一个基于信任管理的分布式访问控制系统的设计与实现*)

王 远 徐 锋 曹 春 吕 建

(南京大学软件新技术国家重点实验室 南京 210093) (南京大学计算机软件研究所 南京 210093)

摘 要 开放协同软件环境下软件系统的安全问题极大地影响了软件系统的开发与应用。信任管理是解决开放协同软件环境下安全问题的一个新思想。本文在分析了开放协同软件系统安全问题的基础上,针对现存信任管理系统的不足,设计并实现了一个适用于开放环境下的基于信任管理的分布式访问控制系统 DACBTM。该系统采用信任度量的方法对软件实体间的信任关系进行评估。本文在系统实现的同时给出了一个经过改进与扩充的信任发现算法,该算法对于安全信息不足的情况给出了合理的解决方案。

关键词 开放协同环境,信任,信任管理,信任评估,信任链

The Design and Implementation of a Distributed Access Control System Based on Trust-Management

WANG Yuan XU Feng CAO Chun LU Jian

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract The security problems of the open coordination software environment make great influence on the development and application of the software systems. Trust management is a new approach to solve these security problems effectively. By analyzing the security problems of the open coordination software systems and the limitations of the traditional trust management systems, this paper designs and implements a distributed access control system, DACBTM, based on trust management, which is suitable for the application system in the open coordination software environment. The system can evaluate the trust relationship between software entities by the approach of trust-evaluation. We also present an improved, effective algorithm for the collection of the security information, which provides a reasonable mechanism to solve the shortness of the security information in the open coordination software environment.

Keywords Open cooperation environment, Trust, Trust-management, Trust-evaluation, Trust link

1 引言

Internet 的发展,极大地影响了软件运行模式。Internet 已经由一个共享资源和交换数据的信息网络,转变成了一个开放的、动态的且高度变化的网络应用平台。运行于其上的软件系统也随之发生了根本性的变化。它们正由封闭的、熟识用户群体和相对静态的方式向着开放的、公共可访问的和高度动态的服务模式转变;其运行也由基于集中稳定的局域网环境和企业内部网环境,转变为依赖于分布在网络中的各个异构的、自治的资源实体,其系统结构具有高度的动态性。

这种高度自治的软件系统引发了许多安全问题,如安全分析主体的复杂化、安全信息的不完整性、安全度量的相对化和安全措施的自适应等。应用系统安全主体的不确定性和软件系统结构的动态性使得软件实体及其所提供的服务在传统的方式下难以维护和管理。同时安全信息的分布性和不完整性使得许多基于传统软件系统形态的安全技术和手段,如访问控制列表(access control list, ACL),一些传统的公钥证书体系等,不再适用于解决此类软件系统中的安全问题,因此需要一种新的安全技术和方法来解决安全问题。

针对于 Internet 网络服务中的安全问题,M. Blaze 等人在 1996 年提出了信任管理的概念[1]。其基本思想就是在承认安全信息不足的前提下,借助可信的第三方提供的附加安全信息来判断软件实体间的信任关系,进行系统的安全决策。信任管理为 Internet 环境下的开放、分布和动态的软件系统提供了一个合理的安全决策框架[6]。基于信任管理的思想,产生了一些信任管理系统,如 KeyNote, Policymaker 等。它们可以部分解决协同软件中所存在的安全问题,但是具有一定的局限性。其主要表现在:

· 对于第三方的安全信息采用严格的形式化方法进行处理,其信任关系的刻画是二值的,即信任和不信任,这种方法过于严格,不能适应安全信息不足、安全主体复杂的情况。

· 信任管理系统借助安全凭证来表达信任关系。当前的信任管理系统其安全凭证表达能力有限,无法表达实体之间复杂的信任关系,尤其是无法反映软件实体之间的相对信任关系。

· Internet 是一个开放协同的软件环境,安全信息具有一种"真"分布性,安全信息的收集与处理相对困难,当前的信任管理系统无法在安全信息不足的情况下做出准确的授权判断。

为了解决上述问题,本文做了如下工作。(1)基于信任度

*)本文由 973 项目(No. 2002CB312002);863 项目(No. 2002AA1160101, No. 2001AA113110);国家自然科学基金项目(No. 60273034, No. 60233010);江苏省自然科学基金和高技术项目(No. BK2002203, No. BK2002409, No. BG2001012)资助。王 远 硕士研究生,主要研究方向:分布对象技术、可信计算、系统安全。徐 锋 博士,主要研究方向:分布对象技术、系统安全、电子商务应用。吕 建 教授,博士生导师,研究方向:形式化方法、分布对象技术、移动 Agent 技术、构件技术。

量思想来解决传统信任管理系统中信任关系刻画的二值性问题。信任度量的核心思想是认为在开放协同的软件环境下，没有绝对的安全，安全与其所依赖的安全信息均是相对的。因此需要将解决安全问题所需要的本质信任内容，显式地提出来并加以研究。(2)对于传统的安全凭证进行了扩充，使其能够对于实体间的相对信任关系和经验信息进行描述。(3)在上述工作的基础上设计并实现了一个基于信任管理的访问控制系统。该系统通过软件实体之间的经验信息来支持软件实体间的相对信任关系，从而在本质上反映了开放协同软件环境下安全的特点，即是一种相对的、动态的安全。系统设计与实现的核心工作是给出了一个经过改进与扩充的信任发现算法，该算法实现了信任评估与信任发现过程的结合，合理的解决了开放协同环境下安全信息不足的问题。

2 基本设计思想

针对 Internet 开放协同软件环境中主体复杂化、安全信息相对缺乏、安全度量相对化以及系统的高度动态化，本文在进行系统设计时，基于信任管理的思想，主要从实体的管理与维护、安全凭证的表达与使用、分布式授权算法和相对度量机制三方面展开工作。

·使用基于角色的访问控制模型，进行实体的管理与维护。角色包括两个层次的映射关系：角色和访问权限和被访问实体之间的映射；访问实体和角色之间的映射。

·扩充传统信任管理中的安全凭证。通过扩充安全凭证，来描述实体间相互关系，有效的进行传统的授权过程和基于经验的信任评估过程等多种授权方式。

·将传统的信任发现算法和信任评估有机的结合。分布开放环境，协同实体的安全信息不足，本文利用参与协同软件实体以往的历史信息，引入一个基于经验的信任度评估模型[5]，进行相对的安全度量。

系统由一个五元组〈S, O, Op, R, P〉构成，其定义如下：

S 为访问实体的集合，主要为分布于 Internet 上的各个软件实体；O 为被访问实体的集合，包括文件，数据库，Internet 上将要被调用的软件实体等；Op 为操作的集合，$Op=\{Execute, Write, Read\}$；$R$ 为系统中所有角色的集合；P 为一组安全凭证的集合。$\forall p\in P$，p 为一个三元组〈$receiver$, $role$, $Authorizer$〉，其中，〈$receiver, role, Authorizer$〉其中 $receiver, role, Authorizer\in R$。$Authorizer$ 指明该条凭证的授权者，$receiver$ 指明该凭证的被授权者，$role$ 指明 $receiver$ 被授予的角色。

为了支持系统正常工作，整个访问控制系统还包括以下一些设施：

·映射表 map。$mapItem$ 为 map 表中的任意一项。$mapItem=\langle Role, OpSet\rangle$，$OpSet=\{\langle o, op\rangle \mid o\in O, op\subseteq Op\}$，$Role\in R$。$OpSet$ 中每一项对应一个被访问实体和其上可执行的操作集。map 表给出了角色与操作之间的关联关系，它根据角色定义机制生成。

·映射函数 $check$。$check:\langle s, r\rangle\rightarrow auth$。$s$ 为请求实体，r 为所请求的角色，$r\subset R$，$auth\{$false，true$\}$。

请求者通常无法将请求定位到具体的角色，其所提供的请求信息通常为如下格式〈s, $OpItem$〉，$OpItem\in OpSet$。因此根据 map 表，可获得请求角色集合 $RoleSet=\{role \mid role\in R\wedge \exists\langle role, Opset\rangle\in map, OpItem\in OpSet\}$。这样用户请求可以转化为相应的 $check$ 函数的输入。$check$ 用来验证请求是否能被执行，返回值为 $true$ 时，验证通过；否则，拒绝请求。在系统中，$check$ 函数由信任引擎来完成，是整个系统的核心，来完成对实体的授权过程。

3 分布式访问控制系统 DACBTM 的设计与实现

本节设计并实现了一个基于信任管理的分布式访问控制系统 DACBTM(A Distributed Access Control System based on Trust-Management)。工作分为三大部分：(1)安全凭证与角色定义；(2)信任引擎(Trust Engine)中的信任管理算法(即 check 函数功能)；(3)系统结构设计与实现。

3.1 DACBTM 系统中的角色定义与安全凭证

该访问控制系统在对实体的管理与授权方面，采用了基于角色的访问控制模型。在系统中，“角色→访问实体集合”的映射将角色与特定的待访问实体连接在了一起，具有某一特定角色的用户在操作权限定义的范围内可以对待访问实体进行操作；“用户←角色”的映射则将指定角色分配给特定的用户。

3.1.1 *角色的定义* 角色的定义完成“角色→访问实体集合”映射并生成 map 表。它包括角色名称，角色属性和角色权限三个主要部分。角色属性定义了具有该角色的软件实体所必需具有的一些基本属性。角色权限部分包括两个域：resource 和 Right，其中 resource 指明了角色所管理的资源，Operation 域指明了角色对所管理实体所能执行的操作。在一个角色的定义中通常有多对 resource 与 Right，即一个角色可以管理一组相关的实体。

3.1.2 *安全凭证定义* 安全凭证构成了集合 P，完成了“用户←角色”的映射。安全凭证的签发者(或接收者)只能是一个软件实体或是一个被定义的角色(本文采用“实体名．角色名”的方式来表达系统中的角色)。安全凭证能进行授权以及表达角色与角色之间的逻辑关系。在 DACBTM 系统中，安全凭证分成两大类：传统的安全凭证与扩充的安全凭证。

·传统的安全凭证。这类凭证主要用于授权与委托以及反映角色间的内在逻辑关系。分为以下三种：

(1) $B.r\leftarrow A$。该凭证形式表示实体 B 将自己的 $B.r$ 角色授予实体 A，B 称为凭证签发实体。

(2) $B.r1\leftarrow A.r$。该凭证的含义为角色 $B.r1$ 中，包含了所有具有角色 $A.r$ 的实体。即具有 $A.r$ 角色的实体，同时也具有角色 $B.r1$。

(3) $A.r\leftarrow f1\cap f2\cap\cdots\cap fn$，该凭证的含义为角色 $A.r$ 中包含同时具有角色 $f_i(1\leqslant i\leqslant n)$ 的实体。

·扩充的安全凭证。这类凭证主要用于支持基于经验的信任评估，分为两大类：

(1) 对于实体经验信息进行刻画的安全凭证。该类凭证的作用就是描述相关实体的经验信息，其形式如下：

①$A.expr(rolename=name, succ=m, fail=n)\leftarrow B$。$expr$ 角色是一个系统角色，刻画了评估实体对于请求实体的经验信息。经验信息采用二元组($succ, fail$)来表示，$succ$ 表示请求实体在充当 $rolename$ 角色时进行成功操作的次数，而 $fail$ 则表示失败的次数。该凭证的含义为：实体 A 关于 B 在充当 $rolename$ 角色时的经验信息为($succ, fail$)。

②$A.rec(reclevel=f)\leftarrow B$。$rec$ 角色也是一个系统角色，用来标记一个实体的可信推荐者。在开放分布环境下，并不是所有实体的提供的经验信息都是可信的，一个软件实体

只会将它的推荐者所提供的经验信息作为有效的信息，*reclevel* 是一个位于 0.0～1.0 之间的浮点数，表示信任等级。该凭证的具体含义为，实体 B 作为实体 A 的一个推荐者，且 A 对 B 的信任等级为 f。

(2) 用于信任评估的安全凭证。在安全信息不足的情况下，本文采用了一种基于经验的信任评估方法。该类凭证与前者配合使用，完成信任评估过程，$v\in[0,1]$。

①$A.r(sucExp\geqslant v)\leftarrow B$，其含义是实体 B 充当实体 A 定义的角色 R 的预期成功率大于或等于 v。

②$A.r(failExp\leqslant v)\leftarrow B$，其含义是实体 B 充当实体 A 定义的角色 R 的预期失败率小于或等于 v。

3.2 信任引擎中的分布式信任管理算法

该算法是整个系统的核心(即 check 函数的执行步骤)。该算法将传统的信任管理系统所使用的信任查找算法与一个基于经验的信任评估模型有机的结合起来，使系统可以有效地利用实体的历史信息进行授权。

定义 1(单步信任链) 对于每个传统凭证，其中所描述的凭证形式“$RE_1\leftarrow RE_2$”，称为一个单步信任链，RE_1，RE_2 均为角色表达式。

定义 2(信任链) 对于一组单步信任链“$RE_1\leftarrow RE_1'$”，…，“$RE_i\leftarrow RE'_i$”，…，“$RE_n\leftarrow RE'_n$”，若 $RE'_i=RE_{i+1}$，则“$RE_1\leftarrow RE_2\leftarrow\cdots\leftarrow RE'_n$”，称为信任链，其中 RE_1 称为链头，RE'_n 称为链尾。

信任链是传统的基于角色的信任管理系统进行授权的基础。传统的基于角色的信任管理系统，在处理授权请求之时，就是通过在网络上查找一条信任链，链头为请求角色，链尾为请求实体。对于信任链中所涉及到的各个单步信任链，则从网络中的各个可信节点获得，这些可信接点就是信任管理中所涉及的第三方实体。

在 DACBTM 中，安全凭证均存放于凭证签发实体的凭证库中，以满足签发者可寻址。

定义 3(签发者可寻址) 对于一组凭证集合 $Rset$，对于任意的信任链“$B.r\leftarrow\cdots\leftarrow A$”，如果该链存在，则从 $B.r$ 出发必然可以完成整个信任链的推导。凭证集合 $Rset$ 称为“签发者可寻址”。

满足“签发者可寻址”，DACBTM 访问控制系统从理论上来说可找到任何存在的信任链，但是开放环境下，安全信息难于收集依然是限制信任管理系统广泛应用的“瓶颈”，本文给出了一个结合信任评估的信任发现算法，以解决该问题。

定义 4(本地有效角色集) 给定请求实体 A，角色集合 R，实体 B 的本地凭证库 $Plib$，按如下步骤进行处理：1)令 R 为空集。2)遍历 $Plib$。对于任意的角色 $E.r$，若存在信任链“$E.r\leftarrow\cdots\leftarrow A$”，则令 $R=R+\{E.r\}$。R 称为实体 A 在 B 的本地有效角色集。

图 1 为算法流程图，结合流程图，下面给出授权算法的主要步骤：

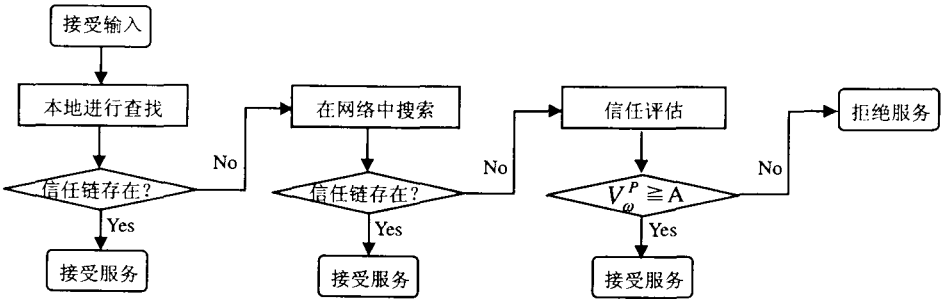

图 1 算法流程图

输入：请求实体 A，请求操作$\langle o,op\rangle_{o\in O,op\in Op}$，实体 A 所携带的凭证集合 credSet。

输出：评估结果(“接受请求”或“拒绝操作”)

1. 分析$\langle o,op\rangle$，获得相关角色集合 RoleSet：RoleSet＝{role| role∈R∧∃⟨role,OpSet⟩∈map,⟨o,op⟩∈OpSet}。
2. 对于∀role，role∈RoleSet，执行以下步骤。
   - 2.1 令 find＝ false(记录查询结果)，目标实体 dest＝o，目标凭证库 destLib＝olib(olib 为实体 o 的凭证库)并设定查询深度 depth。
   - 2.2 令 destLib＝destLib＋credSet，depth＝depth－1，若 depth<0，执行步骤 3。在 destLib 中进行凭证链的查找，若存在凭证链“role←…←A”，令 find＝true，执行步骤 4；否则执行步骤 2.3。
   - 2.3 获得实体 A 在实体 dest 的本地有效角色集 RS，生成临时凭证集 tempSet＝{E.r←A | E.r∈RS}，令 credSet＝credSet＋tempSet，实体 dest 对 credSet 中的所有凭证进行签名。分析有效角色集 RS，获得待访问实体集合 ESet＝{e| ∃e.r,e.r∈RS}，对于∀e∈ESet，令 dest＝e，destLib＝eLib。访问 dest 所在之网络节点，执行步骤 2.2。
3. 信任评估过程，若评估通过，令 find＝true。
4. 若 find 为 true 则返回“接受请求”；若为 false，则返回“拒绝请求”。

上述算法，将传统的信任管理的思想与基于经验的信任评估的思想做了有机的结合，体现了一种“计算分布”的思想，它将整个搜索过程分散到了与之相关的各个软件实体所在的节点之上，从而降低了单个节点的负荷，该算法也降低了网络通信的开销。所需的网络开销仅仅是传递 credSet 时所需的开销，远小于传统算法中传递所有凭证库的开销。在本算法的初始阶段，需要指定算法的搜索深度，因为在开放分布的软件环境下，如果无限定地扩大搜索范围，将会导致系统效率下降。因此，指定合适的搜索深度，将大大地提高系统的效率。但是，在特定的搜索深度之内，无法保证在最坏情况之下也能获得所有的相关凭证，因此，本文引入基于经验的信任评估算法来解决安全信息不足、凭证不完整的情况下所存在的授权失败的问题。图 2 给出信任评估算法的详细描述过程，即授权算法的步骤 3 的详细过程。

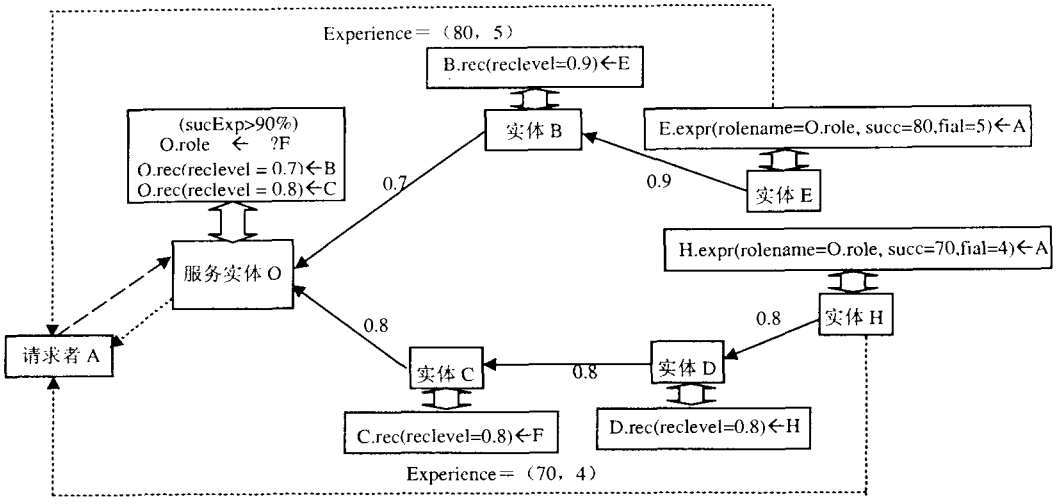

图 2　信任评估过程示意图

图 2 中，每个方框中的内容，为软件实体凭证库中与该次评估过程具体相关的凭证。箭头表示软件实体间的信任关系。虚线以及虚线上的值表示评估实体对于请求实体的经验信息。设有 n 个实体为服务实体 o 的推荐者，对于请求实体 A 的该次请求，评估实体 I 的经验信息记为 $M_i=(succ_i, fail_i)$，经验信息的传递路径中的实体集合记为 $E_m=\{E_{ij}\mid j\leqslant n, n$ 为路径中实体的个数$\}$。

C_i 为每条路径的综合信任度，$C_i=\prod_{j=1}^{n}C_{ij}$，$C_{ij}$ 实体 P_{ij} 对于实体 P_{ij+1} 的信任度。当服务提供实体获得各个评估实体对于请求实体的经验信息之后，服务提供实体将对这些经验信息进行综合，得到最终的经验信息 $M=(succ, fail)$，其中

$$succ=\sum_{i=1}^{n}C_i * succi, fail=\sum_{i=1}^{n}C_i * faili$$

对于，所获得的最终信任 M，服务提供实体根据凭证库中的信任评估凭证，获得期望的成功率 α，如上例所示，服务实体对于请求实体的期望成功率 $\alpha=90\%$。本文利用文[5]中的公式 1 进行计算。

$$V_\omega^P=P_\alpha(X\leqslant succ_\omega)=\sum_{l=1}^{succ_\omega}C_{succ_\omega+fail_\omega}^{l}\alpha^l(1-\alpha)^{succ_\omega+fail_\omega-l}$$

然后，将所得的 V_ω^P 与预先规定的采纳系数 A 进行比较，若 $V_\omega^P\geqslant A$，则评估通过，否则，将拒绝服务。

3.3　DACBTM 系统结构

图 3 给出了 DACBTM 系统的结构。DACBTM 系统是一个发布于 Internet 上的软件实体，提供安全服务。中间件平台若要使用 DACBTM 所提供的安全服务，则需要在其服务调用的入口处增加一个安全处理层，由安全处理层来调用 DACBTM 所提供的安全服务。DACBTM 为所有服务请求所必需调用的第一个服务，若该服务返回 true，则允许请求者继续调用其他服务，否则将拒绝请求者此次访问。

Security Handler 是中间件平台提供的一个消息预处理模块。当有外部的请求到达时，对请求进行预处理。Security Handler 提取请求者的信息，包括请求者的身份信息、操作信息等，然后将这些操作信息交由 DACBTM 系统进行处理。DACBTM 系统的核心是一个信任引擎，信任引擎包括三大主要模块：信任计算模块、经验模块和解析模块。解析模块的主要作用就是分析本地结点软件实体的凭证库，然后将相关的凭证传递给信任计算模块进行处理。经验模块的主要功能是从相关软件实体的凭证库中提取经验信息，然后将这些经验信息交由信任计算模块进行处理。经验模块具有在网络中搜索经验信息的功能，它为本地经验信息和来自于网络其他实体的经验信息提供了统一的接口。信任计算模块具有在网络上搜索凭证以完成信任链的功能以及处理经验信息的功能。其完成整个信任链发现及信任评估工作。搜索引擎对于用户是完全透明的，DACBTM 系统提供了简单易用的接口供其他软件实体使用。如图 3 所示，DACBTM 收到 Security Handler 的信息后进行授权工作。如果请求者的权限通过了验证，DACBTM 系统将结果返回给 Security Handler，Security Handler 再将调用请求转发给实际的服务提供实体，完成一次服务调用；若请求者未通过 DACBTM 的安全认证，Security Handler 将不转发其服务请求，即该次服务被拒绝。

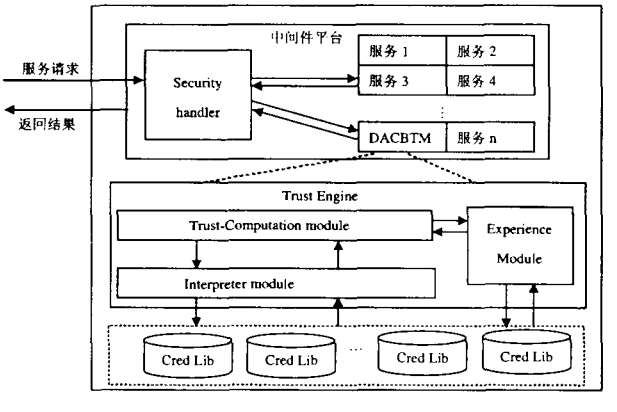

图 3　DACBTM 系统结构

4　相关工作分析与比较

本节将从信任关系的表达、信任发现过程和凭证的管理三方面把 DACBTM 系统与其他系统进行比较。

当前的基于信任管理的访问控制系统，如 PolicyMaker[1]，KeyNote[2]，均可以用来表达复杂的信任关系。从理论上分析，这些系统均可以用于支持分布式的访问控制。但是这些系统必须在某些方面做出相应的扩充，如信任发现算法和凭证的撤销等。

（下转第 248 页）

索引。联邦搜索服务收到的请求被分配到这些节点，这些节点在它们各自元数据的基础上，利用索引执行搜索任务，并返回结果。

(5)元数据收集节点(Metadata Collection Node)

该节点收集所有 harvesting 节点收集到的元数据，并把它们分配到不同的搜索集群节点，即 D1，D2，…，Dn。这类节点的引入有两种功能。一是引入某种形式的负载均衡；二是简化灾难处理过程。

(6)联邦搜索节点(Federated Search node)

该节点负责为用户提供统一搜索界面，将搜索请求分配给 cluster 上的所有 Search nodes(D1…Dn)收集搜索结果，并提交给最终用户。

作为探索性研究的一部分，我们正在采用 GT3.2，建立一个实验系统，使用 2 个 grid 节点从 2 个 DP 中执行高延迟的收集和索引元数据的工作，同时也将利用 grid 将收集到的元数据送到一个搜索引擎的小集群(SP)，每一个搜索引擎将再从 harvesting 节点获得的索引上执行搜索。

总结 互操作性是数字图书馆所面临的重大问题和关键挑战，它几乎渗透到数字图书馆作为一个分布式计算系统的每个方面。至今数字图书馆界已经开发出了许多方法，取得了一些成果，但这些方法在实现 Internet 上大规模的数字图书馆互操作方面有一定的局限性。当前，全球正在兴起的有关网格的研究，使人们感受到一种信息社会的新的基础设施正在出现，这种新的 infrastructure 可能带来信息资源的获取、分布、传输和有效利用的革命性的、结构性的巨大变化。本文从资源共享的角度，提出利用先进的网格技术，在原有 OAI-PMH 框架的基础上，构建数字图书馆网格 DL Grid，利用网格建立和存储用于信息发现的元数据，实现 DLs 信息资源共享和跨仓储无缝查找，从而解决数字图书馆的互操作性问题。

参 考 文 献

1 Paepcke A, Chang C-C K, Garcia-Molina H, et al. Interoperability for Digital Libraries: Problems and Directions-Stanford University. 1998
2 NSDL. National SMETE Digital Library. http: // www. smete. org/nsdl/
3 Shi R, Maly K, Zubair M. Dynamic interoperation of non-cooperating digital libraries. In: Proc. of Digital Library IT Opportunities and Challenges in the New Millennium, Beijing: Beijing Library Press, July 2002. 350～361
4 Metacrawler. http: // www. metacrawler. com
5 Shi R, Maly K, Zubair M. Interoperable Federated Digital Library using XML and LDAP. Global Digital Library Development in the New Millennium, 2001(5): 277～286
6 Enhancing Infrastructure for OAI. http: /dlib. cs. odu. edu/ # dtic, 2004
7 The Open Archives Initiative Protocol for Metadata Harvesting. http: //www. openarchives. org/OAI/2. 0/openarchivesprotocol. htm
8 张付志. 异构分布式数字图书馆互操作技术研究:[博士论文]. 北京:北京理工大学, 2003
9 都志辉，李三立，刘鹏. 网格计算. 清华大学出版社. 北京，2002
10 Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, San Fransisco, CA, 1999. http: // mkp. com/grids, http: // www. gridforum. org/, http: // www. ccgrid. org/
11 Foster I, Kesselman C, Tuecke S. The anatomy of the grid: enabling scalable virtual organizations [J]. CCGRID2001, First IEEE/ACM International Symposium on Cluster Computing and the Grid: 6～7

(上接第 229 页)

DACBTM 系统对于基本信任关系的表达能力与它们基本相同，支持授权、委托等复杂的信任关系，同时引入了信任度的概念以表达实体间的相对的信任关系。DACBTM 系统在实现了凭证搜索算法的基础上，还增加了系统对于安全信息不足即无法查找到足够的信任凭证的情况的处理步骤。现存的信任管理系统 dRBAC[8] 也做了类似的扩充工作。与 dRBAC 系统相比，DACBTM 在算法的搜索过程中，通过将搜索分解为若干个子搜索，使得每个子搜索运行与不同的结点之上，从而降低了单个节点的负荷，同时利用路径信息来缩短搜索路径，提高搜索效率。DACBTM 系统与 dRBAC 系统相比一个重大的改进和扩充就是提供了对于安全信息不足的处理机制。DACBTM 系统利用软件实体的历史信息，采用基于经验的信任评估模型[5]，在一定程度上解决了安全信息不足的问题，DACBTM 系统同时提供相应的历史信息管理和更新机制。

DACBTM 系统提供了凭证管理的功能。DACBTM 系统分析凭证的有效性，在凭证的 Property 域条件不被满足时，系统将把该凭证标记为无效凭证。系统可以定期检查无效凭证，若凭证超过有效期时，系统通过凭证库存取接口将该凭证删除。同时，为了支持信任评估，DACBTM 还提供了经验信息的收集与管理机制。

结束语 在开放协同软件环境下，应用系统的结构发生了根本性的转变，实体的应用需求也变得复杂多变。传统的安全手段和安全凭证已经无法满足系统的应用需求。在开放环境下，系统的动态性和安全信息的不完整性，都导致了用户对于应用系统中所存在的安全问题提出了更高的要求。本文在传统信任管理系统的基础上，设计并实现了一个新型的分布式访问控制系统，该系统适用于开放协同软件环境下的安全授权。它将传统的信任管理系统中所使用的授权方法与基于经验的信任评估方法做了有机的结合，使得系统能够在安全信息不足的情况下进行授权，同时也保证了应用系统的安全性。

本文的进一步工作，是使信任搜索过程和信任评估过程结合得更加紧密，即在信任链的搜索过程中使用信任评估的方法，例如在对于信任链进行双向搜索时，当信任链中断，使用信任评估方法将信任链补充完整。同时，如何对于经验信息采用更为有效和准确的描述方式，也很值得探讨和研究。

参 考 文 献

1 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. In: Proc. of the IEEE Symposium on Research in Security and Privacy, Research in Security and Privacy, Oakland, CA, May 1996. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.
2 Blaze M, Feigenbaum J, Ioannidis J, et al. The KeyNote trust-management system, version 2. IETF RFC 2704, Sept. 1999
3 Li N, Mitchell J C, Winsborough W H. Design of a role-based trust-management framework. In: Proc. of the 2002 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2002
4 Li Ninghui, Winsborough W H, Mitchell J C. Distributed credential chain discovery in trust management(extended abstract). In: Proc. of the Eighth ACM Conference on Computer and Communication Security(CCS-8), ACM Press, Nov. 2001. 156～165
5 徐锋，吕建，郑玮，曹春. 一个软件服务协同中信任度计算模型的设计. 软件学报，2003, 14(6): 1043～1051
6 徐锋，吕建. Web 安全中的信任管理研究与进展. 软件学报，2002, 13(11): 2057～2064
7 马晓星. Internet 软件协同技术研究:[南京大学博士论文]. 2003
8 Freudenthal E, Pesin T, Port L, et al. dRBAC: Distributed role-based access control for dynamic coalition environments. In: Proc. of the 22nd Intl. Conf. on Distributed Computing Systems (ICDCS02), 2002