# 网格环境下基于虚拟组织认证的UML建模研究

刘 欣[1],王汝传[1,2],王海艳[1]

(1.南京邮电大学 计算机科学与技术系,江苏 南京 210003;
2.南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093)

**摘 要**:由于网格环境的复杂性和网格计算的特性,使得网格提出了更高更广泛的安全需求,安全的认证是实现这一需求的关键部分。基于虚拟组织的网格安全认证体系正是为了满足网格计算和安全的特殊需要而提出的。通过统一建模语言UML,详细阐述了基于虚拟组织认证的关键技术,对进一步完善网格环境下采用虚拟组织中的分布式管理的安全实现具有较大的实用价值。

**关键词**:统一建模语言;网格安全;虚拟组织;认证

**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)06-0137-04

# UML Modeling Certification Based on Virtual Organization in Grid

LIU Xin[1], WANG Ru-chuan[1,2], WANG Hai-yan[1]

(1. Department of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. State Key Laboratory for Novel Software Technology at Nanjing University, Nanjing 210093, China)

**Abstract**: Grid environments have a broad range of security requirements that differ from conventional network environment needs. The certification is the key part of these requirements. The certification based on virtual organization just aims at the especial requirement of computing and securing in this kind of large-scale grid environment. In this paper, methods of UML in system are studied, and the modeling process and key techniques of using UML in the certification based on VO are described. It has the significant and practical value to perfect the secure realization using distributed management of virtual organization.

**Key words**: unified modeling language; grid security; virtual organization; certification

## 0 引 言

网格[1]计算环境必须具有抗拒各种非法攻击和入侵的能力,并且在受到攻击和入侵时采取某些措施来维持系统正常高效运行和保证系统中各种信息的安全。其必须提供的基本的安全服务包括:认证、授权、访问控制、完整性、审核、保密以及抗否认等。

在网格计算环境下,采用基于虚拟组织(VO,Virtual Organization)的分布式管理模式,它使得作业实体从资源控制、任务调度和管理的复杂的工作中解脱出来[2]。在虚拟组织中抽象出如下组件:VO管理中心、网格调度中心、认证机构CA(Certificate Authority)、资源,以及使用虚拟组织资源的用户,并把网格的安全功能细化为一个个安全服务组件。这里的安全服务主要包括认证服务、授权服务、委托服务、传输安全、日志审核、数字签名、防火墙等等。若网格安全功能组件涉及到网格组件的双方时,则在网格组件之间的连接网络上描述安全策略[3]。

网格环境中需要信任委托和信任传播,因为不同的组织在不同的PKI(公钥基础设施,Public Key Infrastructure)域中拥有多种资源。由于虚拟组织是一个有着共同策略的组织,虚拟组织中的共同策略也包括在虚拟组织内部,有着共同的公钥基础设施PKI。因此,在虚拟组织内部,其采用的PKI模型是唯一的。不同的虚拟组织的PKI模型可能不一样,有的是层次PKI模型、网状PKI模型、列表PKI模型等等。虚拟

**收稿日期**:2006-09-05

**基金项目**:国家自然科学基金(60573141,70271050);江苏省自然科学基金(BK2005146);江苏省高技术研究计划(BG2004004,BG2005037,BG2005038,BG2006001);国家高科技863项目(2005AA775050);南京市高科技项目(2006软资105);现代通信国家重点实验室基金(9140C1101010603);江苏省计算机信息处理技术重点实验室基金(kjs050001,kjs0606);江苏省高校自然科学研究计划(05KJB520092)

**作者简介**:刘 欣(1983-),女,江苏南京人,硕士研究生,研究方向为基于网络的计算机软件技术、网格技术、信息安全等;王汝传,教授,博士生导师,研究方向是计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

组织内部可以采用 X.509 证书格式进行认证;在虚拟组织之间认证需要采用交叉证书(cross certificate)。基于桥接 CA 的 PKI 模型是通过桥接 CA 来相互连接不同 PKI 中用于交互验证的 CA,具有可伸缩性和管理性强;支持不同类型的证书;低实现成本等优点。

认证是保证网格安全的关键步骤,由于网格安全的特殊需求,使得基于虚拟组织的网格认证模型也有其特殊性。从用户角度看,基于虚拟组织的认证场景包括:用户向虚拟组织登录的认证、用户获取虚拟组织内部资源的认证、用户获取虚拟组织外部资源的认证。本地是指虚拟组织内,而远程是指跨虚拟组织。

在研究虚拟组织认证体系的过程中,对其进行建模是非常重要的一步。统一建模语言 (Unified Modeling Language, UML)是一种定义良好、易于表达、功能强大且普遍适应的可视化图形建模语言[4]。它融合了 Booch, OMT 和 OOSE 三大面向对象方法中的基本概念,而且这些基本概念与其他面向对象技术中的基本概念大多相同,因而,UML 成为了这些方法以及其他方法的使用者乐于采用的一种简单统一的建模语言:UML 已被 OMG ( Object Management Group)接受并推荐使用,已成为事实上的业界标准。文中重点讨论使用 UML 对基于虚拟组织的网格认证体系进行建模的过程。

## 1 网格环境下基于虚拟组织的认证

基于虚拟组织的认证系统实现方案由虚拟组织、虚拟组织发布中心和普通网格用户组成,各部分在防火墙之下通过 Internet 网络连接。其中网格结点中的网格服务器包括了网格调度中心和 CA 服务器,虚拟组织发布中心中包含有桥接 CA。在该体系中,根据网格客户类型的不同,网格客户端的安全配置也有所差异。从安全角度来说,网格用户可分为两种类型:

1) 普通用户:其私钥加密存放于只有其所有者才能读取的文件中。

2) 安全用户:对安全级别要求较高的用户,其私钥存放于硬件令牌(如智能卡或 USB Token Key)中,但客户端可能必须使用如读卡器等硬件辅助设施。

该系统的认证过程由虚拟组织注册发布中心、VO 管理中心、网格调度中心及各级 CA 共同参与。其中虚拟组织注册发布中心用于注册和发布虚拟组织所提供的服务,它类似于 Web Services 中的 UDDI。基于虚拟组织认证中心内包含桥接 CA,它用于连接基于不同公钥基础设施的虚拟组织。网格调度中心的功能是对用户提交的作业进行调度,并对虚拟组织内的资源进行管理。

在基于虚拟组织的认证中定义一些结点:

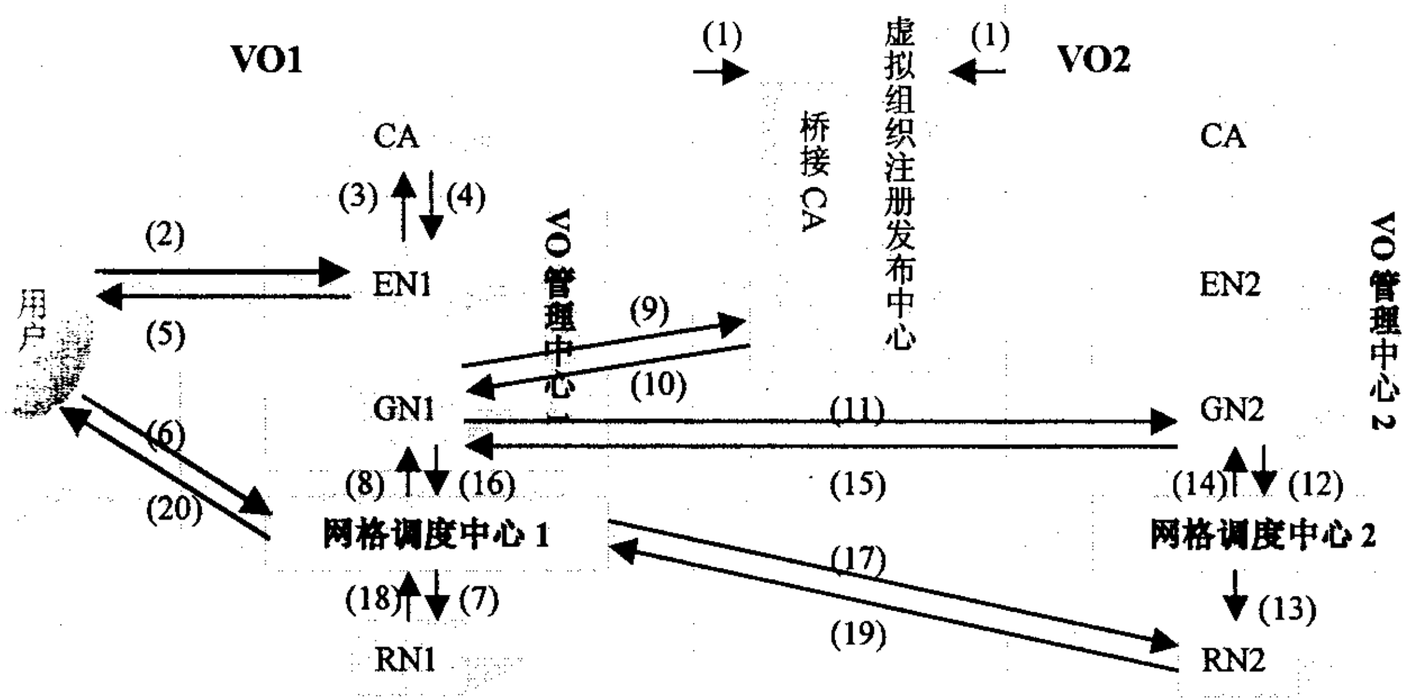
1) 入口结点 EN(entrance node)是指为用户注册和登录到虚拟组织,并获得网格服务的结点。

2) 网关结点 GN(gateway node)是指虚拟组织之间能够进行直接交互的结点。

3) 资源结点 RN(resource node)是指能够为用户提供服务资源的结点。资源包括计算资源、存储资源、打印机、传感器等等。

其中,入口结点和网关结点都包括在 VO 管理中心内部。

图 1 是基于虚拟组织的网格认证场景,其中的认证各步骤为:




注:VO—虚拟组织;EN—入口结点;GN—网关结点;RN—资源结点; CA—认证中心

图 1 基于虚拟组织的网格认证场景

1)虚拟组织 VO1 和 VO2 向虚拟组织注册发布中心注册其服务。

2)用户向虚拟组织 VO1 的 VO 管理中心传递认证信息。

3)入口结点 EN1 把用户的认证信息转发给认证中心 CA。

4)CA 认证通过,并进行电子签名;把信息转交给 VO 管理中心。

5)EN1 把用户认证通过和 CA 签名的信息转交给用户。

6)用户向虚拟组织 VO1 的调度中心 1 提出作业要求。

7)调度中心 1 获取本地网格资源 RN1,并向 RN1 分配任务。

8)调度中心 1 发现虚拟组织 VO1 的资源无法完

成用户任务,则向 VO 管理中心汇报。

9)网关结点 GN1 通过 CA1 的数字签名证书与虚拟组织注册发布中心的桥接 CA 相互认证,并提出服务查询要求。

10)虚拟组织注册发布中心告诉 VO 管理中心 1 有关虚拟组织 VO2 的信息,包括 GN2 地址和有关认证信息。

11)GN1 向 GN2 提出认证要求和请求有关资源的信息。

12)GN2 认证通过,则向 VO2 的调度中心 2 提出资源请求。

13)调度中心 2 选取合适资源 RN2,并告诉网格调度中心 1 的认证信息。

14)网格调度中心 2 通知 VO 管理中心 1 有关资源结点 RN2 的信息。

15)GN2 转告 GN1 有关资源结点 RN2 的信息。

16)GN1 转告任务调度中心 1 有关资源结点 RN2 的信息。

17)任务调度中心 1 向远程网格资源 RN2 认证,并向 RN2 分配任务。

18)RN1 完成任务,向任务调度中心 1 返回运行结果。

19)RN2 完成任务,向任务调度中心 1 返回运行结果。

20)任务调度中心 1 汇集运行结果,并向用户返回运行结果。

## 2　基于虚拟组织认证的 UML 建模

UML 适用于系统开发过程中从需求规格描述到系统完成后测试的不同阶段。在需求分析阶段,可以用用例来捕获用户需求。通过用例建模,描述对系统感兴趣的外部角色及其对系统的功能要求。分析阶段主要关心问题域中的主要概念(如抽象、类和对象等)和机制,需要识别这些类以及它们相互间的关系,并用 UML 类图来描述。为实现用例,类之间需要协作,这可以用 UML 动态模型来描述[5]。

### 2.1　总体需求建模

通常利用情节或经历来描述用户和软件系统的交互方式,从而获取需求(McGraw and Harbison 1997)。Ivar Jacobson(1992)把这种看法系统地阐述成用例的方法进行需求获取和建模。在这一阶段,需要做的工作是确定系统范围和边界、定义活动者和定义用例。

用例图(Use case diagram):从用户的角度出发描述系统的功能、需求,展示系统外部的各类活动者与系统内部的各种用例之间的关系,主要元素是用例和活动者。从本质上讲,一个用例是用户与计算机之间的一次典型交互作用,活动者是指用户在系统中所扮演的角色。用例图用于需求分析阶段,它的建立是系统开发者和用户反复讨论的结果,表明了开发者和用户对需求规格达成的共识。

用例图把系统分成角色(actor)和用例。用例被定义成系统执行的一系列动作,动作执行的结果能被指定角色察觉到。角色是指用户在系统中所扮演的角色。角色的标准是它们必须要在被划分进用例的系统部分以外,能刺激系统部分并接收返回。单个角色可与多个用例联系;反过来,一个用例可与多个角色联系。图 2 是虚拟组织认证的 UML 顶层 Use Case 图。

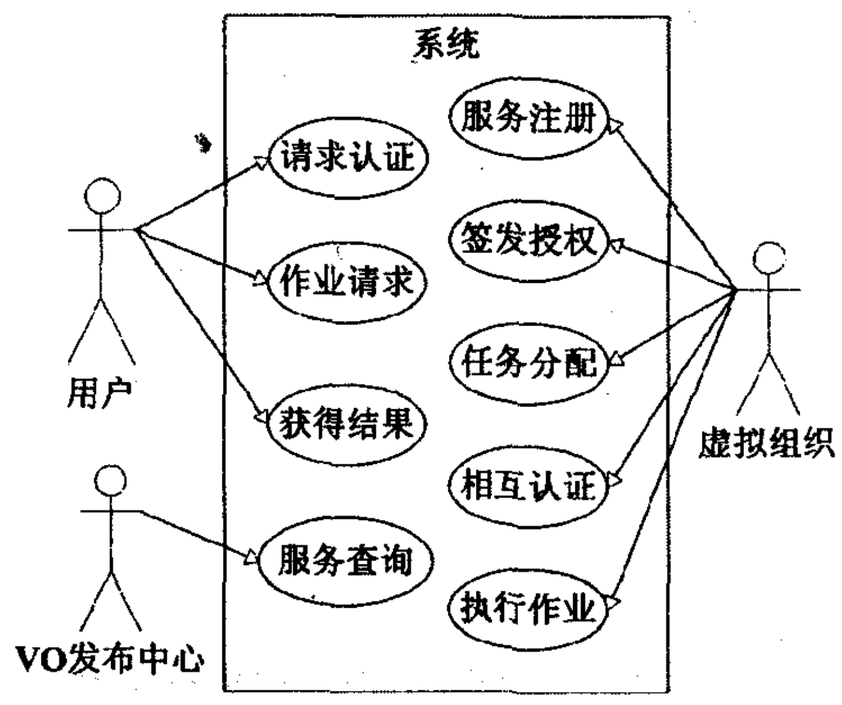



图 2　虚拟组织认证的 UML 用例图

具体描述如下:

在虚拟组织认证系统中,每个虚拟组织都向 VO 发布中心进行服务注册。网格用户要登陆到虚拟组织时,需要先向虚拟组织进行认证,由虚拟组织中的认证中心向用户返回签发的证书。此时用户可以向虚拟组织提出作业请求,若该虚拟组织内部的资源可以完成该作业,则该虚拟组织调用资源,完成作业;否则,虚拟组织与虚拟组织注册发布中心的桥接 CA 相互认证,并提出服务查询要求。VO 发布中心将查询到的资源结果返回,则该虚拟组织在认证通过之后,就可调用其他虚拟组织中的资源来共同完成用户的作业。最后将作业结果返回给用户。

### 2.2　系统分析建模

在对总体需求分析的基础上,对虚拟组织的认证系统进行详细设计。类图(Class diagram)处于分析建模的核心位置,它模拟的是保证系统正常工作的所有必要资源,其他所有的图如果想获取这些资源的信息,最终都必须访问类图。类图描述系统所包含的类、类的内部结构及类之间的关系,它是一种静态结构图,描述的是系统的静态结构。类图的主要功能有:

(1) 定义了一个系统的必要资源。

(2) 定义了存在于资源之间的关系。

(3) 可以生成代码。

(4) 可以用代码生成模型。

(5) 为其他的图提供了基础。

虚拟组织认证系统中主要类如下:“用户”类、“虚拟组织”类、“VO发布中心”类、“证书”类、“认证请求”类、“作业请求”类、“服务调用”类、“服务发布”类、“相互认证”类。在每个类中,类的属性用来描述类的不同特性,它说明了这个类的细节。而类的操作描述了类的行为,它定义了系统的执行逻辑,包括基本和复杂的逻辑。类图中不同类型的关联,展示了类之间或类与其他建模元素之间的关系。类之间的关系见图 3。

系统的动态行为细节使用序列图(Sequence diagram)描述。序列图表示了随时间安排的一系列消息,用来描述对象之间动态交互关系,着重体现对象间消息传送的时间顺序,显示了应用中的对象如何使用消息流合作以获得想得到的结果。根据系统的总体需求设计和用 UML 类图,进行本系统行为全局的描述(见图 4)。

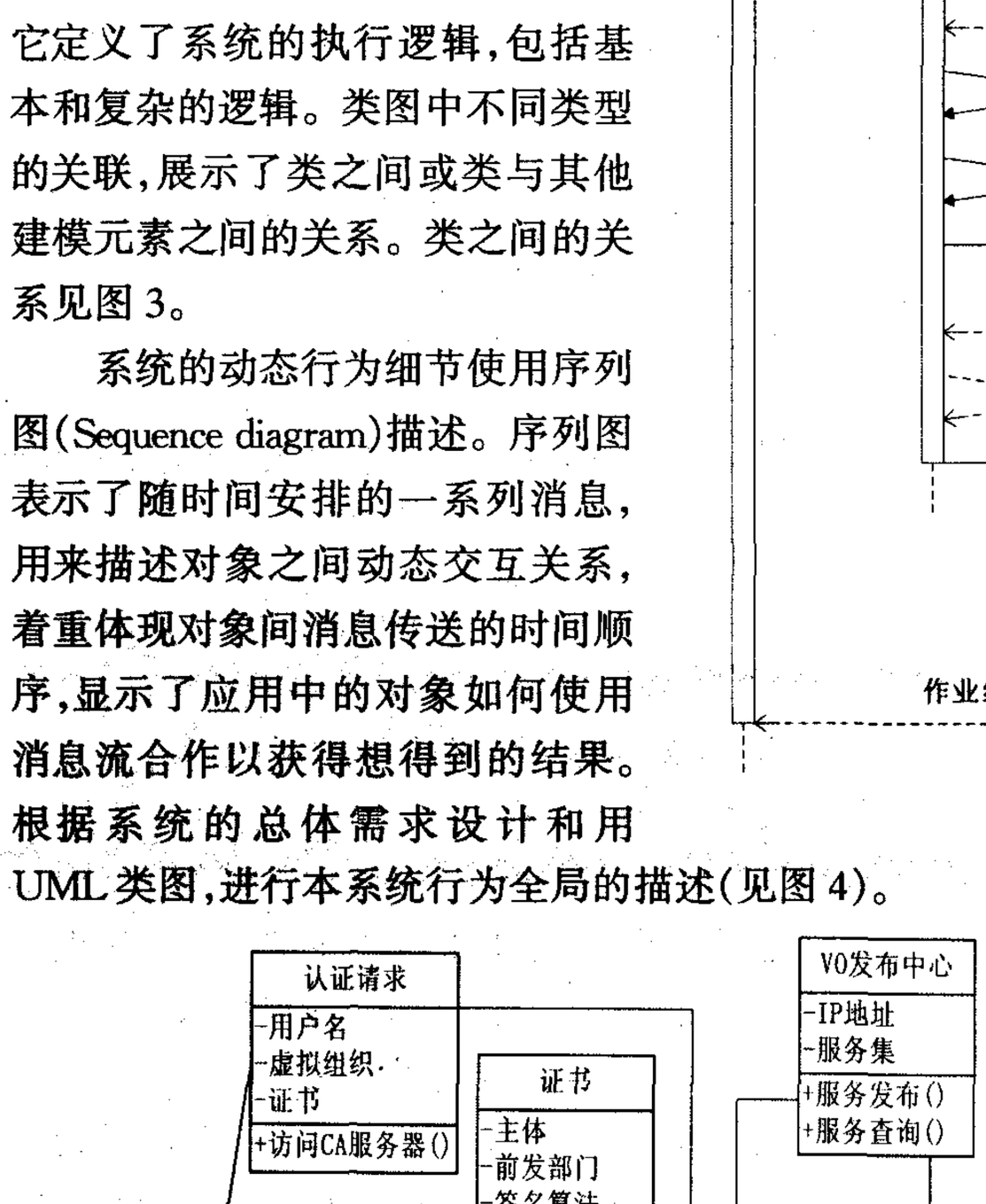



图 3 虚拟组织认证的 UML 类图

图 4 中消息流的具体顺序与图 1 认证场景描述的认证步骤大致相同,这里不再详述。

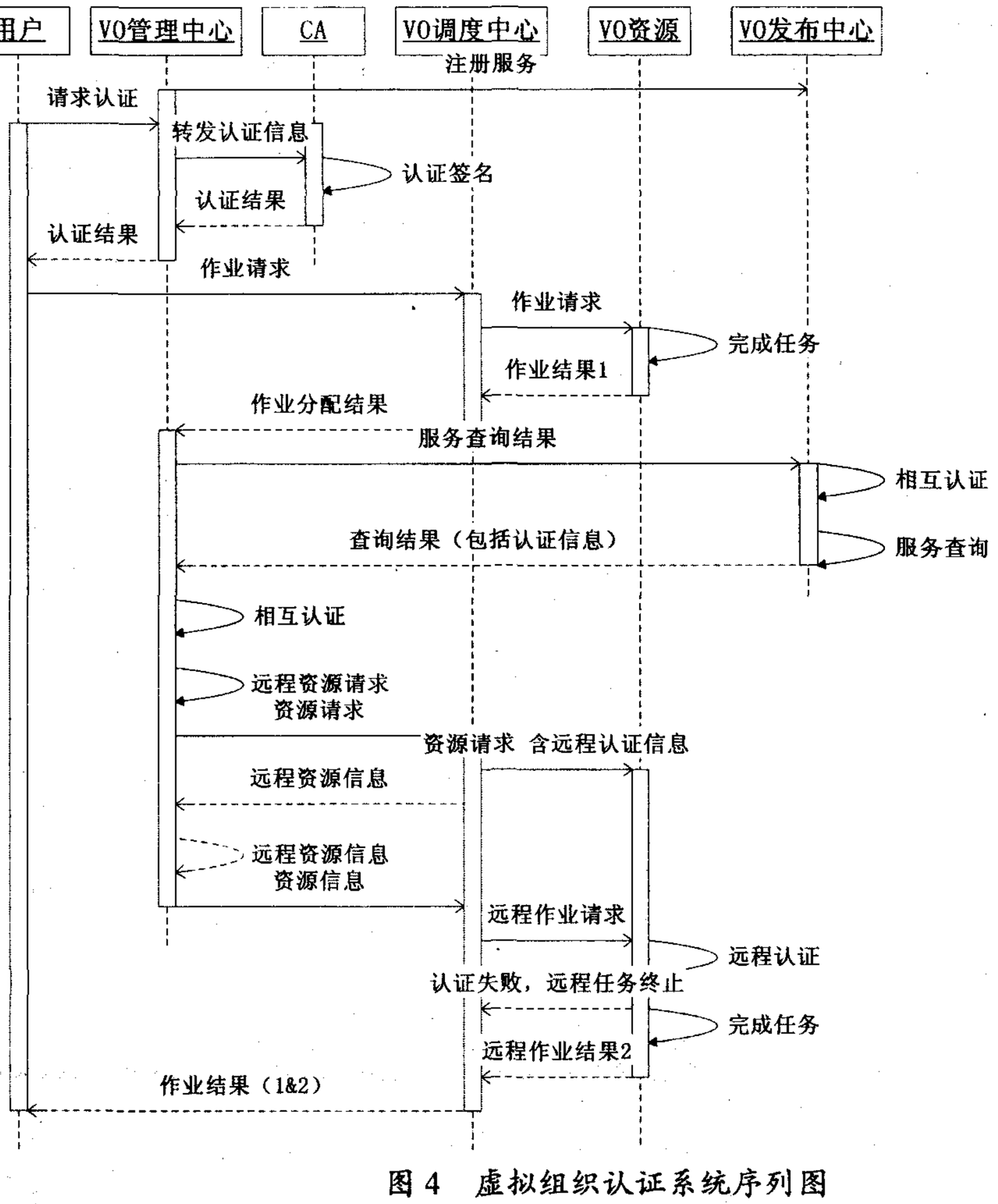



图 4 虚拟组织认证系统序列图

序列图显示了系统中的事物之间发生的动态交互,这些交互为建立系统中各元素的结构奠定了基础。该序列图中,虚拟组织被细化为 VO 管理中心、CA、VO 调度中心和 VO 资源等模型元素。它们之间及与用户、VO 注册发布中心之间的消息传递清楚地显示了该系统中的交互情况。

## 3 结束语

用 UML 进行虚拟组织认证系统的设计有许多优点:

1)UML 融合当前一些流行的面向对象开发方法的主要概念和技术,成为一种面向对象的标准的建模语言,采用图形来描述系统的视图易于理解,起到了桥梁的作用。

2)UML 支持独立于编程语言和开发过程的规范,它支持大多数 OO 语言里定义的面向对象的设计结构,这种一致性保证了能够从模型生成代码或从代码产生模型,即实现建模环境和编码环境的集成。

3)UML 有很好的扩展性,提供了标签、约束、版类等约束机制来进行自我扩展,为以后社区授权服务系

(下转第 144 页)

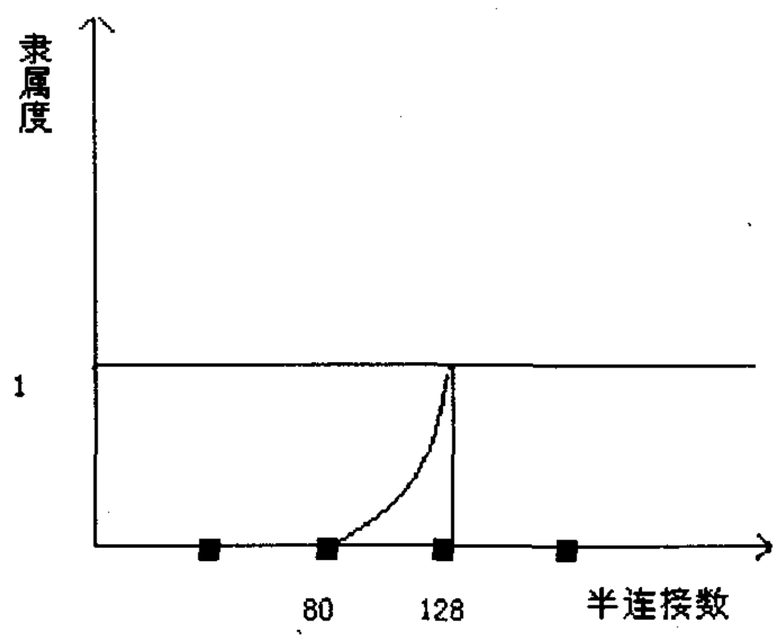



图 5 $B_{连接}$ 的分布图

3)经验法。

就是指根据网络管理员的经验确定隶属度函数。例如:如有采用 UDP 协议,端口是 7626 的网络流,则极有可能是该主机感染了冰河木马,根据经验可以认为这种可能性有 95% 以上,故该情形下该主机感染冰河木马的隶属度是 0.95。

其它的如二元对比法等在该系统中应用的较少。通过以上描述,可以看出该模型的缺点之一是需要采集一段时间内网络正常运转的情况下的参数的数据,同时对使用者的素质要求较高。

## 2 评价与展望

文中提出的改进模糊识别的网络安全管理模型判断准确,能够很好地降低漏报率和误报率。一方面,它直接围绕需要管理的网络的安全状态本身构造模型,因此具有很强的目的性,从而可以提高安全管理中对被管对象的状态识别的准确性;另一方面,本模型从可能性和入侵行为的不确定性角度出发与基于统计的异常状态检测相比,更具人性化,能够更准确地确定网络安全状态。同时,本模型吸取了免疫系统中"多层防御"机制的特点,不同于其它方法仅从一两项参数判断管理目标状态,并改进了最大隶属度模型利用分组机制消除了某些参数的相关性影响,这些特点使得本模型的漏报和误报率大大降低。

但是,本模型也存在着需要参数的统计数据;对使用者要求较高;某些隶属度函数的确定主要依靠专家经验不能从理论上保证入侵定义的完备性等缺点。未来的工作应集中于识别中不确定性传播的推理;隶属度函数库的学习和改进算法研究等方向。

同时这种改进模糊识别模型具有普遍性和推广价值,不仅仅可以用于网络安全状态管理,也可以应用于设备故障判断定位、物种识别、疾病判断、决策判断等等众多领域中。

**参考文献:**

[1] 杨家海,任宪坤,王沛瑜. 网络管理原理与实现技术[M]. 北京:清华大学出版社,2000.

[2] 谢季坚,刘承平 . 模糊数学方法及其应用[M]. 武汉:华中科技大学出版社,2000.

[3] Monji A. Languages and Tools for Rule－Based Distributed Intrusion Detection[D]. Namur, Belgium: Faculte´s Universitaires Notre Dame de la Paix,1997.

[4] 李之棠,杨红云 . 模糊入侵检测模型[J]. 计算机工程与科学,2000,22(2):49－53.

[5] Shan Z,Chen P,Xu Y,et al. A Network State Based Intrusion Detection Model[C]//In Proceedings IEEE 2001 International Conference on Computer Networks and Mobile Computing. Beijing,China:[s.n.],2001:481－486.

[6] 虞和济,陈长征,张 省,等 . 基于神经网络的智能诊断[M]. 北京:冶金工业出版社,2000.

(上接第 140 页)

统的更深入研究或升级带来了方便。

文中在分析网格安全特点的基础上,提出了基于虚拟组织的网格安全体系,可以满足网格的各种安全需求。在该体系的认证模型中,用户只需在提交作业前提出认证需求,当登录成功之后便可以重复调用网格中提供的资源,即实现了"单一登录"。此外采用桥接 CA,可兼容不同的本地安全方案,其可扩展性也很强。进一步采用 UML 对虚拟组织的认证进行建模,给出了系统的总体分析图即用例图、静态类图及描述系统动态行为的序列图,阐述了用 UML 进行系统设计的优点,有助于开发人员对系统有清晰的认识,从而提高了开发效率和质量,为进一步完善虚拟组织的安全认证打下了基础,同时也对探讨网格计算的安全实现具有很好的参考价值。

**参考文献:**

[1] 徐志伟,冯百明,李 伟. 网格计算技术[M]. 北京:电子工业出版社,2004.

[2] Foster I,Kesselman C,Tuecke S. The Anatomy of the Grid－Enabling Scalable Virtual Organizations[J]. International J. Supercomputer Applications, 2001,15(3):200－220.

[3] Pearlman L, Welch V, Foster I, et al. A Community Authorization Service for Group Collaboration[C]// In: Werner B. Proceedings of IEEE Workshop on Policies for Distributed Systems and Networks. Los Alamitos: IEE Computer Society, 2002:50－59.

[4] Pender T. UML Bible[M]. 北京:电子工业出版社,2004.

[5] Selic B. A Generic Framework for Modeling Resources with UML[J]. Computer: Innovative for Computer Professionals, 2000,33(6):64－69.