基于智能网格模型的入侵检测系统*)

王 刚[1] 温 涛[1,2] 郭 权[2] 马学彬[1]

(东北大学软件中心 大连 116023)[1] (东北大学东软信息学院计算机科学系 大连 116023)[2]

摘 要 针对网格平台的异构性、动态性和分布性等特点,结合智能 Agent 技术,提出了一种智能网格模型(Intelligent and Corporative Grid Model,ICGM)。ICGM 具有自组织、自管理和智能协作等特性,能很好地适应复杂网格环境,有效地屏蔽网格平台中的不利特性。在分析网格中入侵检测需求后,设计了基于 ICGM 的网格入侵检测系统(IDS based on ICGM,gIDS)。gIDS 具有较好的智能性、灵活性和扩展性,能有效地检测网格中的入侵行为,确保网格平台的安全。对比实验表明,基于智能网络模型的 gIDS 在检测率、误报率及检测速度方面具有良好的性能,也体现出智能 Agent 技术与网格技术的整合能从一定程度上解决网格自身存在的问题。

关键词 Agent,智能网格,安全,入侵检测

IDS Based on Intelligent and Corporative Grid Model

WANG Gang[1] WEN Tao[1,2] GUO Quan[2] MA Xue-bin[1]

(Software Center,Northeastern University,Dalian 116023,China)[1]

(Department of Computer Science and Technology,Neusoft Information Institute,Dalian 116023,China)[2]

Abstract Focusing on the particular problems caused by characteristics of grid such as distributed and dynamic,ICGM (Intelligent and Corporative Grid Model) is proposed. ICGM integrates grid with intelligent Agent and solves the problems faced by grid through its features of self-organization,self-management and cooperation. Security issues in grid are analyzed and ICGM based gIDS with the attribute of intelligence and flexibility is designed. Results show that compared with IDS not supported by intelligent Agent the ability of cooperative detection of gIDS is improved. The integration of intelligent Agent and grid technologies provides a new way to solve the hard troubles in grid platform.

Keywords Agent,Intelligent grid,Security,IDS

1 引言

海量数据及计算资源需求的剧增使得网格的出现和迅猛发展,为人们在摩尔定律即将不能对硬件性能指数增长发挥作用的情况下带来了新的曙光。计算网格是跨管理域的分布式计算平台,其资源的分布性、动态性和异构性等特性给分布式并行计算带来了技术困难。以自适应、自组织和自动化完成服务过程为特征的智能网格能很好地解决这些问题。最优化、智能化和自动化的实现可以使网格服务很好地适应网格平台特性,为网格用户提供可靠、一致、广泛和廉价的最佳服务。

智能 Agent 是一种复杂的计算机程序,采取自治的行为,协同应用与环境交互,完成给定的目标。Agent 技术强调软件的分布性、自治性和智能性,通常用来构建大规模的分布式软件系统。基于 Agent 实现的智能网格能很好地解决已有网格系统中分布性、动态性和异构性的问题。目前已有相关基于 Agent 实现智能网格的研究。文献[1]使用智能 Agent 实现网格计算系统的资源管理,并给出了基于 Agent 的网格资源管理系统框架。代理被分成消费代理、资源代理和域调度器代理,用以实现资源的调度与管理。文中利用 Agent 谈判协议实现多 Agent 之间的协作,使之协调共同完成所要求任务。NetSolve[2]是一个基于代理的科学计算平台,它采用 Agent 技术管理资源空间和优化计算性能。Agent 用于接受用户的请求,同时在其维护的数据库内搜索、运行和监视满足请求所需的服务和应用,并将服务结果返回给用户。Agent 在 NetSolve 中起到十分重要的作用,但是其并未实现移动性、灵活性和智能性等 Agent 特有的属性。CoABS[3](control of Agent based system)是美国国防部的研发项目,该项目所创建的智能体网格旨在通过网格的共享机制和智能体系统的智能化、自主决策和自组织能力,向网格用户提供他们所需要的任务求解方案和结果。CoABS 是集成了不同的 Agent 系统、对象系统和传统系统的中间件,虽然其将网格概念应用于 Agent,但并没有与以计算资源共享为目标的实际网格平台进行结合。

本文提出了基于智能和协作体系结构的网格模型(Intelligent and Corporative Grid Model,ICGM),尝试利用人工智能和语义的先进性来解决目前网格平台中存在的不足与缺陷。基于智能 Agent 开发的 ICGM 服务能灵活、自主的活动,具有人类智能的本质——社会性智能,并能体现出“协作”、“竞争”和“谈判”等人类智能行为所表现出的主要形式。针对网格中安全问题的严峻挑战,本文最终基于 ICGM 开发了网格入侵检测系统(IDS based on Grid,gIDS),利用 gIDS 中代

*)基金项目:国家高技术研究发展计划项目(2004AA113020)。王 刚 博士研究生,主要研究方向为网格和网络安全;温 涛 教授,博士生导师,主要研究方向为网络安全和知识组织;郭 权 博士,副教授,主要研究方向为网格和网络安全;马学彬 博士研究生,主要研究方向为网络安全。

理组件的智能和协作等特性，适应复杂网格环境，检测网格平台中的入侵行为，确保网格的安全性。

2 智能网格模型(Intelligent and Corporative Grid Model, ICGM)

2.1 智能代理服务(Intelligent Agent based Services, IABS)的抽象结构

IABS的运行环境用环境状态集合 $S=\{s_1,s_2,\cdots\}$ 表示，影响力表示为动作的集合 $Ac=\{a_1,a_2,\cdots\}$，这样，IABS可以抽象地表示为函数：$action: S* \rightarrow Ac$。IABS环境的非确定特性可以描述为：$env: S\times Ac\rightarrow 2^u$，该函数把环境的当前状态 $s\in S$ 和动作 $a\in Ac$ 映射到环境状态的集合 $env(s,a)$ 上，此集合是IABS在环境 s 中执行动作 a 所能得到的所有环境。S 和环境的交互可以表示为历史 h，它是一个序列：$h: s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} s_2 \xrightarrow{a_2} \cdots \xrightarrow{a_{u-1}} S_u \xrightarrow{a_u} \cdots$，其中，$s_0$ 是环境的初始状态，a_u 是IABS选择执行的第 u 个动作，s_u 是第 u 个环境状态。

2.2 自组织模型

自组织是网格中虚拟组织(Virtual Organization, VO)的自我组织能力。VO中的节点来源于不同的机构和组织，代表不同的利益并执行不同的策略。当一个或多个网格节点加入或退出VO时，智能VO能够动态地屏蔽不同节点的异构性来对节点完成注册、认证和注销等行为，从而自主地搭建异构和动态环境下的虚拟组织。

自主组织不同的异构节点要求在VO中必须建成统一的公共知识体系。IABS只有在公认的抽象世界模型中才能做到智能的协作与协商，互不相识的节点也以此为基础，识别、加入和离开虚拟组织。ICGM采用模态逻辑作为认知逻辑，采用Kripke知识模型来表述IABS中的认知准则。在此基础上建立的IABS公共知识模型可以通过语义规则定义为：$(M,w)\models CK_\phi$，当且仅当 $(M,w)\models EK_\phi^k$，$\forall k\in N$。其中，EK 为元模态操作符，表示每个人都知道 φ，其可定义为：$(M,w)\models EK_\varphi$，当且仅当 $(M,w)\models K_{i\phi}$，$\forall i\in\{1,\cdots,n\}$。

公共知识模型中还包含了隐含知识的演绎，这也是IABS智能性的另一个表现，即基于公共知识模型的IABS能够汇集不同IABS的个体知识来演绎出任何一个IABS都不知道的知识。

通过上述认知和公共知识模型，ICGM建立了实现自组织所必备的知识框架，并能有效地对网格的异构性进行屏蔽：1) 异构系统的屏蔽，如节点使用的操作系统类型，主机名称等；2) 异构网络的屏蔽，如网络类型，网络协议等；3) 异构机构和异构策略的屏蔽，如节点所属机构，节点采用的认证和授权等策略。

IABS还满足自组织所要求的智能反应性，如：在动态变化的网格环境中，IABS应有能力基于当前网格节点的加入或退出等情景做出相应决策。同时，还必须满足反应具有实时性，即反应速度能符合系统所限制的时间要求。IABS对环境的观测能力用感知函数 *see* 来表示，和IABS的抽象结构一样，用 S 表示环境，而感知用 P 表示。这样，感知函数便表示为：$see: S\rightarrow P$，下一个状态函数 *next* 可表示为：$D\times P\rightarrow D$，即将数据库和感知映射到一个新的数据库中。IABS的动作action表示IABS的决策过程，实际上是根据当前的环境选择动作的函数：$action: P\rightarrow Ac$。

2.3 自管理模型

ICGM面临的最大挑战是如何协调多个IABS的行为，保证IABS间能协同工作，联合求解。虽然合作能提高IABS协作解决问题的能力，但在网格这样一个动态、复杂环境下，合作和协调的实现是困难的。

IABS协调模型包括三个方面：1) 协调体：系统中的实体，即IABS；2) 协调媒介：使得IABS间相互作用成为可能的各类载体的统一抽象描述，也是协调体得以组织在一起的核心，如：信号灯、黑板灯；(3) 协调规则：用于定义与协调体相互作用的事件相对应的协调媒介的行为。这些规则可以用协调语言或通信语言定义。

IABS的自管理性还体现在当需要多个IABS共同协作来完成一个任务(如，复杂算法的完成)时，IABS的自我修复和优化。IABS通过形成一个团队来联合各IABS，实现IABS间的协同管理和优化：对应目标 φ，$IABS_i$ 相信存在一个可能的合作动作，并最终企图形成一个群组 g($IABS_i$ 相信该群组可以联合地实现 φ)，模型可用公式(1)表示，其中群组 g 中的IABS相互相信：1) g 可以联合地实现 φ；2) 如果 $IABS_i$ 仍然拥有目标 φ 的话，那么 φ 中每个IABS都保持对 φ 承诺：

$$(\Pr e-\text{Team } g\phi\, i)=_{del}(\text{M}-\text{Bel } g(\text{J}-\text{Able } g\,\phi)\wedge \forall j((j\in g)\Rightarrow(\text{Commit } j\,\phi(\text{Goal } i\,\phi)))) \quad (1)$$

ICGM中IABS的检索、资源调度(任务的分配)及再调度、生命周期的建立及IABS的优化、修复等过程的智能性都是通过IABS的自管理性体现出来的。

2.4 服务间通信模型

IABS的通信和协调机制是ICGM中的重要研究问题之一，它可以使IABS之间进行合理、高效地协作。因为IABS基于分布式人工智能(DAI)设计，所以IABS采用言语动作(Speech Acts)作为通信方法，即将通信作为动作的一种形式，用哲学家和预言学家理解人类通信原理的方式构建IABS的通信机制。

3 基于ICGM智能网格模型的入侵检测系统(gIDS)

ICGM智能网格模型通过在Globus网格平台基础上，整合智能代理服务(IABS)而设计。其作为智能网格公共基础设施，用以为智能Agent提供创建、传输、执行、生命周期及应用管理等服务。

在ICGM基础上，设计了基于智能网格的入侵检测系统(gIDS)，其代理组件基于智能代理服务(IABS)开发，具有智能Agent的自组织、自管理和协作通信等特性。分析了网格安全中入侵检测需求，针对用户、应用和资源三种不同实体，gIDS分别采用不同机制对其行为进行分析检测。

3.1 网格中入侵检测需求分析

从安全主体角度，网格安全包括应用安全、用户安全和资源安全。用户向应用提交服务请求，并返回所需任务处理结果，用户需确保应用节点是安全的。实现用户需求的应用被分派到各个资源节点进行处理和计算，申请该应用的用户和处理该应用的资源节点对应用节点应是安全的。而资源节点调用系统资源(进程、存储等)计算应用节点交给的任务，因此资源节点不仅要通过网络检测确保应用节点的安全性和合法性，还要对节点进行主机检测以确保应用服务及本机是安全可信的。表1反映了针对不同类型的主体所应采取的检测内容和方式。

表1 网格中入侵检测需求分析比较

	应用节点	用户节点	资源节点
采用IDS类型	基于网络检测、基于应用检测、基于目标检测	基于网络检测、基于目标检测	基于主机检测、基于网络检测、基于应用检测、基于目标检测
检测内容	网络、数据及用户活动的状态	网络、用户活动的状态	系统、网络、数据及用户活动的状态

3.2 gIDS结构及组件

针对网格中入侵检测各类需求及网格的分布性和动态性等特点，gIDS结构包括五种代理组件：事件监视代理、分析引擎代理、管理代理、响应引擎代理和配置代理。gIDS采用分布式的数据采集和分析检测，但管理域内的核心数据分析是集中控制的。ICGM平台通过智能的通信和决策机制，根据安全和入侵检测的需求，将不同类型和功能的代理组件协调起来，使之相互通信、彼此协作。

为适应网格特性，gIDS将事件监视代理和分析引擎代理按照更细的粒度进行了划分。针对不同的网格节点类型及不同的检测强度要求，细粒度的代理服务使gIDS更加灵活，且避免了不必要的功能冗余，减少了系统负担和网络负载。

gIDS系统组件功能为：

(1) 事件监视代理(EMA)

EMA主要负责信息收集，并对收集数据进行简单的检测和过滤，能鉴别明显的入侵。筛选后的数据提交给AEA处理。EMA组件细化为系统事件监视组件、网络事件监视组件、基于应用事件监视组件和基于目标事件监视组件。

EMA以Kripke知识模型为认知准则，能够跨越异构平台和异构监视对象，协同采集数据。EMA具有IABS的自组织性，可以方便地融合新的采集方式，并能自发创建新的EMA对新节点或新攻击进行监视和数据采集，提高了采集数据的灵活性和可扩展性。

(2) 分析引擎代理(AEA)

AEA对EMA采集的可疑数据进行分析，其包括基于误用检测和基于异常检测两类分析组件，组件的多元化使AEA既可以检测用户的行为模式，也可以对系统和网络中的入侵数据和行为进行分析检测。

基于服务驱动的AEA组件通过将分析检测任务封装到IABS中而实现，具有IABS的自管理等特性。gIDS运行过程中，所有以φ为检测目标的AEA形成一个群组g，g中的实体(AEA)分布在各个网格节点上，保持公式(1)中的承诺，联合对用户、系统和网络进行分析检测，共同完成检测目标φ。这种分布式协作方式使AEA能够更为全面深入地对网络和系统中可疑数据进行分析，更为有效地检测复杂的分布式、协同式攻击，确保网格平台的安全性。同时，基于移动Agent实现的分布式和本地化的分析方式，能分别有效地避免单点失效，减少网络流量消耗。

(3) 管理代理(MA)

MA负责接收从AEA传来的检测报告和数据包，通过数据挖掘等检测手段，从全局角度监视网络的安全状态。同时，MA还具有调度和负载均衡功能，可以对复杂的分析计算任务进行分解，将其派遣到各个网格节点上执行，并对返回的结果进行分析检测。

MA通过IABS的协调模型协调任务代理行为，实现复杂任务的协作完成。基于IABS实现的MA组件具有良好的智能性和灵活性，能够将管理任务自动化，减轻管理员、系统和网络的负担。

(4) 响应引擎代理(REA)

REA负责接收MA传来的报警，并根据报警属性提供主动响应或被动响应。REA继承IABS的感知能力see，能主动对异常检测结果S进行感知P，并采取相应的响应及防御行为$action: P \rightarrow Ac$，实现自动、快速、有效的入侵响应功能。同时，SA通信语言的采用使得REA具有一定的智能性，提高了响应的正确性，减小了自动响应时间。

REA组件基于IABS实现，响应的分布式执行避免了因同时处理过多响应而造成单点瓶颈，具有良好的容错性和健壮性。

(5) 配置代理(CA)

当网格用户请求服务时，该用户主机上的配置代理开始执行。CA的功能是在整个服务执行过程中对涉及到的代理组件进行调用和配置，保证网格服务全过程的有效性、健壮性和安全性。

3.3 系统分析

目前的IDS面临如下问题：1) 误用检测中特征模式匹配算法的低效率是IDS中一个主要瓶颈；2) 网络数据流的高速化使得检测引擎需要分析和处理的数据包急剧增加；3) 随着网络攻击的多样化，攻击特征数不断增加，使得检测引擎需要匹配的特征模式也大大增长。

gIDS整合了网格的超级计算能力和智能Agent的分布性、智能性和移动性等特性，可以有效地解决上述IDS面临的关键挑战。对于各种目的的检测任务，gIDS首先将其分解为若干检测子任务，再将各检测子任务分别派遣到不同网格节点上执行，每个网格节点的检测子任务互相关联、彼此依赖，并通过五种基于智能代理服务IABS开发的组件实现对入侵行为进行智能化、灵活化的分布式采集、分析和检测等功能。

gIDS采用代理组件协作工作的方式完成入侵检测任务，具有很好的灵活性和可扩展性，可以融合多种检测技术，如：神经网络检测技术，生物免疫机制检测和采用数据挖掘的检测技术等。这些检测技术作为代理服务开发，并作为组件整合到gIDS中。

4 实验及分析

原型系统是在GlobusToolkit4.0基础上实现的。Globus提供了基本的GSI、GRAM和MDS服务。本文集成了网格资源信息发现与管理、网格性能监控、网格服务任务封装以及VO管理等中间件系统，主要的工作是设计和开发了智能Agent中间件(AM)，并实现与Globus及其中间件的整合。AM组件封装了Agent的智能性、分布性和移动性等特性。基于AM开发的网格服务可以在分布、动态的网格环境中完成复杂的任务求解，以最小的投入和最大的可重用性的方式满足用户的需求。

为分析gIDS入侵检测系统与ICGM智能网格模型性能，在基于Globus的ICGM网格平台上部署了gIDS，并通过与基于Snort的入侵检测系统相比较，验证gIDS在检测率、误报率和检测响应时间方面的功效。

实验位于百兆局域网内，共包括9台网格节点。其中，2台网格节点配置了GridFtp服务器，2台网格节点部署了gIDS，另外5台网格节点均衡地向2台GridFtp服务器提交

(下转第66页)

[4] Jelger C, Noel T, Frey A. Gateway and Address Auto-configuration for IPv6 Ad Hoc Networks. IEFT Internet-Draft, draft-jelger-manet-gateway-autoconf-v6-02. txt, April 2004
[5] Broch J, Maltz D, Johnson D. Supporting Hierarchyand Heterogeneous Interfaces in Multi-hop Wireless Ad Hoc Networks // Workshop on Mobile Computing Held in Conjunction with the International Symposium on Parallel Architectures, Algorithms, and Networks. Perth, Australia, June 1999
[6] Wakikawa R, Malinen J T, Perkins C E, et al. Global Connectivity for IPv6 Mobile Ad Hoc Networks. Internet Engineering Task Force, Internet Draft (Work in Progress), Nov. 2002
[7] Ratanchandani P, Kravets R. A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks // Proceedings of IEEE Wireless Communications and Networking Conference (WCNC2003). New Orleans, USA, March 2003: 1522-1527
[8] Lee J, et al. Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the Internet // Proceedings of VTC 2003. Volume 1. April 2003: 191-195
[9] Shen Bin, Zou Li, Hu Zhong-Gong. Performance Comparison and Analysis of Three Gateway Discovery Protocols of Internet Connectivity for Ad Hoc Networks. Journal of Communication and Computer, 2006, 3: 53-58
[10] Lee J, Kim D, Choi Y, et al. Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the Internet // 57th IEEE Semiannual Vehicular Technology Conference (VTC2003). Jeju, South Korea, Apr. 2003
[11] Ruiz P M, Gomez-Skarmeta A F. Maximal source coverage adaptive gateway discovery for hybrid ad hoc networks // ADHOC-NOW 2004 (Lecture Notes in Comput. Sci. Vol. 3158). Vancouver, BC, Canada, July 2004
[12] Ruiz P M, Skarmeta A F G. Enhanced Internet Connectivity for Hybrid Ad hoc networks Through Adaptive Gateway Discovery // Proc. of the 29th Annual IEEE Conference on Local Computer Networks. 2004: 370-377
[13] Park B, Lee W, Lee C, et al. LAID: Load-Adaptive Internet Gateway Discovery for Ubiquitous Wireless Internet Access Networks // Proceedings of the International Conference on Information Networking 2006 (ICOIN 2006). Sendai, Japan, 2006: 349-358
[14] Zhang Kaijie, Xiang Yong, Shi Meilin. Adaptive Internet Gateway Discovery Scheme for Mobile Ad Hoc Networks // ChinaCom'06. Beijing, China, 2006, 10: 1-5
[15] Ros F J, Ruiz P M. Low Overhead and Scalable Proxied Adaptive Gateway Discovery for Mobile Ad Hoc Networks // IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS). Vancouver, BC, 2006: 226-235
[16] Jiang Hongbo, Jin Shudong. Design and analysis of adaptive strategies for locating internet-based servers in MANETs. Journal of Performance Evaluation of Elsevier, 2006: 464-479
[17] 沈斌, 石冰心, 李波. 基于自适应策略的移动自组网与 Internet 互联. 华中科技大学学报, 2006, 34(5): 5-8
[18] 胡中功, 邹莉, 沈斌. Mobile Ad Hoc Network 与 Internet 互联的技术研究. 武汉科技学院学报, 2005, 18(6): 65-69

(上接第 44 页)

服务请求，进行数据传输。实验选择 KDD Cup99 数据集[8]中代表性强的正常数据集 2000 个、攻击数据集 4000 个作为测试集。KDD Cup99 为 DARPA 产生的 7 周网络流量数据，包含大量的正常连接和各种攻击连接。为简化实验，通过网络检测来验证 gIDS 的入侵检测性能。

图 1 显示了在网络流量及测试集不断变化过程中，gIDS 和 Snort 的 ROC 曲线情况。由图中可以看出，基于智能网格的 gIDS 比 Snort 具有更高的检测率及更低的误报率，这是因为 gIDS 各组件继承了 IABS 的智能和协作等特性，能自动适应复杂的网格环境，更好地应用网格强大的计算能力对入侵行为进行协作检测，并通过灵活地采用与入侵特征更匹配的采集、分析算法，提高了系统的入侵检测性能。

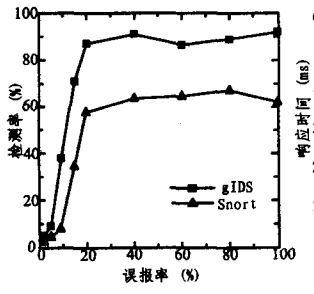

图 1 gIDS 和 Snort 的 ROC 曲线

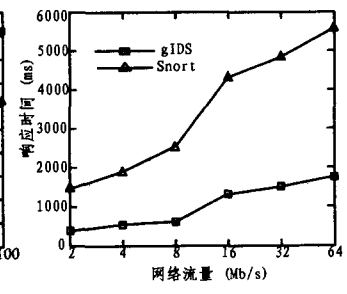

图 2 gIDS 和 Snort 的响应时间

图 2 中，网络流量在 2～64Mbps 范围变化时，首先采用 2000 个正常数据集、2000 个攻击数据集分别对 gIDS 和 Snort 进行攻击测试。当网络流量达到 8Mbps 时，再增加 2000 个攻击数据集继续进行攻击。图中显示出，gIDS 的响应时间明显小于 Snort，且随着网络流量的增加，gIDS 的响应时间变化更加平稳。当攻击变为更加复杂时，gIDS 的响应时间增幅较大，但因智能 Agent 的协调作用，使得之后 gIDS 的响应性能很快恢复平稳。而 Snort 由于攻击数据包的类型和数量突变，导致检测响应时间明显增加。结果表明，gIDS 能很好地适应网格平台特点，根据攻击的变化及时作出相应调整，将大量计算均衡地分布到各网格节点上，减轻了承担安全及管理任务的主机负担，提高了系统检测效率和灵活性。

结束语 网格环境的动态性、异构性和分布性等自身特点给基于网格的应用开发带来极大困难。本文结合智能 Agent 技术，提出并设计了基于 Agent 的智能网格模型 ICGM。ICGM 利用智能 Agent 的移动性和智能性等特性，很好地解决了上述问题。针对网格中安全问题的严峻性，设计了基于 ICGM 智能网格平台的入侵检测系统(gIDS)。gIDS 结合网格服务 API 和智能 Agent 开发，其代理组件继承了 IABS 的智能性和灵活性等特性。基于原型系统的实验表明，gIDS 在检测功能和效率方面体现出了很好的性能优势。下一步的工作重点包括平台健壮性和可靠性方面的研究，同时，智能 Agent 在自身安全性和智能性完善等方面仍存在诸多问题亟待研究。

参 考 文 献

[1] Tianfield H. Towards agent based grid resource management [C] // IEEE/ACM International on Cluster Computing and Grid (CC-Grid'05). Cardiff, UK, 2005: 9-12
[2] Casanova H, Dongarra J. NetSolve's network enabled server: examples and applications[C]. IEEE Computational Science & Engineering, 1998
[3] Kahn M, Cicalese CDT. The CoABS grid[C]. WRAC, 2002: 125-134
[4] Patel J, Teacy W T L, Jennings N R, et al. Agent-based virtual organisations for the grid[C] // Proc. 1st International Workshop on Smart Grid Technologies. 2005
[5] Overeinder B J, Wijngaards N J E, van Steen M, et al. Multi-Agent support for Internet-scale grid management[C] // Proceedings of the AISB'02 Symposium on AI and Grid Computing. April, 2002: 18-22
[6] Foster I. A globus toolkit primer[Z]. www.globus.org/primer, 2005
[7] Kruegel C, Toth T, Kirda E. Sparta-a mobile agent based intrusion detection system[C]. Network Security 2001, Leuven, Belgium, 2001
[8] The UCI KDD Archie. KDD99 Cup Datase[DB/OL]. http://kdd.ics.uci.edu/databases/kddcup99.html, 1999