

iVCE 中基于可信评价的资源调度研究

邓晓衡^{1),2)} 卢锡城¹⁾ 王怀民¹⁾

¹⁾(国防科技大学计算机学院并行与分布式处理国家重点实验室 长沙 412008)

²⁾(中南大学信息科学与工程学院 长沙 410083)

摘 要 随着网格计算、P2P、Web 服务技术在电子商务、电子政务领域应用的不断扩展,基于 Internet 的资源共享的安全可信问题变得越来越重要.该文在基于 Internet 的虚拟计算环境(Internet-Based Virtual Computing Environment, iVCE)的资源共享的用户与资源关于身份可信、能力可信、行为可信的信任模型的基础上,提出了一种可信优化的资源调度算法.算法基本思想在于根据用户对资源可信的需求,对虚拟计算环境中的自主元素可信度综合考察与评价,以用户可信满意度为优化调度目标调度资源,进而基于 min-min 算法优化任务执行时间,满足了资源调度的可信保障,同时具有较好的性能.仿真实验结果表明可信优化调度算法能够在 iVCE 的信任度效益,最早完工时间,失效服务请求数,资源利用率等性能参数方面明显优于 min-min 和 max-min 算法.

关键词 虚拟计算环境;可信计算;资源调度

中图法分类号 TP393

Study on Trust Evaluation Based Resource Scheduling in iVCE

DENG Xiao-Heng^{1),2)} LU Xi-Cheng¹⁾ WANG Huai-Min¹⁾

¹⁾(National Key Laboratory for Parallel and Distributed Processing, School of Computer, National University of Defense Technology, Changsha 410073)

²⁾(College of Information Science and Technology, Central South University, Changsha 410083)

Abstract With the development of grid computing, P2P, Web Service technologies, trust and security become more and more important in resource sharing on the Internet. Based on identity, capability and behavior trust model of resource sharing in the Internet-Based Virtual Computing Environment(iVCE) between user and resource, A trust optimizing scheduling algorithm(TOS) is proposed. TOS integratively evaluates trust degree of automatic entity according to the requirement of the user in iVCE; users' trust satisfaction degree optimization is the goal of TOS. Min-min is imported to optimize task execution time. So many performance parameters such as total trust utilities, makespan, failed task rate, and system resource utilities, are improved compared with min-min and max-min algorithms in the simulation.

Keywords virtual computing environment; trust computing; resource scheduling

1 引 言

Internet 将异构网络以及异构资源连接起来,

为有效利用资源,网格计算、P2P 系统、Web 服务系统都应运而生,形成一个个基于 Internet 的虚拟计算平台(Internet-Based Virtual Computing Environment, iVCE),用户因此可以透明地访问互联网

资源. 围绕如何构建高效、安全可信的虚拟计算环境, 我们基于互联网资源特性提出了 iVCE 的基本概念和体系结构^[1], 适应了互联网发展的规律, 旨在实现资源的有机聚合与协同.

开放网络环境可信任问题的日益突出, 安全可信的资源共享是 iVCE 所重点关注的关键技术问题. 本文在 iVCE 的信任模型基础上提出了一种改进的 min_min 启发式的可信资源调度算法. 该算法针对 iVCE 中的用户、资源的身份可信、能力可信、行为可信分别进行度量与评价, 然后根据服务对于可信指标的需求, 调节其权重, 确立调度优化目标, 实现资源可信调度, 满足了用户对资源的不同需求, 提高了 iVCE 的适应性.

本文第 2 节介绍了可信计算与资源调度的相关工作; 第 3 节阐述了 iVCE 资源聚合与协同的基本思想与概念以及可信安全保障体系; 第 4 节详细论述了基于 iVCE 可信模型的资源调度机制; 第 5 节介绍可信调度机制实验验证方案及实验结果; 最后为总结和进一步的工作展望.

2 相关工作

处理机调度一直以来就是计算机科学最重要的研究领域之一, 其中以基于多处理机系统研究最为广泛深入. 处理机调度不仅需要考虑任务之间的通信代价, 还要考虑调度环境的异构性带来的影响、链路竞争、网络拓扑结构的松散易变性等问题. 如何把复杂应用程序的所有任务调度到多处理器系统, 并追求最小的整体执行时间的问题是一个非常难解的问题, 是 NP 完全问题. 因此, 研究者一般都是采用设计启发式算法获得一个较优解, 形成了表调度、基于任务复制、基于任务聚类 and 基于随机搜索调度算

法的并行静态调度算法^[2].

在同构的多处理机系统中尚且如此, 而在网络系统、P2P 系统以及 Web 服务系统等虚拟计算环境中, 资源具有自治性、异构性、动态性、分布性等特性, 使得资源的调度具有更大的挑战, 需要额外考虑资源可能遭遇的失效, 资源是否可信安全, 资源是否满足用户的 QoS 需求. 在 iVCE 中如果忽略了资源、用户的可信问题, 那么用户恶意行为或破坏性行为将对整个计算系统性能产生巨大影响, 因此资源的管理与调度过程必须既要考虑服务性能问题, 也必须关注用户可信安全问题. Foster 等设计了面向计算服务网格的安全架构^[3], Butt A R 等提出细粒度访问控制模型来保障服务提供者的安全^[4]. 资源调度方面, 研究者将 QoS 和“信任”等资源属性引入网格任务调度, 从而为安全、有效地利用分布的网络资源提供支持^[5]. Abawajy^[6] 提出通过在不同站点复制作业的多个副本, 实现分布式环境下资源失效的容错调度, 从而保证作业在网格环境下可靠运行. Adulrahman 提出一个信任评估的数学模型, 并给出一种虚拟社区中基于信誉的信任的解决方案. Song^[7] 和 Li^[8] 提出了信任 QoS 驱动的网格信任调度框架和算法. 文献[9]提出一种网格环境下基于信任模型的动态级调度. 文献[10]基于性能、信任 QoS 两个因素提出一种启发式网格资源调度算法, 在保证网格性能的同时能提高安全性. 目前, 网格服务调度研究更多地集中在改善 QoS 性能指标方面, 可信研究更多地集中于跨域授权、身份认证、访问控制和信任管理方面, 缺乏有效的模型将网格服务质量、安全可信管理有机结合起来实现资源的高效安全管理. 我们在这方面进行了探索^[11], 提出了互联网环境软件可信模型, 为研究虚拟计算环境资源调度奠定了一定基础.

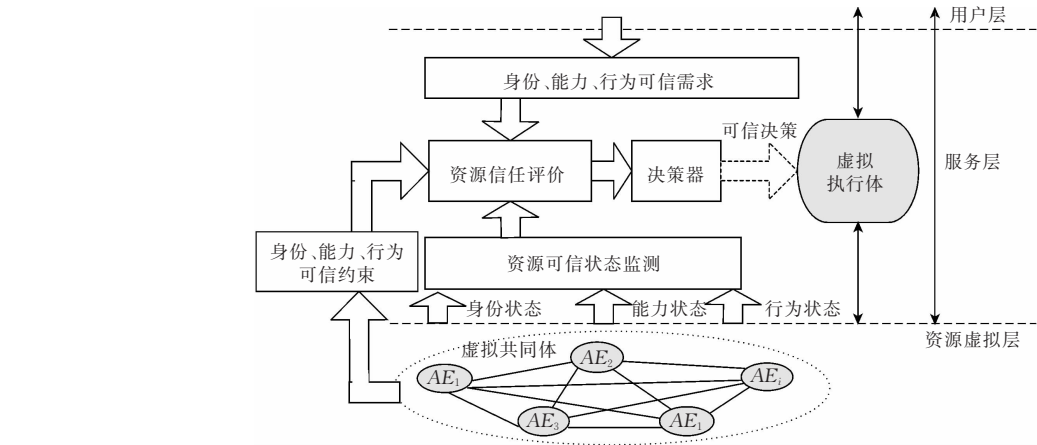


图 1 iVCE 可信保障体系

3 iVCE 的可信安全保障体系与模型

3.1 iVCE 的可信保障体系

基于虚拟计算环境资源协同共享的需求与内在联系提出以身份可信、能力可信和行为可信为核心的可信保证体系^[1],可根据系统状态和应用需求形成对系统的可信预期,据此构造保障自主元素身份可信、能力可信和行为可信的基本框架,协调和控制自主元素的活动,支持系统服务目标的实现.各基本概念在 3.2 节中详述,结构如图 1 所示.

3.2 iVCE 可信模型

根据虚拟计算环境的资源自主协同实现共享过程中的自主元素、虚拟共同体、虚拟执行体的相互关系以及三者内在的特征与属性,我们建立了虚拟计算环境的可信计算模型,下面给出了模型的完整定义.

定义 1(虚拟计算环境 iVCE). 虚拟计算环境 iVCE 为一个三元组, $iVCE=(AE,VC,VE)$,其中, AE 为自主元素(Autonomic Element)的集合,是虚拟计算环境中单个资源或多个资源组合后的虚拟化和自主化的抽象表示总和,其中的每个自主元素是虚拟计算环境进行可信安全资源共享的主体; VC 为虚拟共同体(Virtual Commonwealth)的集合,是虚拟计算环境中具有不同兴趣和不同应用背景的资源组的总和,一个自主元素必须满足虚拟共同体一定的身份认证规则和授权才能与其他自主元素交互信息和协同工作实现资源共享; VE 为虚拟执行体(Virtual Executor)的集合,虚拟执行体是与特定计算应用或任务相绑定的所有自主元素与任务相关的状态集合.它是虚拟计算环境的基本运行管理单位,对于任意虚拟执行体 $ve, ve \in VE$,其中的一个或多个自主元素必须满足 iVCE 的应用可信需求约束,进而实现资源管理与调度,而达到协同共享的目的.

定义 2(自主元素 AE). $AE=(CP,TR)$,其中, CP 表示自主元素的公共属性,即任何自主元素均具有的属性,如自主元素 id、虚拟共同体 id、自主元素名称 name 及描述 des 等、自主元素功能 fun、自主元素类别 class 等; TR 表示自主元素的可信属性,在虚拟共同体以及构建虚拟执行体时信息交互过程中表现出来的可信性.

定义 3(可信性 TR). $TR=(IT,CT,BT)$,其中, IT 是自主元素所具有的身份信任度,即自主元素在 iVCE 中的关于身份认证、授权以及授权委托等信息; CT 是自主元素的能力信任度,包括自主

元素在 iVCE 中声称的其功能、功能相关性能属性以及提供服务所具备的可靠性、可用性等信息; BT 是自主元素的行为信任度,自主元素声称其在 iVCE 的各不同虚拟共同体中所要遵守的组织约定,它既包含 iVCE 对于自主元素的特定行为约束,也包括在自主元素相互间自主协同过程中所应遵循的交互规范,如共享资源时不能未经同意退出或减少共享的资源等.

定义 4(虚拟共同体 VC). $VC=(AE,REQ)$,其中, AE 为基于某一特定计算任务而组成共同兴趣组的自主元素的集合,它们实质上一般为参与到某一互联网服务中来的主机、设备或其他网络资源; REQ 为成功实现某一互联网服务对于资源的功能、服务质量、可信安全等需求的集合.

定义 5(虚拟执行体 VE). $VE=(AE,TC)$,其中, AE 是指为某一用户的一次请求提供互联网服务而相互协同、紧密相关的自主元素的集合; TC 为将相关自主元素聚合共同完成某一计算任务、服务必须遵循的可信约束条件的集合.

定义 6(信任满意度 SAT). $SAT=(IS,CS,BS)$,信任满意度反映了自主元素相互之间交互信息后对对方的可信任状况作出的满意度评判,由 3 个部分组成,其中, IS 为身份信任满意度,表示自主元素对目标自主元素的真实身份、所拥有的授权或授权委托符合了自己预设的要求,其取值为 0 或 1,要么满意,否则不满意; CS 为能力信任满意度,表示自主元素对目标自主元素的服务能力的满意程度,目标自主元素的服务功能,以及性能指标是否满足需求,性能指标一般具有一个最低门限值,若目标自主元素任一指标未满足,其满意度为 0,所有单个性能指标最低要求满足后,则满意度为各单个性能指标的加权求和,其取值范围为 0~1 之间,各权值具有归一化特征; BS 为自主元素对目标自主元素的行为的可信程度的一种主观感受,它表现为对自主元素的完全不信任到完全信任过程,主观感受为完全不满意到完全满意,其取值为 0~1 之间的任意值,与历史的、当前的记录的行为可信度有关,还与调度情况有关,自主元素没有被调度,则行为满意度维持不变,如自主元素被调度,则任务处理的状况将成为更新当前行为满意度的依据.

上述的 iVCE 可信保证体系为资源按需聚合和自主协同的安全性、可依赖性及协同行为的可信性提供保证,可信模型则以资源的可信聚合为基线将 iVCE 中的自主元素、虚拟共同体、虚拟执行体之间在身份、能力、行为可信的角度建立了紧密的联系.

接下来将围绕可信资源聚合,研究 iVCE 中的资源管理调度.

4 iVCE 中基于可信评价的资源调度机制

4.1 自主元素可信度评价

4.1.1 自主元素的身份可信评价

自主元素通常隶属于独立的自治的管理域(administrative domain),不同管理域分别采用各自的策略管理内部资源和用户.根据定义 3,身份信任度反映自主元素是否具有真实可信的身份,参与一个任务执行时是否相对应的权限;一个自主元素自主加入到一个虚拟共同体中,就表明其已经通过虚拟计算环境的身份认证鉴别机制,具有身份的真实性;要实现虚拟计算环境可信安全的资源共享,还要确信自主元素在执行任务时具有足够的权限.目前,在网格、P2P 等分布计算环境中,分布式授权与信任委托是两种主要的手段.在授权语言与 CCA 算法研究方面的主要有 PolicyMaker^[12],KeyNote^[13],SP-KI/SDSI^[14]和 DL^[15]等,国内徐锋将信任度评估模型集成到信任管理系统中增加系统的动态适应性^[16].Hong 等基于 RT 研究了 ABAC 策略的委派深度约束问题.信任管理技术还有待深入研究,尤其在互联网范围中如何控制权限传播问题等^[17].我们提出一种基于契约和协商的授权方法,同时,针对信任委托中除了对委托临时性限制和角色关联性限制的需求外,还有对部分委托限制和委托传播限制的需求.我们提出虚拟计算环境中基于层次角色的受限委托模型 HRRDM^[18],构建角色树解决角色部分委托问题,构建委托传播树以解决委托传播限制问题,构建角色委托链以解决委托传播的依赖性问题,提出委托凭证来支持层次角色委托的临时性、关联性、部分性、传播性需求,并有效地支持虚拟计算环境委托角色授予与撤消的动态特性.基于 HRRDM,可以满足虚拟计算环境下访问控制决策的需求,用以评估自主元素的身份可信度,为虚拟计算环境中的资源管理调度提供支撑.那么评价自主元素的身份可信时,身份真实性和权限满足性都是资源调度的必要条件,以 IT_{ij} 表示自主元素 AE_j 对于自主元素 AE_i 的身份可信度,如果两者完全满足则 $IT_{ij}=1$,否则 $IT_{ij}=0$,则自主元素身份满意度对应为 $IS_{ij}=1$ 和 $IS_{ij}=0$.iVCE 中资源调度时,只能调度身份可信度为 1 的自主元素,否则身份存在安全隐患,可能为非法用户.

4.1.2 自主元素的能力可信评价

自主元素的能力可信是直接反映服务、资源的 QoS 参数值是否达到其承诺的水平的一个综合因素,首先它必须在功能上满足某一互联网服务的需求,当一个自主元素通过认证加入到某一虚拟共同体,表明它与其他成员兴趣相同,由虚拟计算环境的服务部署机制,自主元素就拥有了相应的服务功能,但自主元素的服务能力受到很多具体因素的影响,包括自身的一些属性,如计算速度、存储容量、系统的可靠性、稳定性等,还有与环境相关的属性,如端到端的传输带宽、网络延迟、网络抖动等等.而不同虚拟共同体提供服务不同,对自主元素的能力可信的参数要求又有所侧重,比如计算密集型服务可能不考虑存储容量参数,因为它对存储能力的要求比较低,很容易得到满足;反之,存储密集型服务可能不考虑计算速度.无论服务侧重于什么样的能力可信,自主元素的 QoS 参数将为自主元素的能力可信度评价提供依据.

对于一个虚拟计算环境应用 A ,自主元素 AE_j 对于自主元素 AE_i 的能力可信度表示成 n 维的布尔向量 CT_{ij}^C , n 为所有能力可信参数的类. C 表示 AE_i, AE_j 在虚拟计算环境中所属相同的虚拟共同体的自主元素的集合,若 $CT_{ij}^C[k]=1$,则表示该自主元素的第 k 个分量能力可信指标满足用户的需求;反之,若 $CT_{ij}^C[k]=0$,则第 k 个分量所对应的能力可信度不能满足用户的需求.

当多个自主元素为某一个用户请求的任务进行协同,准备相互绑定成为一个虚拟的服务实体,构建虚拟执行体时,如果自主元素不能满足用户的最低要求,用户满意度就为 0;当用户提交服务请求时,其对资源的能力可信所含的各性能参数的最低要求都被满足,才能认为该自主元素有能力为该任务提供服务,而接纳进入虚拟共同体.我们用特征值 CS'_{ij} 来表征自主元素能力可信向量 CT_{ij}^C 包含的所有值为 1 的分量所对应的能力可信参数的最低要求是否都被满足:若都被满足, $CS'_{ij}=1$;否则, $CS'_{ij}=0$. cs_{ij}^k 为自主元素 AE_j 对于自主元素 AE_i 的能力可信度的 $CT_{ij}^C[k]$ 分量所对应能力可信参数的用户满意函数,自主元素能力可信的用户满意度 CS_{ij} 表示如下:

$$CS_{ij} = \frac{\sum_{k=1}^n CT_{ij}^C[k] \cdot cs_{ij}^k}{n} \quad (1)$$

因此,自主元素能力可信的总体评价为 $CS'_{ij} \cdot CS_{ij}$.当用户提出的服务能力信任需求有一个不能

被满足时,特征值 $CS'_{ij}=0$,则 $CS'_{ij} \cdot CS_{ij}$ 也为 0. 所以,用户的能力信任需求的最低要求没有被满足,服务能力满意度对于用户来说就为 0,那么该自主元素就不能绑定为虚拟执行体的成员,当最低需求满足后, $CS'_{ij} \cdot CS_{ij}$ 可以反映出该自主元素服务能力强弱,可以为资源优化调度提供参考.

4.1.3 自主元素的行为可信评价

在人类的社会生活中,一个社会实体,如个人、公司、产品、单位等,长期以来与其他社会元素交往行为产生的信誉是人们以后决定是否与其协作共事的重要依据,为了防止行为不端的社会实体对其他社会实体产生危害,各国开始对社会实体的信任度进行评价和发布,激励实体努力规范自己的品行,获得良好声誉,赢取更多的合作机会. 在互联网环境中,所有连接在一起的设备与系统构成一个虚拟社会,林闯等提出可信的网络是网络系统的行为及其结果是可以预期的,能够做到行为状态可监测,行为结果可评估,异常行为可控制^[19]. 在虚拟计算环境中,自主元素成为了网络社会里服务提供者、资源、客户、管理者等的载体,自主元素代替它们完成了在 iVCE 中的各种行为,因此其必须遵循 iVCE 中各不同虚拟共同体中所要遵守的行为规则,既包含 iVCE 对于自主元素的特定行为约束也包括在自主元素相互间自主协同过程中所应遵循的信息交互规范. 然而,在虚拟计算环境中,各自主元素也如同社会成员一样,不可能完全遵循约定的规则,甚至可能恶意地破坏 iVCE 系统,影响其他自主元素使用该服务,我们应该根据自主元素遵守规范的程度,客观评价其行为的可信度,由于 iVCE 中资源的动态性,信任评估中存在不诚实反馈等现象,导致信任评价失真,针对现有的信任模型对自主元素行为改变的动态适应能力和对反馈信息的有效聚合能力支持不足,采用基于时间帧的动态信任模型^[20],使用时间帧标示出经验和推荐的时间特性,引入近期信任、长期信任、累积滥用信任和反馈可信度四个参数计算自主元素信任度,并通过反馈机制动态调节各参数,提高信任模型的动态适应能力.

在 iVCE 中,行为可信度是我们选择和调度资源的重要依据,当一个用户请求服务,可能需要调度多个自主元素来完成该任务,如果在该虚拟共同体中,自主元素满足了其认证、授权等身份可信约束,同时也满足了服务功能、服务 QoS 参数等能力可信需求,那么该自主元素就成为了完成此任务的候选自主元素,我们将在评估其行为可信后,依据其行为可信度,优先调度可信度高的自主元素.

自主元素行为信任度 BT 主要根据最近一段时间对自主元素的反馈进行信任评价,为提高信任评价的准确性和动态适应能力,把一段时间分为若干个时间帧,时间帧长度根据具体应用场景确定; BT 由近期行为信任度 SBT 、长期行为信任度 LBT 、累积滥用行为信任 ABT 和反馈行为可信度 FBT 四者共同决定,近期信任反映自主元素近期行为,长期信任反映自主元素长期行为,累积滥用信任为自主元素利用建立的信任进行恶意行为而降低的信任值的总和,反馈可信度度量自主元素提供的反馈是否真实可信,通过反馈机制动态调节 4 个参数表征自主元素行为的动态变化,从而有效地检测和惩罚恶意自主元素的动态行为和不诚实反馈^[20].

在时间帧 n 内,自主元素 AE_i 对 AE_j 的行为信任评价 EBT_{ij}^n 为

$$EBT_{ij}^n = \lambda \cdot DBT_{ij}^n + (1 - \lambda) \sum_{r \in I(j)} \frac{FBT_{ir} \cdot DBT_{rj}^n}{\sum_{r \in I(j)} FBT_{ir}} \quad (2)$$

DBT_{ij}^n 为时间帧 n 中自主元素 AE_i 对 AE_j 的直接行为信任度,由自主元素 AE_i 对 AE_j 的多次交互的满意度的平均值决定, FBT_{ir} 为自主元素 AE_i 对 AE_r 的反馈行为可信度, $I(j)$ 为时间帧 n 中和自主元素 AE_j 进行交互的自主元素集合,一般来讲应该为虚拟共同体中的所有自主元素,但不包括自主元素 AE_i , λ 为信任评价的信心因子, λ 的取值和交互的数目有关,交互的数目越多则 λ 取值越大, $0 \leq \lambda \leq 1$. 其他各参数的命名规则与含义与此类似.

虚拟共同体中的自主元素信息交互后彼此进行满意度的评价,自主元素 AE_i 对 AE_j 的行为满意度为 BS_{ij} ,其取值为 $0 \sim 1$,1 表示自主元素 AE_i 对 AE_j 完全满意,0 表示自主元素 AE_i 对 AE_j 完全不满意,值越大表示满意度越高. 多次交互行为满意度更新策略如下表示:

$$BS_{ij}(k) = (1 - \gamma)BS_{ij}(k-1) + \gamma \cdot BT_{ij}(k) \quad (3)$$

其中 γ 为行为满意度更新因子,当前行为满意度 $BS_{ij}(k)$ 还可作为评价自主元素的行为信任度依据之一,在时间帧 n 中,令自主元素 AE_i 对 AE_j 的直接行为信任度 $DBT_{ij}^n = BS_{ij}(k)$.

在 iVCE 中,有的恶意用户可以通过提交不诚实的反馈来抬高其它恶意自主元素的信誉或者诋毁其它正常节点,特别是协同作弊对系统的危害更大,自主元素必须能鉴别出来,对其行为可信度重新作出正确的评价,提供不诚实反馈会降低其反馈可信度,提供诚实反馈会提高其反馈可信度,减少不诚实

节点提供的虚假反馈对信任值计算造成的影响. 反馈行为信任度 FBT_{ir} 为

$$FBT_{ir} = \begin{cases} FBT_{ir} + \frac{(1 - FBT_{ir})}{2} \cdot \left(1 - \frac{diff_{ir}^n}{\theta}\right), & diff_{ir}^n < \theta \\ FBT_{ir} - \frac{FBT_{ir}}{2} \cdot \left(1 - \frac{diff_{ir}^n}{\theta}\right), & \text{其它} \end{cases} \quad (4)$$

近期行为信任 SBT_{ij}^n 为

$$SBT_{ij}^n = \begin{cases} (1 - \alpha)SBT_{ij}^{n-1} + \alpha \cdot EBT_{ij}^n, & EBT_{ij}^n - ST_{ij}^n \geq -\epsilon \\ (1 - \beta)SBT_{ij}^{n-1} + \beta \cdot EBT_{ij}^n, & \text{其它} \end{cases} \quad (5)$$

在第 n 个时间帧后,使用基于强化学习方法^[21]进行计算,其中 α 和 β 为信任增加和减少学习因子,参数 $\epsilon > 0$ 规定了交互满意度评价时误差容忍范围.

长期信任 $LB T_{ij}^n$ 为

$$LB T_{ij}^n = \frac{LB T_{ij}^{n-1} \cdot (n - 1) + EBT_{ij}^n}{n} \quad (6)$$

最终的行为信任评估结果 BT_{ij}^n 取近期信任和长期信任二者中的最小值,

$$BT_{ij}^n = \min(SBT_{ij}^n, LB T_{ij}^n) \quad (7)$$

累积滥用信任 $AB T_{ij}^n$ 是自主元素的信任和实际的经验信任评价之间的差别,用来反映自主元素每次利用信任进行恶意行为带来信任降低服务的累积和,可以基于此惩罚那些间歇性违反行为准则的自主元素.

$AB T_{ij}^n =$

$$\begin{cases} AB T_{ij}^{n-1} + BT_{ij}^{n-1} - EBT_{ij}^n, & BT_{ij}^{n-1} - EBT_{ij}^{n-1} > \epsilon \\ AB T_{ij}^{n-1}, & \text{其它} \end{cases} \quad (8)$$

4.2 自适应的可信资源调度机制

4.2.1 可信优化调度问题

在 iVCE 的资源管理框架下,自主元素既可以是服务提供者、服务请求者,也可以是资源管理者. iVCE 的资源查找与定位机制可以将具有相同兴趣和背景的资源节点汇聚到一起形成虚拟共同体,各自主元素既可以发出请求,产生需要处理的任任务,也可以为其他自主元素提供服务,当然这必须符合基于该应用的预设可信规则. iVCE 中可信资源调度的基本思想就是:在一个虚拟共同体中,将自主元素请求服务产生的任务集,调度到符合身份、能力和行为可信要求的自主元素上完成相应的处理,最终使得用户请求的服务得到圆满完成. 在此过程

中,完成用户和资源相互之间的信任评价,可为任务形成一个按资源可信度高低排序的资源库,进而提高系统整体的高可用性.

可信资源调度可以描述为一个多维目标优化问题^[21],虚拟共同体 VC 由 $AE = \{AE_1, AE_2, \dots\}$ 组成,部分自主元素产生独立的服务请求 $T = \{T_1, T_2, \dots\}$,问题的目标是在可信决策空间 $TR(x_1, x_2, x_3)^T$,分别对应身份信任、能力信任、行为信任满意度,以 $f_1(x_1), f_2(x_2), f_3(x_3)$ 作为可信优化调度的目标函数,分别代表身份可信满意度函数,能力可信满意度函数和行为可信满意度函数. 因此,希望在自主元素可信的可行集 (TR_1, TR_2, TR_3) 上得到满足以下条件的优化调度方案:

$$\begin{aligned} & \text{Maximize } f_1(TR), \text{Maximize } f_2(TR), \\ & \text{Maximize } f_3(TR) \end{aligned} \quad (9)$$

定义 7. 自主元素可信映射目标函数 $f_i(TR)$: 对于某个可信指标 i ,某一个提供服务的自主元素决策空间为 $TR(TR_1, TR_2, \dots, TR_n)^T$,经过服务可信映射目标函数 $f_i(TR)$ 映射后可得到此维目标的值. 问题的求解方法主要有约束法、加权法,由于约束法相当于穷尽求解过程,不宜于实时的调度系统,目前,在实际的系统中一般采用加权法. 加权法的一般形式如式(10):

$$\text{maximize } \sum_{j=1}^3 w_j^0 f_j(x), f_j(x \geq \epsilon_j), x \in TR \quad (10)$$

其中, w_j^0 为根据调度目标给定的一组权值,它反映了请求对每个优化目标的权重, $\epsilon_j \geq (x_{i1}, x_{i2}, x_{i3})$ 是第 j 维目标函数必须满足的决策空间约束. 式(9)就是使系统的加权目标函数最大.

对于多目标优化问题已有研究证明:在多目标规划中,一般不存在所有目标函数共同的极大点,因此采用求解非劣解.

对于虚拟共同体的可信优化调度同样不可能存在一个所有目标函数共同的极大点,我们可以通过决策空间和权值向量预设,调度最优的自主元素.

例如:选取决策空间为 (IT, CT, BT) (代表身份信任、能力信任、行为信任),那么权重代表了请求服务优化目标的偏向程度. 权重向量 $W = (0, 0, 1)$ 表示只考虑一个目标:行为可信条件下的优化问题. $W = (1/3, 1/3, 1/3)$ 则表示均等考虑 3 个可信因子.

因此,多目标规划方法选择一个“最佳”自主元素,即当一个自主元素发出请求后,经过与其他自主元素交互后,选择一个能使式(10)取最大值的那个自主元素.

4.2.2 可信优化调度算法

关于独立任务的优化调度算法中,min-min^[22]是一种非常经典的算法,研究者基于不同目标提出了许多改进算法,我们基于资源的可信优化目标对min-min算法进行改进,在min-min算法将任务获得的资源可信满意度作为任务调度先后顺序的依据,通过4.1节的可信度评价方法获取虚拟共同体中各自主元素所代表的资源的可信任状态信息,计算出自主元素可信状态矩阵 TR ,为优化调度提供支撑;将服务请求调度到合适的自主元素上执行,达到系统可信优化的目标,同时兼顾了可信需求和效率要求,可信优化调度(Trust Optimizing Scheduling,TOS)过程如算法1所示.

根据可信优化调度问题分析,可信优化调度的整体目标是使得系统整体的可信满意度最大化,同时很好兼顾了执行效率.

算法 1. Trusted Optimizing Scheduling(T , VC , MAP).

- 输入:服务请求 T ,虚拟共同体 VC
输出:各服务请求与分配的自主元素的对应表 MAP
1. 初始化,设置服务请求集合 T ,虚拟共同体的自主元素集合、可信参数权值、能力可信的性能参数权值、自主元素间 TR , SAT 矩阵,初始化期望执行时间矩阵 ETC 等;
 2. 对于请求 T_i ,找出产生该服务的宿主自主元素 AE_k ,即产生 Task 到 AE 的映射表;
 3. For 虚拟共同体中除 AE_k 以外的自主元素 AE_j
 - 3.1. If 自主元素 AE_k 对所有自主元素的身份信任度为 0 then 任务 T_i 被 drop 掉;
 - 3.2. If 自主元素 AE_k 对所有自主元素的能力信任度为 0 then 任务 T_i 被 drop 掉;
 - 3.3. If 自主元素 AE_k 对所有自主元素的行为信任度小于门限阈值,任务 T_i 被 drop 掉;
 4. If 自主元素 AE_j 对所有发出请求的自主元素 AE_k 的 3 个信任度中任一评价低于信任度最低要求, $IT_{jk} < IT_k^0$ or $CT_{jk} < BT_k^0$ or $BT_{jk} < BT_k^0$,则该 AE_j 被排除出调度对象;
 5. 计算出 AE_j 对 AE_k 的三个身份满意度加权 $w_0 \cdot IS_{jk} + w_1 \cdot CS_{jk} + w_2 \cdot BS_{jk}$;
 6. 计算任务 T_i 的宿主自主元素 AE_j 对于虚拟共同体总体的身份满意度和 $sat_i = sat_i + w_0 \cdot IS_{jk} + w_1 \cdot CS_{jk} + w_2 \cdot BS_{jk}$;
 7. 根据任务 sat_i 从大到小,生成任务调度优先队列;
 8. REPEAT
 9. 取出队首任务 T_m ,即具有对于虚拟共同体总体信任满意度的任务;
 10. 计算任务 T_m 在所有符合信任要求的自主元素 AE_i 的最早完成时间;
 11. 将任务 T_m 分配到最小最早完成时间的自主元素 AE_i 执行;

12. 任务 T_m 出队列,更新执行 T_m 自主元素 AE_i 的系统就绪时间;

13. Until 任务队列空.

算法分为 3 个步骤:第 1 步为初始化,然后对不符合信任要求的任务拒绝接入,同时将不满足任何任务信任要求的自主元素排除出调度对象;第 2 步对任务请求按对虚拟共同体的总体信任满意度高低排序,确立任务调度的优先顺序;第 3 步是在第 2 步的基础上将任务调度到能最早完成该任务的自主元素上,并更新系统的状态.

5 仿真实验与性能分析

5.1 仿真实验设计

为验证优化可信调度算法在提高虚拟计算环境的安全可信运行方面的作用,将 TOS 算法与经典的 min_min 和 max_min 算法进行比较. min_min 算法的思想是首先映射小的任务,并且映射到执行快的机器上. 执行过程为:计算要参与映射事件的任务集中每个任务在各个机器上的期望完成时间,找到每个任务的最早完成时间及其对应的机器;从中找出具有最小最早完成时间的任务,将该任务指派给获得它的机器;max-max 算法的基本思想类似,不同之处在于首先调度大任务. 任务到资源的映射是选择最早完成时间最大的任务映射到所对应的机器上.

设计虚拟计算环境模拟器来仿真虚拟共同体中带可信需求的任务在自主元素间的分配,实验仿真环境为 PIV 2.6GHz,512MB,操作系统为 Windows 2000. 虚拟共同体 VC 由若干自主元素 AE 组成,其可为服务提供者,也可为请求任务的发出者. 为真实反映虚拟计算环境资源、用户异构性的特点,实验中采用文献[23]的方法生成 ETC (Expected Time to Compute)矩阵, ETC 中的每个元素为自主元素 AE_j 在不考虑其它负载情况下执行任务 T_i 所需要的时间. 利用参数 ϕ , ϕ 的大小改变分别调节任务异构和资源异构性,随机生成一批独立的任务请求,这些任务请求在自主元素上期望执行时间不具有一致性. 这些请求随机映射到自主元素表明请求的宿主自主元素,可将任务与资源之间的信任关系转化为自主元素之间的信任关系. 通过 iVCE 的身份认证机制,已完成的服务请求在授权上必须满足自主元素的要求,资源是基于同一服务提供支撑,功能上能够满足任务要求,不同自主元素提供服务的能力各不相同,自主元素的能力可信任属性要满足服务请求;自主

元素行为可信,在一定程度上可以由自主元素的服务过程中是否出现异常、失效来表征,对于提高系统的服务请求的成功率有影响.因此,随机生成自主元素身份可信 **IT** 矩阵、能力可信 **CT** 矩阵、行为可信 **BT** 矩阵,在实验中请求任务、自主元素信任关系必须满足各场景的需求,再基于 4.1 节的可信评价,可以得出身份满意 **IS** 矩阵、能力满意 **CS** 矩阵、行为满意 **BS** 矩阵.

在仿真实验中主要通过考察服务请求成功率、虚拟共同体资源利用率、虚拟共同体信任满意度收益、最早完工时间等几个参数来比较 min-min、max-min 算法和 TOS 算法,实验仿真 iVCE 中的虚拟共同体基于 P2P 文件共享系统,能力可信表现为自主元素是否提供传输文件所需的足够带宽(假设节点间网络不存在拥塞).为此,根据自主元素可信状态设计了几种不同的场景:

(1) 所有服务请求通过全部自主元素的授权,服务请求在虚拟共同体中至少找到一个满足带宽要

求的自主元素,自主元素不存在失效或异常,100% 的自主元素提供大于服务请求的带宽;

(2) 1% 的服务请求不能通过任何自主元素的授权,1% 服务请求在虚拟共同体中无法找到满足带宽要求的至少一个自主元素,1% 的自主元素表现为失效或异常,90% 的自主元素提供大于服务请求的带宽;

(3) 5% 的服务请求不能通过任何自主元素的授权,5% 的服务请求在虚拟共同体中无法找到满足带宽要求的至少一个自主元素,5% 的自主元素表现为失效或异常,80% 的自主元素提供大于服务请求的带宽;

(4) 5% 的服务请求不能通过任何自主元素的授权,5% 的服务请求在虚拟共同体中无法找到满足带宽要求的至少一个自主元素,5% 的自主元素表现为失效或异常,50% 的自主元素提供大于服务请求的带宽.

仿真实验模拟虚拟共同体,自主元素数量为

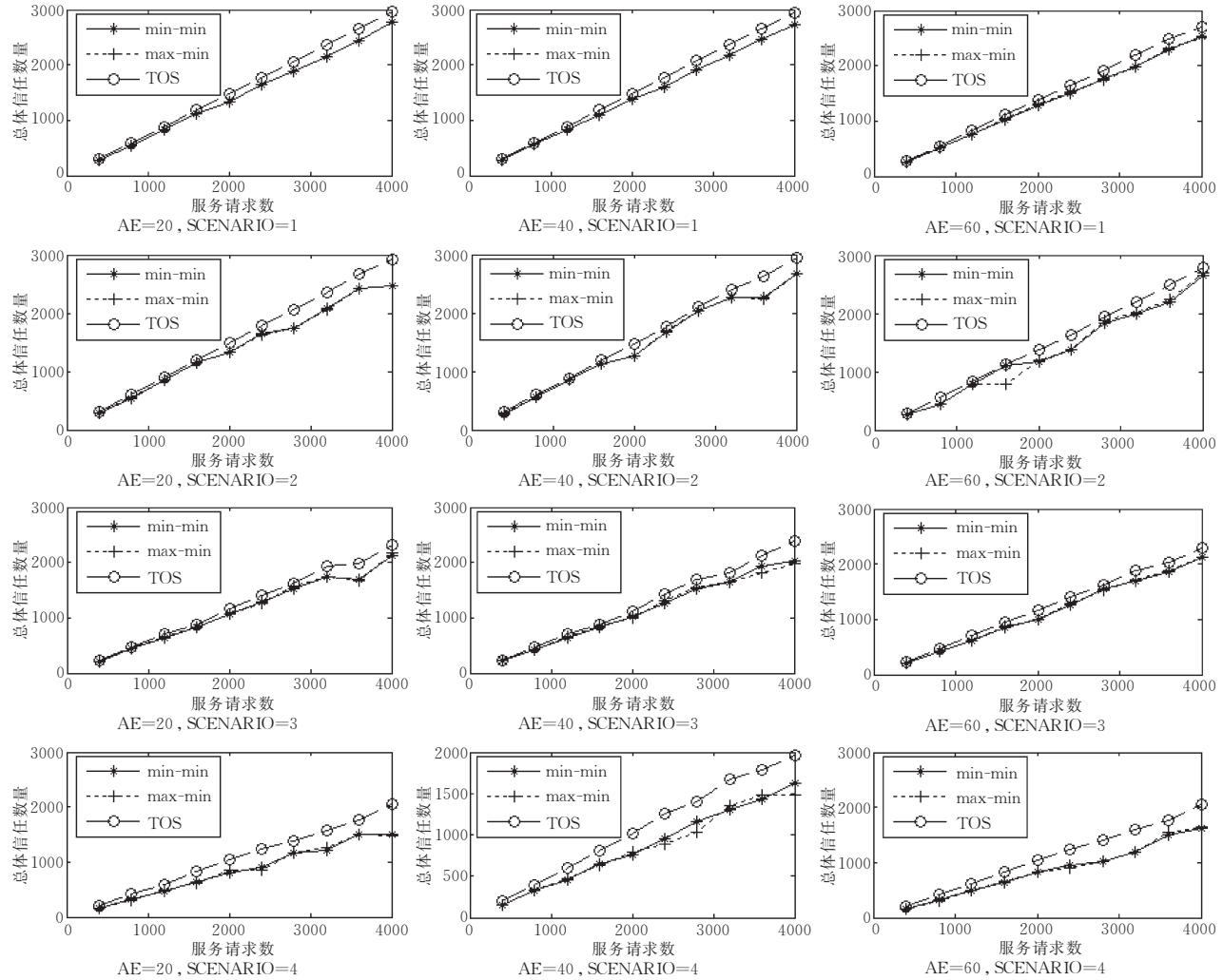


图 2 4 种场景下虚拟共同体总体信任效益比较

204060,服务请求数量从 400 增加到 4000,步长为 400,对于每种不同的实验场景重复进行了 100 次对比实验,取 100 次实验的平均结果作为的实验结果,每一次参数的初始值不同,但同一次实验 3 种算法所利用的 *ETC*、可信度矩阵,以及任务、资源异构性参数等均是相同的.信任度的 3 分量的权值相同均取 1/3.表 1 显示 *ETC* 生成算法在高任务异构性、高资源异构性参数($\phi_b=200, \phi_r=200$)下生成 *ETC* 矩阵的前 5 行、列的取样值;表 2 显示的是资源异构性参数不变情况下,将任务异构性参数变小($\phi_b=20$),前 5 行、列的取样值,验证实验中选取高异构性参数 $\phi_b=200, \phi_r=200$.

表 1 *ETC* 矩阵的前 5 行、列, $\phi_b=200, \phi_r=200$

	AE_1	AE_2	AE_3	AE_4	AE_5
T_1	6618	9917	2154	4498	698
T_2	26457	39644	8610	17981	2791
T_3	19050	28545	6200	12947	2010
T_4	4974	7453	1619	3380	525
T_5	7175	10752	2335	4877	757

表 2 *ETC* 矩阵的前 5 行、列, $\phi_b=20, \phi_r=200$

	AE_1	AE_2	AE_3	AE_4	AE_5
T_1	1821	926	1003	2271	3408
T_2	886	450	488	1105	1658
T_3	1344	683	740	1676	2514
T_4	109	55	60	136	203
T_5	1493	759	823	1862	2794

5.2 实验结果分析

图 2 显示了虚拟共同体中 3 种算法总体信任效益的对比情况,总体信任效益为所有成功调度的请求在处理该任务的自主元素的信任满意度的总和,计算式如下:

$$Total_TU = \sum_{i=1}^t SAT(t2ae(i), map(i))_{sched(i)=1}$$

(11)

其中, t 为服务请求总数, SAT 表示自主元素间的满意度, $t2ae(i)$ 为产生请求 i 的宿主自主元素, $map(i)$ 表示请求 i 被成功调度的目标自主元素, $sched(i)$ 表

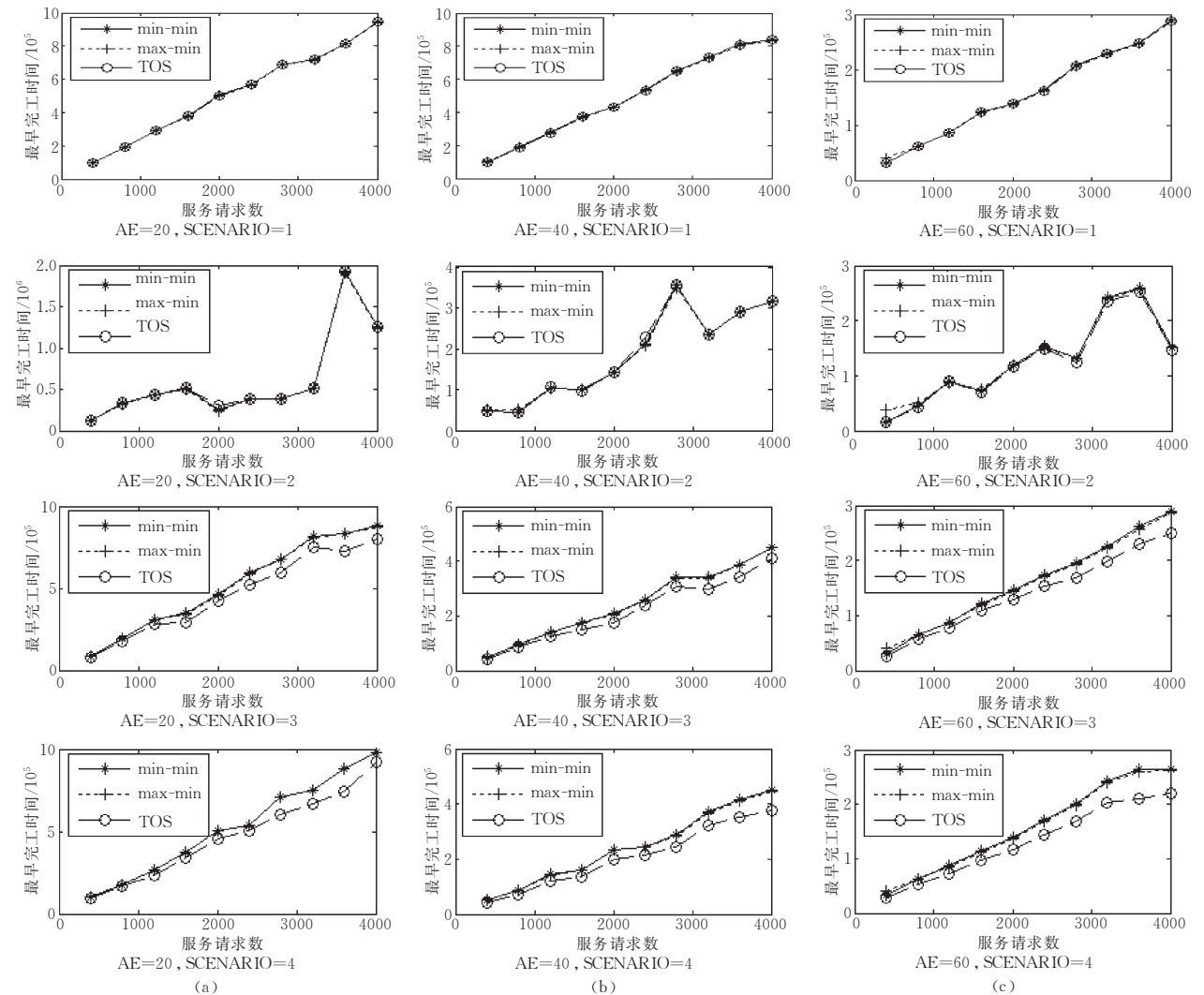


图 3 4 种场景下任务调度最早完工时间比较

示请求 i 被成功调度. 图中显示出各自主元素均能满足所有信任需求, 总体效益很高, 最高达 3000; 由于随机的信任度分布, min-min 和 max-min 算法选择任务策略不同, 但在虚拟共同体整体信任度效益基本保持一致, TOS 能够优先考虑请求与自主元素之间的信任满意度, 因此总体信任度效益高于其他两种算法, 不同规模虚拟共同体下最大相差接近 500, 并且随着不能满足信任需求的自主元素所占比例越来越高, TOS 的总体信任效益明显优于 min-min 和 max-min 算法, 最大幅度达 33%. 由上可以反映出 TOS 算法能够使虚拟计算环境的信任需求得到更好的满足.

图 3 显示了各算法在 4 种场景下最早完工时间 $makespan$ 的对比情况, 最早完工时间为所有请求调度完成之后, 虚拟共同体中自主元素的就绪时间的最大值, 它反映了系统对任务整体的处理效率. 任务数相同的情况下, $makespan$ 越小, 表明执行效率越

高, 吞吐量越大.

$$makespan = \max_{i=1}^{ae} \{R(i)\} \quad (12)$$

$R(i)$ 表示自主元素 i 的最终就绪时间, ae 表示虚拟共同体中的自主元素总数. Min-min 算法只考虑对时间的优化, max-min 则对 AE 的负载均衡为目标进行优化调度, TOS 算法是基于 min-min 算法进行改进的, 在考虑了信任满意度的基础上, 进一步再对时间进行优化, 算法同时具有较好的信任收益和 $makespan$, 在场景 1 中, 自主元素间信任关系完全满足, 3 种算法的 $makespan$ 基本保持了相同, 随着信任需求不能自主元素比例的增加, TOS 算法具有相对更小的 $makespan$, 在场景 4 中 TOS 的 $makespan$ 最大减少幅度最高达到 15%, 而 min-min 和 max-min 算法在各场景下的 $makespan$ 均保持一致.

图 4 显示了 4 种场景下各算法失效的服务请求数目情况, 在场景 1 中所有自主元素相互间的信

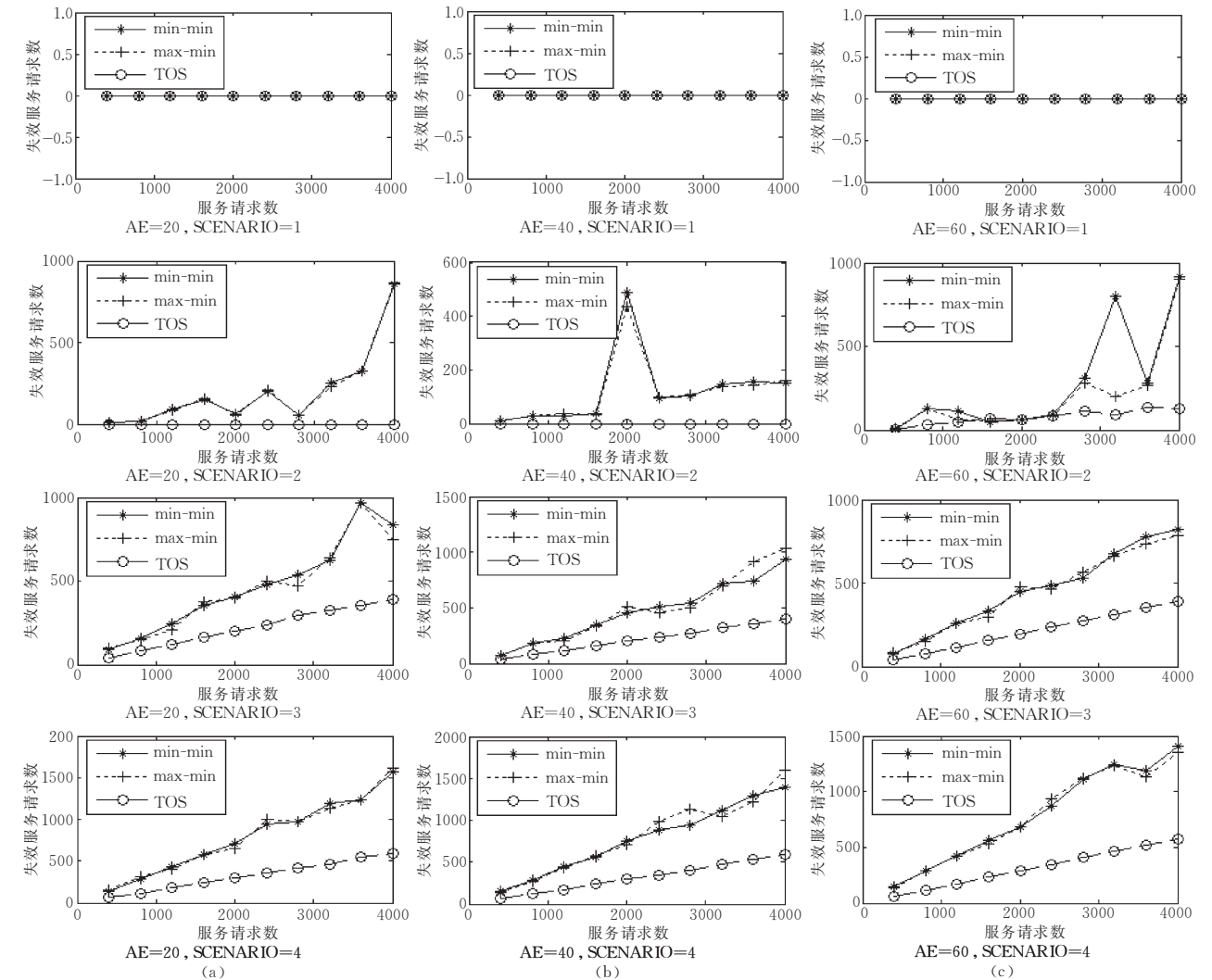


图 4 4 种场景下失效服务请求比较

任关系得到满足,因此服务调度请求全部成功,无失效服务请求;随着自主元素间信任关系的满足程度越来越低,服务请求由于信任需求无法得到满足而导致调度不成功的现象越来越严重,失效的服务请求数量逐步增加,可以看出 TOS 算法在失效服务请求方面明显优于其他两种算法,在场景 4 中,min-min,max-min 和 TOS 算法的最大失效服务请求数分别为 1575,1607,584,对应的服务请求失效率为 39.4%,40.2%,14.6%;从图 4 中还可以看出失效请求数不但与不能信任关系的自主元素比例有关,同时还跟服务请求与自主元素数目的比值成正比,我们将此比值称为服务压力,服务压力越大,虚拟计算环境的运行效率也大幅下降.

TOS 算法调度时先根据虚拟共同体中的局部信息,获取虚拟共同体状态,可实现对服务请求的接纳控制,避免了无效服务请求和信任度不够的自主元素对系统整体性能的干扰,4 种场景下服务请求

准入拒绝率分别为 0,2.91,14.32,14.63,而 min-min,max-min 不能完成服务请求准入控制.TOS 算法能够在调度进行之前根据资源对请求的可信度要求,判断一个请求是否被接入,准入控制对节省系统开销,提高资源效率具有重要意义,这是 TOS 算法能够在 *makespan* 指标上优于 min-min 和 max-min 算法的原因.

系统资源利用率,反映了虚拟计算环境中整体资源的有效利用情况,为在虚拟共同体中由所有自主元素执行任务的时间总和与所有自主元素与 *makespan* 乘积的总和的比值,如式(13)所示.

$$Utility = \frac{\sum_{i=1}^t ETC(i, map(i))}{ae \times makespan} \quad (13)$$

其中,*ETC* 表示服务请求在自主元素上的期望执行时间,*map(i)*表示调度方案中服务请求 *i* 所对应的目标自主元素,*ae* 表示自主元素的数量,*makespan*

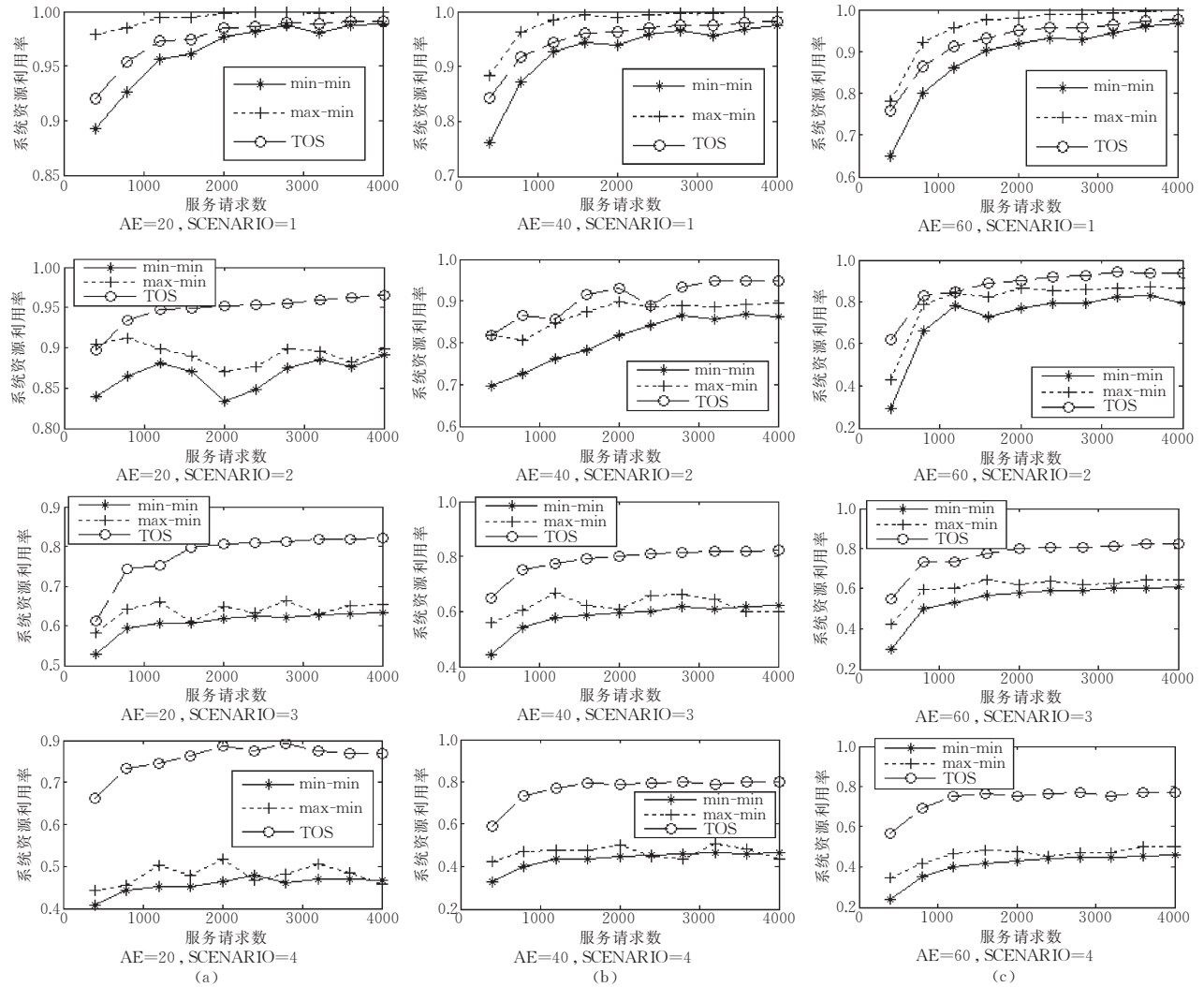


图 5 4 种场景下系统资源利用率比较

为最早完成时间. 图 5 比较了 4 种场景下系统资源利用率情况. 一方面, 在所有场景中, 资源利用率均随着请求数与自主元素数的比值增加而增大; 另一方面, 资源利用率随着信任关系满足状况的恶化而降低, 但 TOS 算法调度过程中考虑信任关系而受影响相对较小, min-min 与 max-min 算法资源利用率随信任关系恶化而严重降低. 在场景 1 中, max-min 算法具有最好的资源利用率, 其次是 TOS 算法, 最差是 min-min; 在场景 2~4 中 TOS 算法资源利用率一直维持在较高的水平, 当服务请求数目超过 1200, 满足信任关系的自主元素的资源基本被完全利用. Max-min 算法适宜于系统负载均衡, 在所有场景中资源利用率均优于 min-min 算法.

5.3 算法性能评价

虚拟计算环境中存在 n 个任务需要调度, m 个资源可供利用, 则 min-min 与 max-min 算法执行的时间复杂度均为 $O(mn^2)$, TOS 算法执行的所需时间包括: (1) 对服务请求接纳控制所需时间为 $O(mn)$; (2) 计算服务请求按对系统总体信任满意度时间对服务请求进行调度所需的时间 $O(mn)$. 因此, TOS 算法整体的时间复杂度为 $O(mn)$. 在互联网环境的大规模虚拟计算环境下 TOS 算法具有明显优越的时间性能, 如果在非常小的规模下, TOS 算法需要较多的预处理, 其计算效率将得不到有效的体现.

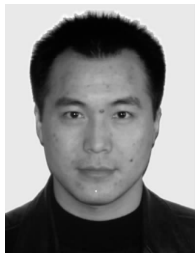
6 结论与进一步的工作

在 iVCE 的可信模型与体系的基础上, 本文详细探讨身份可信度、能力可信度、行为可信度的管理与评价方法, 以可信满意度为目标优化函数改进了 min-min 算法, 对可信资源调度问题进行了建模, 提出了可信优化资源调度算法, 在信任度效益、最早完工时间、请求失效率、资源利用率等方面较好地优化了系统的性能. 可信模型中多种性能相关 QoS 属性包含在能力可信中, 在 iVCE 中多种类型服务共存, 具有多样的能力可信需求, 如何针对不同服务的 QoS 要求, 建立良好的语义上下文, 自适应调整能力可信的参数, 为准确评估能力可信, 使得调度算法在身份可信、行为可信基础上, 能适应不同应用环境, 提供高效的服务将是下一步要研究的内容.

参 考 文 献

- [1] Lu Xi-Cheng, Wang Huai-Min, Wang Ji. Internet-based virtual computing environment. Science in China Ser. Information Sciences, 2006, 36(10): 1081-1099(in Chinese)
(卢锡城, 王怀民, 王戟. 虚拟计算环境 iVCE: 概念与体系结构. 中国科学 E 辑: 信息科学, 2006, 36(10): 1081-1099)
- [2] Maheswaran M, Siegel H J. A dynamic matching and scheduling algorithm for heterogeneous computing systems//Antonio JK ed. Proceedings of the Heterogeneous Computing Workshop. Orlando: IEEE Computer Society Press, 1998: 57-69
- [3] Foster I, Kesselman C, Tsudik G, Tuecke S. A security architecture for computational grids//Proceedings of the 5th ACM Conference on Computer and Communication Security. NY, USA, 1998: 83-92
- [4] Butt A R, Adabala S, Kapadia N H, Figueiredo R, Fortes J A B. Fine-grain access control for securing shared resources in computational grids//Proceedings of the 16th International Parallel and Distributed Processing Symposium. Florida, USA, 2002: 22-29
- [5] Azzedin F, Maheswaran M. Integrating trust into grid resource management systems//Proceedings of the 2002 International Conference on Parallel Processing. Vancouver, British Columbia, Canada, 2002: 47-54
- [6] Abawajy J H. Fault-tolerant scheduling policy for grid computing systems//Proceedings of the 18th IEEE International Parallel & Distributed Processing Symposium. Santa Fe, New Mexico, 2004: 50-58
- [7] Song S, Kwok Y K, Hwang K. Trusted job scheduling in open computational grids: Security-driven heuristics and a fast genetic algorithm//Proceedings of the 19th IEEE International Parallel & Distributed Processing Symposium. Denver, CO, USA, 2005: 33-40
- [8] Li K, He Y, Liu X. Security-driven scheduling algorithms based on eigentrust in grid//Proceedings of the 6th International Conference of Parallel and Distributed Computing Applications and Technologies. Denver, USA, 2005: 1068-1072
- [9] Yuan Lu-Lai, Zeng Guo-Sun, Jiang Li-Li, Jiang Chang-Jun. Dynamic level scheduling based on trust model in grid computing. Chinese Journal of Computers, 2006, 29(7): 1217-1224(in Chinese)
(袁禄来, 曾国荪, 姜黎立, 蒋昌俊. 环境下基于信任模型的动态级调度. 计算机学报, 2006, 29(7): 1217-1224)
- [10] Zhang Wei-Zhe, Fang Bin-Xing, Hu Ming-Zeng, Zhang Hong-Li. A trust-QoS enhanced grid service scheduling computing. Chinese Journal of Computers, 2006, 36(10): 1156-1169(in Chinese)
(张伟哲, 方滨兴, 胡铭曾, 张宏莉. 基于信任 QoS 增强的网格服务调度算法. 计算机学报, 2006, 29(7): 1157-1166)
- [11] Wang Huai-Min, Tang Yang-Bin, Yin Gang, Li Lei. Trust mechanisms of Internet software. Science in China Ser. Information Sciences, 2006, 36(10): 1156-1169(in Chinese)
(王怀民, 唐扬斌, 尹刚, 李磊. 互联网软件的可信机理. 中国科学 E 辑: 信息科学, 2006, 36(10): 1156-1169)

- [12] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management//Proceedings of the IEEE Symp Secur Privacy, 1996: 164-173
- [13] Blaze M, Feigenbaum J, Ioannidis J et al. RFC 2704: The Key Note Trust Management System Version 2. 1999
- [14] Ellison C M, Frantz B, Lampson B et al. SPKI certificate theory. RFC, 1999: 2693
- [15] Li N H. Delegation logic: A logic-based approach to distributed authorization [Ph. D. dissertation]. New York: New York University, 2000
- [16] Xu Feng. Research on trust management in open cooperative software environment [Ph. D. dissertation]. Nangjing: Nangjing University, 2003(in Chinese)
(徐锋. 开放协同软件环境中信任管理研究[D]. 南京: 南京大学, 2003)
- [17] Hong F, Zhu X, Wang S B. Delegation depth control in trust-management system//Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05). Taipei: IEEE Computer Society, 2005: 411-414
- [18] Gui Jin-Song, Chen Zhi-Gang, Deng Xiao-Heng. A hierarchical role-based restricted delegation model. accepted by Journal of Chinese Computers Systems(in Chinese)
(桂劲松, 陈志刚, 邓晓衡. 一种基于层次角色的受限委托模型. 小型微型计算机系统, 2007)
- [19] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)
- [20] Chang Jun-Sheng, Wang Huai-Min, Yin Gang. DyTrust: A time-frame based dynamic trust model for P2P systems. Chinese Journal of Computers, 2006, 29(8): 1301-1307(in Chinese)
(常俊胜, 王怀民, 尹刚. DYTrust: 一种 P2P 系统中基于时间帧的动态信任模型. 计算机学报, 2006, 29(8): 1301-1307)
- [21] Carlstrom J, Rom R. Application-aware admission control and scheduling in Web servers//Proceedings of the IEEE IN-FOCOM Conference. 2002: 506-514
- [22] Maheswaran M, Ali S, Siegel H J et al. Dynamic mapping of a class of independent tasks onto heterogeneous computing systems//Proceedings of the 8th IEEE Heterogeneous Computing Workshop (HCW'99). San Juan Puerto Rico, 1999: 30-44
- [23] Braun Tracy D, Siegel Howard Jay, Beck Noah. A comparison of eleven static heuristics for mapping a class of independent tasks onto heterogeneous distributed computing systems. Journal of Parallel and Distributed Computing, 2001, 61: 810-837



DENG Xiao-Heng, born in 1974, Ph. D., associate professor. His research interests include network modeling and security, network computing, distributed processing.

LU Xi-Cheng, born in 1946, professor, Ph. D. supervisor. His research interests include the grid Computing, data grid, and high-performance parallel and distributed processing.

WANG Huai-Min, born in 1962, Ph. D. candidate. His research interests include distributed objected-oriented technologies and network security.

Background

This paper was partly supported by the Basic Research Program of China (973 Program) under grand No. 2005CB321800; the National Natural Science Foundation of China under grant No. 60573127; The Natural Science Foundation of Hunan Province under grand No. 06JJ30032; the China Postdoctoral Science Foundation under grand No. 20060400879.

As the Internet resources have some important characteristics, such as growing, autonomy and diversity, how to aggregate resources on demand of user, how to cooperate among resources in distributed and autonomous domains and how to modeling the aggregation and cooperation are very challenging problems. Grid, p2p, web services and many

other technologies gave different solutions and partly solved the problems. That full satisfaction to the requirement has a long way to go.

Our research group now are trying to build an open infrastructure on the Internet, called Internet Based Virtual Computing Environment (iVCE), sharing resources dynamically, securely and adaptively. Based on the identity, capability and behavior trust model of iVCE, this paper presented a trust optimizing scheduling algorithm, which greatly improved total trust utilities, makespan, failed task rate, and system resource utilities compared with min-min and max-min algorithms.