第18卷 第9期
2008年9月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.18 No.9
Sep. 2008

基于网格环境的动态自适应信任机制研究

王胜川,刘方爱,石晓晶
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:为了满足网格系统的异构、动态、开放等特性,提出了一种动态自适应的网格信任模型,在该模型中节点是独立自主的,相对于传统信任模型更加适合在网格环境下运行,系统的节点加入更加自由,降低了节点负担和网络阻塞。并将信任度划分为提供服务和使用服务的两种形式,同时在模型中引入了修正因子和上下文环境对节点进行评估和反馈,避免了恶意节点利用高信誉值进行欺骗行为的发生。模拟实验表明该模型节点交易成功率有了很大的提高。

关键词:网格安全;信任模型;网格;信任域
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2008)09-0151-04

Study of Dynamic Adaptive Trust Mechanism Based on Grid

WANG Sheng-chuan, LIU Fang-ai, SHI Xiao-jing
(Sch. of Info. Sci. and Eng., Shandong Normal University, Jinan 250014, China)

Abstract: To satisfy the isomerous, dynamic, open grid system, presents a dynamic self-adaptive trust model. In this model, nodes is independent and self-governed, it is more conformable than conventional trust model, node is more free and the burden of the node is lowed, also net jam is alleviative. Trust is divided into two parts: use services and offer services. Also, indroduced correctional gene and context in order to evaluate the nodes in this model. The simulation results demonstrate the model can resist vicious attack better, this can efficiently improve the probability of successful trade-off.

Key words: grid security; trust model; grid; trust domain

0 引 言

信任管理的基本思想是系统的安全决策需要依靠第三方提供的附加的安全信息来确定系统中安全信息的完整性,比如Globus项目中的GSI主要基于公钥加密体系PKI[1]。由于网格自身的异构、动态、开放、大范围共享资源的特性,系统形态正从面向封闭的、相对静态的形式向开放的、动态协作的服务模式转变。在开放的网格系统中,没有中心化的管理权威可以依赖,这样实体间交互时就产生了动态信任管理问题。所以,在网格环境下建立起合理可靠的信任模型机制,使资源共享的安全性得以保证,成为网格安全研究的一个核心内容。

从社会学的角度看,信任关系是最复杂的社会关系之一,是一个很难度量的抽象的心理认知,信任也是与上下文相关的一个动态过程,随着时间的变化,实体之间的行为上下文可能会动态地变化,并且具有时间滞后性的特点。目前的一些信任模型主要是根据以往的交易经验和其它实体的评价来衡量实体之间的信任关系,节点维护节点信任值表,一旦节点退出网格系统,它所维护的信任值表也将丢失,没有充分体现出网格节点的信任自主性;另外模型未充分考虑交易上下文,而上下文是决定信任的一个重要因素。

收稿日期:2007-12-10
基金项目:国家自然科学基金资助项目(60373063)
作者简介:王胜川(1982-),男,山东济宁人,硕士研究生,研究方向为网络计算、网络安全;刘方爱,博士,教授,博士生导师,研究方向为分布式处理、并行算法、光互联网路由算法、网格计算、网络环境下应用开发技术。

1 动态信任关系

1.1 相关概念

定义1 信任(trust)[2]:信任不同于人们对客观事物的"相信(believe)",而是一种主观判断,信任本身并不是事实,而是关于所观察到的事实的知识。

定义2 直接信任(direct trust):表示在给定的上下文中,一个实体根据直接接触行为的历史纪录而得出的对另外一个实体的信任程度。

定义3 间接信任(indirect trust):表示实体间通过第三者的间接推荐形成的信任度,也叫声誉(reputation)、推荐信任、反馈信任。

1.2 动态信任本体论

信任的动态性是由信任关系中实体的自然属性决定的[3]。在现实世界中,动态性既可以由实体的内因(endogenous factors,例如实体的心理、性格、知识、能力等)引起,也可以由实体的外因(exogenous factors,例如实体表现出来的行为、策略、协议等)引起,但内因很难由其它实体来判断和量化,而外因可以直接观察到,尽管非常模糊和不确定,但是可以进行预测、量化和推理。

Lea[4]通过对 10 年来信任模型的研究总结,提出了一个综合的动态信任 Ontology。Lea 对一些信任模型根据他们采用的输入因子进行了分类,并取这些模型中输入因子的并集,提出 Ontology 模型。信任的主体称为 Turster,信任的客体称为 Trustee。首先,Truster 和 Trustee 之间的信任关系评估决定于 Truster 的主观行为(action),而这种 action 具有其相关的一些行为属性,如 risk, benefit, importance 等,Trustor 利用上下文信息和历史数据进行信任的动态评估;其次,信任关系也依赖于双方的 competence 和 confidence;第三,一些第三方的信息,如声誉、凭证、推荐信息,也可以影响到信任评估。

2 模型的基本思想

2.1 信任度的划分

在单一信任的情况下,恶意节点可以一直以提供服务的情况来增加信任值,而不去访问其它节点。当有破坏价值高的情况下,恶意节点很容易实施自己的破坏行为,被攻击的节点也不能根据信任值来判断该恶意节点使用资源的信任情况,因此容易受到攻击。在文中提出的模型中,定义信任为服务提供质量信任和资源使用信任两种不同的信任评估标准,两种信任的建立均由网格应用中实体之间的具体交互行为决定[5]。

2.2 网格实体的独立自主性

网格中虚拟组织的成员是活动的,节点退出后,它所维护的信任表也就丢失,如果节点信任值只由节点自己维护的话,当节点退出后,许多信任值也就丢失,这样对网格中的信任关系可能会产生很大的影响,并且对一个节点来说,维护复杂的信任表是很困难的事情,应该让信任值由专门的信任代理进行维护,节点只维护自己信任并能直接访问的节点的信任情况,这样降低了节点负担,增加了节点的独立自主性,降低了网络的阻塞[6]。

2.3 节点加入策略

域内每一个节点赋一个权重值,用来表示不同的节点对该域信任值的影响因子。例如:新加入节点的权重值较低,一旦发现该节点是非法攻击者或者有不诚实行为,就大大降低其权重值以减少它对该域信任值的负面影响。而长期存在的,对域的信任值有贡献的成员节点的权重值较高。

在文中提出的模型中,域内信任代理信任表就存放了各节点的平均信任值,可以从一定程度上反映出节点的影响因子,可以由该表得到节点的权重值(见图 1)。

2.4 模型中的辅助因子

(1)交易上下文(C):交易上下文在对信誉度的计算中是一个非常重要的因子。比如:节点 A 对节点 B 在商业交易行为中表现的好坏比较熟悉,如果让节点 A 咨询节点 B 在科研交易中的信誉值则会得到片面的结果。

(2)权重值:可信度高的节点发回的反馈值比从可信度低的节点发回的反馈值拥有更高的优先级,用权重系数来衡量:声誉评价越高,权重系数越大;反之越小。

(3)衰减函数:为了表示信任度随时间变化的动态性,令 $\Gamma(t-t_w,c)$ 表示衰减函数,其中 t 是当前时刻,t_w 是最后一次更新或接触时间,c 是指交易上下文[7]。

(4)调整因子:有的实体会对其它节点的评价时严格一些,而有的评价宽松一些,为了找到合理的评价,使用调整因子 $A(X)$,调整因子可以将信誉进行修正,使结果更加接近真实情况。

2.5 模型结构图

如图 1 所示:

域间信任由域内各个信任代理存储,域间代理负责域内代理的创建、维护等管理行为。域内信任代理维护域间信任关系表 DTT、域内服务提供质量信任关系表 DSQTT 和域内资源使用信任关系表 DRUTT。域内的节点维护本节点的服务提供质量信任关系表 SQTT 和资源使用信任关系表 RUTT。

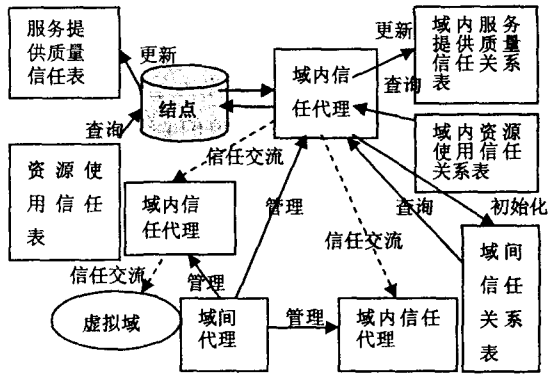

图 1 模型结构图

3　信任值的求解

3.1　域内节点交易策略

该算法如下:

(1)当节点 X 需要使用节点 Y 的服务时,首先向自身维护的 SQTT 表查询,若存在则计算信任值 E,由 E 得到信任等级 T_{XY},将 T_{XY} 与该域服务提供质量的信任门限[8] $T_{service}$ 或本节点设置的信任门限比较,若大于门限则认为 Y 可信,并向 Y 提交服务请求;否则,转(3)。

(2) 节点 Y 收到节点 X 的服务请求后,首先向自身维护的 RUTT 查询,若存在则计算信任值 E,得到信任等级 T_{XY},将 T_{XY} 与该域服务提供质量的信任门限 $T_{service}$ 或本节点设置的信任门限比较,若大于门限则认为 X 可信,并向 X 提供服务;否则拒绝 X 的请求,如果查询不到 X 的直接信任值,转(4)。

(3)X 查询所在域的域内代理 A 维护的信任关系表 DTT 和 DSQTT,计算 Y 提供服务质量的信任值 E,并根据 E 得到新人等级 T_{XY},将 T_{XY} 与该域服务提供质量的信任门限 $T_{service}$ 或本节点设置的信任门限比较,如果大于门限则认为 Y 可信,并向 Y 提交服务请求。然后转(2),否则放弃该请求。

(4)Y 查询所在域的域内代理 B 维护的信任关系表 DTT 和 DSQTT,计算 X 的资源使用的信任值 E,得到信任等级 T_{XY},将 T_{XY} 与该域服务提供质量的信任门限 $T_{service}$ 或本节点设置的信任门限比较,如果大于门限则认为 X 可以信任,并向 X 提供服务;否则拒绝 X 的服务请求。

3.2　域间节点交易策略

A、B 为不同的虚拟域。X 为 A 中的节点,Y 为 B 中的节点,要计算 X 对 Y 的信任值,首先计算域间的信任值 $E(B)$。$E(B)$ 表示域 A 对域 B 的信任值,对 Y 的信任值 $E(Y)$ 的计算:

该算法如下[9]:

(1)A 的信任代理查找它的域间信任关系表,看是否与 B 有直接信任关系,若有,则将相应的信任值赋给 $T_A(B)$;否则转(2),表示 A、B 间无直接信任关系。

(2)A 的域内信任代理向除 B 之外的其它域的域内信任代理发出评估请求,其它的域内信任代理收到请求后,查找自己的域间信任关系表,若与 B 有直接信任关系,则将相应的信任值赋给 $T_{X_i}(B)$,否则 $T_{X_i}(B)=0$。X_i 表示除 A、B 之外的任意一个其它域。最后根据这些应答信息计算:

$$E(B)=\frac{\sum_{i=1}^{n}X_i(B)}{n}$$

N 表示除 A、B 之外的其它域的数目。

(3) 综合(1)、(2) 可以得到自治域之间的信任值计算公式:

$$E(B)=\begin{cases}T_A(B) \\ E(B)=\dfrac{\sum_{i=1}^{n}X_i(B)}{n}\end{cases}$$

N 表示除 A、B 之外的其它域的数目,X_i 表示除 A、B 之外的任意一个其它域。

(4) 再计算 X 对 Y 的信任值[10]:信任代理 A 查找的资源提供质量信任关系表,推荐节点的权重值为:$W_R(Y,Y_i,T)$,上下文因子为 c。

直接信任值为:$\mathrm{DTT}(X,Y,c,t)*F(t-t_w,c)$,若 X、Y 无直接信任,则该值为 0。

信誉值为:

$$\Theta(X,Y,c,t)=\frac{\sum_{i=1}^{n}\mathrm{RTT}(X,Y,c,t)\times W_R(X,Y,c,t)\times F(t-t_w,c)\times A(Y)}{\sum_{i=1}^{n}W_R(X,Y,c,t)}$$

(5) 再计算 X 对 Y 的最终信任值:

$$\Gamma(X,Y,c,t)=(a\times\mathrm{DTT}(X,Y,c,t)\times F(t-t_w,c)+b\times\Theta(X,Y,c,t))\times\begin{cases}T_A(B) & A\text{ 对 }B\text{ 有直接信任} \\ E(B)=\dfrac{\sum_{i=1}^{n}X_i(B)}{n} & A\text{ 对 }B\text{ 无直接信任}\end{cases}$$

权重系数 a 和 b 分别反映了合成总体信任值时,直接信任和信誉所占的比重,二者的和为 1,根据实际情况自己组织内决定取值大小。

3.3　信任值的更新

由于节点本地的信任表中只存储大于本地权限门限的成员,节点的维护工作相对轻松。在节点本地的信任表中,所记录的信息要随着交易的发展和时间的变化不断地更新。因为表中的节点是按照信任等级降序排列,所以要对表中节点位置同步更新,文中的模型中采用直接插入排序算法[11]。

更新信任值的基本思想:如果直接信任值增加了,则认为这代表一次成功的接触,如果直接信任值降低了,则认为这代表多次失败的接触,域内所属成员交互结束后需要向所在域反馈交互信息,各域权利机构根据域成员对此交互满意与否相应增加或降低域间信任关系等级。

4　实验结果分析

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)。显然,在理想情况下,成功交易的次数为 200000 次。

交易成功率(下载成功率) = 成功交易次数(成功下载文件次数)/理想交易次数

网络中节点的恶意行为是单纯的恶意交易行为。该实验主要为检验不同比例的单纯恶意节点对模型以及对使用传统方法的信任模型的影响。下载成功率测试结果如图 2 所示:

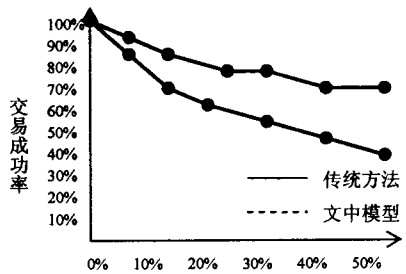

图 2 单纯恶意行为仿真实验结果(下载成功率)

实验结果表明,使用所设计的模型由于引入信任机制,使得网格交易的成功率大幅提高。

5 结束语

文中提出了一种动态自适应的网格信任模型,相对于传统信任模型更加适合在网格环境下运行。该模型中节点是独立自主的,节点的加入更加自由,降低了节点负担和网络阻塞。并将信任度划分为提供服务和使用服务的两种形式,同时在模型中引入了修正因子和上下文环境对节点进行评估和反馈。实验结果表明在存在恶意节点的环境中节点交易成功率得到很大提高。

下一步的工作是在此研究基础上进一步细化该信任模型的具体实施措施,深入研究网格中各层次涉及到的信任继承关系[12],尤其结合基于身份的访问控制理论研究网格中的信任实施和量化方法。

参考文献:

[1] 肖 凌,李之棠.公开密钥基础设施 PKI 结构[J].计算机工程与应用,2002(10):137-139.

[2] 马宝林,孙济洲,于 策,等.基于信任模型的网格安全机制[J].计算机工程,2007(5):123-125.

[3] 李小勇,桂小林.大规模分布式环境下动态信任模型研究[J].软件学报,2007,18(6):1511-1513.

[4] Viljanen L. Towards an ontology of trust[M]. Berlin: Spr-inger-Verlag,2005:175-184.

[5] 王东安,秦 刚,南 凯,等.网格计算中信任管理模型的研究[J].计算机工程,2006(4):32-34.

[6] 陈建刚,王汝传,王海艳.网格资源访问的一种主观信任机制[J].电子学报,2006,34(5):818-821.

[7] 李文娟,王晓东,傅仰耿,等.几种网格信任模型的研究[J].福州大学学报:自然科学版,2006,34(2):189-193.

[8] 王成飞,孙富春.网格环境中基于行为的分层实体自主信任模型[J].计算机工程与应用,2007,43(16):135-138.

[9] Joseph J,Fellenstein C.网格计算[M].北京:清华大学出版社,2005.

[10] Brinklov M, Sharp R. Incremental Trust in Gird Computing [C]//Seventh IEEE International Symposium on Cluster Computing and the Grid (CCGrid'07). [s.l.]:[s.n.],2007: 135-144.

[11] Foster I,Kesselman C.网格计算[M].第 2 版.北京:电子工业出版社,2004.

[12] Papalilo E, Freisleben B. Managing Behaviour Trust in Grids Using Statical Methods of Quality Assurance[C]//Information Assurance and Security,2007. IAS 2007. Third International Symposium. [s.l.]:[s.n.],2007:319-324.

(上接第 150 页)

后用实数编码的入侵检测数据做了模拟实验,对动态变化的自体下,模型中自体集的动态演化和自适应性生成的检测器得到了验证,达到了预期的目的。自体集的建立、完备性以及大小的设置是下一步研究的内容,模型算法的实际应用和深入的理论分析也需要进一步研究和探索。

参考文献:

[1] Jiao Li-chen, Du Hai-feng, Liu Fang, et al. Immunity optinize compute, learn and identify[M]. Beijing: Science publish company,2006:366-367.

[2] Hofmeyr S A, Forrest S. Architecture for an artificial immune system[J]. Evolutionary Computation, 2000, 8(4): 443-473.

[3] Forrest S, Perelson A S. Self-nonself Discrimination in a Computer[C]//In Proc. of IEEE Symposium on Research in Security and Privacy. Oakland, CA:[s.n.],1994:202-212.

[4] Ayara M, Timmis J. R de Lemos, et al. Negative selection: how to generate detectors[C]//In Proceedings of ICARIS. Canterbury: University of Kent,2002.

[5] Li Tao. Idid: An Innovative Immune-based Dynamic Intrusion Detection Model[J]. Chinese Science Bulletin, 2005, 50 (17):1912-1919.