到 $i \in \{i \mid 1,2,\cdots,n,b\}$,那么最后 $X_b(scene_i) = REC_b(scene_i)$.

5　基于信任度量结果的博弈服务

5.1　应用背景与博弈策略

通过概率密度方法的信任度量,已经可以判断各个实体出现异常行为的几率.但如何制定策略使得各实体能尽可能的执行正常行为呢?博弈论提供了理论依据.为了说明情况,本文将应用背景放在网络的代理服务中,其中代理服务商作为代理服务提供者,而使用代理服务的访问者作为用户,用户可以通过代理提供者访问网页、进行游戏或者下载文件.假定用户是理性的,即用户的行为目的是为了使自身收益最大化.下面首先介绍文中用到的符号所代表的意义:

$AgLos_{+}^{-}$ 表示代理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或者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.

$AgProfit_{+}^{+}$ 表示代理提供者接受用户的不欺骗访问时,代理提供者得到正常的平均收益,如有偿数字资源服务下载.

$AgLos_{-}^{+}$ 表示用户不欺骗访问时,代理提供者拒绝接受而受到的平均损失,如因拒绝正常的用户访问引起的信任损失等.

$UrProfit_{+}^{-}$ 表示用户采取欺骗行为且代理提供者接受访问时,用户得到的超额收益,如过量下载或者以通过代理服务器发起网络攻击等.

$UrProfit_{+}^{+}$ 表示用户不欺骗且代理提供者接受访问时,用户获得的平均收益,如正常访问网络资源或者与进行通信等.

$UrCost$ 为用户采取欺骗行为所需要的成本.如购买软件、学习欺骗的方法和技巧所需要的时间和精力等.

$UrRisk$ 表示用户采取欺骗行为所可能受到的惩罚,如停止对用户的代理服务或法律起诉等.

如果选择的可信路径 TP(Trust Path)长度为 k,其中路径上各实体用 $v_1, v_2, \cdots, v_k$ 表示,信任等级为 $X_{v_1}(scene_i), X_{v_2}(scene_i), \cdots, X_{v_k}(scene_i)$.进行服务博弈分析的时候,可以将可信路径看做一条信任等级为 $X_{TP}(scene_i)$的通路,其中 $X_{TP}(scene_i) = (TS_{TP}, AS_{TP})$,$TS_{TP} = \prod_{m=v_1}^{v_k} TS_m$ 且 $AS_{TP} = \prod_{m=v_1}^{v_k} AS_m$.那么代理提供者和用户的支付矩阵分别为

$$\boldsymbol{Array}_{Ag} = \begin{bmatrix} -AgLos_{+}^{-} \cdot \gamma_1^{TS_{TP}} & AgProfit_{+}^{+} \cdot \gamma_2^{TS_{TP}} \\ 0 & -AgLos_{-}^{+} \cdot \gamma_3^{TS_{TP}} \end{bmatrix} \quad (9)$$

$$\boldsymbol{Array}_{Ur} = \begin{bmatrix} UrProfit & -UrCost \cdot \gamma_6^{TS_{TP}} \\ UrProfit_{+}^{+} \cdot \gamma_5^{TS_{TP}} & 0 \end{bmatrix} \quad (10)$$

其中:$UrProfit = UrProfit_{+}^{-} \cdot \gamma_4^{TS_{TP}} + UrProfit_{+}^{+} \cdot \gamma_5^{TS_{TP}} - UrCost \cdot \gamma_6^{TS_{TP}} - UrRisk \cdot \gamma_7^{TS_{TP}}$,

$\gamma_n \in [1, +\infty)$且 $n = 1,2,\cdots,7$,γ_n 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.

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[13],但我们可以求出混合策略的纳什均衡.假定代理提供者以 P_{ac}的概率选择提供服务,以 $1-P_{ac}$的概率选择拒绝服务,即代理提供者的混合策略为 $Str_{Ag}=(P_{ac},1-P_{ac})$.由于用户通过可信路径的后 $X_{TP}(scene_i)=(TS_{TP},AS_{TP})$,那么用户以 $P_{error}=1-TS_{TP}\times AS_{TP}$的几率进行欺骗,所以用户的混合策略为 $Str_{Ur}=(P_{error},1-P_{error})$,那么用户的预期支付函数为

$$\begin{aligned}&PAY_E(Str_{Ag},Str_{Ur})\\&=Str_{Ur}\cdot\boldsymbol{Array}_{Ur}\cdot\boldsymbol{Str}_{Ag}^{\mathrm{T}}\\&=(P_{error},1-P_{error})\\&\quad\cdot\begin{bmatrix}UrProfit & -UrCost\cdot\gamma_6^{TS_{TP}}\\ UrProfit_{+}^{+}\cdot\gamma_5^{TS_{TP}} & 0\end{bmatrix}\cdot\begin{bmatrix}P_{ac}\\1-P_{ac}\end{bmatrix}\\&=P_{error}\cdot P_{ac}\cdot(UrProfit_{+}^{-}\cdot\gamma_4^{TS_{TP}}-UrRisk\cdot\gamma_7^{TS_{TP}})\\&\quad+P_{ac}\cdot UrProfit_{+}^{+}\cdot\gamma_5^{TS_{TP}}-P_{error}\cdot UrCost\cdot\gamma_6^{TS_{TP}}\end{aligned}$$

对上式中 P_{error}求偏导,可以得到代理提供者最优化的一阶条件:

$$\begin{aligned}&\frac{\partial PAY_E(Str_{Ag},Str_{Ur})}{\partial AS_{TP}}\\&=P_{ac}\cdot(UrProfit_{+}^{-}\cdot\gamma_4^{TS_{TP}}-UrRisk\cdot\gamma_7^{TS_{TP}})-UrCost\cdot\gamma_6^{TS_{TP}}\\&=0\end{aligned}\tag{11}$$

则

$$P_{ac}=UrCost\cdot\gamma_6^{TS_{TP}}/(UrProfit_{+}^{-}\cdot\gamma_4^{TS_{TP}}-UrRisk\cdot\gamma_7^{TS_{TP}})$$

观察分析结果可以看出,代理提供者接受概率仅仅和用户的收益与支付有关.用户共有四项收益与支付途径,其中用户欺骗相关的 3 项决定了接受概率.所以,代理提供者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,从而提高自己的接受概率.

混合纳什均衡策略给用户一个不确定的博弈结果,非法用户往往得不到支付矩阵和决策概率,无法判断代理提供者会如何处理其提出的请求.当然,这些用户可以通过监听和入侵合法用户等手段,获取代理提供者的支付矩阵和决策概率,但代理提供者如何决策并不能确定.在博弈过程中,代理提供者以 P_{ac}的概率接受访问,而以 $1-P_{ac}$拒绝访问,此访问控制策略具有随机性,用户的请求可能以一定的概率给以拒绝,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.由于式(13)是对式(12) 的一阶求导,所以概率 P_{ac}是临界点,只有代理提供者以混合纳什均衡策略 P_{ac}概率接受访问,以 $1-P_{ac}$概率拒绝访问,用户对欺骗和不欺骗两种选择是无差异的(即有相同的收益),用户不存在投机机会,此时用户往往更倾向于诚实.下面给出一个信任等级与双方支付关系的一个性质.

定理 2 代理提供者和用户的收益和支付与用户的信任等级成正比.

证明 由支付距阵可知代理提供者和用户的正常收益、额外收益分别为 $AgLos_{+}^{-}\cdot\gamma_1^{TS_{TP}}$、$AgProfit_{+}^{+}\cdot\gamma_2^{TS_{TP}}$、$AgLos_{-}^{+}\cdot\gamma_3^{TS_{TP}}$、$UrProfit_{+}^{-}\cdot\gamma_4^{TS_{TP}}$、$UrProfit_{+}^{+}\cdot\gamma_5^{TS_{TP}}$、$UrCost\cdot\gamma_6^{TS_{TP}}$ 和 $UrRisk\cdot\gamma_7^{TS_{TP}}$,在网络信任模型分析中,代理提供者和用户具有相同地位,所以设两个实体 a_i 和 a_j 的行为信任等级分别为 TS_{a_i}和 TS_{a_j},则两实体的同一支付值的比为 $\gamma_x^{TS_{a_i}}/\gamma_x^{TS_{a_j}}=\gamma_x^{TS_{a_i}-TS_{a_j}}$,其中 $\gamma_x\in\{\gamma_1,\gamma_2,\gamma_3,\gamma_4,\gamma_5,\gamma_6,\gamma_7\}$.假设实体 a_i 的信任等级高于a_j,那么 $TS_{a_i}>TS_{a_j}$,同时 $TS\in[0,1]$,则 $1>C=TS_{a_i}-TS_{a_j}>0$,由于 $\gamma_x\in[1,+\infty)$且 $1>C>0$,所以 $\gamma_x^C\in(1,\gamma_x)$,即实体 a_i 和 a_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,实体信任等级越高,代理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.

5.2 数据分析

为了简化例子并与实际应用相符合,数据分析的时候采用标签集合来反映信任等级,如 3.2 节所述,该集合将信任分为 Very Untrusted(VU),Untrusted(U),Un-Decided(UD),Trusted(T),Very Trusted(VT)五个等级,分别为非常不信任、不信任、怀疑、信任、非常信任,分别对应数字 1 – 5.博弈分析的参数因子 γ_x 分别为 1.20、1.10、1.23、1.30、1.25、1.20 和 1.10,其它参数如表 2 所示,这里列出的主要是式(14)中计算所需的参数值.

表 2 博弈参数与结论表

信任等级	$UrProfit_{+}^{-}$	$UrCost$	$UrRisk$	P_{ac}
VU	67.0	50.0	74.56	13.2
U	76.5	50.0	105.24	37.7
UD	84.6	50.0	138.92	64.1
T	91.4	50.0	146.00	81.3
VT	100.0	50.0	229.62	95.7

上例数据结果的统计如图 3.从这个例子中可以看到用户因欺骗所获得的收益 $UrProfit_{+}^{-}$和用户所受到的惩罚 $UrRisk$ 随着信任等级的升高而增大.当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提升,代理提供者的接受概率也相应增加,这与本文得出的结论是一致的.表 2 和图 3 中的各参数都是 100 倍放大所得,如 $P_{ac}=0.957$ 则记为 95.7.

代理提供者根据混合博弈均衡策略概率进行,在

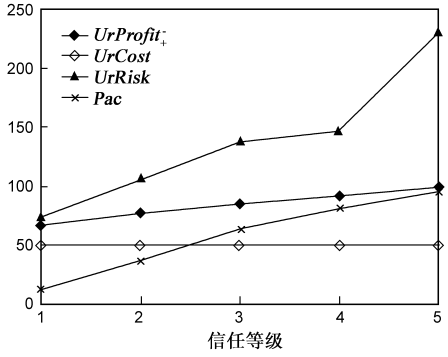


图3　博弈参数变化图

用户信任等级、$UrProfit_{+}^{-}$、*UrCost* 和 *UrRisk* 确定的情况下,以 P_{ac}的概率接受服务,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,代理提供者没有给用户提供任何的投机机会,也就是说用户知道代理提供者会因为他们"滥用"代理而暂停他们使用代理的权限,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.

6　小结

本文提出了网络环境下一种基于概率密度的信任博弈模型,从信任证据收集、信任度量和服务博弈三个方面进行阐述.综合运用了数据挖掘、概率密度函数分析和博弈论等技术手段与理论进行分析和建模,并且避免了单一的信任度量接口和单纯的信任度量决策手段.通过与网络环境的结合,使得研究的成果更具有实际意义.

参考文献:

[1] Chang E, Thomson P, Dillon T et al. The fuzzy and dynamic nature of trust[A]. LNCS 3592[C]. Berlin: Springer-Verlag, 2005.161 – 174.

[2] Marsh S. Formalizing Trust as a Computational Concept[D]. University of Stirling, 1994.

[3] Golbeck J. Computing and Applying Trust in Web-Based Social Networks[D]. University of Maryland, College Park, 2005.

[4] Koutrouli E, Tsalgatidou A. Reputation-based trust systems for P2P applications: design issues and comparison framework[A]. LNCS4083[C]. Berlin: Springer-Verlag, 2006.152 – 161.

[5] Almenarez F, Marin A, Campo C. TrustAC: Trust-Based access control for pervasive devices[A]. LNCS 450[C]. Berlin: Springer-Verlag. 2005.225 – 238.

[6] Jameel H, Hung L X, Kalim U. A trust model for ubiquitous systems based on vectors of trust values[A]. In Proceedings of the 7th IEEE Int'l Sympon Multimedia[C]. Washington: IEEE Computer Society Press. 2005.674 – 679.

[7] Papapanagiotou K, Marias G F, Georgiadis P. Performance evaluation of a distributed OCSP protocol over MANETs[A]. In Proceedings of 3rd IEEE Consumer Communications and Networking Conference (CCNC '06)[C]. Las Vegas, USA: IEEE Press. 2006.1 – 5.

[8] Hu Y C, Perrig A, Johnson D B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks[A]. In Proceedings of the 8th International Conference Mobile Computing and Networking[C]. ACM Press. 2002.12 – 23.

[9] Yi S, Naldurg P, Kravets R. A security-aware routing protocol for wireless ad hoc networks[A]. In Proceeding of the 6th World Multi-conference on Systemics, Cybernetics and Informatics[C]. USA: IEEE Press. 2002.226 – 236.

[10] Chun H Y, David J, Adrian P. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks[J]. Ad Hoc Networks, 2003, 1(1): 175 – 192.

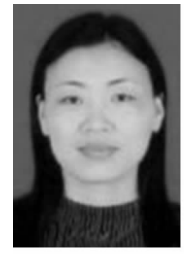
[11] 易平,蒋嶷川,等.移动 ad hoc 网络安全综述[J].电子学报,2005,33(5):893 – 894.
Yi P, Jiang Y C, et al. A Survey of Security for Mobile Ad Hoc Networks[J]. Acta Electronica Sinica, 2005, 33(5): 893 – 894. (in Chinese)

[12] Agrawal R. Mining association rules between sets of items in large databases[A]. In Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data[C]. Washington, DC, USA: ACM Press. 1993.207 – 216.

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

作者简介:

陈　晶　男,1981 年生于湖北武汉.武汉大学计算机学院讲师、博士.研究方向为无线网络、网络安全.　E-mail: ever_cs@163.com



杜瑞颖　女,1964 年生于河南新乡.武汉大学计算机学院教授、博士.研究方向为无线网络及安全.

王丽娜　女,1964 年生于辽宁营口.武汉大学计算机学院教授、博士.主要研究领域为信息安全,可信计算.

田在荣　男,1980 年生于湖北仙桃,武汉大学电子信息学院博士研究生.主要研究方向为无线网络.