信任机制及其在网格安全中的应用*)

陈建刚[1] 王汝传[1,2] 王海艳[1]
(南京邮电学院计算机科学与技术系 南京 210003)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]

摘 要 分析了网格计算环境对信任机制的需求,将信任机制分为理性信任和感性信任,并给出了相应的两种信任机制模型,结合网格计算的安全功能,给出了有感性信任参与下的网格安全服务,最后结合基于角色的访问控制(RBAC)机制给出了该模型的一个实例,即通过理性信任和感性信任的评判得到信任度等级,根据该信任度等级来决定用户所分配的角色和权限集。

关键词 网格计算,感性信任,理性信任,角色的访问控制

An Application of Trust Mechanism in Grid Security

CHEN Jian-Gang[1] WANG Ru-Chuan[1,2] WANG Hai-Yan[1]
(Institute of Computer Science, Nanjing University of Post and Telecommunications, Nanjing 210003)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)[2]

Abstract According to the requestment of Grid Computing for trust mechanism, the trust mechanism is divided into object trust and subject trust and the two trust mechanism models are proposed respectively. The Grid security model joined with subject trust mechanism is provided and an instance of the model including the model of role based access control(RBAC)is shown, in which, the trust level obtained by the evaluation of the object trust and subject trust decides the assignment of the subset of roles and permissions.

Keywords Grid computing, Subject trust, Object trust, RBAC

1 引言

网格计算的出现和兴起,使得软件系统正从面向封闭的、熟识用户群体和相对静态的形式向更加开放的、公共可访问的和高度动态的服务模式的转变。这种转变使得网格计算系统的安全分析复杂化,同时由于网格计算环境的大规模性、异构性、分布性、动态性和开放性等特点,传统的安全技术或者措施已经不能满足网格应用的需要。如访问控制列表(Access Control List,简称 ACL)无法满足网格计算此类新兴的分布系统的安全需求:(1)用户身份鉴别困难,用户不一定为系统所熟知;(2)缺乏委托机制,分布的系统管理任务需要委托机制的支持;(3)表达能力和可扩展性差,无法处理多变的安全条件和个性化的安全需求;(4)本地信任策略不能跨越管理域,而网格计算应用往往需要跨越多个管理域。虽然有一些改进方法,如将基于身份标识的公钥系统与 ACL 结合使用,但仍然无法从根本上解决所有问题。

因此,人们迫切需要通过对网格计算的安全策略进行专门系统的研究,提出一种新的能够适应网格计算等开放网络环境的安全模型。信任机制作为一种新的能够适应开放网络环境安全技术,引起了人们的关注。"信任(Trust)"是指可以致力于完成他人的合法期望的一种能力,信任既是道德的组成部分,也是任何社会存在的关键前提条件。信任区别传统的认证机制,传统的认证主要用于证明身份,说明拥有该证书或令牌的实体是合法实体,而这并不等同于说明该实体就是信任的(有能力进行交互并且交互过程中不会出现欺诈行为)。但是信任和认证模型是紧密相连的,对于一般的交互过程,通常先进行身份认证,再结合信任模型来评判交互对方的信任度,然后根据对方的信任程度给对方相应的授权。信任和认证都是属于对交互对方的一种确信关系,因而我们将认证称为理性信任(不需要主观因素的考虑,依靠传统密码学原理来构造),将信任称为感性信任(主要靠主观因素来决定信任等级),并把两者通称为信任,即在此信任包括了理性信任和感性信任。对网格计算中的理性信任研究比较成熟,主要是使用 PKI 技术来实施认证过程。对感性信任机制主要有以下几类:基于 Dempster-Shafer(D-S)证据理论[1~3]来刻画主观信任度,通过制定相应的规则对信任度进行分类评判(分为信任,不信任和不确定三类);基于模糊集合的信任关系[4],对信任关系进行等级划分,建立信任集合的隶属函数。基于概率统计的信任关系[5],统计交互成功和交互失败的次数来作为信任等级的划分。目前网格环境中的信任模型也有如上两类:使用 D-S 证据理论的信任模型[6]和基于模糊逻辑的信任模型[7]。而基于行为的网格信任模型[8]最早由 F. Azzedin

*)本课题得到国家自然科学基金(60573141 和 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、kjs06)和江苏省高校自然科学研究计划(05KJB520092)资助。
陈建刚 博士研究生,主要研究方向为网格技术、信息安全等。**王汝传** 教授,博士生导师,主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等。**王海艳** 副教授,博士生,主要研究方向为计算机软件、计算机网络、信息安全、移动代理等。

提出，以信任和声望作为度量，并引入了信任衰减函数来反映信任随时间而变的特性。后来，F. Azzedin 又提出了一个信任中介系统来扩展信任的范围[9]，并引入了准确度和诚实度作为度量，从而解决了推荐者恶意推荐的度量问题。在此，主要针对网格计算中信任机制模型和感性信任在网格安全中的作用来展开讨论。

2 网格计算环境的理性信任模型

在安全系统中，理性信任(认证)不同于授权，授权是指根据个体身份赋予个体访问系统资源权限的过程，而认证仅确保个体是他所声称的个体，而不涉及其访问权限。网格认证主要有两种模式：a)基于用户标识的(identity-based)；b)基于用户凭证的(token-based)。不管采用何种方法，网格认证的最终目的是确保合作方信任用户并提供其所需服务，并为日后审核和计帐的需要作相关的记录。

网格认证从总体上来说，是要给用户提供单点登录(Single Sign-On，SSO)、实现实体间相互认证、支持各参与方的协同工作以及支持动态区域内的安全管理。网格认证的功能可分解为如下几项：(1)实现单点登录(SSO)；(2)用户信用凭证的保护；(3)基于用户的信任关系；(4)局部安全方案的互用性；(5)所有认证代码的公开性；(6)统一的认证结构；(7)支持动态组的安全通信；(8)兼容、支持多个本地认证方案。

因而在建立认证模型过程中，我们需要考虑下面几点：

• 尽量保持网格计算环境中现有的各自治域的认证体系不变，将它们作为网格计算环境中在自治域内运作时需要进行的相关认证。

• 在建立虚拟组织(VO)完成某一任务时，则需要对这些自治域的认证体系进行整合，以便于不同域节点之间安全高效的进行跨域交互。整合过程中尽量采纳现有的各自治域的认证体系，充分利用现有认证资源。

• 尽量使用国际上目前制定的网格计算安全规范中的认证规范，在这基础上来构建整个网格计算的认证基础设施。

• 该认证系统模型是作为网格安全模块的一个组成部分，因而要能够无缝地融合在网格安全平台中。

通过如上考虑，根据网格计算的组成结构我们可以得知，网格计算环境的理性信任结构模型如图 1 所示。

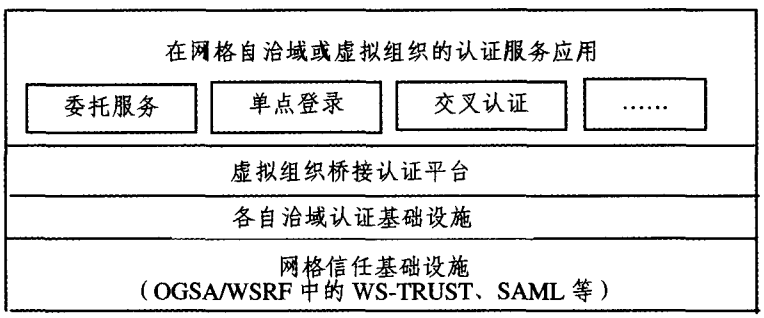

图 1 网格计算环境下的理性信任结构模型

整个理性信任模型按照功能可以自下而上划分为 4 个层次：网格信任基础设施层、各自治域认证基础设施层、虚拟组织认证平台层、认证服务应用层。其中

• 网格信任基础设施层：该基础设施包括现有的网格计算安全服务中的有关认证规范，如 GSI 中的证书链和 WS-Security 中的 WS-TRUST 等。这些认证服务是针对网格计算环境而规定的，对上层认证体系的建立具有指导性的作用。

• 各自治域认证基础设施层：每个自治域都根据网格计算环境的特点和自身环境的认证需求来制定本域的认证模型系统，如采用网状、层状和列表状的 PKI 模型等。各自治域认证基础设施主要是为上层虚拟组织的认证建立和认证应用提供基础认证平台。

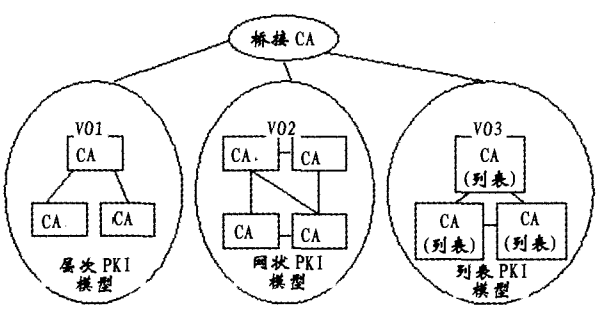

图 2 网格计算环境下虚拟组织的桥接 CA 认证机制

• 虚拟组织桥接认证平台层：该层主要是保证建立的虚拟组织的认证结构，虚拟组织是一个有着共同策略的组织，在组成虚拟组织时就需要有一种认证体系来统一管理这些不同的认证系统，可以采用基于桥接 CA 的认证模型，该模型如图 2 所示。它具有以下优点：(1)可伸缩性和管理性强：桥接 CA 通过多个不同的 PKI 域之间的 CA 可自由地、伸缩地建立信任关系。(2)支持不同类型的证书：支持 X.509 证书和它们的变形如属性证书等等，因此具有很好的应用前景。(3)低实现成本：以点对点的方式支持证书路径发现和相互交互，因此降低了实现成本。

• 认证服务应用层：即使用下面各层认证体系来提供不同的认证服务，如委托服务、单点登录和交叉认证等。

3 网格计算环境的感性信任机制

根据网格计算环境的特点，我们将网格计算中的感性信任关系分为直接信任和推荐信任两种。直接信任是指两个代理(信任代理和被信任代理)根据过去发生的直接交往行为而得出的信任等级关系，这种交互包括代理间协作完成某项任务，代理使用资源完成任务等。

推荐信任是指通过网格计算环境中有声望的实体代理的推荐活动而得出的信任等级关系。根据社会网络关系，我们知道在交互双方没有接触过的前提下，代理都倾向于使用一些自己比较信任的中间代理作为推荐代理来评判交互对方，而这些推荐代理的推荐能力则可以通过他们的声望来表示，声望(Reputation)定义为一个代理对另一个代理能够行使推荐活动的能力、诚实性和可靠性的一种主观评判。通常声望越大，则越容易取得信任。不难理解，当代理间长时间没有直

接的或间接的信任接触行为发生时，推荐代理的声望及其信任关系可能会随时间而衰减弱化。图 3 为这两种信任关系的示意图，其中图(B)中需要对由推荐代理产生的推荐信任链路进行综合，最终得到交互双方的信任关系。

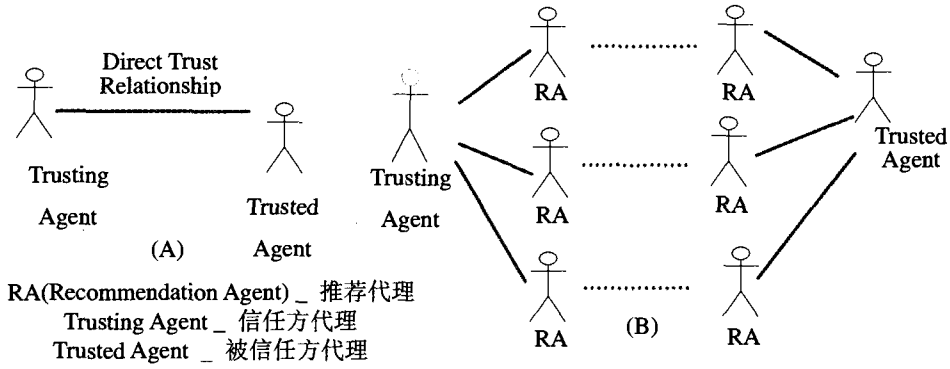

图 3 (A)代理间的直接信任关系示意图 (B)通过推荐代理的推荐信任关系示意图

在网格计算环境中，信任代理首先进行信任链路的搜索过程，通常有直接和间接(推荐)两种链路需要建立，然后是信任链路的筛选，剔除掉那些不符合指定条件的链路，比如当一个推荐代理不可靠(声望值很低)时，应该将以该推荐代理推荐得到的推荐链路删除，即该链路不能参与最终信任合成过程。在剩余的信任链路中，通过对直接链路得到的直接信任和推荐链路得到的被信任代理的声望进行合成，从而得到合成后的信任值，最后和信任策略集中的对交互对方的信任期望值进行匹配，匹配成功说明交互双方达到其满意的可信程度，因而可以进行交互，在交互过程中，同时针对交互时行为进行信任日志管理，记录下对方在交互过程中是否有违规行为发生，违规行为的例子有：(1)对初始请求的资源掌握过长的时间；(2)试图访问受保护的本地数据；(3)在资源上启动了非法的任务；(4)违背了提供资源的协定。交互结束后根据信任日志对对方的这次交互行为进行信任评价，从而可以更新对对方的信任关系，并记录在相关的信任关系表，以供以后交互请求时使用，还可以作为间接推荐的推荐代理来使用。整个网格计算环境的感性信任服务建立流程如图 4 所示。从以上考虑，我们认为感性信任机制的建立主要需要解决如下问题：

(1)信任关系的评估问题，即使用什么方法来对信任关系进行建模；

(2)推荐信任的建立问题，即如何通过中间节点的推荐来建立信任链路；

(3)信任链路的综合问题，即对所得到的信任链路怎样进行合成。

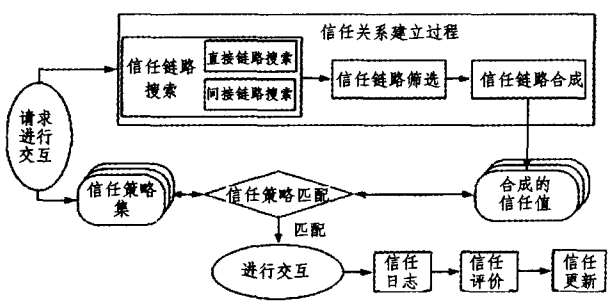

图 4 网格计算环境的感性信任服务建立流程图

4 有信任机制参与的网格安全模型

我们知道在传统的安全模块中，各个组成部分在网格对外提供服务时都有其相应的职能，如访问控制负责对用户的使用权限进行分配和限定。而感性信任服务作为一个新的组成部分，如何实现并发挥其功能和如何与原有的组成部分相协调则是需要认真研究的问题。对于一般的安全实施过程而言，首先是进行理性信任服务(调用认证服务)，认证通过后便是授权服务，确定用户的使用权限，而在用户使用系统资源的过程中需要对其行为进行追踪并审核；而从感性信任关系建立的流程可以看出，感性信任服务本身也就包含了这么一个过程，对信任关系的建立可以作为认证授权过程，而对运行过程的信任监测和更新则是审核过程，所以健全的感性信任服务可以单独作为安全模块进行使用，但这样却丧失了很多传统的安全服务的优势，同时也是对现有安全资源的浪费，因而主要还是需要将感性信任服务融入到现有的安全基础设施中。在加入感性信任服务之后，可以这样来考虑整个安全过程(如图 5 所示)：

(1)调用理性信任服务(认证服务)，通过认证机制对交互双方进行身份认证；

(2)认证通过后，调用感性信任服务，通过推荐代理的信任机制完成对被信任方的信任等级评判，确定信任度；

(3)在确定完对用户的信任度后，根据信任度的高低来指定对用户的权限授予(授权服务)，即信任度越高，则给用户的权限越大(当然还需要一些别的参考，比如有偿服务过程需要看用户给的报酬大小)；

(4)在资源访问及作业运作过程中，通过感性信任服务中的信任监控和信任特性调整的使用，调整对用户的信任度，而授权服务则动态地查看用户的信任度，从而动态地调整用户的使用权限。

该过程主要强调需要根据用户的信任度来授予权限，而不仅仅是根据用户的身份来授予权限，这类似于社会网络中的人际交往关系，也更具合理性。

在此我们提供一个网格服务实现例子来说明感性信任的使用，该网格服务模型如图 6 所示，采用 RBAC 来作为访问控制机制。从网格服务端对资源保护的角度来考虑，网格服务需要对用户身份、诚实度和所提交的作业有感性信任评判，用户身份可通过理性信任服务过程产生，作业信任度可通过对作业代码的扫描来检测是否包含恶意代码来确定，而用户的诚实度则依赖于具体的感性信任机制，如采用模糊集合理论来建立感性信任机制，建立信任等级关系，信任域 $U=\{u_0, u_1, u_2, u_3\}$ 为：u_0：表示“完全信任”；u_1：表示“比较信任”；u_2：表示“一般信任”；u_3：表示“不信任”。分别对应于[0,1]区间

的[0.9,1],[0.7,0.9],[0.5,0.7],[0,0.5]。

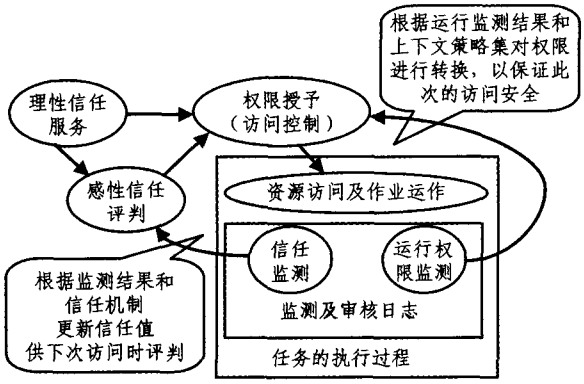

图5 网格计算环境的信任服务的使用示意图

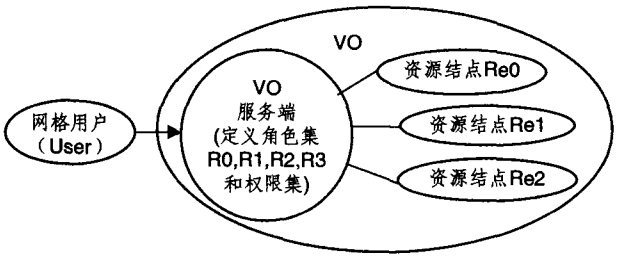

图6 网格服务实例模型

定义角色集$R=\{R0,R1,R2,R3\}$，它们之间是一种简单的继承关系即$R0\subseteq R1\subseteq R2\subseteq R3$，而权限集$P=\{P0,P1,P2,P3\}$，权限集$P$对应着的操作资源对$\{O,Re\}$为：操作$O$在此假定只有一种操作即运行用户的作业$Run$，而资源对应着VO内部的资源集合，在此假定为只有3个资源：{Re0,Re1,Re2}，而对应关系为：

$P3=Runon\{Re0,Re1,Re2\}$；

$P2=Runon\{\{Re0,Re1\}|\{Re1,Re2\}|\{Re2,Re0\}\}$；

$P1=Runon\{\{Re0\}|\{Re1\}|\{Re2\}\}$；$P0=RunonNULL$。

它们之间的继承关系为$P0\subseteq P1\subseteq P2\subseteq P3$（具体在$P1$和$P2$之间还需要细分）。相应的角色权限对应关系定义为：

$R3=\rangle P3=\rangle\{P0,P1,P2,P3\}$；

$R2=\rangle P2=\rangle\{P0,P1,P2\}$；

$R1=\rangle P1=\rangle\{P0,P1\}$；$R0=\rangle P0=\rangle NULL$。

角色和权限都有三种状态：激活(*active*)，分配(*enable*)和禁止(*disable*)，每个角色和权限在一次会话中都处于三种状态之一。

用户在通过理性信任服务和感性信任评判后得到信任度级别，而这种信任级别和角色集也是对应的：

$u3=\rangle R3=\rangle\{R0,R1,R2,R3\}$；$u2=\rangle R2=\rangle\{R0,R1,R2\}$；

$u1=\rangle R1=\rangle\{R0,R1\}$；$u0=\rangle R0=\rangle\{R0\}$。

因而网格服务端根据得到的用户信任度就能够给用户分配一个角色（该角色也是本次会话中的开始时的激活(active)角色），并得到一个角色子集（包括所分配的角色和所继承的角色），该角色子集即属于分配(enable)的角色，而没有分配的角色即属于禁止(disable)角色。相应的根据角色权限对应关系，得到相应的权限子集（包括所分配角色对应的权限和所继承角色对应的权限集合），因而系统就完成对用户的角色权限分配过程，用户所提交的任务就能够在所允许的资源上进行运行，相应的会话过程就产生了。该过程的对应分配关系如图7所示。

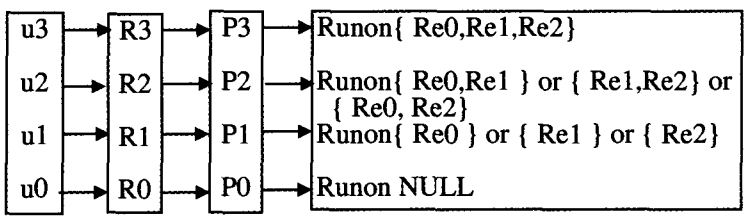

图7 实例模型中的信任度和角色权限的对应关系

结论 由于网格的开放网络环境，信任机制在网格计算中有广阔前景，目前国际上最具有影响的网格计算项目之一Globus中的安全模块GSI(Grid Security Infrastructure)已经尝试把Web服务安全规范融入到网格安全体系结构中，其中所包含的信任模型(WS-Trust)、隐私权模型(WS-Privacy)、联合信任(WS-Federation)、策略表达(WS-Policy)等规范都是关于网格计算信任的安全性规范，可见信任机制在以后的网格计算安全模块中占有重要地位。本文主要结合信任机制的特点分析了其在网格安全中的作用，并给出了信任机制参与的网格安全模型，通过实例分析了其在安全服务过程中的使用。

参考文献

1 Josang A, Knapskog S J. A metric for trusted systems[A]. Proceedings of the 21st National Security Conference[C], NSA, 1998. 16～29

2 Yu B, Singh M P. Distributed Reputation Management for Electronic Commerce[J], Computational Intelligence, 2002,18(4): 535～549

3 Yu B, Singh M P. Detecting Deception in Reputation Management[A]. In: Proceedings of the Second International Joint Conference on Autonomous Agents and Multi-Agent Systems[C], Melbourne, Australia, 2003. 73～80

4 唐文，陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报，2003,14(8):1401～1408

5 徐锋，吕建，郑玮，曹春. 一个软件服务协同中信任评估模型的设计[J]. 软件学报，2003,14(6): 1043～1051

6 Lin C, Varadharajan V, Wang Y, Pruthi V. Enhancing grid security with trust management[A]. Services Computing Proceedings [C] IEEE, 2004. 303～310

7 Song S, Hwang K. Fuzzy trust integration for security enforcement in grid computing[A]. In: International Symposium on Network and Parallel Computing(NPC2004)[C], 2004

8 Azzedin F, Maheswaran M. Evolving and managing trust in grid computing systems[A]. Electrical and Computer Engineering. IEEE CCECE 2002[C], Canadian, 2002. 1424～1429

9 Azzedin F, Maheswaran M. A trust brokering system and its application to resource management in public-resource grids[A]. In: 18th International Parallel and Distributed Processing Symposium (IPDPS'04)[C], 2004. 22～32