一种改进的基于行为的网格信任模型

An Improved Behavior – Based Trust Model in Grid System

易 磊　杨长兴　（中南大学信息科学与工程学院 计算机系 湖南长沙 410083）

摘　要： 网格环境中的信任问题是当前网格研究的一个热点，为了解决网格环境的动态性和不确定性带来的安全问题，文章在研究现有信任关系的基础上提出了一种新的基于行为的信任模型来处理实体间的信任关系，引入身份权概念，对域内信任关系和域间信任关系采取不同的方法进行处理。实验及分析结果表明，该模型能有效地解决网格环境中存在的安全问题。

关键词： 网格 信任模型 行为信任 身份权

网格计算技术是近年来国内外计算机业研究的热点，是构筑在因特网上的一组新兴技术，目的是为用户提供一种全面共享各种资源的基础设施。但因其大规模、分布、异构和动态等特性使得网格计算环境非常复杂，提出了比传统网络环境更高更广泛的安全需求。为了使网格计算更安全、更具吸引力，用户实体间的互信问题显得格外重要，这种互信具体包括两种信任：身份信任和行为信任。其中身份信任主要负责的是用户身份验证以及用户权限问题等，主要通过诸如加密、数字签名、认证协议以及存储控制方法来实现，而行为信任关注的却是更现实、更广泛意义上的可信赖性问题，用户实体间可根据过去相互间直接的或间接的行为接触经验而及时动态地调整更新彼此间的信任关系，从而最大程度地保证网格行为的安全可靠。本文从网格的结构特点出发，在现有信任模型的基础上，给出了一个基于行为的分层信任模型，用来建立不同管理域之间的信任关系。

1　信任关系

1.1　信任定义

Farag Azzedin 在文献[1]中对信任在网格环境中的定义为：信任是指其他实体对某个实体的行为能否达到他们所期望的能力的可靠信心值。这种可靠信心在很大程度上由实体本身的过去行为所决定，并且随实体的行为而动态变化。

1.2　信任关系分类

实体之间的信任关系可以分为两类：直接信任和推荐信任。

直接信任：是指两个实体之间曾经有过直接的交易，它们之间建立了一种直接信任关系，信任值来源于根据双方的交易情况得出的直接经验。

推荐信任：是指两个实体之间没有进行过直接的交易，而是根据其它实体的推荐建立的一种信任关系，它们之间的信任值是根据其它实体的评估得出的结果。

1.3　信任关系的性质

根据上面对信任的定义，网格环境中实体之间的信任关系有以下性质：

（1）信任关系总是存在于两个实体之间的；

（2）主观性；

（3）非对称性；

（4）有条件的传递性；

（5）传播性；

（6）动态性。

2　信任模型

2.1　几种典型信任模型的分析比较

目前主要有以下三种信任模型：基于信任域的信任模型、基于主观逻辑的信任模型和基于模糊逻辑的基本行为信任模型。

基于信任域的信任模型[2-4]将网格划分成若干自治域，将节点间信任关系分为域内信任关系和域间信

任关系，设置不同的策略来处理这两种信任关系。该模型的优点在于：①使用不同的策略来区别对待这两种信任关系，比较符合现实社会情况；②算法复杂度小，域内信任值的计算复杂度仅依赖于域内节点数目，域间计算复杂度仅取决于域的个数。缺点是：①该模型没有考虑交易上下文，而上下文环境是决定信任的一个必要因素；②未充分体现网格节点的信任自主，异域节点每次交易都要严格按照域间信任抉择的顺序进行，过于繁复；③没有给出系统初值的建立办法；④对其他域的推荐信任未设置推荐权；⑤未考虑时间衰减。

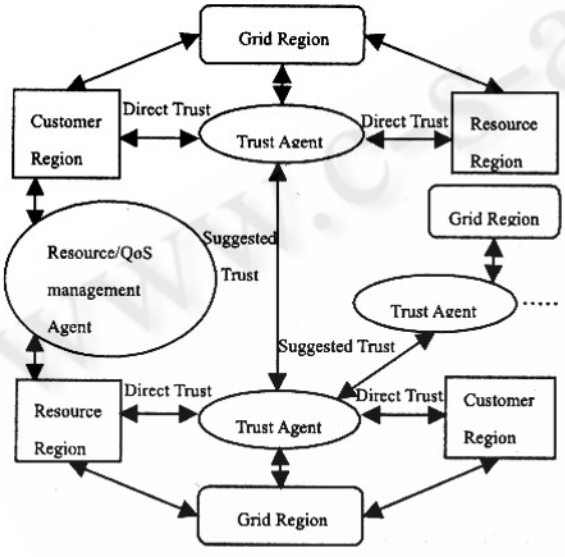

Figure 1 The Framework of Trust model

图 1 信任模型框架图

基于主观逻辑的信任模型[5]使用 3 个维（分别为信任度、不信任度和不确定度，三者和为 1）来度量信任。若 AB 之间存在之间直接对话，则根据三个维度的值进行信任抉择；若 AB 之间没有直接信任对话，则 A 将对 B 的数字签名要求在与自己有直接信任联系的节点中广播，收到要求的节点对 A 做出回复，A 根据收到的推荐值与推荐节点的推荐信任度计算 B 的信任值。该模型的优点在于：①基于主观逻辑。将主观逻辑应用于网格信任领域可以说是一种突破；②基于网格应用全生命周期的研究基础上，从系统初值产生到信任抉择都有相应的算法支撑；③应用该策略可以设置对安全层透明的信任管理层，增加了信任抉择的弹性和可测量性，这一点很适合目前的开放网格体系结构。缺点是：①无法实现身份认证和行为认证的统一；②无法消除恶意推荐带来的负面影响；③节点独立完成信任抉择，增加了节点开销，使得系统设计复杂，很难实现应用。

基于模糊逻辑的基本行为信任模型[1]按照信任度的大小将信任划分成不同的等级。节点维护两张表：直接信任关系表 DTT（Direct Trust Table）和推荐信任关系表 RTT（Recommended Trust Table），并设权值来分别表示直接信任和间接信任的重要性。该模型的优点在于：①使用直接信任和推荐信任的综合来产生信任值，且加入信任衰减函数和推荐信任因子，考虑较为全面；②使用模糊逻辑来判断信任符合人类社会行为习惯。缺点在于：①未考虑身份信任；②节点间的信任关系的维护是一个非常烦杂的工作；③很难找到一个合适的衰减函数来度量时间推移对信任值产生的影响。

2.2 改进思想

综上所述，以上三种模型各有利弊，但同时设计理念并非完全垂直。针对网格自身的特点，本文提出以下改进想法：信任域的划分思想是合理的，不同的域可以各自采取不同的策略；在主观逻辑信任模型的基础上减轻节点开销，由信任代理存储域间信任关系表；考虑交易上下文；设置信任管理层，提高节点的自主信任抉择；选择合适的衰减函数；节点信任初始值的建立考虑身份信任等等。

在此模型中，将整个网格系统划分成多个自治的网格区域，同时又把每个网格区域的节点虚拟划分成资源域和客户域，资源域和客户域与本域的信任代理是直接信任的关系。整个模型框架如图 1 所示。

首先进行信任模型的初始化，即确定节点的初始信任值。节点的初始信任值由本域的信任代理（特殊的节点）评估产生。节点加入某个域的初始时刻，由代理根据节点的身份权来决定节点的信任初始值，在本文中身份权是指隶属于节点身份并与域的结盟条件相对应的节点的属性值，信任代理根据其身份权选择将其加入资源域还是客户域，并按照本域的指标（每个域建立的目标不同，会有不同的评价指标）给出初始信任值。另外也可以参照节点加入时为其提供推荐的节点的信任值来决定该节点的信任值。

然后针对节点属于相同或不同域的情况，将信任模型分为域内信任关系和域间信任关系分别进行

考虑。

2.3 域内信任关系

域内信任关系是同一域内实体之间的交易。这里信任值的计算不采用传统的计算方法，即根据实体之间以往的交易情况以及综合其它实体的评估来计算信任值，而是采用了一种新的计算方法：节点首先查询存储在本地的节点信任关系表，若存在对应交易节点且交易类型为本次交易类型则根据相应信任值进行决断。若信任值超过某一预定阀值，则同意交易，否则交易结束；若不存在交易节点记录，或虽存在交易节点记录但交易类型并非本次交易类型的，则转换查找交易类型为信任推荐，若能在本地信任关系表中找到某一与本节点有过直接交易且与对方节点有过直接交易的节点，则使用该节点提供的推荐值，否则查找失败，信任值为 0，表示两者之间无信任关系。

在这个模型中，节点只负责维护节点信任关系表，采取表 1 的数据结构。

表 1　节点信任关系表

Node ID	Transaction Type	Domain ID Node Belong to	Trust Value	Generation Time

节点 ID 是指与本节点有过交易的其他节点标识；交易类型即交易上下文服务环境，是一个环境变量，其值如打印、计算等等，并且将信任推荐作为一种交易类型；所属域名即指与其交易节点所在的域名；信任值是指上一次交易完成后给出的评价，取值范围在[0,1]之间；信任值生成时间是在信任更新时使用的，并与衰减函数有关。

2.4 域间信任关系

域间信任关系基于不同域实体之间的交互。两个域之间的信任值是根据它们的直接信任关系和其它域的评估综合得出的，不同于域内信任值的计算方法。

每个自治域有一个信任代理(Trust Agent)，该信任代理负责维护两张表：域内节点信任关系表和域间信任关系表。域内节点信任关系表是包含域内所有节点的权值表，采取表 2 的数据结构；域间信任关系表包含了所有与之有过直接交易的域，采取表 3 的数据结构，两个域有直接交易是指两个域的节点之间有过直接交易。这里域间信任关系指的是域作为一个整体与其它域之间的直接信任关系，域间节点之间的交易会影响域间信任关系。

表 2　域内节点信任关系表

Node ID	Transaction Type	Trust Value	Generation Time

表 3　域间信任关系表

Domain ID	Transaction Type	Trust Value	Suggest factor

每个表项具体含义同表 1。域名 ID 是指与本域有过交易的其他域的标识，推荐因子是指本域对与其有过交易的其他域的推荐系数。

当交易发生时，首先询问域代理，域代理向其他域发出信任请求，由节点归属域的代理查找它的域内节点信任关系表并回复，本域的域代理得到回复后，根据域信任关系表中对应域的整体信任值和回复值计算节点信任值，并将所得结果回复询问节点。

举例说明，计算不同自治域之间两个实体 i 对 j 的信任值 Trust(i,j) 的步骤如下：

(1) 首先计算域间的信任值[1]

为了方便计算域之间的信任度，本文规定信任度取值在[0,1]之间。根据对信任的定义及其属性的描述，给出如下定义：

定义 1：域 D_i 对 D_j 的整体信任度是 $r(D_i,D_j,t,c)$，其中 t 是当前时间，c 是指定的服务。

定义 2：域 D_i 对 D_j 的直接信任度是 $\Theta(D_i,D_j,t,c)$，t 和 c 的含义同上。

定义 3：除了 D_i，其他域对 D_i 的推荐信任度是 $\Omega(D_j,t,c)$，t 和 c 含义同定义 1。

定义 4：域信任关系表 $DTT(D_i,D_j,c)$ 存储了对其他域的评价。

定义 5：其他域 D_k 对 D_j 的推荐因子 $R(D_k,D_j,c)$，这是为了防止联合欺骗行为引入的。

定义 6：时间衰减函数 $\Psi(t-t_{ij},c)$，信任值随时间而减弱。

$$\Gamma(D_i,D_j,t,c)=\alpha\times\Theta(D_i,D_j,t,c)+\beta\times\Omega(D_j,t,c)$$

$$\Theta(D_i,D_j,t,c)=DTT(D_i,D_j,c)\times\Psi(t-t_{ij},c)$$

$$\Omega(D_j,t,c)=\frac{\sum_{k=1}^{n}DTT(D_k,D_j,c)\times R(D_k,D_j,c)\times\Psi(t-t_{ij},c)}{\sum_{k=1}^{n}R(D_k,D_j,c)}$$

$$\Psi(t-t_{ij},c)=\frac{1}{1+(t-t_{ij})/S(c,d_i,d_j,\cdots)}$$

其中 $S(c,d_i,d_j,\cdots)$ 为衰减速率。

(2) 再计算 i 对 j 的信任值：查找 D_j 的域内节点信任关系表找到 j 的信任值 weigh(j)，得到 $Trusti(j)=weigh(j)\times\Gamma(D_i,D_j,t,c)$。

2.5 信任值更新

每隔一段时间，需要进行信任值的更新。

更新节点信任关系表体现在时间和交易两方面。具体如下：设置一个时间阀，每隔一个时间阀，删除信任表中已经过期的记录；交易发生后评估交易对象的信任值，若非首次交易对象，则更新信任表的相应记录，更新的内容包括交易时间和信任值；若为首次交易对象则在信任表中增加相应记录来存储该对象的各项数据，并且若该对象的信任值是通过信任推荐得到，则同时更新推荐者的推荐信任值；交易完成后，向信任代理汇报交易对象的信任评估，引发信任代理更新信任表。

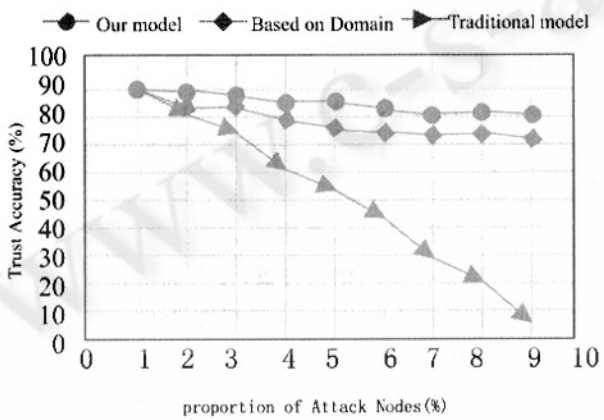

图 2　受到攻击时信任准确度的变化

更新代理的域内节点信任关系表和域信任关系表同样体现在时间和交易两方面。可以简单地选择一个函数作为时间衰减函数以体现时间流逝对信任值的削弱作用。更新时间可以是每隔一个固定时间段对两张表的全部节点统一更新或者可以在收到信任请求的时刻单独更新相应对象的信任值。收到域内节点交易后的信任汇报后，代理需要更新信任关系表。若节点的交易对象为本域节点则更新域内节点信任关系表的相应记录；若为异域节点，则根据实际信任值与收到的推荐值来更新对应域的整体信任值，即更新域信任关系表。更新本域结点的信任值时，需要综合考虑提交的信任值与提交报告节点的信任值。更新异域的域间信任关系时，无需考虑本域提交报告节点的信任值。

3　实验结果及分析

为了验证该模型的准确性和高效性，进行了模拟实验。在实验中，每个节点维护一定量的关于其它节点的历史信息。每次随机的选取一定比例的节点作为攻击者，提供错误的评估信息。本文设计的仿真实验模拟规模为 2000 个节点的网格环境，可提供下载的文件总数为 10000，将 10000 个文件随机分配到各信任域的各个节点，每个节点在整个仿真过程中必须完成 100 次交易（下载 100 次）。该实验主要为检验不同比例的恶意攻击节点对本文的模型以及对使用传统方法和使用基于域的信任模型的影响。信任准确度测试结果如图 2 所示。

实验表明传统的计算方法很容易受到攻击者的攻击，因为任何一个非法用户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。

4　结论

本文提出了一个基于行为的信任模型，用以解决处于不同管理域的实体之间交互的安全性。实验及分析结果表明，该模型能很好地解决网格环境中的安全问题和信任问题。

参考文献

1 Azzedin F, Maheswaran M. Evolving and managing trust in grid computing systems[C]. In: Canadian Conference on Electrical and Computer Engineering, IEEE CCECE 2002, Volume 3, 2002: 1424 ~ 1429.

2 Alfarez Abdul—Rahman, Stephen Hailes. Supporting trust in virtual communities[C]//Proceedings of the 33rd Hawmi International Conference on System Sciences. [S. l.]: [s. n.], 2000: 6007.

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

4 王东安、秦刚、南凯、阎保平，网格计算中信任管理模型的研究[J]，计算机工程，2006，32(7)：32 - 34.