多域环境中基于蚁群算法的抗攻击时态信任模型

文珠穆[1] 李瑞轩[1] 卢正鼎[1] 冯本明[2] 唐 卓[1,2]

(华中科技大学计算机科学与技术学院 武汉 430074)[1] (湖南大学计算机与通信学院 长沙 410082)[2]

摘 要 针对多自治域环境中的域间信任关系动态的、不确定性等特点,提出了一种基于时间的动态信任关系模型。每个自治域都维护有一个描述该域和其他域之间的信任度的信任向量。在本模型中,两个域间的信任关系取决于时间和域间的互操作记录。基于蚁群算法给出了根据多自治域的当前环境来实时地计算域间信任关系的基本方法,当局部的信任度发生改变时,可以根据蚁群算法及时调整全局信任关系。最后,通过仿真实验验证了域间信任关系的建立及变化过程。

关键词 时态信任,蚁群算法,信任向量,多域环境

Robust Temporal Trust Model Using Ant Colony Algorithm in the Multi-domain Environment

WEN Zhu-mu[1] LI Rui-xuan[1] LU Zheng-ding[1] FENG Ben-ming[2] TANG Zhuo[1,2]

(School of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan 430074, China)[1]

(College of Computer and Communication, Hunan University, Changsha 410082, China)[2]

Abstract This paper introduced a model for time-based temporal trust. The trust in multi-domain environment is uncertain, which is variation for various factors. Every domain is endowed with a trust-vector, which figures the trust intensity between this domain and the others. The trust intensity is dynamic due to the time and the inter-operation between two domains, a method was proposed to quantify this change based on the mind of ant colony algorithm and then an algorithm for the transfer of trust relation was also proposed. Furthermore, this paper analysed the influence to the trust intensity among all entities that is aroused by the change of trust intensity between the two entities, and presented an algorithm to resolve the problem. Finally, we show the process of the trusts' change that is aroused by the time's lapse and the inter-operation through the Simulation Experiment.

Keywords Temporal trust, Ant colony algorithm, Trust-vector, Multi-domain Environment

1 引言

近年来,随着因特网和分布式对象技术的飞速发展和普遍应用,出现了越来越多的分布式系统。同时,随着电子商务和供应链等技术的推动,系统间的协作已十分普遍,这也促使分布式系统的规模越来越大,复杂性越来越强。从安全角度理解,许多分布式系统实际上由多个自治域(以下简称域)构成。要使分布式系统充分而安全地发挥其作用,多域间安全地进行协作,信任管理是关健问题之一。自从 Marsh[1] 将信任研究引入到计算机领域,信任机制正逐渐因其灵活性和可扩展性得到越来越多的研究者重视。人们在分布式网络、普适计算[2]、对等计算、自组织网络[3]等多个领域中提出了众多信任模型[4]。在这些模型中,信任通常被量化为一个确定性的实数[5]。然而,在多自治域环境中,域间实体的信任具有很大的主观性,所以采用确定性数值对信任进行描述存在天然的不足。例如,如果域 A 中的实体非常信任域 B 中的实体,就很难确定信任度的具体数值应为多少。所以不确定性是信任的重要属性,即自治域之间的信任关系具有模糊性和随机性。

信任管理技术作为一种支持分布式访问控制的技术,近年来得到了广泛的研究。它可以较好地用于支持多域间的安全互操作。随着网络技术和信息系统技术的发展,在开放环境下实现互操作不仅是一种需求,也成为可能。开放式环境的一个显著特点即是用户集合不可预知。在互操作的初始状态,一个域中的用户集合对于另一个域中用户是不可知的。两个不同的自治域互操作过程中信任关系的建立取决于这两个域的历史交互记录。也就是说,在开放式的多域环境下,当两个域相互不可知的情况下,域间的信任程度是很低的。只有当两个域间的交互越来越频繁,而且这种交互成功的次数越多,这两个域间彼此信任的程度才越高。

两个行为主体间的信任度不仅仅是建立在这两个主体交互结果的基础上,这种信任关系有时也会随时间的变化发生

到稿日期:2008-08-15 返修日期:2009-04-24 本文受国家自然科学基金项目(项目编号:60403027,60773191,60873225),国家高技术研究发展计划(863计划)项目(2007AA01Z403)资助。

文珠穆(1976—),男,博士研究生,主要研究方向为分布式异构系统中的安全,E-mail:hust_tz@126.com;李瑞轩(1974—),男,博士,副教授,主要研究方向为分布式系统、分布式系统安全;卢正鼎(1944—),男,教授,博士生导师,主要研究方向为分布式系统、智能信息系统、信息安全;冯本明(1985—),男,硕士研究生,主要研究方向为分布式系统安全;唐 卓(1981—),男,博士研究生,讲师,主要研究方向为分布式系统安全。

改变。在现实中情况也往往如此：两个原本相互熟悉的人如果很长时间内没有来往，其相互间的信任也会越来越淡。本文利用蚁群算法模型来描述这种多域间信任的量化。蚁群算法是近年来出现的一种新型的模拟进化算法，是由意大利学者 M. Dorigo[6,7] 等人首先提出来的。实验观察表明，蚂蚁在运动过程中会留下一种信息素，其后面的蚂蚁可根据前边走过的蚂蚁所留下的信息素选择其要走的路径。一条路径上的分泌物越多，蚂蚁选择这条路径的概率就越大。而且路径上的蚂蚁信息素是在不断地挥发的，如果长时间没有蚂蚁经过，这条路径上的信息素就会越来越少。蚂蚁群体的集体行为实际上构成一种学习信息的正反馈现象。M. Dorigo 等对蚂蚁行为的数学描述可以应用于当前的开放环境中域间的信任关系。从前面的描述，两个域间的信任程度如同蚂蚁的路径上的信息素，走的蚂蚁越多，也就是说交互成功的次数越多，信任程度就高。而这种信任程度同时也在随时间递减。

本文在多自治域环境中建立了一种动态的、随时间和事件变化的动态信任关系模型。在此模型中，采用信任度来描述域间的信任程度。系统中每两个自治域间的一次交互，将会使域间的信任度增加，同时域间的信任程度会随时间递减。如果两个自治域长时间没有进行交互，其间的信任程度将会越来越弱。本文第 2 节是相关工作和进展，第 3 节介绍本文的模型以及域间信任度计算算法，第 4 节介绍仿真实验，最后总结全文。

2 相关工作及进展

传统的信任评价模型以概率统计作为基础，例如类似于产品质量的关键属性只能用 1～10 等离散量表示。Billsus 等指出大多数信誉累积计算方法缺乏健全的信誉和信任理论支持[8]。目前比较著名的信任评价模型有 Beth 模型[9] 和 Jo sang 模型[10]。Beth 等人[11] 首先提出了信任定量化的概念和方法，将信任分为直接信任和推荐信任，根据肯定和否定经验数计算实体完成任务的概率，以此表示信任，并给出了信任合成的方法。Beth 模型通过经验的概念来描述和度量信任水平，肯定经验与否定经验分别反映了实体执行任务的成败。对于直接信任与推荐信任，Beth 模型分别给出了由肯定经验与否定经验所表述的信任度的计算方法。但该模型的计算方法中采用了简单的算术平均，使计算结果的准确性易受恶意推荐的影响。Jo sang 等[12] 提出主观逻辑(subject logic)的方法，其实质利用了证据理论(D-S 理论)。Jo sang 模型通过事实空间和观念空间的概念来描述和度量信任水平，并给出了一套主观逻辑算子，用于信任度的计算。Jo sang 模型没有明确区分直接信任和推荐信任，而是使用三元组{信任程度，不信任程度，不确定程度}来表述主观信任度。但 Jo sang 模型同样难以抵抗恶意推荐的影响。Rahman 等人[13] 提出的信任度评估模型同样将信任关系分为直接信任和推荐信任，给出了信任度的传递协议和计算公式，但没有给出信任度综合计算公式。麻省理工大学的 Mui 等[14] 从社会学和进化论的角度给出了一个信任和信誉的计算模型。

文献[15]提出用模糊集合理论来描述信任，认为信任是具有树状层次结构的概念树。设定两个概念树之间的差异不超过根结点所定义的阈值，设定信任的子因素的权重分配。对于复杂的信任类型，需要构造多级概念树，通过从叶到根的反复迭代来获取信任向量等，都对评价对象提出了种种假设，或认为评价已符合树状层次结构的特点。如此种种影响了信任评价结果的客观性和可信性。

上述现有的信任模型都需要通过一定的算法得到多条信任路径，并根据所得到的多条信任路径进行综合计算，得到一个综合信任值。目前研究中得到的寻找信任路径算法都或多或少存在一些缺点，例如 Yahalom 等在文献[16]中提到的算法被证明是 NP 完全问题，他们在文献[17]中的算法把网络模型描述为树的结构，算法复杂度是对数阶的。Reiter-Stubblebine[18] 提出了 PGP 中信任机制的 BDP 近似算法，得出了较多的不相交路径，但没考虑如何使各条路径的信任度进行优化，不能防止联合欺骗的行为。白保存等[19] 改进了 Reiter-Stubblebine 的算法，其中利用了 Dijstra 算法，但在复杂的网络环境中运行效率较低。

3 模型描述

3.1 模型概述

本节从定义自治域间的信任关系开始，对本时态信任关系模型给出了一个形式化的描述，并给出了相应的域间信任关系的计算和调整方法。在本模型中，使用蚁群算法中的信息素计算方法来描述随时间和历史互操作记录发生改变的自治域间的相互信任关系。本文认为，蚁群算法中路径留下的信息素对于蚂蚁寻路的启发作用对于两个域中的实体是否能相互信任，或者在多大程度上能相互信任，本质上是类似的。

信任分为身份信任和行为信任。身份信任涉及用户或服务器的身份认证。行为信任针对两个实体之间进行事务处理时，根据实体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多域环境中如何对其他主体的信任度进行定义、评价和推导。身份信任一般应用于系统初始化或当一个新域加入到多域环境中时，首先采用的认证方式。本文所采用的身份认证的策略为层次 CA 策略和网状 CA 策略。对于行为信任，本文定义信任模型是以域(domain)为单位，分层次的信任计算模型，如图 1 所示。多域环境的信任关系分两个层次：以域为单位的全局信任关系；域内的本地信任关系。

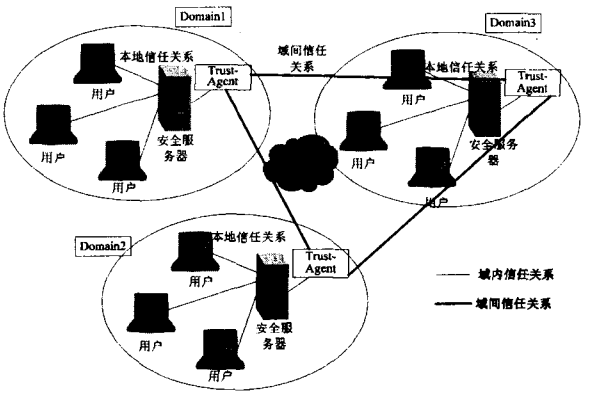

图 1 多域环境的时态信任模型

(1)域间信任关系：域间信任关系是域和域之间的，信任评价的对象也是以域为单位。域的受信任程度是根据域内的所有用户在多域中的网络行为以及该域提供的服务，被其它域进行评价的。因此域的信任度是该域组织在多域中的信任度的综合体现。

(2)域内信任关系:用户的信任度是由本域管理者来评价的,域管理者评价域内用户可以采取本域的管理策略,充分体现了域内自治的特点。当域的用户访问域内服务时,提供服务者向用户所属域的 Trust Agent 查询请求该用户的信任系数。

图 1 中,在域的安全服务器上运行 Trust Agent 进行信任管理。Trust Agent 的功能有:(1)更新域的信任表;(2)允许用户加入域,继承域的信任属性;(3)查询其它域的信任度,响应其它域的信任查询;(4)为域内用户计算关于其它域的信任度。

这样形成了一个分级的、各个域自治的信任模型。假设多域环境中有 N 个域,每个域平均有 M 个用户,那么整个多域环境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。而是为每个用户做全域内评价,那么信任计算的复杂度是 $O(f(N\times M))$。这样不仅减少了整个多域环境中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多域内进行交互,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或开除。

3.2 域间信任关系的定义

在讨论信任管理之前,需要明确信任的定义。信任是在一定范围内,根据实体间的多次交易而动态变化。另外,为了建立信任关系时,实体在决策之前,也会听取其它实体的意见。在多域环境中,当实体想做出基于信任的决策,也需要依赖其它实体的关于特定实体的信息和意见。我们定义:"信任是对某实体本身行为的期望。包括在某些指定内容方面对该实体过去行为的观察,以及其它实体对该实体的推荐信息。信任程度随时间是递减的。"

定义 1 自治域 i 对自治域 j 在 t 时刻的信任程度信任度表示为:$P_{ij}(t)$,取值范围为$[0,1]$,$P_{ij}(t)=0$ 表示不信任,$P_{ij}(t)=1$ 表示完全信任。

定义 2 信任度向量动态记录该自治域与其他自治域间的信任度。假设该分布式环境中有 n 个自治域,则每个自治域 i(node)都维护一个本地的信任度向量:

$$P_i(t)=(P_{i1}(t),P_{i2}(t)\cdots P_{in}(t)) \tag{1}$$

该向量是交互事件和时间的函数。如果一个自治域 i 与另一个自治域 j 在时刻 t 有交互事件,则两个自治域间的信任度增加,即

$$P_{ij}(t) > P_{ij}(t-1) \tag{2}$$

信任关系不是绝对的,而是动态变化的。信任在两个实体之间是一对一的关系,但不是对称的。信任存在推荐关系,当某个实体没有直接与其它实体交往时,只能靠其它实体提供推荐信息来参考。信任是和内容相关的。当一个实体在某种程度上信任其它实体时,总是针对某一特定内容的。同时随时间的流逝,任意两个自治域间的信任度会逐渐减少,如果在一个相当长的时间内两个自治域间没有交互记录,则这两个自治域间的信任度会减少至 0,即两个自治域间的实体会变得不信任。

3.3 动态信任关系的量化表示

为了量化两个自治域间的信任度的增加和减少。给出信任素的定义:

定义 3 信任素表示两个自治域间信任的基本因素,自治域 i,j 在 t 时刻的信任素表示为 $\tau_{ij}(t)$。在初始状态下,可以根据实际情况设定两个自治域间的实际信息素,或者使每两个自治域间的信任素的数量相等,设 $\tau_{ij}(0)=C$(C 为常数)。若初始时刻自治域间信任度 $P_{ij}(0)=0$,则 $\tau_{ij}(0)=0$。

同时约定,η_{ij} 为信任透明度,本文定义为一个自治域信任另一个自治域的启发信息,取 $\eta_{ij}=1/d_{ij}$,d_{ij} 为两个自治域间的路径长度,α 为路径 i,j 上信任信息的重要程度,β 为启发信息的重要程度(初始值根据实际情况给出)。

在 t 时刻,自治域 i,j 之间的信任度定义为

$$p_{ij}(t)=[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}/[\sum_{i,j}[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}],i\neq j \tag{3}$$

如果自治域间没有交互,两个自治域间信任素的浓度会慢慢挥发而变稀释,用参数 $1-\rho$ 表示信任素的消逝程度,$\sigma\tau_{ij}$ 表示自治域 i,j 每次交互时,两者间信任素的增量,则有

$$\tau_{ij}(t+n)=\rho\tau_{ij}(t)+\sigma\tau_{ij} \tag{4}$$

$$\sigma\tau_{ij}=\begin{cases}\dfrac{Q}{\dfrac{1}{1-\tau_{ij}(t)}-1}, & \text{若实体 } i,j \text{ 在 } t \text{ 时刻进行一次交互}\\ 0, & \text{否则}\end{cases} \tag{5}$$

其中 Q 为常数,表示总信任量。

依据确定性理论,可以定义自治域之间信任度的传递关系为:

$$P_{i,i+2}(t)=P_{i,i+1}(t)\times P_{i+1,i+2}(t) \tag{6}$$

且若经过传递建立的信任度值大于自治域间的直接信任值,比如说在某一时刻 t,若 $P_{i,i+1}(t)\times P_{i+1,i+2}(t) > P_{i,i+2}(t)$,则取自治域间的直接信任值为 $P_{i,i+1}(t)\times P_{i+1,i+2}(t)$。

如果将自治域间的信任关系表示成一个无向图 G,每个自治域是图中的一个顶点,自治域间的信任度是两个自治域间邻接边的权值,则可以将这个图表示成邻接矩阵的形式。任意两个自治域间的信任度可以从两个方面来取得:一是两个顶点间直接邻接边的权值,记为 v;另外,假设两个顶点间有 n 条路径,每条路径长度为 l_k,$k\in[1,n]$,路径上每条边的权值表示为 V_{ij},那么由以上的自治域间信任度的传递关系可以得出两个顶点间每条路径的权值为 $\prod_{1}^{l_k}v_{i,j}$ $k\in[1,n]$,那么这两个顶点间的实际信任度则为

$$\max(v,\prod_{1}^{l_k}v_{i,j})\ k\in[1,n] \tag{7}$$

3.4 信任模型的抗攻击策略

在信任模型中,很容易收到恶意推荐-同谋推荐等形式的信任攻击,在此引入推荐因子防止攻击。

定义 4 推荐因子 $R(k,t)=\sum_{i=0}^{n}P_{ik}(t)(i\neq k)$ 表示在时刻 t 全局信任模型中其它自治域 i 对 k 节点的直接信任度之和。

在当前时间 t,自治域 $i(D_i)$ 与自治域 $j(D_j)$ 之间的信任关系的计算是根据 D_i 和 D_j 的直接信任关系,以及其它自治域对 D_j 的推荐信任度来共同决定的。对应直接信任和推荐信任的权值分别是 α 和 β,其中 $\alpha+\beta=1$。如果 D_i 更加在乎与 D_j 的直接信任,那么 α 大于 β。

直接信任的计算是:D_i 的直接信任度是直接信任值和衰减函数的乘积。D_i 推荐信任的计算是:推荐因子 $R(k,t)$ 和衰减函数乘积之和的均值。在实际的系统中,实体使用相同的信息来计算直接信任和推荐信任。例如,推荐信任和直接信任是相同的。因为推荐信任主要基于其它域对于某个特定域

的推荐。本文引入的推荐因子 R 来防止几个域的同谋欺骗。

信任度＝α×直接信任度＋β×间接信任度

直接信任度＝$P_{ij}(t)$ ×衰减函数

间接信任度＝ $R(k,t)$ ×衰减函数

因为每个节点都要向另一些节点发布建议值，所以在任意一对节点之间就很有可能存在多条建议路径。这就存在把这些不同的信任值进行合成的问题。在进行信任值的合成时，建议路径数越多，得出的合成信任值的可靠性也就越高，这点非常类似于选举系。

3.5 自治域间信任度的更新

在目前大部分的信任关系模型中，信任度的更新往往采用“两个节点信任度的变化将立即引起全局信任度的变化”的这一原则，这种原则带来实时性非常高的信任度更新策略。但是如果从整个多域环境的访问过程考虑，上述的“有变化立即更新”的原则给网络带来的很大的流量压力，也占用了域服务器的大量资源。这里把动态路由的算法引入到我们的模型中，可以减少网络的查询流量，提高信任更新过程的可靠性，算法的基本思想是：当一个域有访问需求的时候，域服务器才来计算域之间的信任度。

首先，每个域服务器都维护着一张全局的 Trust-Agent 域服务器的逻辑位置拓扑图，在图中，每个逻辑位置相邻的域服务器有一个权值，它反映的是相邻节点之间的信任度。当有访问需求时，只要在图上查找到目的节点权值最大的路径（即信任度 $P_{ij}(t)$）。

更新算法描述如下：

1）动态的维护全局域服务器的带权值的逻辑结构拓扑图。

2）当有访问需求时，求出到目的节点权值最大的路径（即信任度 $P_{ij}(t)$）。

最后，可以给自治域间的信任度设一个阈值 R，表示自治域间是否可以相互验证其证书，如果 $P_{ij}(t)>R$，则说明自治域 i,j 在 t 时刻有足够的信任度，可以相互验证证书，否则，不能相互验证证书。

3.6 算法描述

1）初始化

$t=0$

设置自治域个数 n、信任度阈值 R、总信任量 Q

初始时刻自治域间信任度 $p_{ij}(0)$，$p_i(0)$ 自治域的本地信任向量。

初始时刻自治域间信任素 $\tau_{ij}(0)=C$，$\eta_{ij}=1/d_{ij}$，$\Delta\tau_{ij}=0$。

2）计算 t 时刻，每一对自治域 v,s 间的信任度：

$p_{vs}(t)=[\tau_{vs}(t)]^{\alpha}[\eta_{vs}]^{\beta}/[\sum_{v,s}[\tau_{vs}(t)]^{\alpha}[\eta_{vs}]^{\beta}]$，转 4）。

3）若自治域 v,s 在 t 时刻有成功交互，则两者间的信任度更新为

$\tau_{vs}(t+n)=\rho\tau_{vs}(t)+\tau_{vs}$，转 4）。

4）由于自治域 v,s 间信任度的变化，更新整个系统中所有自治域间的信任度：

4.1）根据 DFS 算法求 v,s 间的所有简单路径 path；

4.2）对 path 中的每一条路径，加上边〈v,s〉，使之构成一个环路；

4.3）依次计算每个环路的所有边的乘积 W；

4.4）对每个环路的每一条边连接的两个自治域 s_i,s_j，计算其通过环路的其他边传递得来的信任度的值 $p_{si,sj}(t)=W/V_{si,sj}$；

4.5）若 $p_{si,sj}(t)$ 大于自治域 s_i,s_j 当时的信任度，则令 $V_{si,sj}=p_{si,sj}(t)$，否则，不变。

从上面的算法可以看出，该算法的复杂度主要体现在系统信任度的更新上。由于本文采用的是本地的信任向量来描述一个本地节点与其他相邻节点的连接状况，所以可采用邻接表来描述整个系统中的信任向量。这样求 v,s 间的所有简单路径时，找邻接点所需的时间为 $O(e)$，其中 e 为自治域间相连的边数。由此，根据 DFS 算法来计算 v,s 间的所有简单路径的时间复杂度为 $O(n+e)$，n 为自治域个数。由于每个本地信任向量的维数为 n，则实际上 e 为 n^2 数量级，故算法中 4.1 步的时间复杂度为 $O(n^2)$。而 4.3 步中依次对每个环计算其所有边的权值的乘积，时间复杂度为 $O(n^2)$，其他步骤的时间复杂度均为 $O(n)$，故算法的时间复杂度为 $O(n^2)$。

4 仿真实验及分析

在本文的仿真实验中模拟了 4 个自治域：A，B，C，D。模型中的各个变量初始设为 $a=1$，$\beta=5$，$\rho=0.9$，$n=4$，$\tau_{ij}(0)=100$，初始无向图如图 2 所示，该图所对应的邻接矩阵如图 3 所示。

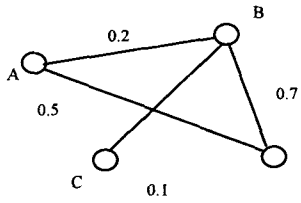

图 2 初始无向邻接图

$$\begin{bmatrix} 1 & 0.2 & 0 & 0.5 \\ 0.2 & 1 & 0.1 & 0.7 \\ 0 & 0.1 & 1 & 0 \\ 0.5 & 0.7 & 0 & 1 \end{bmatrix}$$

图 3 初始无向邻接矩阵

根据模型中信任度的传递关系计算方法，图 2 中的无向邻接图是一个不稳定状态，依照第 3 节中的信任度传递模型，节点间的信任度将会进一步进行调整。比方说，在自治域节点 A 和 C 中间存在两条简单路径：ABC，ADBC。根据式（6）计算，节点 A 和 C 之间的信任度应该调整为：max(0.02，0.035) ＝0.035。同样，也可以调整其他节点间的信任度。调整后的邻接矩阵如图 4 所示。

$$[\tau_{ij}(0)]=\begin{bmatrix} 1 & 0.2 & 0.035 & 0.5 \\ 0.2 & 1 & 0.1 & 0.7 \\ 0.035 & 0.1 & 1 & 0.07 \\ 0.5 & 0.7 & 0.07 & 1 \end{bmatrix}$$

图 4 调整后的邻接矩阵

$$[\tau_{ij}(t)]=\begin{bmatrix} 1 & 0.18 & 0.0315 & 0.45 \\ 0.18 & 1 & 0.09 & 0.63 \\ 0.0315 & 0.09 & 1 & 0.063 \\ 0.45 & 0.63 & 0.063 & 1 \end{bmatrix}$$

图 5 一个单位时间后的信任素矩阵

如前所述，在本实例中可以进一步分析自治域节点间的信任素随时间以及节点间互操作的变化。假如在单位时间内，任意两个自治域节点间均没有进行操作，那么根据参数 $\rho=0.9$，单位时间后，节点间的信任素矩阵将会变成如图 5 所示。观察可知该矩阵不需要进行调整。若在第二个单位时间内自治域 A 和 B 之间进行了一次成功的互操作，那么根据式（4）

和式(5)，自治域 A 和 B 间的信任素更新为：

$$\tau_{AB}(2t)=\rho\tau_{AB}(t)+\sigma\tau_{AB}=0.9\times0.18+\frac{1}{\frac{1}{1-0.18}+1}$$

$$=0.162+0.45=0.612$$

可以找到所有通过节点 A 和 B 之间的环路为：ACBA，ACDBA，ADBA，根据文中的信任素更新算法，可以将信任素矩阵调整为图 6 所示。

$$[\tau_{ij}(2t)]=\begin{bmatrix}1 & 0.612 & 0.055 & 0.45\\ 0.612 & 1 & 0.09 & 0.63\\ 0.055 & 0.09 & 1 & 0.063\\ 0.45 & 0.63 & 0.063 & 1\end{bmatrix}$$

图 6　第 2 个单位时间后的信任素更新矩阵

$$[p_{ij}(2t)]=\begin{bmatrix}1 & 0.322 & 0.029 & 0.237\\ 0.322 & 1 & 0.047 & 0.332\\ 0.029 & 0.047 & 1 & 0.033\\ 0.237 & 0.332 & 0.033 & 1\end{bmatrix}$$

图 7　更新后得到的域间信任度矩阵

根据式(3)，可以得到自治域节点间在第二个单位时间后的信任度矩阵如图 7 所示。$P_{ij}(2t)$说明了各个自治域之间的信任关系，行向量即是每个自治域的本地信任度向量 $P_i(t)$。例如，第一个行向量是(1，0.322，0.029，0.237)，其说明了当时自治域 A 和其他自治域之间的信任度分别为 0.322，0.029 和 0.237。

最后，本文对任意两个节点的信任关系的变化进行模拟，得出当两个节点间的交易次数增加时，其信任度也在不断接近 1，如图 8 所示。当两个节点长时间没有进行交易，其信任度将越来越趋近于 0，如图 9 所示。

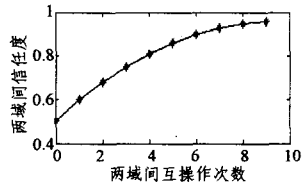

图 8　某两个域间信任度随互操作次数的变化

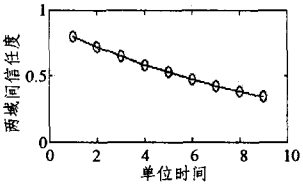

图 9　某两个域间信任度随时间变化

图 8 和图 9 反映了域间信任度单纯地随成功的操作次数以及时间的变化情况。真实情况中两个域之间的信任通常是同时受这两种因素的影响的。域间的信任度在衰减的过程中受成功的互操作的影响会不时地增加，如图 10 所示。

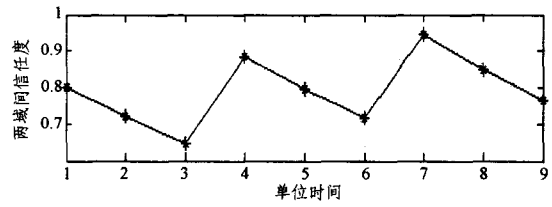

图 10　域间信任度变化

从图 10 中的曲线可以看出，两个域间的信任度在衰减的过程中，在第 4 个和第 7 个单位时间处两域之间存在成功的互操作，这两次互操作使得两域间的信任度增加，同时时间的作用也使信任度发生减少。

结束语　多自治域环境的不确定性和异构性给不同域间实体信任的建立带来了新的挑战。本文根据蚁群算法提出了一种基于时间的动态信任关系模型。在本模型中，两个域间的信任关系是时间和域间互操作记录的函数，因此可以根据多自治域的当前环境来实时地计算域间的信任关系。而且当局部的信任度发生改变的时候，可以根据本文中的算法来及时地调整全局的信任关系。最后，通过仿真实验验证了域间信任关系的建立以及变化过程。

在以后的工作中，本模型可以通过以下几个方面进行扩展：域间的互操作考虑具体的操作内容，不同的操作对域间信任变化的影响也不一样。同时，操作结果好坏的评价也将是影响多自治域间信任关系变化的重要因素。

参 考 文 献

[1] Marsh S P. Formalising trust as a computational concept[D]. University of Stirling, 1994

[2] Yu Bin , Munindar SirIsh P . An evidential model of distributed reputation management [A]//Proceedings of First International Joint Conference on Autonomous Entities and Multi-Entity Systems[C]. 2002:294 -301

[3] Aberer K, Despotovic Z. Managing trust in a peer-2-peer information system [A]//Proceedings of the l0th International Conference on Information and Knowledge Management [C]. New York, 2001

[4] Beth T, Borcherding M, Klein B. Valuation of trust in open networks[A]//ESORICS 94[C]. Brishton, 1994

[5] Abdul Rahman A, Hailes S. A distributed trust model [A]// New Security Paradigms Workshop[C]. ACM, 1997

[6] Colomi A, Dorigo M, Maniezz O V. Distributed Optimization by ant Colonies[C]//Proceeding of The First European Conference Artificial Life. Paris, France. Elsevier Publishing, 1991:134-142

[7] Dorigo M, Maniezzo V, Colomi A. The ant system:Optimization by a colony of cooperating agents[J]. IEEE Transaction on System, 1996, 26(1):1-26

[8] Xie D Q, Leng J. PKI principle and technology [M]. Beijing: Tsinghua University Press, 2004:135-141(in Chinese)

[9] Beth T, Borcherding M, Klein B. V aluation of trust in open networks [A]//Gollmann D, ed. Proceedings of the European Symposium on Research in Security (ESORICS) [C]. Brighton: Springer-Verlag, 1994:3-18

[10] Jo sang A. A model for trust in security systems[C]//Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. 1997. http://security. dstc. edu. au/ staff/ajo sang/papers. html

[11] Beth T, Borcherding M, Klein B. Valuation of trust in open networks[C]//Proceedings of the European Symposium on Research in Security(ESoRICS). Brighton: Springer-Verlag, 1999: 59-63

[12] Josang A. A model for trust in security systems [C]//Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. 1997

[13] Yahalom R, Klein B, Beth T. Trust relationships in secure systems a distributed authentication perspective[C]//Proc. 1993 IEEE Symp. on Research in Security and Privacy. 1993:150-164

[14] Mui L, Mohtashemi M, Halberstadt M. A computational model of trust and reputation [C]//Proceedings of the 35th Hawaii In-

ternational Conferrence on System Sciences. 2002

[15] 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

[16] Yahalom R, Klein B, Beth T. Trust relationships in secure systems a distributed authentication perspective[C]// Proc. 1993 IEEE Symp. on Research in Security and Privacy. 1993:150-164

[17] Yahalom R, Klein B, Beth T. Trust- based navigation in distributed systems[J]. Special Issue "Security and Integrity of Open Systems"of the Journal "Computing Systems", 1994

[18] Reiter M K, Stubblebine S G. Resilient authentication using path independence[J]. IEEE Transactions on Computers, 1998, 47 (12)

[19] 白保存,李中学,陈旺. PKI 信任度模型路径算法研究[J]. 计算机工程与应用,2005,41(21):182-185

(上接第 19 页)

[21] McDonald R, Hannan K, Neylon T, et al. Structured Models for Fine-to-Coarse Sentiment Analysis[C]// Proceedings of ACL. 2007

[22] Puspesh K. Multi-document Update and Opinion Summarization [D]. Partial fulfillment of the requirement for the degree of Masters of Technology, Indian Institution of Technology, 2007-2008

[23] Hu M, Liu B. Mining Opinion Features in Customer Reviews[C] //Proceedings of 19th National Conference on Artificial Intelligence. San Jose, USA, July 2004

[24] Popescu A-M, Etzioni O. Extracting Product Features and Opinions from Reviews[C]//Proceedings of EMNLP. 2005

[25] Zhuang Li, Jing Feng, Zhu Xiaoyan. Movie Review Mining and Summarization[C]// Proceedings of CIKM-06. Virginia, USA 2006

[26] Liu B, Hu M, Cheng J. Opinion Observer: Analyzing and Comparing Opinions on the Web[C]// Proceedings of the 14th International Conference of World Wide Web. Chiba, Japan, 2005

[27] Liu Bing. Web Data Mining: Exploring Hyperlinks, Contents and Usage Data[C]. Springer, December 2006

[28] Carenini G, Ng R T, Zwart E. Extracting knowledge from evalua-tive text[C]// Proceedings of the 3rd international Conference on Knowledge Capture Banff, Alberta, Canada, October 2005

[29] Ding Xiaowen, Liu Bing. The Utility of Linguistic Rules in Opinion Mining[C]// Proceedings of SIGIR-07. Amsterdam, July 2007

[30] Jindal N, Liu Bing. Identifying Comparative Sentences in Text Documents[C]// Proceedings of the 29th Annual International ACM SIGIR Conference. Seattle, 2006

[31] Jindal N, Liu Bing. Mining Comprative Sentences and Relations [C]// Proceedings of 21st National Conference on Artificial Intellgience. Boston, Massachusetts, USA, July 2006

[32] Hou Feng, Li Guo-hui. Mining Chinese Comparative Reviews by Semantic Role Labeling[C]// Proceedings of 7th International Coference on Machine Learning and Cybernetics. Kunming, 2008

[33] Ku Lun-Wei, Liang Yu-Ting, Chen Hsin-Hsi. Opinion Extraction, Summarization and Tracking in News and Blog Corpora[C] //the Proceedings of 21st National Conference on Artificial Intellgience. Boston, Massachusetts, July 2006

[34] Hu Meishan, Sun Aixin, Lim Ee-Peng. Comments-oriented document summarization: understanding documents with readers' feedback[C]// Proceedings of the 31st Annual International ACM SIGIR Conference. Singpore, 2008

[35] Kim S M, Hovy E. Extracting Opinions, Opinion Holders, and Topics Expressed in Online News Media Text[C]//Proceedings of the Workshop on Sentiment and Subjectivity in Text of COLING-ACL. Sydney, Australia, 2006

[36] Qiu G, Liu K, Bu J, et al. Extracting Opinion Topics for Chinese Opinions Using Dependence Grammar[C]// Proceedings of SIGKDD-ADKDD. San Jose, California, USA, 2007

[37] Bethard S, Yu H, Thornton A, et al. Automatic Extraction of Opinion Propositions and their Holders[C]// Proceedings of the AAAI Spring Symposium. Stanford, USA, 2004

[38] Kim S M, Hovy E. *Identifying Opinion Holders for Question* Answering in Opinion Texts[C]// Proceedings of AAAI-05 Workshop on Question Answering in Restricted Domains. 2005

[39] Choi Y, Cardie C, Riloff E, et al. Identifying sources of opinions with conditional random fields and extraction patterns[C]//Proceedings of HLT/EMNLP-05. Vancouver, B. C., 2005

[40] Stoyanov V, Cardie C. Partially Supervised Coreference Resolution for Opinion Summarization Through Structured Rule Learning[C]// the Proceedings of EMNLP. 2006

[41] Lang Jun, Qin Bing, Liu Ting, et al. Intra-document Coreference Resolution: The state of the art[J]. Journal of Chinese Language and Computing, 17(4): 227-253

[42] Mishne G, de Rijke M. A study of blog search[C]// Proceedings of 28th European Conference on Information Retrieval. London, 2006

[43] Furuse O, Hiroshima N, et al. Opinion Sentence Search Engine on Open-domain Blog[C]// Proceedings of IJCAI. 2007

[44] Skomorowski J. *Topical Opinion Retrieval*[M]. *Dissertation of* Master of Mathematics in Computer Science. Waterloo, Canada, 2006

[45] Zhang Wei, Yu C, Meng Weiyi. Opinion Retrieval from Blogs[C] //Proceedings of ACM 6th CIKM. Lisboa, Portugal, 2007

[46] Mishne G. Using blog properties to improve retrieval[C]// Proceedings of ICWSM. 2007

[47] Mishne G. Applied Text Analytics for Blogs[D]. University of Amsterdam, 2008

[48] Weerkamp W, de Rijke M. Credibility Improves Topical Blog Post Retrieval[C]// Proceedings of ACL08. 2008

[49] Yi J, Niblack W. Sentiment Mining in WebFountain[C]// Proceedings the 21st International Conference on Data Engineering. Tokyo, Japan, 2005: 1073-1083

[50] Java A, Kolari P, Finin T, et al. The BlogVox Opinion Retrieval System[C]// Proceedings of the Fifteenth Text REtrieval Conference. 2006

[51] 姚天昉,聂青阳,李建超,等. 一个用于汉语汽车评论的意见挖掘系统[C]//中国中文信息学会二十五周年学术会议论文集. 北京:清华大学出版社,2006:260-281