云计算环境下基于动态博弈论的用户行为模型与分析

陈亚睿[1],田立勤[2,3],杨 扬[1]
(1.北京科技大学计算机与通信工程学院,北京 100083; 2.华北科技学院计算机系,北京 101601;
3.青海师范大学计算机学院,青海西宁 810008)

摘 要: 云计算环境下,开放的运行环境使其面临重大的安全挑战,有效地确定不可信云终端用户并正确分析云用户的异常行为是在复杂动态环境下保证云安全的基础.提出了一种基于动态博弈的用户行为模型,通过不完全信息多阶段博弈来分析终端用户的类型,博弈时将用户的当前行动和历史行动相结合,并考虑了网络中存在的误报和漏报的情况,以加强对云终端用户类型推断的准确性和全面性.理论证明和实验验证表明该机制能快速甄别系统中潜在的不可信云终端用户,有效遏制不可信云终端用户的侵入行为,为主动安全机制的实现奠定基础.

关键词: 云计算; 用户行为分析; 动态博弈; 信念修正
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2011) 08-1818-06

Model and Analysis of User Behavior Based on Dynamic Game Theory in Cloud Computing

CHEN Ya-rui[1], TIAN Li-qin[2,3], YANG Yang[1]
(1. *School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing* 100083, *China*;
2. *Department of Computer Science and Technology, North China Institute of Science and Technology, Beijing* 101601, *China*;
3. *School of Computer Science and Technology, Qinghai Normal University, Xining, Qinghai* 810008, *China*)

Abstract: The open environment in cloud computing is much more complex and unpredictable, so how to identify untrustworthy cloud end-user by analyzing abnormal user behaviors is an important topic in cloud security. This paper proposes a model for behavior analysis based on incomplete information multi-stage dynamic games, in which current action and historical action, false negative and false positive in network detection methods are considered to improve the accuracy and comprehensiveness of the dynamic judgment of end-use trustworthiness. The experimental results show that it can discriminate potential untrustworthy cloud end-user, and decrease intrusion effectively while perfect Bayesian equilibrium is reached, laying the foundation for active safety mechanism.

Key words: cloud computing; user behavior analysis; dynamic game theory; belief updating

1 引言

随着云计算的飞速发展,人们在享受它带来的降低运营成本,改善运营效率等种种便利的同时,也面临着更为严峻的信息安全挑战.云系统中的海量重要用户数据,对攻击者具有更大的诱惑力,同时云系统为用户提供的开放访问接口,使云终端用户可以直接使用和操作云服务提供商的软件、操作系统、甚至是编程环境和网络基础设施,由此对云资源的影响和破坏远比目前利用因特网进行资源共享要严重的多.因此访问云资源的云终端用户身份是否真实,行为是否可信是保证云计算安全的重要内容.目前身份认证技术比较成熟,但身份认证并不能阻止身份认证失败或合法身份的恶意端用户对系统的破坏,因此对云终端用户行为进行有效分析控制是当前云计算应用中一个研究重点.

文献[1]提出了用户行为信任的评估、预测与控制架构.文献[2]建立可量化的信任证据与信任等级之间的对应关系.文献[3]论述了使用贝叶斯网络对用户行为信任进行预测.文献[4]在文献[3]基础上,将行为信任预测结果和博弈分析相结合.用博弈的方法对信息安

收稿日期:2011-02-16;修回日期:2011-04-18
基金项目:国家 973 重点基础研究发展规划(No.2010CB328105,No.2011CB311809);国家自然科学基金(No.60873192,No.61070182,No.60932003);河北省自然科学基金(No.F2010001745);新世纪优秀人才支持计划(No.NCET-10-0101)

全进行分析评价,已经引起安全领域的重视.文献[5]提出服务提供者识别入侵者的博弈模型.文献[6]研究了无线网络中,用不完全信息贝叶斯博弈解决恶意节点和普通节点的鉴别、共存问题.文献[7]将博弈论和随机 Petri 网相结合,提出了随机博弈网,并描述了网络安全中的攻防关系.

以上这些方法均存在一定局限性和缺陷,文献[1]从宏观的角度对用户行为可信的整体架构、管理机制等方面进行了研究,有关云瘦客户的特点没有考虑.文献[2,3]使用了贝叶斯网络对用户行为信任进行预测和控制,但没有考虑不可信用户为了提高可信度进行的伪装欺骗.文献[4]中的博弈虽然考虑了用户的欺骗行为,但该文使用的是静态博弈,忽略了系统的动态性.文献[5~7]中的博弈分析方法都不适合云终端用户行为动态变化的特点.

本文借鉴上述相关研究成果,将博弈论运用到云终端用户动态行为的研究中,根据用户历史和当前行为,用不完全信息动态博弈对云终端用户的类型、可信等级判断及修正展开分析讨论.本文的贡献在于将云终端用户和云服务提供商之间的攻防抽象为不完全信息动态博弈,根据博弈结果,动态调整用户信任等级,并据此采取相应的访问控制措施.实验证明系统达到博弈均衡时,该方法具有自约束力,可以使不可信云终端用户发送恶意请求的概率稳定在较低的水平,博弈结果为云服务提供商采取准确的应对措施提供有力的依据.

2　基于动态博弈论的博弈模型

我们用不完全信息多阶段动态博弈来描述云服务提供商和云终端用户之间的博弈过程,其每个阶段博弈重复进行信号博弈.假设云终端用户通过身份认证,将用户分为两个类型:可信云终端用户和不可信云终端用户.前者总是正常使用云服务提供商提供的服务,后者可能对系统发动攻击,也可能通过正常使用服务来伪装成可信用户,潜伏在系统中,等到一定时机对系统发动攻击.由于云服务提供商对用户何时终止发送请求并不知晓,因此假设博弈重复 k 次,$k=0,1,\cdots$.为了分析方便,假定重复博弈不考虑贴现,即每个阶段博弈,参与者的效用保持不变.

在博弈模型中,我们进行如下定义.

(1)参与者:包括云终端用户 i 和云服务提供商 j.其中 i 是信号发送者,有两个类型,$\theta_i=0$:可信云终端用户;$\theta_i=1$:不可信云终端用户.j 是信号接收者,θ_j 仅有一个类型:云服务提供商.

(2)行动集:参与者的行动集依赖于他的类型.不可信云终端用户的行动集 $M_i=\{m_1,m_2\}=\{$正常请求,异常请求$\}$,可信云终端用户的行动集 $M_i=\{m_1\}=\{$正常请求$\}$.云服务提供商的行动集 $A_j=\{a_1,a_2\}=\{$提供服务,拒绝服务$\}$.

(3)支付:

U_n:用户发出正常请求被允许访问时获得的收益.

C_n:用户发请求的开销等.

C_a:不可信用户发送异常请求的成本.

U_a:不可信用户发出异常请求未被阻止时获得的效用,也是云服务提供商损失的收益.

P_a:不可信用户发送异常请求被检测出来受到的惩罚.

S_n:云服务提供商允许正常请求时的收益,拒绝正常请求会损失 S_n 的收益.

假设系统的误报率为 α,漏报率为 β.根据云终端用户 i 和云服务提供商 j 的类型,博弈双方的支付矩阵如表 1 所示.

表 1　博弈双方的支付矩阵

		云服务提供商	
		提供服务	拒绝服务
不可信用户	异常请求	$\beta U_a-C_a,-\beta U_a$	$-(1-\beta)P_a-C_a,(1-\beta)U_a$
可信用户	正常请求	$(1-\alpha)U_n-C_n,(1-\alpha)S_n$	$-\alpha P_a-C_n,-\alpha S_n$
		云服务提供商	
		提供服务	拒绝服务
可信用户	正常请求	$(1-\alpha)U_n-C_n,(1-\alpha)S_n$	$-\alpha P_a-C_n,-\alpha S_n$

(4)策略:信号博弈根据发送者的类型与发送信号间的关系,分为混同策略、分离策略和准分离策略[8].本文讨论的是准分离策略下的博弈:不可信云终端用户以概率 p 发送异常请求,以概率 $1-p$ 发送正常请求,可信云终端用户以概率 1 发送正常请求.

图 1 给出了博弈的扩展式描述.自然赋予端用户类型为不可信云终端用户的先验概率是 ϕ,为可信云终端用户的先验概率是 $1-\phi$.叶子结点是博弈双方采取相应策略时的效用.

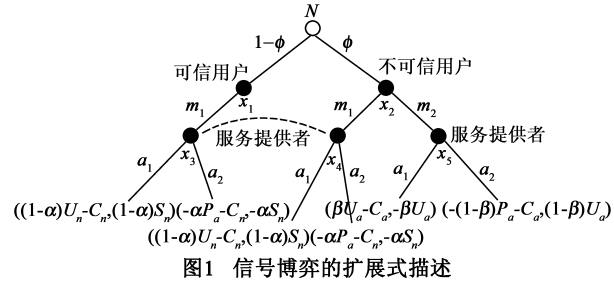

图1　信号博弈的扩展式描述

3　信念及信念修正

3.1　信念

定义 1　信念:在一个博弈周期,云服务提供商根据云终端用户的行动对其类型的推断.具体来说,就是

云服务提供商对收到的用户请求是来自可信用户还是不可信用户无法准确分辨,只能通过其发送的信号对用户类型进行推断,这种推断即为信念.在图 1 所示的博弈中,云服务提供商根据接收到的信号对云终端用户类型有下面 4 种信念,$\mu(\theta_i=0\mid m_1)$,$\mu(\theta_i=1\mid m_1)$,$\mu(\theta_i=0\mid m_2)$,$\mu(\theta_i=1\mid m_2)$.$\mu(\theta_i=1\mid m_1)$表示云服务提供商根据本次博弈收到的信号是正常请求,推断用户为不可信云终端用户的信念,其余表达含义类似.因为只有两类用户,所以

$$\mu(\theta_i=0\mid m_1)=1-\mu(\theta_i=1\mid m_1),$$
$$\mu(\theta_i=0\mid m_2)=1-\mu(\theta_i=1\mid m_2).$$

3.2 信念的计算

根据贝叶斯法则,收到正常请求后云服务提供商推断发送者为不可信云终端用户的信念计算公式为:

$$\mu(\theta_i=1\mid m_1)=\frac{p(m_1\mid\theta_i=1)\mu(\theta_i=1)}{p(m_1)}=\frac{p(m_1\mid\theta_i=1)\mu(\theta_i=1)}{\sum_{\theta_i=0,1}p(m_1\mid\theta_i)\mu(\theta_i)}\tag{1}$$

其中 $\mu(\theta_i=1)$是用户类型为不可信云终端用户的先验概率,$p(m_1\mid\theta_i=1)$是不可信用户发送正常请求的概率,$p(m_1)$表示用户发送正常请求的全概率,因为可信用户和不可信用户都可能发送正常请求,由全概率公式 $p(m_1)=\sum_{\theta_i=0,1}p(m_1\mid\theta_i)\mu(\theta_i)$.用公式(1)的方法可以计算其余信念,这里不再详述.

3.3 信念修正

我们在公式(1)中加入重复博弈的因素,构造第 k 个阶段博弈,云服务提供商的信念修正公式,如下

$$\mu_j^{k+1}(\theta_i\mid m_i^k,h_i^k)=\frac{\mu_j^k(\theta_i\mid h_i^k)P(m_i^k\mid\theta_i,h_i^k)}{\sum_{\tilde{\theta}_i}\mu_j^k(\tilde{\theta}_i\mid h_i^k)P(m_i^k\mid\tilde{\theta}_i,h_i^k)}\tag{2}$$

其中 $\tilde{\theta}_i\in\{0,1\}$,$m_i^k$ 是用户 i 在第 k 个阶段博弈的行动,h_i^k 是用户 i 在第 k 个阶段博弈前的历史行动,$h_i^k=(m_i^1,m_i^2,\cdots,m_i^{k-1})$.$\mu_j^k(\theta_i\mid h_i^k)$是第 k-1 个阶段博弈结束时云服务提供商 j 修正后的信念,它也是第 k 个阶段博弈开始时的初始信念,第 1 次博弈云服务提供商的初始信念依赖于先验概率 ϕ.$P(m_i^k\mid\theta_i,h_i^k)$第 k 个阶段博弈类型为 θ_i 的用户发送行动 m_i^k 的概率.但在实际的系统中,因检测技术缺陷和网络不稳定等客观原因,总不可避免的存在误报和漏报的情况,这些都会使用户行为信号的传递出现偏差.延续第 2 小节的假设,系统存在误报率 α 和漏报率 β,因此对公式(2)中 $P(m_i^k\mid\theta_i,h_i^k)$进行如下修正:

不可信用户发送正常请求的概率

$$P(m_i^k=m_1\mid\theta_i=1,h_i^k)=(1-\alpha)(1-p)+\beta p\tag{3}$$

不可信用户发送异常请求的概率

$$P(m_i^k=m_2\mid\theta_i=1,h_i^k)=\alpha(1-p)+(1-\beta)p\tag{4}$$

可信用户发送正常请求的概率

$$P(m_i^k=m_1\mid\theta_i=0,h_i^k)=1-\alpha\tag{5}$$

可信用户发送异常请求的概率

$$P(m_i^k=m_2\mid\theta_i=0,h_i^k)=\alpha\tag{6}$$

把公式(3)~(6)带入公式(2),第 k 个博弈阶段,如果云服务提供商收到的信号是正常请求 m_1,用公式(7)对用户为不可信用户的信念 $\mu_j^{k+1}(\theta_i=1\mid m_i^k=m_1,h_i^k)$进行修正.为了描述方便,将 $\mu_j^{k+1}(\theta_i=1\mid m_i^k=m_1,h_i^k)$简写成 μ_j^{k+1},后面的分析也沿用这个简写.

$$\mu_j^{k+1}=\frac{\mu_j^k((1-\alpha)(1-p)+\beta p)}{\mu_j^k((1-\alpha)(1-p)+\beta p)+(1-\mu_j^k)(1-\alpha)}\tag{7}$$

如果收到的信号是异常请求 m_2,用公式(8)对用户为不可信用户的信念 μ_j^{k+1} 进行修正.

$$\mu_j^{k+1}=\frac{\mu_j^k(\alpha(1-p)+(1-\beta)p)}{\mu_j^k(\alpha(1-p)+(1-\beta)p)+(1-\mu_j^k)\alpha}\tag{8}$$

4 博弈的精炼贝叶斯纳什均衡

不完全信息动态博弈的均衡是精炼贝叶斯纳什均衡(Perfect Bayesian Equilibrium,PBE),它既包含策略,又包含信念,是所有参与人策略组合和信念的一种结合[9].根据文献[9]给出的 5 个 PBE 条件,我们有如下定义.

定义 2 具有可观察行动不完全信息多阶段博弈的均衡由策略组合 σ 和信念 μ 组成,当(σ,μ)满足条件 $B(1)$-$B(4)$和 P 时,(σ,μ)称为精炼贝叶斯纳什均衡(PBE).

$B(1)$:信念是独立的.

$B(2)$:如果 $\mu_j^k(\theta_i\mid h_i^k)$表示已知历史行动 h_i^k 时参与人 j 的信念,那么在可能的情况下,参与人 j 应当使用贝叶斯法则来修正在第 $k+1$ 个博弈阶段的信念为 $\mu_j^{k+1}(\theta_i\mid h_i^{k+1})$.

$B(3)$:发送者不会发送自己未知的信号.

$B(4)$:当类型相互独立时,参与人 i 和参与人 j 对第三个参与人 k 的类型持有相同的信念.

P:对每个类型为 θ_i,历史行动为 h^t 的参与者 i,参与者 i 有别于 σ_i 的策略 σ'_i 满足:$u_i(\sigma\mid h^t,\theta_i,\mu(\cdot\mid h^t))\geqslant u_i((\sigma'_i,\sigma_{-i})\mid h^t,\theta_i,\mu(\cdot\mid h^t))$,其中 $u_i(\sigma\mid\cdot)$是参与者 i 在策略 σ 下的期望收益.

接下来我们首先论证云终端用户和云服务提供商之间的动态博弈存在混合策略 PBE,然后再进一步证明纯策略 PBE 不存在.

定理 1 云终端用户和云服务提供商之间的不完全信息多阶段博弈中存在混合策略 PBE,$PBE=((p_k^*,q_k^*),\mu_j^{k+1}(\theta_i=1\mid m_i^k,h_i^k))$.

证明　因为云服务提供商只有一个类型,故 $B(1)$ 满足.信念修正公式(2)是用贝叶斯法则推导出来的,因而 $B(2)$也满足.云终端用户的信号集和行动集一致,因而不会发出自己未知的信号,故 $B(3)$满足.因为我们讨论的博弈模型只有云终端用户和云服务提供商两个参与人,信念的修正不受其它参与人的影响,因而 $B(4)$ 也满足.下面只需证明策论组合满足条件 P,则定理 1 即可证明.

第 k 个博弈阶段,终端用户先行动,以概率 p 发送异常请求,概率 1-p 发送正常请求.当检测系统检测到异常请求信号 m_2 时,云服务提供商可能以概率 q 拒绝服务,或以概率 1-q 提供服务.

云服务提供商采取拒绝服务策略时的期望收益为 $u_j^k(a_j^k = a_2 \mid m_i^k = m_2, h_i^k)$,简写成 $u_j^k(a_2 \mid m_2)$,于是

$$u_j^k(a_2 \mid m_2) = \mu_j^k p(1-\beta)U_a + \mu_j^k(1-p)(-\alpha S_n) + (1-\mu_j^k)(-\alpha S_n) \tag{9}$$

公式(9)中,异常请求可能来自三部分:被检测出来的不可信用户发送的异常请求、被误报的不可信用户的正常请求、被误报的可信用户的正常请求.三种情况的收益之和为云服务提供商对异常请求采取拒绝服务策略的期望收益.

与公式(9)类似,云服务提供商采取允许服务策略的期望收益为 $u_j^k(a_1 \mid m_2)$,

$$u_j^k(a_1 \mid m_2) = \mu_j^k p(-\beta U_a) + \mu_j^k(1-p)\alpha S_n + (1-\mu_j^k) \tag{10}$$

因此云服务提供商的期望收益为 E_j^k,

$$E_j^k = q u_j^k(a_2 \mid m_2) + (1-q)u_j^k(a_1 \mid m_2) \tag{11}$$

对公式(11)关于 q 求偏导,可得最优化的一阶条件

$$\frac{\partial E_j^k}{\partial q} = u_j^k(a_2 \mid m_2) - u_j^k(a_1 \mid m_2) = 0 \tag{12}$$

把公式(9)和公式(10)带入公式(12),解得

$$p_k^* = \frac{2\alpha S_n}{(U_a + 2\alpha S_n)\mu_j^k(\theta_i = 1 \mid m_2)} \tag{13}$$

也就是说,当不可信云终端用户以概率 p_k^* 发送异常请求,云服务提供商提供服务和拒绝服务的收益没有差异.

同样不可信用户可能选择发送正常请求或发送异常请求.同理可得,云服务提供商以概率 $q_k^* = \dfrac{\beta U_a + \alpha U_n + C_n - C_a - U_n}{(1-\alpha)(P_a - U_n) - \beta(P_a - U_a)}$拒绝服务时,不可信云终端用户发送正常请求和异常请求的收益没有差异.

因此,策略组合 $\sigma = (p_k^*, q_k^*)$是阶段博弈达到均衡时,参与人的纳什均衡解.博弈达到均衡状态时,任一参与者改变策略将使他的效用降低,每个参与人的策略在阶段博弈中是最优的,条件 P 满足.定理 1 得证.

定理 2　云终端用户和云服务提供商之间的博弈不存在纯策略 PBE.

证明　假设存在纯策略 PBE,则在第 k 个阶段博弈,对用户发送的异常请求云服务提供商的最优策略是拒绝访问此时理性的用户为了使自己效用最大,将发送正常请求.对用户的正常请求,云服务提供商的最优策略是提供服务,此时 $q_k = 0$.假设博弈存在均衡,则用户发送正常请求的收益应大于发送异常请求的收益,可得 $q_k > \dfrac{\beta U_a + \alpha U_n + C_n - C_a - U_n}{(1-\alpha)(P_a - U_n) - \beta(P_a - U_a)}$,这与$q_k = 0$ 矛盾.因此不存在纯策略 PBE,得证.

5　应用实例与实验效果分析

5.1　应用实例背景

云计算这种模式非常适合高校图书馆数字资源的建设,数字图书馆云战略已被纳入中国高等教育文献保障系统三期建设项目.在这种服务模式中,云服务提供商是数据库商,云终端用户是租用数字资源的高校,数据库商通过云服务向高校提供数字资源,高校用户通过付费来使用数据库.用户身份信任的依据是用户的 IP 地址,只要 IP 地址在合法的范围内就可以访问数据库.但只有身份信任是不够的,因为一些学生在校内使用网络工具大批量下载电子资源或私设代理服务器牟取非法所得,此时用户的身份是可信的,但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,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、暂停访问等.如果惩罚过大,则直接影响数据库商和学校之间的合作,如果惩罚过小,达不到制止滥用数据库的目的.如果数据库商根据本文得到的 PBE 对用户动态划分行为信任等级并制定相应惩罚措施,那么云终端用户很清楚不可信行为会导致自己信任等级下降,且这一影响短期内不易消除,因而不敢随意进行不可信操作.

5.2　数据假定与博弈计算

为了简化例子并与实际应用相符合,假设数据库商将高校用户的行为信任等级划分为四级:可信、比较可信、可疑和不可信,信任度依次下降,划分阈值分别为 0.5,0.85,0.95.信念小于 0.5,认为用户可信,允许访问数据库资源;信念在 0.5 到 0.85 之间,认为用户比较可信,也允许访问数据库;信念在 0.85 到 0.95 之间,认为用户可疑,提出警告;当信念上升到 0.95 以上,认为用户不可信,停止其对电子资源的访问.

实验中以 0 表示云终端用户的正常请求,以 1 表示异常请求.异常请求判定标准由数据商规定,如单位时间下载量、访问频率等.假设可信用户发送的请求序列

为[0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],不可信用户发送的请求序列为[0,0,0,0,0,1,1,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0].博弈开始时设不可信云终端用户的先验概率 $\phi=0.5$,即认为用户初始状态可信.令 $\alpha=0.01$,$\beta=0.001$,$S_n=500$,$U_a=2000$,假设博弈进行 30 次.图 2 描述了数据库商信念修正结果变化的过程,图 3 描述了对应的云终端用户发送异常请求的概率趋势.

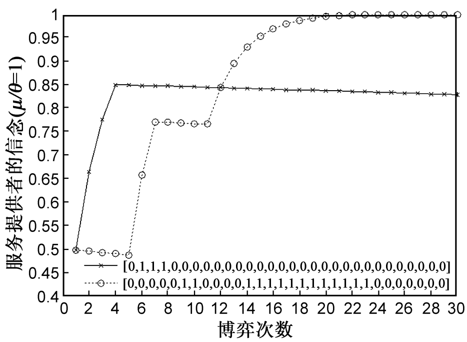

图2　信念的修正过程

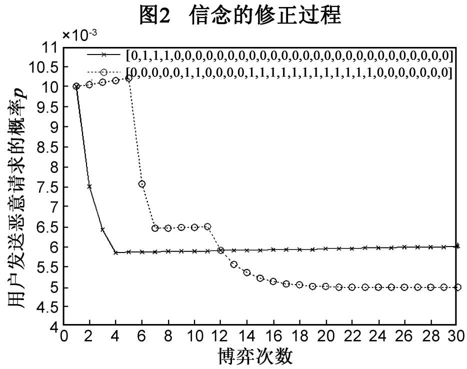

图3　用户发送异常请求的概率趋势

5.3　决策与实验效果分析

图 2 描述了信念的修正过程,当数据库商收到异常请求时,认为云终端用户不可信的信念上升,连续的异常请求导致用户不可信的信念快速向 1 收敛,用户的信任度快速下降.可信用户请求序列在第 2、3、4 个博弈周期存在误报的情况,虽然数据库商认为用户不可信的信念上升,但没有立刻中止服务,这样减小了可信用户的正常请求因误报被拒绝.不可信用户的连续异常请求,使数据库商认为用户不可信的信念上升并逐渐认定用户不可信,当信念大于阈值时,停止服务.当停止发送异常请求后,数据库商认为用户不可信的信念有所下降,但是下降速度缓慢,用户信任度值缓慢上升.由此可见,本文提出的方法具有信任度"慢升快降"的特性,能防止低信任的不可信云终端用户经过几次欺骗性的"正常请求"后信任值很快上升的欺诈行为,是提前的欺骗预防评估策略.

数据库商这种信念的修正,也遏制了云终端用户发送异常请求的概率.从图 3 可以看出,用户发送异常请求的概率 p 随着博弈的进行,逐渐下降并趋稳定.对比图 2 和图 3,可以发现,云服务提供商认为用户不可信的信念快速增加时,用户发送异常请求的概率相应快速下降.这是因为进行不完全信息多阶段博弈时,用户知道云服务提供商将根据他请求信号动态修正信念,因此为了避免过早被判定为不可信用户,理性的云终端用户降低了发送异常请求的概率.

6　总结

本文建立了云服务提供商和云终端用户之间的重复博弈模型,这种不完全信息动态博弈更符合现实中的攻防情况.通过多次观察子博弈中云终端用户的行动,并结合其历史行动,对用户的信任等级动态更新,并采取相应访问控制措施,同时本文提出的机制重点考虑了检测系统和网络的不确定性因素给博弈分析带来的影响.理论证明了精炼贝叶斯均衡的存在,在达到均衡状态时,理性的云服务提供商和云终端用户都不会单独改变策略,从而抑制了不可信云终端用户发送异常请求的概率.实验表明,这种机制能对访问过程中的异常行为进行实时监控与防范,且能防止通过信任欺骗来获取高信任值.

参考文献

[1] 林闯,田立勤,王元卓.可信网络中用户行为可信的研究[J].计算机研究与发展,2008,45(12):2033-2043.
Lin Chuang,Tian Liqin,Wang Yuanzhuo.Research on user behavior trust in trustworthy network[J].Journal of Computer Research and Development,2008,45(12):2033-2043.(in Chinese)

[2] 赵洁,肖南峰,钟军锐.基于贝叶斯网络和行为日志挖掘的行为信任控制[J].华南理工大学学报,2009,37(5):94-100.
Zhao Jie,Xiao Nanfeng,Zhong Junrui.Behaviour trust control based on bayesian networks and user behavior log mining[J].Journal of South China University of Technology,2009,37(5):94-100.(in Chinese)

[3] Tian Liqin, Lin Chuang, Sun Jinxia. A kind of prediction method of user behaviour for future trustworthy network[A].Proc.of ICCT'06[C].Beijing:IEEE Press,2006.199-202.

[4] 田立勤,林闯.可信网络中一种基于行为信任预测的博弈控制机制[J].计算机学报,2007,30(11):1930-1938.
Tian Liqin, Lin Chuang. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network[J]. Chinese Journal of Computers, 2007, 30(11):1930-1938.(in Chinese)

[5] K Murali, T V Lakshman, Detecting network intrusions via sampling:a game theoretic approach[A].Proceedings of IN-

FOCOM 2003[C]. San Francisco: IEEE Press, 2003. 1880 – 1889.

[6] Wang Wenjing, M Chatterjee, K Kwiat. Coexistence with malicious nodes: A game theoretic approach [A]. Proc of GameNets'09[C]. Istanbul: IEEE Press, 2009. 277 – 286.

[7] Wang Yuanzhuo, Lin Chuang, Wang Yang, Meng Kun. Security analysis of enterprise network based on stochastic game nets model[A]. Proc. of ICC'09[C]. Dresden: IEEE Press, 2009. 1 – 5.

[8] 张维迎. 博弈论与信息经济学[M]. 上海:上海人民出版社, 2004.
Zhang Weiying. Game Theory and Information Economics [M]. Shanghai: Shanghai People's Publishing House, 2004. (in Chinese)

[9] Drew Fudenberg, Jean Tirole. Game Theory[M]. Cambridge, Mass: MIT Press, 1991.

作者简介

陈亚睿　女, 1978 年 10 月出生于天津市, 北京科技大学博士研究生. 主要研究方向为计算机网络, 可信网络.
E-mail: chenyarui@tsinghua.org.cn

田立勤　男, 1970 年出生于陕西定边, 教授, 北京科技大学博士, 硕士生导师, 研究方向为计算机网络, 无线传感器网络和可信网络.
E-mail: tianliqin@tsinghua.org.cn

杨　扬　男, 北京科技大学教授, 博士生导师, 主要研究方向为计算机网络通信、网格计算、服务科学与云计算.
E-mail: yyang@ustb.edu.cn