基于动态联盟的一种身份信任计算模型

童岚岚,刘连忠
(北京航空航天大学 计算机学院 北京市网络技术重点实验室,北京 100191)

摘 要:在动态联盟中,身份管理是确保信息安全的一种手段,但是随着联盟成员数日益增多,传统的身份管理难以妥善应对当前较为复杂的环境,尤其当成员之间无交互历史时,数据交换的可靠性无法保障。文中研究了不同计算环境中的多种信任管理方法,并把P2P的推荐评价机制应用到动态联盟的身份管理中,提出了一种基于推荐的身份信任管理的算法。在这种算法中,身份的信任值由多因素加权综合而成,其中推荐信任值在算法中起到关键的作用。该算法试图为解决复杂的动态联盟环境下的身份管理问题提供一种途径。

关键词:动态联盟;信任;算法;身份管理
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)02-0152-04

One of Arithmetic Models of Identity Trust Management Based on Dynamic Federation

TONG Lan-lan, LIU Lian-zhong
(Beijing Key Laboratory of Network Technology, School of Computer Science and Engineering, Beihang University, Beijing 100191, China)

Abstract: In the environment of dynamic federation, the identity management is one of the methods for security issues. However, with the increasing of the members, it is more difficult for traditional identity management to deal with the complex situation, especially when members have no communication records, the security of data switching can not be guaranteed. Focused on some of trust management models, applying the reputation and evaluation mechanism in P2P to dynamic federation, the article brings forward an identity trust algorithm based on reputation. The algorithm, in which trust is weighted by various factors, and reputation rate is a key problem, is expected to offer one method to solve the identity management in the complex dynamic federation.

Key words: dynamic federation; trust; arithmetic; identity management

0 引 言

近年来,随着因特网和分布式技术的飞速发展和普遍应用,分布式系统之间的信息交互越来越频繁,系统所在的不同域之间便产生了跨域访问的需求。文中的域指组织域,即由一个或多个安全域组成的资源集合。

两个或两个以上的组织域往往为了完成同一个任务协商一致,自由地结为联盟。而任务完成时联盟也同时解散,这就意味着联盟的缔结和解散是自由的,动态的。然而,联盟间的协作却不可避免,如何安全有效地管理互操作中的各种用户身份成为了当下关注的问题,可信的身份在很大程度上决定了联盟中互操作的安全可信。

实体身份的可信度,是决定该身份能否进入外域的"敲门砖",也是保证本域内安全操作的基础之一。然而,由于联盟环境的错综复杂,身份的信任值会随着该身份的各种行为、他人的评价以及所在域信任值等因素发生波动。同时实体身份的信任值变化又会在一定程度上影响所在域的信任值,可见,身份信任的管理并不只是一个孤立的简单的处理过程。文中试图探索出一种处于该种复杂环境中的身份信任的计算模型。

1 动态联盟

联盟是指由若干组织域为完成一个共同任务而形成的组织形式。这种组织形式的最大特点是其动态性,即联盟关系随着任务的完成度发生线性的变化,所以很多时候被称为动态联盟。动态联盟的整个生命周

收稿日期:2009-06-24;**修回日期**:2009-09-14
基金项目:国家863重点基金项目(2005AA113040)
作者简介:童岚岚(1979-),女,硕士研究生,从事信息安全方面的研究;刘连忠,教授,从事计算机网络、数据库技术、网络信息安全等方面的研究。

期中存在着大量的通信,来实现远程交互访问[1]。同时,由于联盟成员是相对独立的实体,即针对不同的资源有不同的权限。因此,联盟中实体身份的的信任度也具有动态性和相对性等特性,动态性主要表现在信任值随着身份的行为方式和时间推移动态变化,相对性体现在实体身份相对于不同的环境表现出相应的与之匹配的信任值。

2 信任管理主要理论与方法

信任管理的基本思想是承认系统中安全信息的不完整性,系统的安全决策需要依靠可信第三方提供附加的安全信息。信任管理(Trust Management)的概念最初是由 M. Blaze 于 1996 年提出的[2],旨在"采用一种统一的方法来描述和解释安全策略、安全凭证和用于直接授权关键性安全操作的信任关系"。

2.1 自动信任协商

Winsborough 等人[3]提出了自动信任协商(Automated Trust Negotiation)的概念。它是对 Internet 上完全陌生的通信双方通过不断交换证书和策略来建立他们之间的信任。协商者之间的交互应该根据一定的策略遵循相应的协议来进行。自动信任协商策略(Automated Trust Negotiation Strategy)决定了协商的执行方式与过程,确定了什么时候提交凭证,提交哪些凭证等问题。针对特定的协商策略,应该制定相应的协商协议,确定协商者信息交换的格式、顺序,以使双方实现互操作。自动信任协商也属于信任管理的范畴,是对 Blaze 所提出的信任管理的进一步的发展。

2.2 信任评估模型

2.2.1 二元评价的简单加和平均

该类信任模型对交易结果给出正面(满意)和负面(不满意)两种评价,分别计算正面评价和负面评价的数目,然后用正面评价的值减去负面评价的值作为对节点的信任度。该方法的优点是任何人都能够理解信誉值所代表的本质属性,不足之处是比较简单(primitive),只能给出参与者信誉值的简单影像。

2.2.2 Reputation - based

在文献[4]中,Li X, Liu L 提出了基于声誉(reputation)的信任模型,对节点的评价反馈进行统计和分类计算得到节点的信任度,但是模型没有提出具体的识别欺骗行为和对欺骗者进行惩罚的方法和机制,并且没有考虑直接的个人交易历史经验。2004 年,Dou W 在 EigenRep 的全局信任模型基础上更进一步[5],不仅提出了更好的全局信任度的算法,提高了算法的收敛性,更给出了算法的分布式实现方法。EigenRep 的核心思想是,当节点 i 需要了解任意节点 k 的全局可信度时,首先从 k 的交易伙伴(曾经与 k 发生过交易的节点)获知节点 k 的可信度信息,然后根据这些交易伙伴自身的局部可信度(从 i 的眼光来看)综合出 k 的全局可信度。

2.2.3 PKI - based

此类模型中,存在少数领袖节点(leader peers),领袖节点负责整个网络的监督,定期通告违规的节点。这些领袖节点的合法性通过 CA 颁发的证书加以保证。这类系统往往是中心依赖的,具有可扩展性单点失效等问题,如 eDonkey 的诸多 server。

2.2.4 基于概率(probability)

Jsang[6]提出的基于贝叶斯网络的信任模型将二元的评价作为输入并通过 beta 概率密度函数的统计更新来计算信誉值,更新的信誉值是结合原有的信誉值和新的评价计算的。Y. Wang 提出的基于贝叶斯网络的信任模型主要关注于描述信任的不同方面,使得节点可以根据不同的场景来按需获取节点不同方面的性能。当节点无法确定文件提供者的可信度时,利用其他节点的推荐信息来建立信任关系。该信任模型能够适应于规模较小的 Gnutella 网络,或具有 small - world 特性的大规模 Gnutella 网络。

2.2.5 Fuzzy Logic

著名的 Regret 信誉系统属于该类模型。Regret[7]不仅考虑了信誉的个体尺度和社会尺度,再对信誉进行合成时,还考虑了信誉的本体论尺度。Regret 信誉系统利用模糊规则确定社会结构如何为该结构中的代理所给出的信息提供可靠度,同时也利用模糊规则将被信任方邻居的结果信誉和他们的社会关系与被信任方的信誉联系起来。S. Song 等人[8]提出了的信任模型利用模糊逻辑推理知识来计算节点局部信任度和汇聚全局的信誉,较好地解决了由于信息模糊或不完备等因素造成的信任计算粗糙问题。

3 基于动态联盟的身份信任计算

在很多 P2P 网络的商业交易行为中,参与交易的双方大多数情况下都是陌生的,交易者一般根据对方所在的交易平台的可信度来判断交易的可信,或者根据对方的历史行为情况作为参考,而参与交易活动的第三者的推荐值往往起到了意想不到的决定性作用。文中参考 P2P 网络中的推荐评价体系,给出了在动态联盟中的参与信任的 7 类因素。

3.1 信任的分类

假设,存在联盟 F 由 A, B, C 三个组织域组成。域 B 的实体 e 要求访问域 A。那么在该联盟 F 环境中,域 A 向各联盟成员询问实体 e 的信任值,该值由以下几

种因素组成：

(1) 实体 e 自我评价的信任值 IT；

(2) 域 B 的自我评价的信任值 ST_b；

(3) 域 B 对实体 e 的推荐信任值 FIT；

(4) 域 C 的自我评价的信任值 ST_c；

(5) 域 C 对域 B 的推荐信任值 AT_{cb}；

(6) 域 C 对实体 e 的推荐信任值 FT_c，如果过往行为中实体 e 从未访问域 C，那么域 C 对实体 e 的推荐信任值无效；

(7) 域 A 对实体 e 的推荐信任值 FT_a。

图 1 是动态联盟中交互示意图。

域 C(第三方他域) 代表除当前交互双方所在域的其他所有域。这样根据 C 域存在的情况又分为两种：

a. 域 C 是由一个或多个域的逻辑组成集合；

b. 不存在域 C。

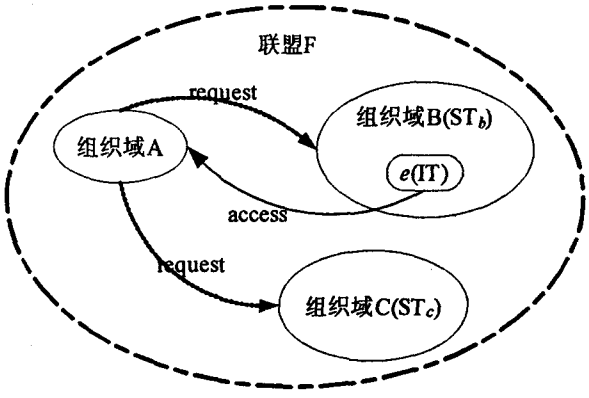

图 1 动态联盟中交互示意图

在情况 a 中，域 C 的所有自评价值和对他者的推荐值存在一个考虑权重的聚合算法，该算法在 3.2 节提出；情况 b 相对简单，实体 e 的信任值不需要考虑后 3 种因素的影响。

FT_a 也有两种情况：

a. 实体 e 在历史行为中没有访问过域 A；

b. 实体 e 在历史行为中访问过域 A。

实体 e 在域 A 中没有历史行为的信任记录，那么此时域 A 推荐的信任值无效；反之，那么域 A 的推荐值对此时实体 e 的信任值会有影响，而且所占的比例应该大于其他因素的信任值。

图 2 中虚线表示约束作用，实线表示传递作用。在交互行为的生命周期中，对于被访问的域 A，FT_a 是最重要的，其次是实体 e 所在的域 B 给出的推荐值。然而，FIT 受到域 B 自身评价值的约束，同时 AT_{cb} 也会影响 FIT。而第三方他域 C 的自我评价值对其进行的推荐值 FT_c 和 AT_{cb} 也起到约束作用。

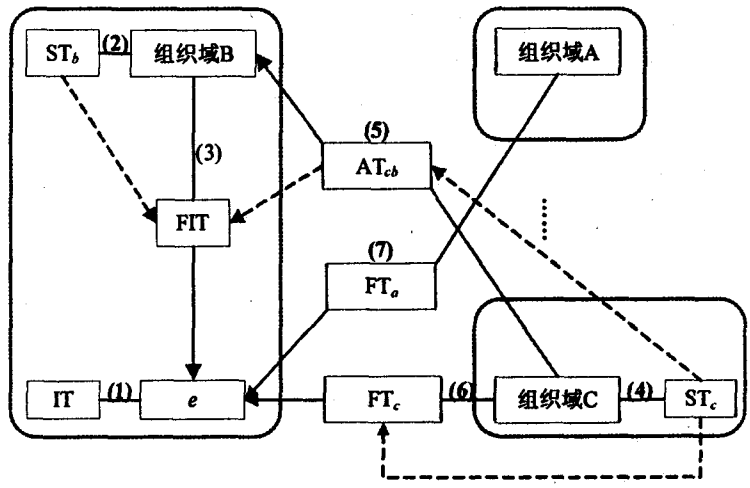

图 2 信任分类示意图

文中提出了第三方他域 C 在联盟交互中确定实体的信任的作用，是在文献[9] 提出的信任计算模型 TBAC 的算法中稍作改进。引入第三方的概念，在原有的可信计算模型基础上增加了推荐信任的因素，同时第三方域的推荐在一定程度上使“陌生”的交互者的互操作更安全可信。

从上文的分析中可以发现，实体 e 信任值主要是从域 A 的视角进行计算的。如果实体 e 访问别的域，在同样的条件下，很可能会得到差异很大的信任值，可见，这种模型的计算方式充分地体现了信任的主观性，也符合了人们在处理“信任”时的普遍的感性方式。

3.2 信任的计算

3.2.1 各信任分类因素的计算

● 域 C 对域 B 的推荐信任值 AT_{cb} 计算。

AT_{cb} 在组织域之间不存在交互历史作为参考的情况下，需要联盟内其他组织域的推荐，从而得到以下公式。

$$AT_{cb}=\frac{\sum_{a\in F\,a\neq c\,a\neq b}[T_{ca}\times(1-e^{-\frac{iN_{ca}+jN_{ab}}{5}})\times T_{ab}]}{\sum_{a\in F\,a\neq c\,a\neq b}[T_{ca}\times(1-e^{-\frac{iN_{ca}+jN_{ab}}{5}})]}$$

以下对此式中的参数进行说明：

(1) AT_{cb}：域 c 对域 b 的初始域间推荐信任值。

(2) 域 a：联盟内与域 c 和域 b 均有交互历史的第三方域，起到推荐作用。

(3) T_{ca}，T_{ab}：域 c 对 a 的域间信任值和域 a 对 c 之间此刻的域间信任值，前者表示域 c 的推荐值在 a 处的重视程度，域间信任值越大的域做出的推荐重要程度越高；后者表示域 a 对域 b 的信任推荐值。这样根据对推荐者的信任值便可以确定推荐者所推荐信任值所占权重。

(4) N_{ca}，N_{ab}：域 a 中用户访问域 c 的次数和域 b 中

的用户访问域 a 的次数。$1-\exp(-(aN_{ca}+bN_{ab})/5)$ 随 $N_{ca}+N_{ab}$ 负指数增长的特点很适合用于强调域间交互次数的重要性。当 $N_{ca}+N_{ab}=+\infty$ 时,$1-\exp(aN_{ca}+bN_{ab})/5)$ 取得最大值1,表明此信任推荐值权重已不受交互次数的约束。

(5)i,j:域 a 对其与推荐方以及推荐方与被推荐方交互次数的权值指数。要求 $i+j=1$,i 越大说明域 a 对其与推荐方之间交互次数的重要性越重视,当 $i=1,j=0$ 时,说明只考虑其与推荐方的交互次数,不考虑推荐方与被推荐方的交互次数。

● 域 B 对实体 e 的推荐信任值 FIT。

FIT 可以根据实体所具有的角色来计算。在域内每一个角色都附有一定的信任值,也即当实体最初被授予此角色时,同时获得此角色附带的信任值作为其域内信任值,一般来说,层次越高或者权限中所访问资源密级越高的角色,其信任值也会越大。因此当实体被建立之初肯定会被分配若干角色,选取这些角色中附带信任值中最大的信任值作为此实体的初始域内信任值。

● 他域对实体的推荐信任值 FT_c,FT_a。

实体在本域的域内信任值在动态更新时会综合此实体在联盟内其他域以及本域中的行为历史,可以作为联盟内其他域对此实体的推荐信任值,因此在确定实体外域信任值时不需像确定域间信任值那样去和联盟内所有和目标域有过交互的域进行交互了,可以直接取此值作为实体外域信任 FT。

● 个体自我评价信任值 IT,ST_b,ST_c。

自我评价值由个体自主提出,在交互行为中,IT 在整体信任值中占比重大于其他个体。

3.2.2　综合信任值的计算

各信任确定后,实体 e 的综合信任值 INT 也就能够通过计算得出了。综合信任值的计算方法是对以上信任值加权平均得到:

$$FT'_c = ST_c \times FT_c$$

$$AT_{cb}' = ST_c \times AT_{cb}$$

$$FIT' = FIT \times ST_b$$

$$FT_c'' = iFIT' + jAT_{cb}'$$

$$i+j=1, i \geq j$$

$$FT' = xFT_a + yFIT'' + zFT_c'$$

$$x+y+z=1, x \geq y \geq z$$

$$INT = FT' \times IT$$

一般来说,外域信任推荐值最能反映实体的直接行为,域内信任值次之,域间信任值最弱。根据上式可得到实体当前的信任值,随着实体的交互行为和时间推移,信任值体现出其动态性,而有效的信任值应在相应的时间区间进行实时的更新。

4　结束语

动态联盟环境下,实体频繁的在各个组织域中进行着各种工作,随着技术的进步,交互变得越来越简单便捷,然而也会带来另外一些问题,例如,该实体在不同安全级别的信任域中的信任值应该如何评估,各个信任域中的操作是否会影响该实体身份的安全性。信任管理作为信任评估的一种手段,主要基于凭证和基于信誉两种方式。身份信任管理机制可帮助计算联盟中实体身份的信任值,提供一种有效的"软安全"信息保护手段。

参考文献:

[1] Maler E, Reed D. The Venn of Identity - Options and Issues in Federated Identity Management[J]. IEEE Security & Privacy, 2008, 6(2): 17-23.

[2] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management[C]//Proeeedings of the IEEE Conference on Security and Privacy. Oakland, CA: [s.n.], 1996.

[3] Winsborough W, Seamons K. Automated Trust Negotiation [C]//DARPA Information Survivability Conference and Exposition. Hilton Head, South Carolina: [s.n.], 2000.

[4] Li Xiong, Liu Ling. A Reputation - Based Trust Model for Peer - to - Peer Ecommerce Communities[C]//Proeeedings of IEEE Conference of E - Commerce. USA: ACM Press, 2003: 275-284.

[5] 窦　文,王怀民,贾　焰,等. 构造基于推荐的 Peer - to - Peer 环境下的 Trust 模型[J]. 软件学报, 2004, 15(4): 571-583.

[6] Jøsang A, Fabre J, Hay B, et al. Trust Requirement in Identity Management[J]. Australian Computer Society, 2005, 44: 99-108.

[7] 田慧蓉. P2P 网络信任模型与激励机制的研究[D]. 北京:北京邮电大学, 2006.

[8] Xue G T, You J Y, Jia Z Q. An Interest Group Model for Content Location in peer - to - peer systems[C]//Proeeedings of the IEEE International Conference on E - Commerce Technology for Dynamic E - Business. [s.l.]: [s.n.], 2004.

[9] 刘　鹏. 基于信任的联盟互操作动态访问控制研究与应用[D]. 北京:北京航空航天大学, 2008.