一个软件服务协同中信任评估模型的设计*

徐 锋, 吕 建+, 郑 玮, 曹 春

(南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093)
(南京大学 计算机软件研究所,江苏 南京 210093)

Design of a Trust Valuation Model in Software Service Coordination

XU Feng, LÜ Jian+, ZHENG Wei, CAO Chun

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)
(Institute of Computer Software, Nanjing University, Nanjing 210093, China)
+ Corresponding author: Phn: 86-25-3593670, E-mail: lj@nju.edu.cn
http://www.nju.edu.cn
Received 2002-07-08; Accepted 2002-11-20

Xu F, Lü J, Zheng W, Cao C. Design of a trust valuation model in software service coordination. *Journal of Software*, 2003,14(6):1043~1051.
http://www.jos.org.cn/1000-9825/14/1043.htm

Abstract: Internet-Based Web application systems are gradually built as software service coordination systems. In an open, dynamic and changeful application environment, trust is an important thing for security and reliability of software services and systems. In this paper, first an Agent-based software service coordination model is presented. Then a trust valuation model is given to value trust relationships between software services. Trust is abstracted as a function of subjective expectation and objective experience, and a reasonable method is provided to combine the direct experience and the indirect experience from others. In comparison with an other's work, a complete trust valuation model is designed, and its reasonability and operability is emphasized. This model can be used in coordination and security decision between software services.
Key words: software service; trust; trust valuation

摘 要: 基于 Internet 的 Web 应用系统逐步表现为由多个软件服务组成的软件服务协同系统,面向开放、动态和多变的应用环境,软件服务之间的相互信任对软件服务个体和应用系统的安全保障与可靠运行均具有重要的意义.首先给出一个基于 Agent 的软件服务协同模型,随后针对该软件服务协同模型提出一个用于度量软件服务间信任关系的信任评估模型.信任被抽象成一个由信任评估主体对客体的主观期望和客观经验共同作用的函数,模型还提供了一个合理的方法用于综合直接经验和第三方推荐经验.与几个现有的工作相比,设计了较完

* Supported by the National Natural Science Foundation of China under Grant No.60273034 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2001AA113110, 2002AA116010 (国家高技术研究发展计划(863)); the Foundation of Nature Science and High-Tech of Jiangsu Province of China under Grant Nos.BG2001012, BK2002203, BK2002409 (江苏省自然科学基金和高技术项目)

第一作者简介: 徐锋(1975－),男,江苏张家港人,博士生,主要研究领域为分布对象技术,系统安全,电子商务应用.

整的信任评估模型,并强调其合理性和可操作性.信任评估模型可为软件服务之间的协同与安全决策提供依据.

关键词: 软件服务;信任;信任评估

中图法分类号: TP311 **文献标识码**: A

目前,以 Web 服务为代表的软件服务及软件服务协同已成为一种新兴的 Web 应用形态.应用系统表现为由多个软件服务组成的动态协作系统,而软件服务本身也可由其他软件服务动态组合而成.系统形态正从面向封闭的、熟识用户群体和相对静态的形式向开放的、公共可访问的和动态协作的服务模式转变.新的软件应用形态打破了传统的安全技术假设,软件系统的开放性、分布性和协作性与系统安全的内在要求:封闭、集中和独立相抵触,应用系统的安全问题变得愈来愈复杂和难以处理.为了解决开放环境下的系统安全问题,多个公钥证书认证体系,如 X.509,PGP 被提了出来,并与访问控制列表(ACL)结合用于建立应用系统的安全授权机制[1].其本质是依靠可信任第三方提供认证信息来进行安全决策.然而,在一个开放、动态和多变的 Web 环境中,存在完全可信的第三方是不现实的.因此,安全授权往往需要收集尽可能多的可信第三方提供的认证信息,以期作出正确的安全决策.这就需要提供一种合理的方法用于量化、推导和综合评估这些可信第三方以及目标对象的信任程度.Beth 等人提出了几个信任评估模型[2~4],Herrmann 等人则将信任评估与安全策略的实施相结合用于保障分布构件结构的应用系统安全[5].然而,上述工作在完整性、合理性和可操作性方面还存在一些问题.为此,我们结合软件服务协同的应用背景,提出一个用于协同和安全决策的信任评估模型.

本文首先介绍一个基于协同 Agent 的软件服务协同模型,随后针对该模型提出一个基于概率统计解释的信任评估模型,并进行模拟实验以初步验证模型的合理性,最后比较相关工作并作总结.

1 软件服务协同模型

软件服务是指具有自描述、自包含和模块化特征的软件实体,通过网络媒介向外发布,用于构造新的软件服务或应用系统.一些较早出现并且现今仍广泛使用的网络服务,如 telnet,ftp 等均可看做是软件服务的雏形.随着 Internet 的普及和 Web 应用需求的增加,功能更为复杂和专业的 Web 服务出现并得到迅速发展.基于 XML 的 Web 服务体系结构,从一定程度上统一了 Web 服务的描述格式和交互协议,而 SUN 提出的智能 Web 服务概念则强调为不同的服务调用者提供个性化的服务,软件服务逐渐从简单的功能封装向能够自主适应服务调用对象和网络应用环境的方向发展.

随着软件服务朝着智能化方向的发展,由多个软件服务构造而成的应用系统(软件服务)更多地表现为软件服务实体间主动的协作活动.为完成某项任务或实现某个功能,满足应用需求(包括功能、性能、安全等方面)的多个软件服务实体结成协作联盟,并分别担任相应的组织角色.协作联盟能够随应用环境、协同目标以及联盟成员的变化而动态地加以调整,已完成特定任务或不可用的软件服务可能被联盟排除,而新的软件服务也可能应某种需求而被联盟吸收.一个较为抽象的软件协同模型如图 1 所示,软件服务是一个相对独立的实体,通常由应用逻辑和协同逻辑两部分组成,前者描述软件服务的功能,后者描述与其他软件服务之间的协同.其中,软件服务的协同逻辑被抽象为一个相对独立的协同 Agent,代表软件服务处理所有协同相关事务,多个软件服务之间的协同实际上是各自 Agent 之间的协同.协同 Agent 在与其他软件服务结成联盟时,负责寻找、评价协作伙伴,并进行结盟前的协商.当联盟建立之后,协同 Agent 用于完成软件服务之间应用语义相关的协作活动.

在模型中,软件服务的功能体并不直接与其他软件服务进行交互,所有交互和协同均由相应的协同 Agent 完成.其优点在于:(1) 软件服务的功能独立于软件服务间的交互协议和协同方式,有利于软件服务的实现;(2) 协同 Agent 将功能体与外界隔离,能够有效地保障软件服务功能体的安全.对于后者,协同 Agent 实际上承担了整个软件服务的协同和安全决策任务,根据自身的经验和可信任第三方提供的信息,判断候选协作对象的可信任程度,拒绝与有潜在危险或不可靠的软件服务交互,而一个合理的信任评估模型则是指导协同 Agent 作出正确的安全决策的关键.

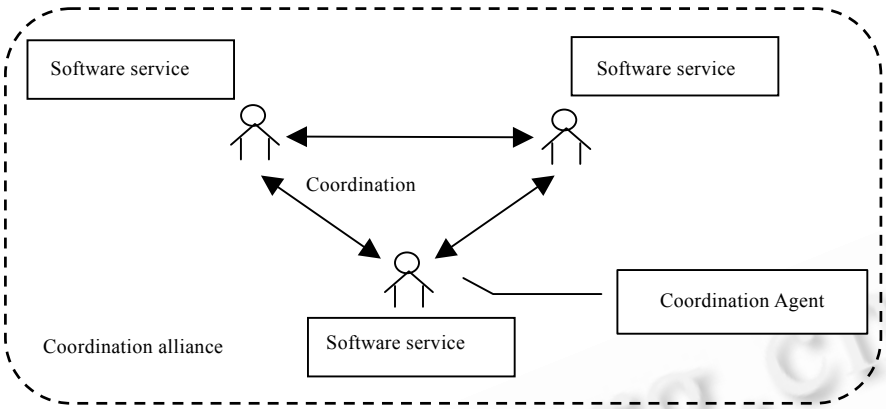

Fig.1 Software service coordination model

图 1 软件服务协同模型

2 信任评估模型

目前,对于信任还没有一个精确的、广泛可接受的定义.但多数学者[2,3,6~8]认为,信任是一种主观信念.其中,Gambetta 给出了一个比较完整的信任定义,“信任(或不信任)是一个 Agent 评价其他 Agent 或 Agent 团体实际行为的主观可能性程度,评价在对该行为进行监控(或根本不可能监控该行为)之前和与该行为对其自身行为产生影响的情况下进行”[8].

定义给出了信任的几个重要特征:(1) 主观性,不同的个体对同一事物的看法会受个体喜好等因素影响而有所不同;(2) 可能性预期,信任的程度可表示为对事件发生概率的可能性估计;(3) 内容相关,信任是对事物的某个方面(如完成某项任务的能力)而言的.

我们认为,在软件服务协同系统中,信任是指一个协同 Agent 对其他软件实体是否能够正确地、非破坏性地进行某项(类)协作活动的主观可能性预期,预测的依据来源于此前该 Agent 所观察到(包括其他可信任第三方提供)的目标服务的行为,预测结果受该 Agent 对此项协作活动的重要程度评价(如关键协作活动、次要协作活动等等)的影响.为了能够使信任评估模型对服务之间的信任关系进行度量,我们将所有该 Agent 的观察结果和第三方提供的观察结果定义为客观经验,前者称为直接经验,后者称为推荐经验(间接经验).对应于目标服务活动的成败,经验简单地分为成功经验和失败经验,其计数定义为经验值.

2.1 实 体

信任评估模型的实体对应于软件服务协同模型中的协同 Agent,在信任评估中可能担任的角色为:评估主体、经验推荐者、评估客体.Agent 能够自主记录、分类和收集来自经验推荐者(可信任第三方)所提供的客体经验值,并根据推荐者的可信程度决定取舍或进行相关处理,最终给出对客体的信任评估.另外,Agent 也能够将收集到的经验值推荐给其他 Agent 使用.

2.2 信任分类

信任评估模型中信任是内容相关的,即一个实体对另一个实体的信任是就其能完成某项(类)协作活动而言的.信任应按其内容进行分类,并对应于相应的经验分类.但实际的分类视信任的应用需求而定,如 Yahalom 等人在考察了一些认证协议之后,将与认证协议有关的信任内容分为密钥生成、实体标识、保密、抗干扰、时钟同步和算法步执行[9].而在软件服务协同系统中,信任不仅用于处理服务个体和系统的安全问题,还用于解决其运行的可靠性问题.另外,服务的功能呈现出多样性.因此,在信任模型中给出一个具体的信任分类标准是困难的,并且不具有多大的实际意义.我们强调信任的内容相关性,但同时认为信任的分类应在实际的应用中完成.

信任分类将为软件服务之间的协同和安全决策提供更细致和精确的依据.例如,当需要信任一个服务完成某项特定的协作活动时,并不需要信任它能够正确地完成它所能完成的全部协作活动.另外,可以对不同类属的

信任分别进行评估,并根据其重要程度的不同进行综合处理.

2.3 信任关系及其度量

在信任评估模型中,当实体 A 具有对实体 B 的可信度评价时,则 A 与 B 之间存在信任关系.信任关系分为两类,如图 2 所示:(1) 直接信任关系,A 具有对 B 能够完成某项协作活动的可信度评估;(2) 推荐信任关系,A 具有对 B 提供的关于目标实体 C 的某类经验信息的可信度评估.

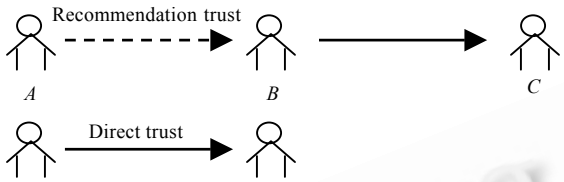

Fig.2 Direct trust and recommendation trust

图 2 直接信任与推荐信任

对信任关系进行评价的主要依据来源于相关的经验信息,实体间的信任传递主要表现为经验信息的传递和采纳,而判断一个实体是否成功地完成某项协作活动与判断一个实体是否诚实地提供经验信息相比,要涉及较少的主观判断.因此,直接信任比推荐信任具有更多的理性成分,较易建立合理的数学模型进行处理,而推荐信任的处理则具有更多的个性化需求.

2.3.1 直接信任

经验是信任评估的主要依据,若实体 A 具有对实体 B 的某类经验信息(包括所有的直接或间接的经验),则 A 与 B 之间存在直接信任关系.对该直接信任关系的评估可用 B 能以 A 期望的成功概率或可接受的失败概率完成某项(类)协作活动的可能性来度量,该度量的依据来源于 A 所获得的关于 B 的相关经验信息,该经验信息具体表现为 A 所能获得的 B 进行该类协作活动的成败次数.

设 A 对 B 关于 ω 类协作活动的成功经验值和失败经验值分别为 m_ω 和 n_ω,其意义是 A 收集到的所有关于 B 完成ω类协作活动的成功次数和失败次数.在考察 B 进行该类协作活动的成功概率和失败概率时,这些成功和失败的事件可以看做是一个样本空间,其容量为 $m_\omega+n_\omega$.由于所有协作活动只有成功和失败两种结果,则在 B 进行多次此类协作活动时,它能够成功完成协作活动的次数 X 和失败次数 Y 均可看成是一个随机变量,并服从 $B(n,p)$的二项分布.A 对 B 的行为预期可以从 B 协作行为的成功概率角度考察,但当特别关注 B 行为失败所带来的损失时,也可以从其失败概率的角度进行考察,如 Povey 等人曾提出了从风险管理的角度建立信任模型的思想[10].按照基本的概率统计原理,从上述两个角度均可给出效用相同的直接信任关系评估方法.为表述方便,我们引入变量 V_ω^P 和 V_ω^N 分别表示从成功和失败两个角度进行考察时所得到的直接信任评估值.

设定 A 对 B 完成此类协作活动的成功率期望为α,即 A 希望 B 成功完成协作活动的可能性≥α. V_ω^P 为在此期望的成功概率下,B 成功完成ω类协作活动的次数 $X\le m_\omega$ 的概率.由经验信息可得 $X\sim B(m_\omega+n_\omega,\alpha)$,则有如下计算公式:

$$V_\omega^P=P_\alpha(X\le m_\omega)=\sum_{l=1}^{m_\omega}C_{m_\omega+n_\omega}^{l}\alpha^l(1-\alpha)^{m_\omega+n_\omega-l}. \tag{1}$$

设定 A 对 B 可接受的失败率为β,即 A 希望在与 B 进行协作活动时,其失败的可能性≥β. V_ω^N 为在此可接受的失败率下,B 进行ω类协作活动失败的次数 $Y\ge n_\omega$ 的概率.同样有 $Y\sim B(m_\omega+n_\omega,\beta)$,则有如下计算公式:

$$V_\omega^N=P_\beta(Y\ge n_\omega)=\sum_{l=n_\omega}^{m_\omega+n_\omega}C_{m_\omega+n_\omega}^{l}\beta^l(1-\beta)^{m_\omega+n_\omega-l}. \tag{2}$$

显然,上述两个直接信任评估值均为 A 对 B 的经验值和主观期望值的函数.

直接信任评估可以用于简单的信任判断,按照概率统计中假设检验的方法,设定一个较小数值的显著水平 λ.当 $V_\omega^P<\lambda$ 时,则认为 B 不可能以≥α的成功率完成ω类协作活动;同样,当 $V_\omega^N<\lambda$ 时,则认为 B 不可能以≥β的失败率完成ω类协作活动,出现上述情况应拒绝与 B 进行协作活动.另外,直接信任评估值的大小可用于对多个候选协作伙伴进行比较和选择,也可作为安全策略等实施的依据,例如当信任度达到某个程度时,可以免除一些严

格的安全检查以节约系统开销.

2.3.2 推荐信任

推荐信任是一个实体对另一个实体所推荐的经验信息的可信程度(或采纳程度),同样是该实体历史经验的反映.但对一个实体的经验推荐活动很难简单地划分为成功和失败两种结果,即使进行划分往往也会带有很大的随意性和主观性.因此,很难给出能够客观反映推荐行为的经验信息.而实体间的推荐信任关系往往左右着实体对直接信任作出合理的评估,实体间推荐信任关系的建立是相当谨慎的,可以认为是一种相对正式和稳定的关系.基于上述考虑,我们认为,实体间一旦建立推荐信任关系,则对该信任关系的评价在较长的一段时间内是不变的.在模型的实际使用中,实体间的推荐信任关系及其评价可作为初始参数进行设置.

考虑到模型的可操作性和使用效率,我们采用了 PGP[11]中对证书推荐者信任度的划分,并引入了对应的采纳系数用于描述对推荐经验信息的采纳程度,见表 1.

Table 1 Recommendation trust level and accepted coefficient

表 1 推荐信任度与采纳系数

Recommendation trust level	Accepted coefficient
Full trusted	1
Marginally trusted	0.5
Distrusted	0

当然,其他一些更细致的推荐信任程度的划分也是可行的,如 Abdul-Rahman 等人在文献[12]中将推荐信任度划分为 4 个等级.但对推荐信任度进行过细的等级划分不仅没有太大的实际意义,反而会降低模型的可操作性.

2.4 经验推荐与综合

在模型中,当实体 A(评估主体)需要对实体 B(评估客体)的ω类直接信任关系进行评估时,往往需要收集多个可信任实体 R(经验推荐者)所推荐的相关经验信息,而可信任实体所推荐的经验信息也可能来自于其他可信任实体,经验推荐关系形成经验推荐路径,路径的终点则是对 B 有直接经验的经验推荐者 R_n,如图 3 所示.

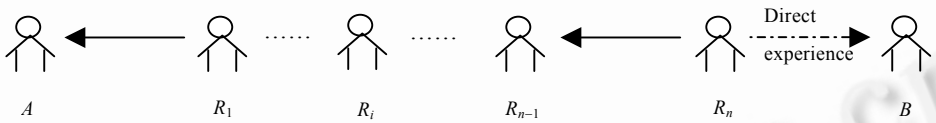

Fig.3 Experience recommendation path

图 3 经验推荐路径

位于经验推荐路径上的不同实体对其推荐者的信任程度有所不同,因此它对推荐经验信息的采纳程度也不同,若完全信任,则采纳所有推荐经验,若部分信任,则采纳一半推荐经验.采纳系数用于经验信息的衰减,以减低推荐信任度较低的实体对直接信任评估结果的影响.设推荐路径的终点实体 R_n 对评估客体 B 的直接成功经验和失败经验分别为 M_d 和 N_d,评估主体 A 对经验推荐者 R_1 的经验采纳系数为 C_1, R_1 对 R_2 的经验采纳系数为 C_2,以次类推, R_{n-1} 对 R_n 的经验采纳系数为 C_n,其中 $C_i \neq 0(i=1...n)$,则定义 A 对从该经验推荐路径上获得的经验信息的等效采纳系数为 C,简称该推荐路径的等效采纳系数,其计算公式如下:

$$C=\prod_{i=1}^{n} C_i. \tag{3}$$

当 A 从多个推荐路径获得经验信息时,必须注意到一些推荐路径的终点可能是同一个经验推荐实体,即从几条不同的推荐路径所获得的经验信息可能来自同一个实体的直接经验,如图 4 所示,A 与最终推荐实体 E_1 之间存在两条经验推荐路径.

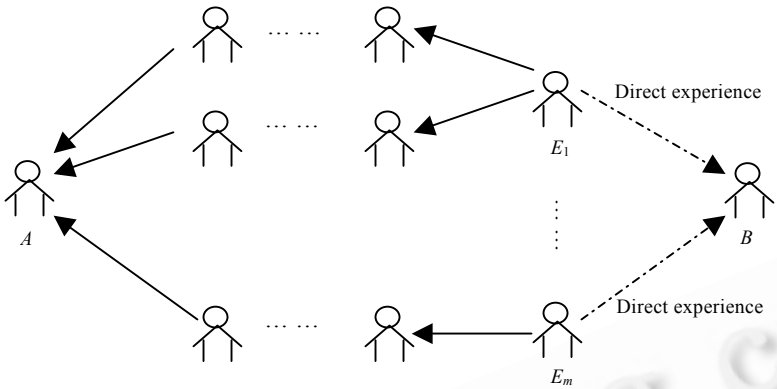

Fig.4 Combination of multi experience recommendation paths

图 4 多条经验推荐路径的综合

因此,在对推荐经验值进行综合计算时应消除这些重复的经验信息,同时必须符合如下事实:(1) 经验信息不会因多次推荐而增多,即从源自同一最终推荐实体的多个推荐路径上获得的经验值的总和不能大于该最终推荐实体的直接经验值;(2) 对于相同的直接经验值,从多个推荐路径获得的经验值应不小于任何单个推荐路径.

设 $E_i(i=1...m)$ 分别为经验推荐路径上各不相同的最终推荐者,它对 B 的直接经验值分别为 M_i^d 和 N_i^d, $C_{i,j}(i=1...m, j=1...n_i)$ 为各推荐路径的等效采纳系数,其中 $C_{i,*}$ 是一类以 E_i 为最终推荐实体的推荐路径的等效采纳系数,而 n_i 是该类推荐路径的个数.为方便描述,定义 C_i 为 E_i 到 A 的等效采纳系数,则上述事实可等价地表述为:(1) $\forall i \in [1...m]$ 满足 $C_i \le 1$;(2) $\forall j \in [1...n_i]$ 满足 $C_i \ge C_{i,j}$.另外,若在 A 和 E_i 之间存在一条推荐路径,其等效采纳系数为 1,则表明 A 能够完全采纳实体 E_i 的推荐经验,而无须考虑 A 与 E_i 之间的其他路径,可等价地表述为:(3) $\forall j \in [1...n_i]$,当 $\exists C_{i,j}=1$ 时, $C_i=1$.为此,我们选择了满足上述 3 个性质的 $1-C_{i,j}$ 的调和平均计算公式:

$$C_i=\begin{cases}1, & \text{if} \quad (\forall j \in [1...n_i]) \wedge (\exists C_{i,j}=1)\\ 1-\dfrac{1}{\sum\limits_{j=1}^{n_i}\dfrac{1}{1-C_{i,j}}}, & \text{else}\end{cases}. \tag{4}$$

最后,设 A 对 B 的直接经验值为 M_d 和 N_d,则 A 对 B 具有的所有成功经验值 M 和失败经验值 N 是其直接经验值与从所有推荐路径获得的推荐经验值之和,综合计算公式如下:

$$M=M_d+\text{int}\left(\sum_{i=1}^{m}C_i\cdot M_i^d\right), \tag{5}$$

$$N=N_d+\text{int}\left(\sum_{i=1}^{m}C_i\cdot N_i^d\right). \tag{6}$$

把由上述公式计算得到的综合经验值代入第 2.3.1 节中式(1)或式(2),即可得到 A 对 B 的信任度,并进行相应的信任判断.

3 模拟实验与讨论

为验证模型的合理性,我们设置了一个与实际应用相近的实验场景,在此场景下设计并进行了模拟实验.

3.1 实验场景

在一个软件协作联盟建立之前,联盟发起者 A 希望评价软件服务 G 的某类行为的可信程度以决定是否与该服务进行协作活动.为此,A 需要通过其他可信任的第三方(B,C,D,E,F)来收集关于软件服务 G 的经验信息,它们之间的经验推荐路径及采纳系数如图 5 所示.

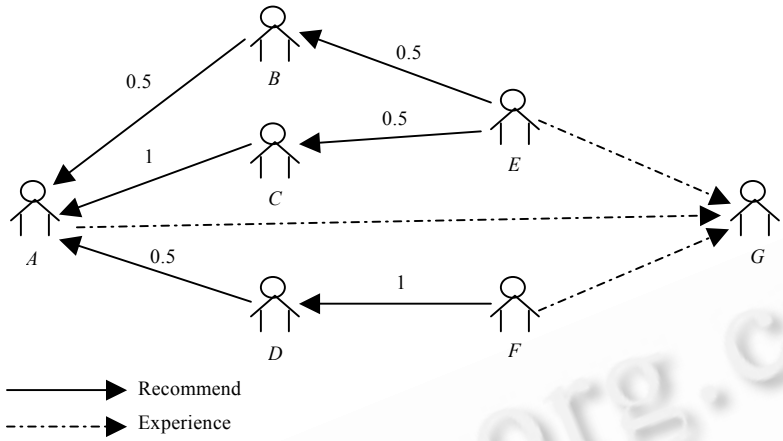

Fig.5 Experiment scenario

图 5 实验场景

图 5 中给出的数据意义如下,A 部分信任 B 的推荐经验,对其推荐经验值的采纳系数 $C_{A\to B}=0.5$;B 部分信任 E 的推荐经验,对其推荐经验值的采纳系数 $C_{B\to E}=0.5$;A 完全信任 C 的推荐经验,对其推荐经验值的采纳系数 $C_{A\to C}=1$;C 部分信任 E 的推荐经验,对其推荐经验值的采纳系数 $C_{C\to E}=0.5$;A 部分信任 D 的推荐经验,对其推荐经验值的采纳系数 $C_{A\to D}=0.5$;D 完全信任 F 的推荐经验,对其推荐经验值的采纳系数 $C_{D\to F}=1$.

3.2 实验设计与结果

由于无法确切了解经验推荐者的行为,在模拟实验中我们假设信任评估主体 A 对最终推荐实体的推荐信任程度取决于该最终推荐实体所提供的推荐经验值的相对误差程度,即推荐信任程度越低,该最终推荐实体所提供的推荐经验相对误差范围越大,反之亦然.令最终经验推荐者 E,F 的每次推荐经验值(包括成功经验和失败经验)服从某个正态分布 $N(\mu,\sigma)$,μ为该最终推荐实体的直接经验值,σ表示该推荐值的误差程度,该值越大误差程度越大.针对上述实验场景中评估主体 A 对最终经验推荐者 E,F 的推荐信任程度的差异,我们分别给定 $\sigma_E=0.003*\mu$ 和 $\sigma_F=0.005*\mu$.

为使实验更接近实际情况,如信任评估主体只有在对被评估实体直接经验缺乏时才需要获得更多的推荐经验信息,我们设定 A 对 G 的直接经验少于两个最终经验推荐者 E,F,在模拟实验中,E 和 F 获得的关于 G 的经验总数取 100~500 之间的随机数,而 A 对 G 的直接经验总数则取 50~100 之间的随机数.设置假设检验的显著水平λ=0.01,A 对 G 的成功率期望为 0.90,在不同的被评估实体 G 的固有成功率(从 0.6~0.98,其中间隔为 0.01)下,各进行 1 000 次的随机模拟实验并统计拒绝的次数,其结果形成如图 6 所示的拒绝曲线.图中,横坐标为被评估实体 G 的固有成功率,纵坐标为每 1 000 次模拟实验中 G 被 A 拒绝的次数.各曲线依次为采用如下不同经验信息进行判断的实验结果:(1) 全部经验信息;(2) 除推荐路径"$E\to C\to A$"的全部经验信息;(3) A 对 G 的直接经验信息;(4) 推荐路径"$F\to D\to A$"所提供的推荐经验信息.

3.3 结果分析与讨论

从如图 6 所示的实验结果可以看出,采用全部经验信息的拒绝曲线相对于采纳其他经验信息的拒绝曲线,其曲线的下降过程最快,而仅采用 A 对 G 直接经验的拒绝曲线其下降过程最慢,这表明模型在获得较全面的经验信息时,其判断的精确性较高.另外,可以看到,所有曲线只在横坐标 0.9(A 对 G 的期望成功率)附近发生很陡的下降,说明模型能够很好地根据经验信息计算出一个合理的信任值,用于对被评估实体的固有成功率进行判断,即当被评估实体的固有成功率低于评估主体的期望成功率时被拒绝,否则被接受.

从实验结果中我们还注意到,所有拒绝曲线发生跳变的区域都在期望成功率附近,但均偏向左侧,这意味着一些固有成功率低于期望成功率的实体可能不会被拒绝,而固有成功率高于期望成功率的实体几乎不被拒绝.

实际上,信任度的使用方式并不局限于这种绝对的是非判断,也可用于多个未被拒绝实体间的比较和选择.

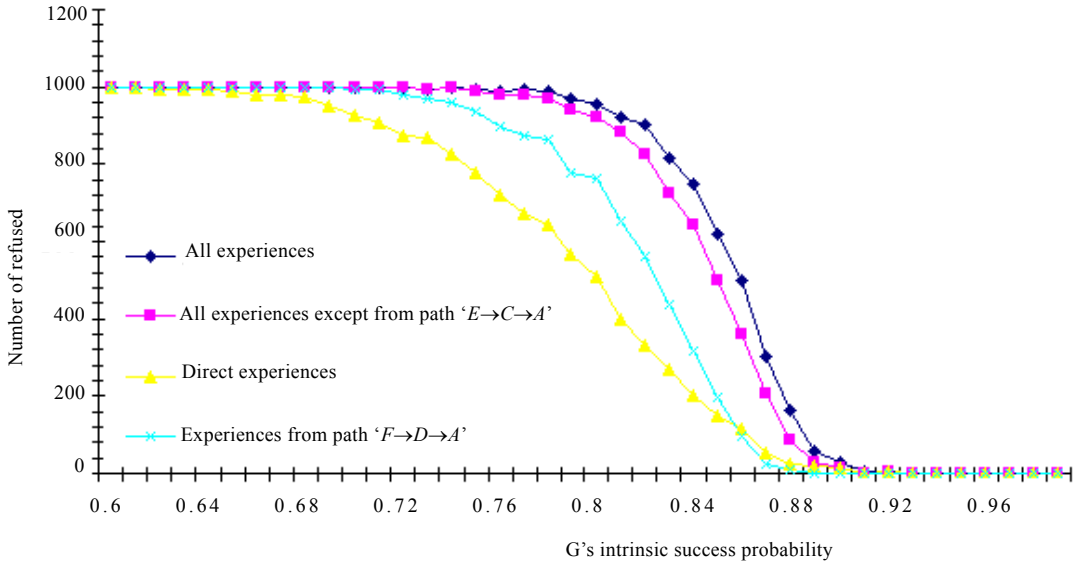

Fig.6 The experimental results

图 6 实验结果

4 相关工作与总结

在研究开放网络和分布系统安全问题的过程中,已有多位学者在其不同的研究背景下提出了各自的信任评估模型,但这些模型在完整性、合理性或可操作性等方面存在一些问题.Abdul-Rahman 等人提出了一个分布式信任模型[2,12],将信任关系分为直接信任和推荐信任两类,并采用一系列离散值对信任关系进行度量.模型强调了信任度的有条件传递性,并给出了具体的传递协议和计算公式,但没有给出具体的信任度综合计算公式.另外,模型没有解释直接信任度的实际意义及获取方法.T.Beth 等人提出了一个基于经验和概率统计解释的信任评估模型[3],并将其应用于开放网络的安全认证问题[9,13,14]的研究.模型引入经验的概念来表述和度量信任关系,并给出了由经验推荐而引出的信任度推导和综合计算公式.但该模型对直接信任的定义过于严格,直接信任关系仅建立在没有否定经验的实体之间.推荐信任关系同样采用经验信息进行度量,而在实际应用中对实体推荐行为的成败判断具有很大的随意性和主观性,难以获得能够客观反映推荐行为的经验信息.Jøsang 等人在安全认证和系统安全度量[4,6,7]等问题的研究中,提出了一个安全系统的信任模型.模型引入了事实空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系[6].观念被表示为对系统某个属性的确信程度、否定程度和不确定程度所组成的三元组.在模型实际应用中,需对要考察的系统属性进行分类,并分别给出观念值,虽然 Jøsang 等人给出了一些指导原则,但该过程的处理仍较为复杂和困难.

在软件服务协同系统安全的研究背景下,我们借鉴了上述已有的工作,从信任的定义、度量、经验传递和综合计算等方面出发给出了一个较完整的信任评估模型,并强调了模型的合理性和可操作性.主要工作有:(1) 从信任的定义出发,使用概率统计学中假设检验的思想对直接信任关系的度量进行解释,并给出了一个直接信任度计算公式,采用成功经验和失败经验两类信息对信任关系进行度量,计算结果可直接用于信任决策;(2) 强调信任传递应表现为客观经验信息的传递和采纳,而不是信任值的传递(多数信任评估模型采用此方式解释信任传递),降低了推荐路径上各实体主观意志对最终评价结果的影响,有利于信任评估主体对信任关系作出较客观和合理的评价;(3) 引入经验采纳系数,用于描述对具有不同推荐信任度的第三方实体所推荐经验的不同采纳程度,并给出了一个符合一般事实的经验传递和综合计算公式;(4) 通过模拟实验,初步验证了模型的合理性.

系统安全和可靠性问题中的信任研究是一个崭新的课题,在信任的定义、信任的合理表达等方面还需要深

入地研究和探讨.另外,信任模型在实际应用中还需要解决诸如如何合理分类经验信息、如何保障经验信息的可靠传递以及如何搜索经验推荐路径等问题.这些将是我们进一步研究的内容.

References:

[1] Blaze M, Feigenbaum J, Ioannidis J, Keromytis AD. The role of trust management in distributed systems security. In: Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999. 185~210.

[2] Abdul-Rahman A, Hailes S. A distributed trust model. In: Proceedings of the 1997 New Security Paradigms Workshop. Cumbria, ACM Press, 1998. 48~60. http://www.ib.hu-berlin.de/~kuhlen/VERT01/abdul-rahman-trust-model1997.pdf.

[3] Beth T, Borcherding M, Klein B. Valuation of trust in open network. In: Gollmann D, ed. Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3~18.

[4] Jøsang A. The right type of trust for distributed systems. In: Meadows C, ed. Proceedings of the 1996 New Security Paradigms Workshop. Lake Arrowhead: ACM Press, 1996.

[5] Herrmann P, Krumm H. Trust-Adapted enforcement of security policies in distributed component-structured applications. In: Proceedings of the 6th IEEE Symposium on Computers and Communications. Hammamet: IEEE Computer Society Press, 2001. 2~8. http://www.computer.org/proceedings/iscc/1177/11770002abs.htm.

[6] Jøsang A, Knapskog SJ. A metric for trusted systems. In: Global IT Security. Wien: Austrian Computer Society, 1998. 541~549.

[7] Jøsang A. A subjective metric of authentication. In: Quisquater J, ed. Proceedings of the ESORICS'98. Louvain-la-Neuve.: Springer-Verlag, 1998. 329~344.

[8] Gambetta D. Can we trust trust? In: Gambetta D, ed. Trust: Making and Breaking Cooperative Relations. Basil Blackwell: Oxford Press, 1990. 213~237.

[9] Yahalom R, Klein B, Beth T. Trust relationships in secure systems—a distributed authentication perspective. In: Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy. IEEE Press, 1993. 50~164. http://isbn.nu/0818633700.

[10] Provey D. Developing electronic trust policies using a risk management model. In: Proceedings of the 1999 CQRE Congress. 1999. 1~16. http://security.dstc.edu.cn.au/staff/povey/papers/CQRE/123.pdf.

[11] Abdul-Rahman A. The PGP trust model. 1996. http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/pgptrust.html.

[12] Abdul-Rahman A, Hailes S. Using recommendations for managing trust in distributed systems. In: Proceedings of the IEEE Malaysia International Conference on Communication'97 (MICC'97). Kuala Lumper: IEEE Press, 1997. http://citeseer.nj.nec.com/360414.html.

[13] Reiter MK, Stubblebine SG. Toward acceptable metrics of authentication. In: Proceedings of the 1997 IEEE Symposium on Research in Security and Privacy. Oakland: ACM Press, 1998.

[14] Levien LR. Attack resistant trust metric [Ph.D. Thesis]. Berkeley: University of California, 2002.