

移动 Agent 系统安全问题的动态信任计算模型

蒋伟进[†], 吕斯健

(湖南工商大学 计算机与信息工程学院, 长沙 410205)

摘要: 在移动云计算中, 由于数据存储和数据处理是在云端以远程方式进行的, 因而信任是移动云计算安全中一个非常重要的因素. 针对移动云计算环境中移动 Agent 系统安全和信任管理问题, 借鉴人类信任机制 (Human Trust Mechanism, HTM), 研究主观信任形成、信任传播与信任进化规律, 提出主观信任动态管理算法 (MASTM), 基于移动 Agent 与执行主机的交互经历以及第三方推荐信息收集基础信任数据, 给出了公信主机选择算法, 孤立恶意主机算法和综合信任度计算算法, 实现选择信任机群, 孤立恶意主机的功能, 以增强移动 Agent 与主机的安全交互效果. 对所给出的算法均进行了模拟验证, 验证了其可行性和有效性.

关键词: 移动云计算; 移动 Agent 系统; 主观信任; 客观信任; 移动互联网; 动态信任计算

中图分类号: TP393

文献标志码: A

DOI: 10.13195/j.kzyjc.2020.1154

开放科学 (资源服务) 标识码 (OSID):



Mobile Internet Mobile Agent System Dynamic Trust Model for Cloud Computing

JIANG Wei-jin[†], LV Si-jian

(College of Computer and Information Engineering, Hunan University of Technology and Business, Changsha 410205, China)

Abstract: In mobile cloud computing, trust is a very important parameter in mobile cloud computing security because data storage and data processing are performed remotely in the cloud. Cloud computing environment of the mobile Agent system security and trust management issues, drawing on human trust mechanism (Human Trust Mechanism, HTM), focusing on the formation of subjective trust, confidence and trust propagation laws of evolution, dynamic management algorithm proposed subjective trust (MASTM), based on Mobile Agent and execution host of interactive experiences and recommendation information to third parties collect data based on trust, credibility given host selection algorithm, isolated malicious hosts trust calculation algorithms and integrated algorithm, choose to trust the fleet, malicious hosts a stand alone features to enhance the mobile Agent host interaction effects and safety. Given algorithm simulation and verification were carried out to prove its feasibility and effectiveness.

Keywords: Mobile Cloud Computing; Mobile Agent System; Subjective Trust; Objective Trust; Mobile Internet; Dynamic Trust Computing

0 引言

“云计算”作为一种新的互联网应用商业模式, 为用户屏蔽了数据中心管理、大数据处理、应用程序部署等问题. 用户通过网络可以根据其业务需求快速申请或释放资源, 并以按需支付的方式对所使用的资源付费, 就如同现在使用水电一样方便快捷, 用户不必购置部署硬软件基础设施, 将其从 IT 基础设施管理与维护的沉重压力中解放出来, 更专注于自

身的核心业务发展. “云计算”以其经济便利的服务优势占据了巨大的市场. 从技术层面看, “云计算”有两个重点, 一是资源池中大规模动态资源的分布构建方法研究; 二是分布式协同应用开发平台上的计算方法与编程方法研究. 对于后者来说, 移动 Agent 计算范围为“云计算”环境下应用系统的设计与开发提供了普适参考模型. 移动 Agent 模型在技术方面能够实现移动互联网云计算的核心思想和计算原理,

收稿日期: 2020-08-18; 修回日期: 2020-10-22.

基金项目: 国家自然科学基金项目 (61472136, 61772196); 湖南省自然科学基金面上项目 (2020JJ4249); 湖南省社会科学基金重点项目 (2016ZDB006); 湖南省社会科学成果评审委员会课题重点项目 (湘社评 19ZD1005); 湖南省学位与研究生教育改革研究项目 (2020JGYB234); 湖南工商大学学位与研究生教育教学改革项目 (YJG2019YB13); 湖南工商大学教学改革项目 (校教字 [2020]15 号).

[†]通讯作者. E-mail: jwjnudt@163.com.

在服务方面能够实现云计算的商业服务形态.但由于云环境的虚拟性、动态性、开放性以及公用性,给移动 Agent 范型的应用带来了极大的安全性挑战^[1].

移动 Agent 技术是一项涉及多学科的、处于国际研究前沿的新兴技术,移动 Agent 技术是人工智能领域 Agent 和 Internet 相结合的产物^[2].在云计算环境下对移动 Agent 系统信任安全域资源分配问题进行研究^[3-4],能够丰富云计算和移动 Agent 模型的理论体系,增强 Agent 应用系统的安全性能,推进移动 Agent 技术在云计算环境下更广泛的应用于各个领域,因此,对云计算环境下移动 Agent 系统设计中的安全信任问题研究,具有重要的意义.

1 相关工作

移动 Agent 系统信任问题既有网络信任问题的一般性又有它自身的特殊性.早在 1996 年,M.Blaze 等人第一次提出了“信任管理”的概念,被用来解决系统网络服务的安全问题,其基本思想是:信任管理是提供一个适合网络应用的、开放的、分布和动态特性的安全决策框架^[5-6].1999 年,D.Povey^[7]在 M.Blaze 定义^[6]的基础上,结合 D.Gambetta 和 A.Abdul-Rahman 等人 [8,9] 的研究成果,给出了更具普适性的概念:信任管理被认为是对信任意向进行获取、评估和实施的过程.这一关于信任的描述表达了交互实体之间存在一种约定关系以及对遵守该约定关系的一些期望.

1.1 基于传统信任管理模型的网络互信机制

目前,信任管理模型总体上分为两类:

第一类是客观理性模型,对繁杂的信任关系用一种理性的、准确的方法来进行表述和处理,具有客观、静态管理特征.典型代表是 M.Blaze 信任管理模型^[6]:信任管理所要回答的问题是:“安全凭证集 C 是否能够证明请求 r 满足本地安全策略集 P”.

第二类是主观经验模型,认为信任是对客体的特定特征或行为的特定级别的主观判断,这类信任模型认为信任是带有主观性、非理性的,具有经验主义式的体验,包括信任的具体内容以及信任水平的划分,并根据客体行为的结果变化而不断修改.典型代表是 D.Povey 结合 A.Abdul-rahman 和 D.Gambetta 等人的观点提出的信任管理模型,主要功能是进行“信任意向的获取、评估和实施”,主要涉及两方面的研究内容:一是怎样对信任进行描述和衡量;二是基于经验推荐如何对信任度进行推演和计算等.

1.2 基于 SPKI 信任模型的 MAS 互信机制

简单公钥基础设施 (Simple Public Key Infrastructure,SPKI) 方法由 Carl Ellison 和 Bill Frantz 提出^[10-12],SPKI 信任管理模型的作用是提供建立信任链、选择信任路径进行认证的基本规则.主要分为以下四种:严格层次信任模型、对等模型、网状模型和可扩展的多级信任模型.但四种模型中没有一种信任管理模型能够统揽解决开放网络系统中的所有信任问题,每种信任模型既有优势也有不足.目前,在网络中使用较多的是集中控制信任模型,即“层次模型”.随着开放式、分布式网络系统中实体交互过程中信任判定主观化、个性化需求日益增多,“对等信任管理模型”和“网络信任管理模型”的研究变得越来越重要.

在实际应用中,文献^[13]基于网络对等信任模型,提出了移动 Agent 系统客观信任对等模型.采用 SPKI+RBAC 身份属性证书解决移动 Agent 和执行主机之间的身份认证、操作授权及访问控制问题.基于 SPKI 技术构建移动 Agent 系统客观信任管理模型,主要解决三个问题:建立移动 Agent 系统中各个实体之间的信任关系;确定主机和移动 Agent 信任证书内容;判定移动 Agent 系统中实之间的信任状态.

1.3 现有研究工作进展

上述信任管理模型为解决网络实体(服务方和请求方)交互过程中的信任问题提供了思路和框架.但还存在很多不足,主要有:信任策略验证能力和效率较低.信任策略的制定过于繁复,信任管理模型的使用成本高,效率低,严重阻碍了模型的实际应用.提供服务的主体仅考虑服务方的信任与安全需求而没有考虑请求方的信任与安全需求.这种模型不适合移动 Agent 系统中为保护移动 Agent 安全对执行主机进行信任判定的需求.在云计算环境下,目前关于“信任”没有明确的统一定义,在很多研究中信任与安全相关的概念有很多混同的用法,这很不利于对信任问题深入细化的研究.

在上述相关信任管理分析研究的基础上,结合我们近年的工作^[14-17],本文对移动 Agent 系统信任问题的研究采用客观理性模型与主观经验模型相结合的方法,在移动 Agent 系统客观信任对等管理的基础上,提出主观信任动态管理方法,可避免和解决上述问题.从设计原则上降低了信任验证的复杂度,与现有的基于 PKI 的信任管理模型相比,基于 SPKI+RBAC 设计信任证书,降低了信任验证的复杂度,既可满足移动 Agent 系统信任传递与验证的需

求,又可控制信任链过长导致的信任程度的衰减.

2 基于移动 Agent 的互信计算分析方法

通过分析主观信任的形成、传播、进化规律,提出主观信任动态管理算法 MASTMA. 使用信任度的概念,对移动 Agent 系统交互行为安全效果进行测量、计算与评价,并对下一次交互的可信程度进行预测. 交互主机可以给予自己的信任需求设定信任门限,选择可信机群、孤立恶意主机.

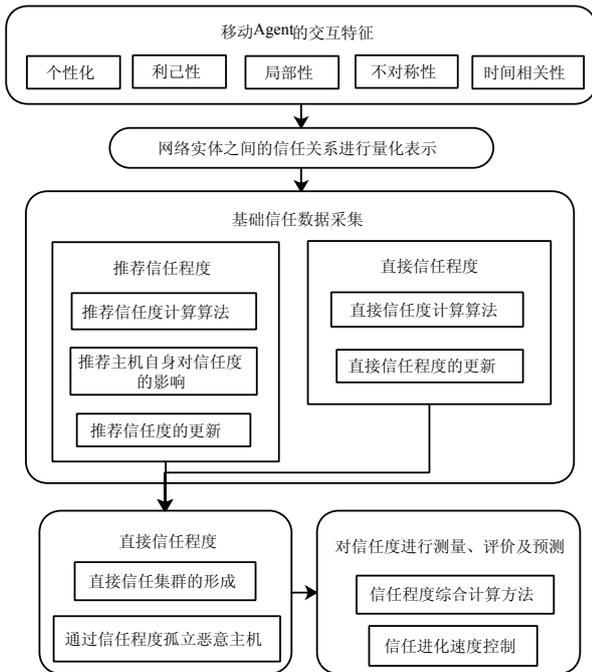


图1 基于移动 Agent 的互信计算分析方法架构图

对于基于移动 Agent 的互信计算分析方法的架构如图 1, 其中信任的动态性主要体现在以下几点: 由于推荐信任算法的存在, 对于信任程度的最终评判, 取决于推荐主机自身对信任度的影响, 以及不同主机不同的信任推荐情况; 在直接信任度计算算法中, 信任度也将根据主机之间的交互经验对信任基础进行计算, 并且可以通过主观信任集群对恶意主机进行鼓励, 实现信任的动态赋予; 并且在主观信任动态管理方法中, 同时综合考虑了以上两种信任算法的结果, 并对信任的进化速度进行了控制.

2.1 基于移动 Agent 的主观信任分析模型

传统的移动 Agent 系统客观信任对等管理模型, 使用 SPKI 证书能够在交互发生前判定对方的信任状态, 提高移动 Agent 系统安全交互的可能性. 但判定信任本质上只是一种可能性, 是一种预测. 实体交互前的信任判定是否真正“属实”, 取决于交互过程完成后, 检查交互实体有无恶意为来确定. 只使用客观信任对等管理模型不能及时发现交互者恶意为, 不能及时修正信任状态, 也不能及时惩戒违规者.

在客观信任对等管理模型基础上, 我们针对移动 Agent 系统主观信任需求研究主管信任动态管理方法, 基于交互行为好坏, 测量交互主机的信任状态, 实现主观信任的形成、传播、进化等动态管理功能.

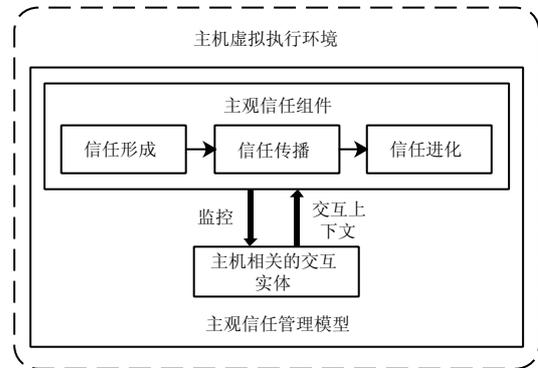


图2 动态信任计算模型

2.1.1 动态信任计算模型

我们设计的移动 Agent 系统动态信任计算模型的组成如图 2 所示^[14-15]. 主机处于开放的、动态的网络环境中, 执行移动 Agent 的平台位于主机上, 为移动 Agent 提供执行环境, 在一个主机上的平台不一定是唯一的, 可以有多个. 主观信任管理模型位于的平台中, 由三个信任组件构成: 分别是信任形成组件、信任传播组件和信任进化组件, 这些管理机制为交互实体提供信任交互上下文, 对实体的交互过程和行为进行监控. 信任形成组件主要实现信任数据的采集与计算, 信任传播组件主要实现信任数据的协议交换, 信任进化组件主要实现信任数据的更新.

2.1.2 计算处理方法

(1) 采集基础互信数据

信任形成组件完成基础信任数据采集功能. 主机对主机的信任数据采集分为两部分内容: 一是直接信任信息, 来自主机和主机直接交互的经验; 二是推荐信任信息, 来自其他主机 ($k=1, 2, \dots$) 和主机交互得到的直接经验, 对主机来说是间接经验. 二者均来源于“主机对交互方行为结果的判定”. 这个组件要解决的问题是: 怎样把实体交互行为的好坏转化为实体信任程度的高低? 即解决信任的量化表示问题.

(2) 互信数据在实体间的传播

信任传播组件完成主机信任数据之间的交换任务. 凡加入移动 Agent 系统的主机, 均有权利向系统内其他主机询问欲交换主机的信任数据, 同时也有义务向询问者提供自己采集到的关于其他主机的信任数据, 若没有积累被询问到的主机的相关信任数据, 则按指定方式回答.

(3) 互信数据的更新判定

信任进化组件完成信任数据的更新, 要解决的问题是在系统规定的更新周期内, 根据给定的算法对历史信任数据和新采集到的信任数据进行综合权衡与计算, 得到主机最新信任状态. 在每一个主机上主观信任管理模型作为一个自约束单元进行信任信息收集、信任信息交换、信任信息更新, 支持该主机完成对其他主机的信任状态判定.

2.2 恶意信任主机的量化

目前对网络交互实体信任问题的研究中, 基于交互实体的交互行为测量其信任程度的量化与计算中, 通常使用平均值算法, 即对采集到的基础数据求平均值, 该算法简便易用, 但局限性在于无法限制恶意推荐带来的影响. 由于在移动 Agent 系统中, 恶意主机对移动 Agent 带来的危害是灾难性的, 所用算法有必要重点考虑孤立恶意主机, 消除恶意主机影响.

2.2.1 交互主机信任量化方法

我们把持续的系统运行时间划分成相等间隔的考察周期, 每一考察周期称为一个“时间帧”, 用 $\tau(\tau=1,2,\dots,n)$ 表示. 再把交互主机的交互行为转化为其信任程度的量化计算中^[18], 采用高斯可能性分布理论对平均值算法进行改进, 给出一种更优化算法, 算法如下.

算法 1 交互主机信任量化算法.

初始化: 设主机 H_a 收到的关于主机 H_x 的基础数据为: $\{D_1, D_2, \dots, D_k\}$, 其中: $D_i = n_1 / (n_1 + n_2)$, ($0 \leq D \leq 1$), n_1 是考察周期内从 M_i 采集到的关于主机 H_x 的肯定性交互结果次数, n_2 是其否定性交互次数.

第 1 步: 对关于主机 H_x 的推荐数据求平均值和方差分别计算如下:

$$\bar{D} = \frac{1}{k} \sum_{i=1}^k D_i, S^2 = \frac{1}{k} \sum_{i=1}^k (D_i - \bar{D})^2 \quad (1)$$

第 2 步: 令: $\mu = \bar{D}$, $\sigma^2 = S^2$, 根据高斯分布理论, 以 $K(\mu, \sigma^2)$ 为特征参数, 对于一个随机变量 T , 得到 T 的概率密度函数 $p(x)$, 其中 (μ, σ^2) 分别称为高斯分布的期望和方差. 当 $\mu = 0, \sigma^2 = 1$ 时, T 的分布称为标准正态分布.

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} (\sigma > 0), (-\infty < x < +\infty) \quad (2)$$

第 3 步: 可求出随机变量 T 在 $(-\infty, v), (v, +\infty)$ 范围内出现的可能性. 其中, $P(\leq V)$ 表示 T 在小于等于 v 的范围内出现的可能性, $P(> V)$ 表示 T 在大于 v 的范围内出现的可能性.

$$P(\leq v) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{v-\mu} e^{-\frac{x^2}{2}} dx, P(> v) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v-\mu}{\sigma}}^{\infty} e^{-\frac{x^2}{2}} dx$$

对于给定区间值 (v_1, v_2) , T 在指定区间出现的可能性:

$$P(v_1, v_2) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v_1-\mu}{\sigma}}^{\frac{v_2-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx, (v_1 < v_2) \quad (3)$$

第 4 步: 随即变量 T 在指定范围 $(v,1), [0,1]$ 中出现的可能性分别为:

$$P(v, 1) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx,$$

$$P(0, 1) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{0-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \quad (4)$$

第 5 步: 求出随即变量 T 在 $(v,1)$ 范围内与在 $[0,1]$ 范围内出现可能性的比值:

$$P_{ax}(v) = \frac{P(v, 1)}{P(0, 1)} = \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx / \int_{\frac{0-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \quad (5)$$

2.2.2 主机信任度的量化进化

随着时间的推移, 关于主机 H_x 的推荐信任程度被更新, 第 $n+1$ 时间帧的推荐信任程度来自第 n 时间帧的推荐信任程度和第 $n-1$ 时间帧的推荐信任程度. 采取继承部分历史信任数据, 添加部分当前信任数据的更新策略, 用因子 $\beta(\tau)$ 控制和调整更新速度.

$$T_{x-rec}^{n+1} = T_{x-rec}^n + \beta(\tau) (P_{x-rec}^n - T_{x-rec}^n),$$

$$(0 \leq \beta(\tau) \leq 1) \quad (6)$$

当 $\beta(\tau)=1$ 时, 使用当前信任数据, 更新最快.

当 $\beta(\tau)=0$ 时, 使用历史信任数据, 更新最慢.

当 $0 < \beta(\tau) < 1$ 时, 如 $\beta(\tau)=0.5$ 时, 历史信任数据和当前信任数据各取一半.

$$T_{x-rec}^{n+1} = T_{x-rec}^n + 0.5P_{x-rec}^n, (\beta(\tau) = 0.5)$$

$\beta(\tau)$ 因子的选择对于不同的移动 Agent 系统可以有所不同. 更新是一个过程, 需要给定合适的更新周期. 对于某些实时应用系统, 更新速度太慢, 数据陈旧, 导致信任程度评价结果失去适时性, 预测偏差增大; 但更新速度太快, 将引起系统不稳定或震荡. 后面将给出关于 $\beta(\tau)$ 更新速度的一些模拟实验与讨论.

2.3 主机经验信任计算

基于交互经验的互信计算方法事实上, 主机 H_a 对主机 H_x 的信任评价主要受直接交互经验的影响. 如果主机 H_a 与主机 H_x 已经有过交互经验, 用上一节给出的算法对直接信任基础数据进行计算, 主机 H_a 可由直接经验获得对主机 H_x 的信任程度, 这里称为直接信任程度, 记为 $T_{x-dir}(v)$.

2.3.1 基于交互经验的互信计算方法

把持续的系统运行时间划分成相等的统计周期, 每一考察周期称为一个“时间坝”, 用 $\tau(\tau =$

$1, 2, \dots, k$) 表示. 对每一时间帧 τ 内, 假设 H_a 和 H_x 直接交互 $n_1 + n_2$ 次, 肯定性事件 n_1 次, 否定性事件 n_2 次. 定义直接经验数据 D_{ax} 由式 (7) 计算.

$$D_{ax} = \begin{cases} \frac{n_1}{n_1+n_2} (n_1 + n \neq 0) \\ 0.5 (n_1 + n_2 = 0) \end{cases} \quad (0 \leq D_{ax} \leq 1),$$

$$(\tau = 1, 2, \dots, n) \quad (7)$$

在 k 个连续时间帧内, 对:

$$\bar{D}_{ax} = \frac{1}{k} \sum_{i=1}^k D_i, S_{ax}^2 = \frac{1}{k} \sum_{i=1}^k (D_i - \bar{D}_{ax})^2 \quad (8)$$

令: $\mu = D_{ax}, \sigma^2 = S_{ax}^2$, 有 $K(\mu, \sigma)$, 根据上述高斯可能性分布理论, 可得到主机 H_a 对 H_x 的直接信任程度 $T_{x-dir}^\tau = P_x^\tau(v)$. 下面讨论随着时间的推移直接信任程度的更新.

2.3.2 经验信任度的更新

随着时间的推移 ($\tau = 1, 2, \dots, n$), 直接信任程度被更新, 第 $n+1$ 时间贯的直接信任程度来自第 n 时间贯的直接信任程度和第 $n-1$ 时间贯的直接信任程度. 采取继承部分历史信任数据, 添加部分当前信任数据更新策略, 用因子 $\lambda(\tau)$ 控制和调整更新速度.

$$T_{x-dir}^{n+1} = T_{x-dir}^n + \lambda(\tau) (P_{x-dir}^n - T_{x-dir}^n),$$

$$(0 \leq \lambda(\tau) \leq 1) \quad (9)$$

当 $\lambda(\tau)=1$ 时, 使用当前信任数据, 更新最快.

当 $\lambda(\tau)=0$ 时, 使用历史信任数据, 更新最慢.

当 $0 < \lambda(\tau) < 1$ 时, 如 $\lambda(\tau)=0.5$ 时, 历史信任数据和当前信任数据各取一半.

$$T_{x-dir}^{n+1} = 0.5T_{x-dir}^n + 0.5P_{x-dir}^n, (\lambda(\tau) = 0.5)$$

同样, $\lambda(\tau)$ 因子的选择对于不同的移动 Agent 系统可以有所不同. 需要给定适当的更新周期 τ . 如果更新速度太慢, 数据陈旧, 导致信任评价结果失去适时性, 预测偏差增大; 如果更新速度太快, 将引起系统不稳定或震荡. 后面将给出关于 $\lambda(\tau)$ 更新速度的一些模拟实验与讨论.

2.4 主机信任的整体评价

对移动 Agent 系统中交互主机信任程度测量、评价及预测的准确性是优化新任管理的基础. 更一般的情况是, 同时考虑直接信任数据和推荐信任数据, 更为合理的算法是将与已获得的主机 H_k 的直接信任程度和推荐信任程度进行综合运算, 最后可得出主机 H_a 对主机 H_k 的信任程度的综合评价结果. 2.2 节和 2.3 节分别讨论了推荐信任程度和直接信任程度的计算与更新. 在此基础上, 本节研究信任程度综合计算方法以及信任进化速度的控制问题^[17].

信任度根据公式 (10) 给出的方法进行更新. 该

方法实现两个功能: 第一, 如果实体 H_a 在与实体 H_x 多次交互中, 发现 H_x 持续保持好的行为 (肯定事件), H_x 的信任度 T_x 将保持持续增长, 趋向最大值 1, 如果实体 H_x 有恶意行为, 它的信任度将迅速下降; 第二, 在时间坝 $n-1$ 和 n 之间如果信任度有一个变化大的变化量, 这个大的变化量将对 H_x^n 产生个大的影响, 反之也成立. $\sigma(\tau)$ 称为更新系数, 控制更新速度.

$$T_x^{n+1} = T_x^{n-1} + \sigma(\tau) (T_x^n - T_x^{n-1}) \quad (10)$$

3 仿真实验分析

下面通过一系列的模拟实验对上述动态信任度量与评价方法中所给出的式 (1) 式 (10) 的关键性质和参数选择进行验证. 我们通过 Calheiros 等人^[19] 提出的一种通用且可扩展的仿真框架 CloudSim 进行模拟实验, 该框架可以对新兴的云计算基础架构和应用程序服务进行建模、仿真和实验. 通过对用户提交的多个作业进行模拟, 并且每个作业都具有不同的计算参数需求, 例如不同的处理器速度, 硬盘存储器, 内存和可变带宽和延迟等网络参数.

3.1 实验情况

实验一验证式 (5) 算法, 其结果如图 3 所示. 设信任需求门限值为 T_o , 令 $v = T_o$, 可以看到在计算基值 v 取不同数值时, 主机 H_x 的直接 (或推荐) 信任程度 T_x 的变化情况 (取决于所采集的数据是直接还是推荐信任数据). 可以看出 T_o 值越高, 对满足 $T_x > T_o$ 的主机的期望值要求也越高, 满足条件的主机数越少. 例如, 当计算基值 $v =$ 信任门限 $T_o = 0.8$ 时, 由图 3 可以看出只有主机交互行为的数学期望值 $\mu > 0.6$ 的待选主机才能列入可信交互对象.

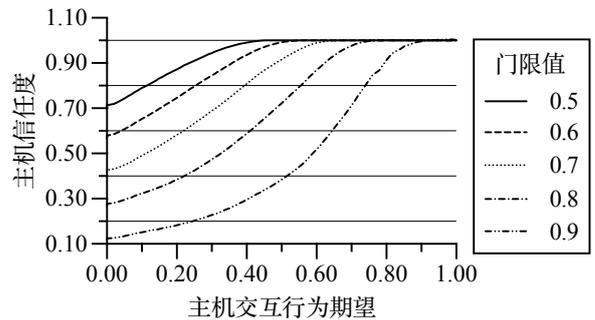


图 3 信任门限不同时主机信任度与其交互行为间的关系

实验二验证式 (6), 其结果如图 4 所示. T_{ax} 在两个时间贯之间的变化量 $0 < \Delta T_{ax} < 1$, 参数 w 控制 T_{ax} 进化速度. 实验结果显示: 当系数 $w = 1$ 时, $\sigma(\tau)_{\min} = 0$, 进化速度最慢, $\sigma(\tau)_{\max} = 0.46$ 进化速度最快, 这时 ΔT_{ij} 在下一个时间坝中对 T_{ax} 值的最大影响是 0.46.

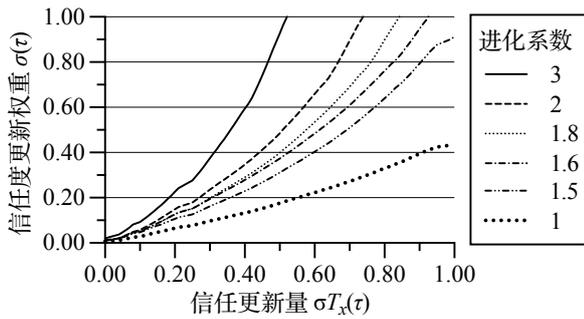


图4 信任更新权重 $\sigma(\tau)$ 在不同进化系数时的变化趋势

式(8)、(9)给出了主机 H_a 基于对主机 H_x 的直接经验数据,对有不良或恶意推荐行为的主机 M_k 进行孤立的算法.仿真模拟结果如图5、图6所示.

由图5可以看出推荐者 M_3 对主机 H_x 的推荐数据与主机 H_a 对 H_x 的直接经验数据一致性最好,而推荐者 M_1 和 M_2 的推荐数据与 H_a 的直接经验数据一致性较差,分别远高于和远低于 H_a 的直接经验数据.依据所用算法, H_a 可以得出结论: M_3 更可信,而 M_1 和 M_2 可能有恶意推荐嫌疑.

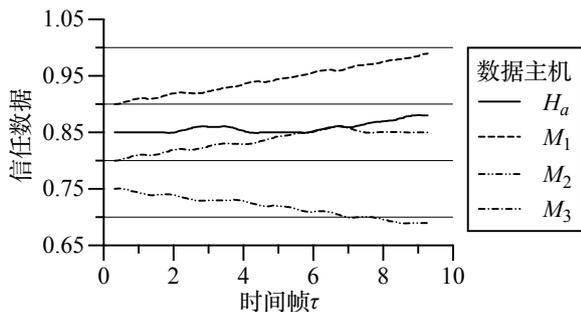


图5 推荐者数据与直接经验数据的一致性

由图6可知,根据式(10),在考察过程中,由于推荐者 M_3 对主机 H_x 的推荐数据与主机 H_a 对 H_x 的直接经验数据一致性最好,主机 H_a 对他的直接信任程度逐渐提高,提高幅度取决于致性程度,一致性程度越高提高越快;而推荐者 M_1 和 M_2 的推荐数据与 H_a 的直接经验数据一致性较差^[20],无论远高于或远低于 H_a 的直接经验数据,主机 H_a 对它们的直接信任程度逐渐降低,降低幅度取决于偏差程度,偏差程度越大,降低越快.因此式(10)算法的功能能有效孤立恶意推荐主机.

因此,可以得出如下结论:模拟实验结果验证了本文给出的“公信主机选择算法”、“孤立恶意推荐者算法”以及“信任度综合计算算法”的正确性^[21].可以用来评价移动 Agent 系统中待交互主机的主观信任状态,并预测待交互主机在下一个时间帧的可信程度.所给出的一系列算法能够激励可信主机,孤立恶意主机,具有“惩恶扬善”的作用.能够有效的对移动 Agent 系统进行主观信任动态管理.

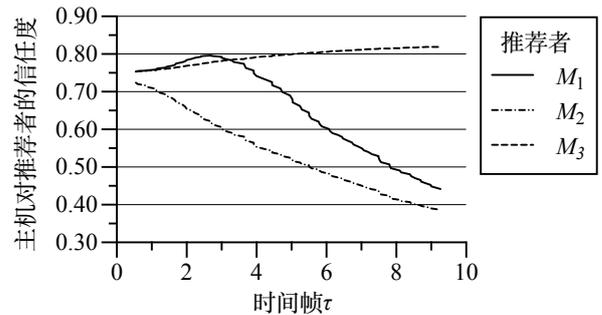


图6 推荐者信任数据 T_{mk} 的比较

3.2 与现有信任模型比较

QoS 信任模型于 2015 年提出被 Manuel 等人提出^[22],是一种通过可用性,可靠性,周转效率和数据完整性四个参数对主机信任值进行计算的新型信任模型.并分别给出了上述四种属性的计算方式定义,通过其定义信任管理系统对云计算资源的信任进行管理.在本文算法与 Manuel 构造的 QoS 算法相比,本文的移动 Agent 系统信任管理机制具有下列优点:

(1) 模型表达能力好

本文基于 Gauss 可能性分布理论给出的算法 $P(v, \mu, \sigma)$ 再把执行主机和移动 Agent 交互行为量化为其信任度的计算中,可以选择计算门限值 v , 算法 $P(v, \mu, \sigma)$ 中的特征参数 (μ, σ) 分别是数学期望和方差,不仅能度量主机信任程度高低,而且能表示主机信任程度的稳定性,根据算法 $P(v, \mu, \sigma)$ 使用推荐信任数据和直接数据可分别计算出推荐信任度、直接信任度,在此基础上进行综合信任度的计算,具有更强的灵活性和表达力.

(2) 算法针对性强

本文基于直接信任度给出孤立恶意(交互或推荐)主机算法,更突出移动 Agent 系统主观信任判定需求.表现为以下两点:(1) 主机 H_x 对主机 H_a 无恶意行为并不能代表对主机 H_b 无恶意行为,反之也一样,主机 H_a 有理由认为对 H_x 的直接信任度比推荐信任度更可信;(2) 主机 H_a 根据推荐信任度与直接信任度的一致性好坏来判定是不是恶意推荐者,与直接信任度值相比过高的推荐者和过低的推荐者都有恶意推荐嫌疑,主机更信任与自己直接信任度具有较好一致性的推荐者.本文给出的孤立恶意主机算法充分体现了以主机 H_a 直接交互经验为参照值,针对 H_a 孤立恶意主机的效果较好.

(3) 初始信任的动态设置

对于刚刚加入移动 Agent 系统的新主机 H_a ,虽然没有直接经验数据,但能够立即获取 H_x 的推荐信任数据,使用“公信主机选择算法”选择可信任交互对象,具有较好的自启动性.

4 结论

本文将移动 Agent 系统中的信任问题划分为客观信任和主观信任两部分分而治之, 在分析 SPKI 相关证书的使用方法的基础上, 在基于 SPKI 的移动 Agent 系统客观信任对等管理框架下, 研究解决移动 Agent 系统中的主观信任动态管理方法问题, 分析了移动 Agent 系统中的实体信任需求, 提出了主要由信任形成组件、信任传播组件、信任进化组件三个信任组件组成的主观信任动态管理模型. 基于 Josang 网络信任管理模型中提出的描述和度量信任的基本思想, 在移动 Agent 系统中引入事实空间和观念空间两个基本概念. 将移动 Agent 系统事实空间中“实体交互行为结果的好坏”转化成观念空间中“实体可信程度的高低”. 提出了主观信任动态管理算法. 最后, 通过模拟实验验证了所提算法度量移动 Agent 系统中主机信任程度的可行性, 以及对形成信任机群提高移动 Agent 系统中交互的安全程度的有效性.

参考文献 (References)

- [1] Boss G, Malladi P, Quan D, et al. Cloud computing. IBM white paper, 2007, 2009.
- [2] Whaiduzzaman M, Sookhak M, Gani A, et al. A survey on vehicular cloud computing[J]. Journal of Network and Computer applications, 2014, 40: 325-344.
- [3] Gray R, Cybenko G, Kotz D, et al. Mobile agents and state of the art[J]. Handbook of Agent Technology. AAAI/MIT Press, Cambridge, 2012.
- [4] Busi N, Padovani L. A distributed implementation of mobile nets as mobile agents[C]. International Conference on Formal Methods for Open Object-Based Distributed Systems, 2005: 259-274.
- [5] Gambetta D. Trust: Making and breaking cooperative relations[J], 1988.
- [6] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management[C]. Proceedings 1996 IEEE Symposium on Security and Privacy, 1996: 164-173.
- [7] Povey D. Developing electronic trust policies using a risk management model[C]. International Exhibition and Congress on Network Security, 1999: 1-16.
- [8] Abdul-Rahman A, Hailes S. A distributed trust model[C]. Proceedings of the 1997 workshop on New security paradigms, 1998: 48-60.
- [9] Abdul-Rahman A, Hailes S. Using recommendations for managing trust in distributed systems[C]. Proceedings IEEE Malaysia International Conference on Communication, 1997.
- [10] Ellison C. SPKI certificate theory”, Request for Comments 2693, Network Working Group, IETF, Reston, VA, September[J], 1999.
- [11] Ellison C, Frantz B, Lampson B, et al. SPKI certificate theory[R]. RFC 2693, 1999.
- [12] Ellison C. RFC2692: SPKI Requirements: RFC Editor, 1999.
- [13] 黄刘生, 田苗苗, 黄河. 大数据隐私保护密码技术研究综述 [J]. 软件学报, 2015, 26(04): 945-959.
(Huang L S, Tian M M, Huang H. Preserving privacy in big data: a survey from the cryptographic perspective[J]. Journal of Software, 2015, 26(04): 945-959.)
- [14] 蒋伟进, 钟珞, 张莲梅, 史德嘉. 基于时序活动逻辑的复杂系统多 Agent 动态协作模型 [J]. 计算机学报, 2013, 36(05): 1115-1124.
(Jiang W J, Zhong L, Zhang L M, et al. Dynamic Cooperative Multi-Agent Model of Complex System Based-on Sequential Actions' Logic[J]. Chinese Journal of Computers, 2013, 36(5): 1115-1124.)
- [15] Jiang W, Zhang L, Pu W. Research on grid resource scheduling algorithm based on MAS cooperative bidding game[J]. Science in China F, 2009, 52(8): 13021320.
- [16] Jiang W J, Wang Y, Jiang Y R, et al. Research on mobile Internet mobile agent system dynamic trust model for cloud computing[J]. China Communications, 2019, 16(7): 174-194.
- [17] Jiang W J, Chen J H, Xu Y H. A Network Celebrity Identification and Evaluation Model Based on Hybrid Trust Relation[J]. Tehnički vjesnik, 2018, 25(4): 1136-1143.
- [18] 吕玲玲, 杨志鹏, 张磊. 基于合约设计的移动边缘计算任务卸载策略研究 [J]. 控制与决策, 2019, 34(11): 2366-2374.
(LYU L L, Yang Z P, Zhang L. Contract theory based task offloading strategy of mobile edge computing[J]. Control and Decision, 2019, 34(11): 2366-2374.)
- [19] Calheiros R N, Ranjan R, Beloglazov A, et al. CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms[J]. Software: Practice and experience, 2011, 41(1): 23-50.
- [20] Wang S Z. Research on Trust Security and Resource Allocation of Mobile Agent System in Cloud Computing Environment[M]. China Fortune Press, 2012.
- [21] Haiyang H, Runhua L, Hua H. Multi-objective optimization for task scheduling in mobile cloud computing[J]. Journal of Computer Research and Development, 2017, 54(9): 1909.
- [22] Manuel P. A trust model of cloud computing based on Quality of Service[J]. Annals of Operations Research, 2015, 233(1): 281-292.

作者简介

蒋伟进(1964—), 男, 二级教授, 博士, 从事社会计算、群智协同、分布式网络等研究, E-mail: jwjnudt@163.com;
吕斯健(1996—), 男, 硕士生, 从事分布式计算、网络安全等研究, E-mail: me@lvsijian.cn.