网格信任模型①

王维盛[1]，陶彦玲[2]

[1](西北师范大学 数学与信息科学学院，兰州 730070)
[2](西北师范大学 图书馆，兰州 730070)

摘 要：为了解决网格环境的动态性和不确定性带来的安全问题，需要对用户在网格环境下的行为进行评价，反映出该用户网络行为的可信程度。探讨了网格环境下的安全需求，给出了网格信任的相关定义，在前人研究的基础上，提出了一种新的网格信任模型，用来处理网格环境中用户之间的信任关系。该模型对网格环境中用户的信任度和声誉进行了分析，对域内的信任关系和域间的信任关系分别采用不同的方法来进行处理。研究了如何在网格计算中建立信任模型，来排除内部恶意用户，提高系统的安全可靠程度。

关键词：网格；信任模型；信任度；声誉；信任代理

Grid Trust Model

WANG Wei-Sheng[1], TAO Yan-Ling[2]

[1](School of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China)
[2](Library, Northwest Normal University, Lanzhou 730070, China)

Abstract: It is necessary to evaluate the network behavior of users in grid computing in order to resolve the security problems due to the dynamics and uncertainty of the grid environment. Thus, evaluation of the user’s behavior can reflect his reliability. This paper discusses the security requirements in grid environment, offers the correlative definitions of trust, According to the former analysis, a new grid trust model is proposed. This model is used to discriminate the trust relationships between users in the grid environment. It provides a method to analyze the trust degree of users and the report in the grid environment. The two different trust relationships within and between domain are handled with different approaches. This dissertation studies how to build a trust model for grid computing in order to find out malicious users and improve security and reliability of system.

Key words: grid; trust model; trust degree; report; trust agent

1 引言

对于网格应用来说，由于平台的灵活性和自由性，以及用户加入和离开的自由性，导致了网格应用无法要求用户提供关键认证信息，只能对用户进行注册登记而无法进行严格的认证。一种普遍被采用的方法是对用户评定信任等级，通过信任的传递和传播，用户可以获得目标用户先前的历史经验，据此选择可靠的交易对象，或选择更安全的资源服务对象[1]。

在社会网络中，信任关系是人际关系的核心，个体间的信任度往往取决于其他个体的推荐，同时，作为推荐者的可信度也决定其推荐个体的可信度。这种互相依赖的信任关系组成了信任网络[2]。在这样的信任网络中，任何用户的可信度都不是绝对可靠的，但可以作为其他用户决定其交互行为的依据。这类信任模型实际上是基于用户声誉的，反映一个用户过去长期的行为，能为没有直接接触的用户提供信任值[3,4]。它存在的弱点是不能有效防止协同作弊和诋毁的安全隐患。F.Azzedin 和 M.Maheswaran 首次将信任机制融入到网格的资源管理中，根据实体所在管理域之间的直接信任值和推荐信任值来计算网格中两个实体间的信任值，不足之处是认为域内所有实体的信任值相同。文献[5]将运用 PageRank 思想的 EigenTrust 模型引入到

① 收稿时间:2010-12-07;收到修改稿时间:2011-01-15

网格中，通过实体之间的局部信任值来计算实体的全局信任值，但是模型不能解决恶意推荐和欺骗同盟问题。文献[6]则把网格实体之间的信任关系分为域内信任关系和域间信任关系，两者采取不同的处理方式，域内实体的信任值远远高于非域内实体，比较符合实际情况，而且算法复杂度小，但是模型没有考虑时间因素的衰减，而且没有给出信任值的具体计算公式。文献[7]提出了一种分层信任模型来建立不同管理域之间的信任关系，存在的不足是没有充分体现实体的自主信任，当实体与其它域的实体进行交互时，即使已经有过直接的交互，也要严格地重新按照域间信任的流程进行，使算法复杂度增大。

针对以上问题，本文提出的网格信任模型，用户利用自己的直接交易经验、系统中域内用户的信任和全局用户声誉，对和自己将要交易的用户进行信任度评估。

2 网格信任模型的实现机制

在网格环境的信任机制研究中，通常分为基于用户身份的信任机制和基于用户行为的信任机制两类，前者关注于对网格环境中用户身份的真实性进行认证，以判定是否授权用户进行访问[8]，主要通过密码技术中的加密、数据隐藏、数字签名、认证协议和访问控制来完成。尽管这些技术的使用解决了信任评估中一些亟待解决的问题，但同时又引入了一些新的问题，例如，利用数字签名无法防止非法者的重放攻击。后者可以更好地解决网格用户间的可信性问题，行为信任针对两个用户之间进行事务处理时，根据用户在交易过程中所表现的行为给对方做出评价。对主体的行为信任进行建模的目的是为了形式化地研究在网格中如何对其他主体的信任度进行定义、评价和推导。在网格环境中网格用户的行为实时反映了其可信属性，其一段时期的行为数据从实质上反映了该用户域的信任值。本文将仅限于讨论行为信任，并约定文中后续部分如无特殊说明所提信任均指行为信任。

根据网格及其用户具有分布性、数量多、规模差异大等特点，考虑构建一种基于轻量级目录访问协议 LDAP 的用户信息目录树体系结构。该方案就是利用 LDAP 的目录链接功能，将整个目录分割为多个子目录，主目录的不同分支存放在不同的服务器中，所有分支合起来才构成完整的目录树。本文定义的网格环境的信任模型是以域(domain)为单位，分层次的信任计算模型，如图 1 所示。域中包含一个目录域服务器及若干用户，我们将它们统一描述为用户。网格系统内信任关系分三个层面：用户直接信任关系、域内信任关系和父子域间信任关系。

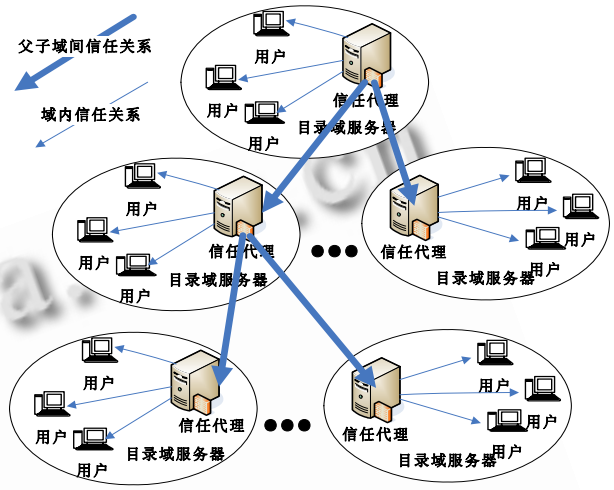

图 1 基于目录域服务器的网格信任模型

1)用户直接信任关系：用户根据与被交易用户直接交易的信息及自己的评估标准自主地评价被交易用户的信任度。

2)域内信任关系：用户的域内信任关系属于本地信任关系。信任度是由本地目录域管理者来评价的，域管理者评价域内用户可以采取本地域的管理策略，充分体现了域内自治的特点。当域的用户访问网格中其他域的服务时，提供服务者向用户所属域的信任代理查询该用户的信任度。

3)父子域间信任关系：用户的域间信任关系属于父子信任关系。是父域对子域的信任评价。子域的受信任程度是根据子域内的所有用户在网格中的网络行为以及该域提供的服务，是被其它域进行评价的。因此域的信任度是该域组织在网格中的信任度的综合体现，不代表任何具体的用户。

在目录域服务器上的信任代理负责信任管理。信任代理的功能有：1)允许用户加入域；2)计算并更新域中用户的域内信任表；3)检测并接受其它域中用户与该域中用户直接交易后的反馈信息，计算并更新该域中用户的声誉表；4)响应其它域的信任代理关于信任和声誉的查询请求；5)对于恶意用户，所属域可以对其进行相应的惩罚；6)用户从一个域转移到另一个域

时，允许继承在源域中的信任属性。

根据前面对信任概念的分析，我们得知信任关系(Relation)基于特定环境而存在，在特定环境中，存在多个影响信任关系的因素，这些因素称之为信任属性。比如交易过程中的交易金额，文件共享服务中文件的密级或重要程度等。信任属性的不同组成状态构成了不同的信任类型，信任类型（Type）根据信任内容划分，由具体信任属性（Attribute）刻画，可表示为 T(a1，a2，…，an)。其中 T 表示信任类型，ai 表示信任属性。信任属性是一个多维数组，其中有交易时的各种关键因素，因为，一个用户是否信任目的用户，可以认为目的用户所提供的服务质量是否达到该用户的 QoS 需求，因此，本模型引入 QoS 需求的概念对网格用户的信任度和声誉进行的量化评估，QoS 需求包括安全需求、通信需求(带宽、延时等)、计算能力需求、存储需求等诸多项目[9]。根据用户的实际情况和资源的种类，每个用户的 QoS 需求的项目数量是不同的，而且每个项目在整个 QoS 需求中所占的权重也不同。

信任类型本质上是一种概念，可以由信任属性刻画，信任关系与信任属性之间存在一定的函数关系：R=f(a1，a2，…，an)。

域中每个用户都维护一张直接信任表，表中包含了所有与之有过直接交易的用户信任信息；此外，每个域中的信任代理都维护两张表，一张是域内用户信任表，表中包含了采取本地域的管理策略评价的所有域内用户的信任信息，另一张是域内用户声誉表，表中包含了根据其它域的信任代理反馈的信息，而评价出的所有域内用户的声誉信息。

用户的信任值及声誉值是对一组交易情况的综合评判，我们采用简单的数学方法进行用户的信任值及声誉值的处理，计算的通用公式设计为：

$$S(t,c)=\sum_{k=1}^{n}(\omega_k \bullet a_k)] \bullet \lambda(t-t_{i,j},c)$$

其中，表示第 k 个 QoS 需求项目，是该项目的权重，在计算用户直接信任值时，它的值由评估用户来设定；在计算域内信任值时，它的值由被评估域的信任代理来设定；在计算全局声誉值时，它的值由被评估域的父域信任代理来设定。$\lambda(t-t_{i,j},c)$ 是时间衰减函数。信任值的下标 t 表示在某一时间下的信任值，c 表示在一定上下文关系下的信任值。信任不是简单的信与不信，一个主体对另一个主体的信任是有程度的，如不信任、一般信任、较信任、很信任、非常信任。因此，信任是在一定取值范围内连续变化的。

3　信任评估流程

在该模型中，实体利用自己的直接交易经验、系统中域内实体的信任和全局实体声誉，对和自己将要交易的实体进行信任度评估。

假设域 Di 和域 Dj 为父子域，域 Dk 中的实体 X 想要和域 Dj 中实体 Y 进行交易，在交易前先要考察实体 Y 的信任度。那么，怎样来实现和约束正确的信任关系，进行资源访问和交易呢？

我们的信任评估流程是：

1）实体 X 首先查询本地信任表，若有和实体 Y 的直接交易记录，并且，信任值大于设定的信任阀值，则实体 X 可以和实体 Y 进行较安全的交易，否则，转入下一步；

2）实体 X 请求本地域的信任代理，由域 Dk 的信任代理分别询问域 Di 和域 Dj 的信任代理，查询各自管理的声誉表和域内信任表，前者返回域 Dj 的声誉值和域内信任值，后者返回实体 Y 的声誉值和域内信任值，然后，域 Dk 的信任代理进行综合评判，并将结果返回给实体 X，若信任值大于设定的信任阀值，这时候可进行低风险的交易，否则，要么取消交易，要么进行高风险的交易；

3）如果实体 X 和实体 Y 进行交易，当交易结束后，实体 X 向本地域信任代理反馈交易情况，域 Dk 的信任代理分析判断，若情况属实，将结果分别反馈给域 Di 和域 Dj 的信任代理，从而影响域 Dj 和实体 Y 的声誉值，若情况有虚假，则域 Dk 的信任代理对实体 X 进行惩罚。

如果用户 X 和用户 Y 进行交易，当交易结束后，用户 X 向本地域信任代理反馈交易情况，域 Dk 的信任代理分析判断，若情况属实，将结果分别反馈给域 Di 和域 Dj 的信任代理，从而影响域 Dj 和用户 Y 的声誉值，若情况有虚假，则域 Dk 的信任代理对用户 X 进行惩罚。

当用户从一个域转移到另一个域时，为了描述方便，我们称用户转移前所属域为源域，转移后所属域为目标域。如果用户是普通用户而发生转移时，保持本地信任表不变，源域的信任代理将该用户的声誉值及域内信任值推荐给目标域的信任代理，若目标域的

信任代理接受，则源域的信任代理记录下该用户的地址变更情况，为其它域的信任代理查询该用户信息指明新路径，若目标域的信任代理不接受，则将该用户按照新用户加入，源域的信任代理删除该用户的相关记录，其它域的信任代理查询该用户信息时，将告知该用户已不存在；如果用户是目录域服务器而发生转移时，只允许子域树的整体转移，源域的父域信任代理将源的声誉值及域内信任值推荐给目标域的信任代理，若目标域的信任代理接受，则源域的父域信任代理记录下域的地址变更情况，为其它域的信任代理查询该域信息指明新路径，若目标域的信任代理不接受，则放弃本次转移。

对于新加入用户的信任度初值的设定，我们采取的办法是：不给新用户分配利益，即对新用户的信任度初值总是设为零。因为，如果初值设定太小，则初次欲提供服务的用户因信誉度太低而很难得不到任务，如果初值过大，该用户可能以欺骗的方式骗得一个任务后，再重新以一个新的身份再次骗得一个任务，这种恶意用户不停地注册新用户的行为，将导致整个系统崩溃。此外，无论管理域对新加入的用户，赋予的原始信任度是多少，都不能反映新用户的真实身份，也就是说，如果新用户的信任度初值不设为零，那么，不管该初值是否合理，都是一种欺骗行为。

根据以上分析信任评估流程，使用户直接信任值成为评估交互行为的第一因素，这较好地符合了实际情况。由于网格环境的分布性和异构性，所以在设计网格安全机制中考虑网格中用户的动态主体特性就显得特别重要。用户能根据自己的评估标准自主地选择符合的交互用户，信任代理也能实时地依据直接交互的评估来更新用户的信任值和声誉值。另外，自主信任较好地防范了入侵者恶意推荐带来的影响，并且能够有效地发现入侵同盟，使整个网格环境更加安全。

4 信任度的基本计算

根据前面的分析，该信任模型中的信任由直接信任、域内信任和全局声誉三部分组成。如图 2 所示。将直接信任关系表示为 Ti(V，t)，域内信任关系表示为 Tj(V，t)，全局声誉表示为 Re(V，t)，则 T(V，t)=α×Ti(V，t)+β×Re(V，t)+γ×Tj(V，t)其中，α、β 和 γ 分别是直接信任、全局声誉和域内信任的权值，并且 α+β+γ=1。α、β 和 γ 的值由用户自己确定。

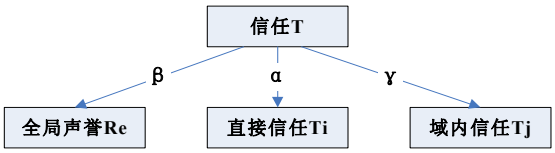

图 2 信任关系

建立以域为单位的信任关系，某个域的用户是由该域来管理、评判该用户的信誉，域内的所有用户在域外(网格系统内)的网络行为都代表“域”这个组织，这样形成了一个分级的、各个域自治的信任模型。假设网格系统中有 N 个域，每个域平均有 M 个用户，整个网格的信任计算复杂度是 O(f(N))；如果不采用分层次的信任模型，而是为每个用户进行全局评价，那么信任计算的复杂度是 O(f(N×M))。这样不仅降低了整个网格系统信任度的计算复杂度，而且没有改变域内原有的安全策略；同时域内的所有用户都代表该域在网格内进行交互，从长远来看，提升了域的可信程度；对于恶意用户，可以通过其所属域进行相应的惩罚。

5 信任计算模型的仿真与性能分析

实验环境：选择十几台计算机，用户端安装 Windows XP，目录域服务器选用 Windows Server 2003。因为 Windows Server 2003 的活动目录（Active Directory）是面向 Windows 的目录服务，它是基于 LDAP 而实现的，这样我们就构造了一个简单且实用的实验环境，来验证本文提出的信任模型的性能。

实验内容简介：为了比较不同的信任策略对于应用的有效性，我们构造了多个仿真实验，实现了基于传统的方法、基于推荐的方法和本文提出的域与自主性相结合的方法的仿真。为了简化分析，仿真实验的交易内容仅涉及文件下载服务，能否成功下载文件是判断交易成功与否的标准，而信任策略的成功则不仅体现在引导成功交易上还体现在避免恶意欺诈上。

实验中设计了以下两类节点：

1）目录域服务器：由 Windows Server 2003 服务器来充当，负责信任代理职能，包括域内节点的加入、移动、删除、信任初始化；维护存储本域节点信任值的域内实体信任表，采取本地域的管理策略评价所有域内实体的信任信息；维护存储域内实体全局声誉表，根据其它域的信任代理反馈的信息，评价所有域内实体的声誉信息；回答本域节点的信任提问；回答其他

域代理的信任提问；进行信任值的定期和交易更新等。

2）普通节点：即归属于各个域，域中每个实体都维护一张实体直接信任表，记录了所有与之有过直接交易的实体信任信息。本地可能存放有一个或多个文件，能为其他节点提供下载，同样自己也需要从其他节点下载文件。

节点在不同时刻的交易行为可以分为：1) 善意的交易行为；2) 恶意的交易行为；3) 善意的信任汇报行为；4) 恶意的信任汇报行为。

仿真实验的流程如下：

1）域的初始化：生成域代理节点；

2）节点初始化：生成交易的全部节点，节点随机加入域，由所属域的代理来生成该节点的证书，决定节点的信任初值，完成节点的信任初始化；

3）文件初始化：全部文件随机分配至任一域的任一节点；

4）节点随机选择文件进行下载；

5）输出交易成功率和信任度。

实验结果分析：我们设计的仿真实验模拟规模为 17 个节点，可提供下载的文件总数为 200。我们将 200 个文件随机分配到各信任域的各个节点。我们在网络中设置一定比例的恶意节点，这些节点以一定的概率进行恶意的交易或恶意的信任汇报。

随着恶意节点所占比例的增加，下载成功率有所下降。随着恶意节点的增加，实验表明完全忽略全局声誉的作用容易受到攻击者的攻击,因为任何一个非法实体都可以提交一个错误的评估来影响整个评估系统的准确性。本文所采用的计算方法不容易受这种攻击的影响，并且能更准确地反映节点之间的信任关系。

对于本文提出的域与自主性相结合的下载策略，我们进一步分析全局声誉对不同节点信任度的影响情况，所有节点都进行善意的交易，它们的信任度都稳步上升，节点出现不同程度的恶意行为，将导致信任度急剧下降，相应的节点所在域的全局声誉值也随之下降，由此与该节点属于同一个自治域的其它节点的信任度也有所下降，这种情况正好反应了该信任模型提供的激励机制的有效性。激励机制的引入，对防范协同作弊和诋毁的安全隐患起到较好的效果，考虑到信任值的稳定性，应赋予全局声誉值较低的权重。

模型性能分析：本文提出的信任计算模型区分了实体直接信任关系、域内实体信任关系和域内实体全局声誉关系，每个域设置一个信任代理，根据域内和域间交易两种情况，采取不同的方法计算信任值，更加准确的评估了实体间的信任关系，有效地解决了网格系统中存在的实体行为信任问题。

通过把网格分成若干个自治域，并对域内实体间的信任关系和域间实体间的信任关系分别处理，与传统的方法相比，该模型的计算及存储复杂度更小，对信任值的计算更为合理、高效。该方法对信任值的计算时间不会单纯的随节点数的增加而增加，域内实体信任值及域内实体声誉值的计算仅受域内节点数而不是全局节点数的影响，也就是说当节点数增加而域的数目不变时，计算时间将不受影响。同理可知，与传统的方法相比，该模型的信任/声誉关系表信息的存储复杂度也更小。

6 结语

在信任模型中划分信任域、设置信任代理的方式是比较合理的，这样做不仅比较符合现实世界的情况，也有利于将个体从繁琐的信任迭代计算中解脱出来，提高网格应用效率。使用信任策略来实现可信赖的网格应用，将大大提高网格交易的成功率和交易的安全性。从目前研究的发展趋势来看，动态信任关系的度量模型与预测技术不但是解决大规模开放分布式网络安全问题的基础性工作和必须首先解决的核心科学问题，也是近年来可信网络、可信软件等新型可信计算领域的基础性研究课题。结合人类的心理认知过程，进一步研究信任关系的内涵，尤其是动态信任关系的相关性质、信任的表述和度量的合理性，这对信任关系的建模是非常重要的，也是信任关系建模的基础。

参考文献

1 徐志伟,冯百明,李伟.网格计算技术.北京:电子工业出版社, 2004.32−71.

2 McKnight DH, Chervany NL. Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model. 34th Annual Hawaii International Conference on System Sciences (HICSS-34). 2001,7:7022−7031.

3 刘浩,张连明,卿桐.一种综合的 P2P 网络信任模型.计算机工程与应用,2010,46(15):93−98.

(下转第 85 页)

参考文献

1 Hand DJ, Mannila H, Smyth P. Principles of Data Mining (Adaptive Computation and Machine Learning), MIT Press, 2001.

2 Andrews R, Diederich J, Tickle AB, A survey, critique of techniques for extracting rules from trained artificial neural networks, Knowledge Based Systems, 1995,8(6): 373–389.

3 Bologna G. Is the worth generating rules from neural network ensembles. Journal of Applied Logic, 2004,(2): 325–348.

4 Elalfi AE, Haqueb R, Elalami ME. Extracting rules from trained neural network using GA for managing E-business. Applied Soft Computing, 2004,(4):65–77.

5 Kahramanli H, Allahverdi N. Rule extraction from trained adaptive neural networks using artificial immune systems. Expert Systems with Applications, 2009,(36): 1513–1522.

6 Lale Özbakir a, Adil Baykasoglu b, Sinem Kulluk a, Hüseyin Yapici c. An ant colony based algorithm for rule extraction from trained neural networks. Expert Systems with Applications, 2009. doi:10.1016/j.eswa.2009.04.058

7 Diego A. Computational Intelligence: For Engineering and Manufacturing. Boston, Springer US, MA: USA, 2007.

8 Dorigo M, Maniezzo V, Colorni A. Positive feedback as a search strategy. Technical Report N.91-016 Politecnico di Milano, 1991.

9 Hiroyasu T, Miki M, Ono Y, Minami, Y. Ant colony for continuous functions. The Science and Engineering, Doshisha University. 2000.

10 Tan C, Yu Q, Ang JH. A dual-objective evolutionary algorithm for rulesextraction in data mining. Computational Optimization and Applications, 2006, 34: 273–294.

11 Chen T, Hsu TA. Gas based approach for mining breast cancer pattern.Expert Systems with Applications, 2006,30: 674–681.

(上接第 110 页)

4 Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems. IEEE Canadian Conference on Electrical & Computer Engineering (CCECE'02). May 2002. 1424–1429.

5 Alunkal B, Veljkovic L, Laszewski GV, et al. Reputation-based Grid resource selection. Proc. of the Workshop on Adaptive GridMiddleware. New Orleans, 2003.

6 王莉苹,杨寿保.网格环境中的一种信任模型.计算机工程与应用,2004,40(23):50–53.

7 王珊,高迎,程涛远,等.服务网格环境下基于行为的双层信任模型的研究.计算机应用,2005,9:1974–1991.

8 王东安,徐浩,南凯,等.基于推荐的网格计算的信任模型计算机应用研究.计算机应用研究,2006,2:96–98.

9 李文娟,王晓东,傅仰耿,傅志祥.几种网格信任模型的研究.福州大学学报(自然科学版),2006,34(2):190–193.