P2P中基于信任和属性的访问控制

封孝生 王桢文 黎湘运
(国防科技大学C4ISR技术国防科技重点实验室 长沙 410073)

摘 要 P2P具有无集中控制节点、节点对等自治和网络动态的特点,这些特点为实施访问控制带来很大的挑战,传统的访问控制技术不能很好地适应对等网环境。首先对现有的对等网环境中的访问控制技术进行研究,然后在基于信任模型的角色访问控制的基础上,针对无法区分通过信任模型计算出相同结果的用户的问题,提出了基于信任和属性的访问控制。基于信任和属性的访问控制引入资源属性和用户属性来分别描述资源和用户,依据用户属性、信任模型计算出的数值、环境属性和授权策略来建立用户角色指派关系,依据资源属性和授权策略来建立角色权限指派关系,从而解决基于信任模型的角色访问控制存在的问题。

关键词 访问控制,属性,P2P
中图法分类号 TP309 **文献标识码** A

Trust-Attribute-based Access Control in P2P Environments

FENG Xiao-sheng WANG Zhen-wen LI Xiang-yun
(C4ISR Technology National Defense Science and Technology Key LAB, National University of Defense Technology, Changsha 410073, China)

Abstract Traditional access control models which are based on identity are not adaptive in P2P environments, which characterize non-centralization, autonomy and dynamic characteristic. We analyzed the access control issue in P2P environments. The existing trust-based role access control lacks measures to distinguish users whose results from a trust model are same. We proposed trust-attribute-based access control to deal with this problem. Trust-attribute-based access control describes users and resources using user attributes and resource attributes. The model builds user role assignment using user attributes, the result from a trust model, environment attributes and authorization policy and builds role permission assignment using resource attributes and authorization policy.

Keywords Access control, Attribute, P2P

1 引言

对等网络(Peer-to-Peer, P2P)中每一个节点不仅使用其它节点提供的资源,而且提供资源给其它节点访问。考虑来自服务使用方的不安全因素,节点需要防止自己提供的资源被未授权的用户访问。由于P2P具有无中心控制、节点高度自治性和动态性的特点,传统的访问控制方法依赖具有集中控制功能的控制点,难以适应P2P环境,因此有必要研究P2P环境中的访问控制方法。

本文将在基于信任模型的角色访问控制的基础上,针对无法区分通过信任模型计算出相同数值的用户的问题,提出基于信任和属性的访问控制模型。基于信任和属性的访问控制模型引入资源属性和用户属性来分别描述资源和用户,依据用户属性、信任模型计算出的数值、环境属性和授权策略来建立用户角色指派关系,依据资源属性和授权策略来建立角色权限指派关系,从而解决基于信任模型的角色访问控制存在的问题。

2 相关工作

P2P环境下现有的访问控制方法有传统访问控制方法、基于证书的访问控制方法和基于信任模型的角色访问控制方法。

(1)传统访问控制方法是对RBAC进行扩展,使得在没有集中控制点的情况下,可以进行授权管理和访问检查。如文献[1]实现了节点每次访问资源不需要在集中服务器上进行身份认证和访问控制,但是节点在新加入、申请角色或者变更角色时需要与权威节点交互。文献[2]讨论了两种角色分配协议:中心化协议和非中心协议。在中心化协议中,社区中存在一个权威节点。在非中心化协议中,社会角色的分配是通过新节点在加入时与社区中每个节点协商来决定的。

(2)基于证书的访问控制方法利用证书来进行授权管理,将授权管理分散于各个节点,从而适应P2P环境。文献[3]提出的访问控制模型将节点分成两类:L1和L2。L1负责存储和管理访问控制列表、发送授权证书。L2能够确认由用户提供的授权证书、发布事件和存储授权证书。在访问控制过程中节点使用证书来访问资源。在文献[4]中,节点将资源进行分级,为资源关联安全级别标签。对资源具有访问权限的节点应有至少与资源相同等级的安全标记,而这些安全标记用资源拥有者发布的公钥证书当中的属性来表达。文献[5]中,作者提出一种可以在P2P环境中高效地产生公钥的机

到稿日期:2010-03-24 返修日期:2010-07-19 本文受国家自然科学基金(60903225,70971134)资助。
封孝生(1971—),男,副教授,主要研究方向为信息安全、信息管理与智能决策等,E-mail:fxs365@sina.com;王桢文(1984—),男,博士生,主要研究方向为信息安全、信息管理与智能决策;黎湘运(1984—),男,硕士生,主要研究方向为信息安全、信息管理与智能决策。

制，在此基础上设计了授权服务系统 Akenti，Akenti 可以通过再次产生公钥来撤销和赋予节点权限。

(3)基于信任模型的角色访问控制方法就是利用信任模型的计算结果作为授权的依据。文献[6]将对等网络中基于信任的访问控制过程分解成 4 个阶段：实体识别；协作监视；信任计算；根据信任值和访问控制策略进行访问控制决策。文献[7]研究混合式 P2P 网络中的访问控制，综合考虑了全局可信度和领域范围的局部可信度。文献[8]提出的信任模型将信任分为直接信任和间接信任，直接信任又可以分为直接经历信任和推荐信任，节点可以通过多条推荐信任路径计算出网络中任何一个节点的信任值。文中提出的基于上述信任模型的访问控制策略是：依据节点所拥有的信任值来分发和更新角色。在文献[9]中，节点为每个共享的文件设计两个限值：总体信任值和总体贡献值。当访问请求者的总体信任值和总体贡献值达到了限制值，就允许访问文件。每次文件转移后，总体信任值和总体贡献值都会被更新。文献[10]讨论利用点与点的信任值计算出组间的信任值，把这些信任值运用在角色划分和为节点指派角色中，给出了基于角色的访问控制的一种实现方式。

传统的访问控制方法技术成熟，能够准确执行资源保护策略，但难以摆脱对集中控制点的依赖。基于证书的访问控制的优点是，资源的保护方对访问请求者进行授权，授权结果以证书的形式存在，由访问请求者进行管理，改变了传统访问控制中需要集中管理授权关系的方式。基于证书的访问控制是从访问控制的工作流程方面研究 P2P 环境中的访问控制，关于如何建立授权关系，没有研究具体的方法。信任模型可以在没有统一的用户管理、身份不易确定的环境中，为陌生实体建立信任关系提供机制，而且这种机制不需要执行集中控制功能的节点的参与。基于信任模型的角色访问控制适应 P2P 环境的无中心控制、节点对等自治和动态性的特点。基于信任模型的角色访问控制存在局限性：无法区分通过信任模型计算出相同数值的用户。现有的基于信任模型的角色访问控制根据用户的信任度来为用户分配角色，而影响用户信任度的因素并非用户自身的特征。用信任度来区分用户是一种依据单一条件来对用户进行区分的方法。这样可能导致不同特征的用户，信任模型的计算结果都一样，有相同的信任度。如果这时授权策略需要赋予这些用户不同的角色，基于信任模型的角色访问控制就不能执行这样的授权策略。

本文在基于信任模型的角色访问控制的基础上，针对无法区分通过信任模型计算出具有相同信任度的用户的问题，提出基于信任和属性的访问控制。基于信任和属性的访问控制集中考虑基于证书的访问控制和基于信任模型的角色访问控制的优点，引入属性描述用户和资源，从而实现 P2P 环境中有效的访问控制。

3 基于信任和属性的访问控制模型

最早 Mohammad A. Al-Kahtani 和 Sandhu Ravi 提出，将 RBAC 和属性结合起来进行授权。文献[11]研究了基于用户属性建立用户角色指派关系的方法，提出了 RB-RBAC 模型，通过设定规则可以自动利用用户属性为用户分配角色。GARBAC[12]扩展了 RB-RBAC 模型，研究了基于用户属性的用户角色对应关系，把为用户分配角色的模块分为两种：基于单一属性的用户角色分配和基于复合属性的用户角色分配。本文提出的基于信任和属性的访问控制模型(TABAC)进一步研究利用用户属性、资源属性和环境属性来建立用户角色指派关系和角色权限指派关系的方法，并将它用到 P2P 环境的访问控制中。

3.1 模型的基本概念

用户属性描述是对用户的抽象概括。用户和用户属性描述之间是多对一的关系。角色沿用 RBAC 中角色的概念。权限是针对资源可以进行的动作，由操作和资源组成。访问控制系统通过设置访问控制策略来说明用户和角色之间以及权限和角色之间的关系。因此访问策略有两种：用户角色关系策略(URP)和角色权限关系策略(RPP)。图 1 描述了用户和资源的对应关系。

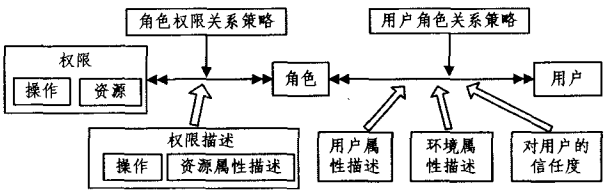

图 1 基于信任和属性的授权

对等网络中，资源分散存储在节点上。每个节点可以作为服务器，独立为其它节点提供资源。节点的对等和自治特点决定了角色权限指派关系考虑的是角色和存储在本地的资源所对应的权限之间的关系。请求访问资源的用户可能在本节点上，也可能在其它节点上，取决于用户在哪个节点上进行注册。

(1)属性表达式。*AttrExpress* 表示属性表达式，是对用户的某个方面的特征的描述。*AttrExpress* 的定义为 *AttrExpress*::=(*AttrName*, *AttrValue*)，它可以表示用户属性、资源属性和环境属性。

(2)对用户的信任度。$trust_{ij}$ 表示节点 i 对用户 j 的信任度。对用户的信任度是对请求访问资源的用户的信任度，它是利用信任模型计算出的结果。信任度反映节点主观上对用户的信任程度。不同的节点对同一用户的信任度是不同的，因此对用户的信任度不能作为用户的属性。本文的研究中未考虑具体的信任模型，只使用现有的某种信任模型得出节点对用户的信任度，并将它用来作为为用户分配角色的依据之一。

(3)用户属性描述。*SubDes* 表示用户属性描述。用户属性描述由一系列属性表达式的与连接组成，它从多个角度表现用户的特征。*SubDes* 的定义如下：

SubDes::=*AttrExpress*|*SubDes* AND *SubDes*

(4)资源属性描述。*RExpress* 表示资源属性描述，由一系列属性表达式的与连接组成。*RExpress* 的定义如下：

RExpress::=*AttrExpress*|*RExpress* AND *RExpress*

(5)权限描述。*PermDes* 表示权限描述，由资源属性描述和操作组成。*Operation* 表示操作集。*PermDes* 的定义如下：

PermDes::=(*RExpress*, *Operation*)

(6)环境属性描述。*EExpress* 表示环境属性描述，其定义如下：

EExpress::=*AttrExpress*|*EExpress* AND *EExpress*

(7)属性约束。*AttrCon* 表示属性约束，由一系列属性约

束对(*AttrConPair*)的与连接组成。*AttrCon* 定义如下：

AttrCon::=*AttrConPair*|*AttrCon* AND *AttrCon*

AttrConPair::=(*AttrName*,*AttrValueSet*)

AttrName::=属性名

AttrValueSet::=属性值集合

(8)角色权限关系策略(RPP)。RPP 由资源保护政策决定，决定了一个角色能够拥有的权限。RPP 包括角色、权限约束集和约束 3 个部分。角色(*role*)指明了此 RPP 所针对的角色。权限约束集(*PermConSet*)指明了此角色允许拥有的权限所对应的权限描述，由若干个权限约束(*PCons*)的或连接组成。约束(*RConstrain*)用于表达资源保护政策中允许指派给这个角色的权限的个数和定义不能被此角色拥有的权限，由允许指派给这个角色的权限的个数(*PNum*)和权限描述对集合(*PermPairs*)组成。RPP 的定义如下：

RPP::=(*role*,*RConstrain*,*PermConSet*)

RConstrain::=(*PNum*,*PermPairs*)

PermPairs::=*PermPair*|*PermPairs* AND *PermPairs*

PermPair::=($PermDes_i$,$PermDes_j$)

PermConSet::=*PCons*|*PermConSet* OR *PermConSet*

PCons::=(*AttrCon*,*Operation*)

(9)用户角色关系策略(URP)。URP 由资源保护政策决定，它决定了能够拥有一个角色并且使用这个角色的用户，另外指明了此用户能够使用这个角色时的环境属性要求和信任度要求。URP 包括角色、用户属性约束集、约束、信任度取值范围和环境属性约束 5 个部分。角色(*role*)指明了此 URP 所针对的角色。用户属性约束集(*SubConSet*)指明了可以拥有此角色的用户所对应的用户属性描述。信任度取值范围(*TrustValue*)规定了节点对使用这个角色的用户的信任度的取值范围。约束(*SConstrain*)用于表达资源保护政策中角色允许关联的用户个数和角色互斥约束，由角色允许关联的用户个数(*SNum*)和互斥角色集合(*mutexRoles*)组成。环境属性约束(*EAttrCon*)表达与用户和资源无关的对系统环境的要求，如时间约束、紧急级别的约束。URP 定义如下：

URP ::= (*role*, *SubConSet*, *SConstrain*, *TrustValue*, *EAttrCon*)

SConstrain::=(*SNum*,*mutexRoles*)

SNum::=由存储资源的节点定义的角色 *role* 能关联的用户个数

mutexRoles::=由存储资源的节点定义的与 *role* 互斥的角色集合

SubConSet::=*AttrCon*|*SubConSet* OR *SubConSet*

TrustValue::=由存储资源的节点定义的 *role* 对应的信任度取值范围

EAttrCon::=*AttrCon*

3.2 授权规则

授权分成两个部分，角色权限指派关系和用户角色指派关系，通过这两个指派关系，用户和权限就建立了授权关系。模型中，建立用户角色指派关系需要获取用户属性信息(可能来自其他节点)，然后根据用户属性信息、对用户的信任度、环境属性信息和角色的 URP 共同决定用户和角色是否存在指派关系。利用权限的权限描述和角色的 RPP 共同来决定角色和权限是否存在指派关系。这里引入属性来描述资源是为了实现自动建立角色权限指派关系，管理员只需维护资源属性，降低工作量。

(1)建立角色权限指派关系的授权规则。当权限 p 满足角色 r 的 RPP 时，角色 r 和权限 p 角色权限指派关系，认为角色 r 拥有权限 p；

权限 p 满足角色 r 的 RPP，当且仅当以下两个条件同时满足：

1)权限 p 的权限描述满足角色 r 的 RPP 中的权限约束集。

2)权限 p 满足角色 r 的 RPP 中的约束。

下面先给出检查属性描述满足属性约束的满足性规则，再给出检查权限描述满足权限约束集的满足性规则，最后给出权限满足 RPP 中的约束的满足性规则。

规则 1 如果对属性约束 *AttrCon* 中出现的每一个属性约束对 *AttrConPair*=(*AttrName*,*AttrValueSet*)，在资源属性描述 *RExpress* 中都存在一个属性表达式 *AttrExpress*=(*AttrName*,*AttrValue*)，使得 *AttrConPair*. *Attr Name*=*AttrExpress*. *AttrName* 且 *AttrExpress*. *AttrValue*∈*AttrConPair*. *AttrValueSet*，那么 *RExpress* 满足 *AttrCon*，记为 *RExpress*∈*AttrCon*。规则 1 对于用户属性描述和环境属性描述的情况也同样适用。

规则 2 如果权限 p 的权限描述 *PermDes* 和权限约束 *PCons* 满足 *PermDes*. *RExpress*∈*PCons*. *AttrCon* 且 *PermDes*. *Operation*⊂*PCons*. *Operation*，那么权限 p 满足权限约束 *PCons*，记为 $p\in PCons$。其中 *PermDes*. *RExpress* 表示 *PermDes* 的资源属性描述，*PCons*. *AttrCon* 表示权限约束 *PCons* 的属性约束，*PermDes*. *Operation* 和 *PCons*. *Operation* 分别表示 *PermDes* 和 *PCons* 中的操作集。

规则 3 对于权限 p，如果角色 r 的 RPP 的权限约束集中存在一个权限约束 *PCons*，使得权限 $p\in PCons$，那么权限 p 满足角色 r 的 RPP 中的权限约束集。

规则 4 如果权限 p 的权限描述和角色 r 拥有的任意一个权限的权限描述所组成的权限描述对不在 RPP 的约束的 *PermPairs* 中出现，那么权限 p 的权限描述满足角色 r 的 RPP 的约束的 *PermPairs*。

规则 5 如果角色 r 所拥有的权限数目小于角色 r 的 RPP 的约束的 *PNum*，并且权限 p 的权限描述满足角色 r 的 RPP 的约束的 *PermPairs*，那么权限 p 满足角色 r 的 RPP 中的约束。

(2)建立用户角色指派关系的授权规则。

当用户 u 满足角色 r 的 URP 时，用户 u 和角色 r 存在用户角色指派关系，用户 u 可以使用角色 r 拥有的权限。

用户 u 满足角色 r 的 URP，当且仅当以下 4 个条件同时满足：

1)用户 u 的用户属性描述满足角色 r 的 URP 中的用户属性约束集；

2)对用户 u 的信任度满足角色 r 的 URP 中的信任度取值范围；

3)节点的环境属性描述满足角色 r 的 URP 中的环境属性约束；

4)用户 u 满足角色 r 的 URP 中的约束。

利用规则 1 可以对 1)和 3)进行满足性检查，利用 P2P 环

境中的信任模型进行访问控制的节点可以计算出对用户的信任度，根据数值检查满足角色 r 的 URP 中的信任度取值范围。下面给出检查用户满足 URP 中的约束的满足性规则。

规则 6 如果用户 u 所拥有的角色集与角色 r 的 URP 的约束中的互斥角色集合的交集为空，并且与角色 r 存在用户角色指派关系的用户的个数小于角色 r 的 URP 的约束中的 $SNum$，那么用户 u 满足角色 r 的 URP 中的约束。

4 基于信任和属性的访问控制流程

访问检查开始后，系统从访问请求中提取请求发起者所在的节点的地址。无论消息是直接到达本节点的，还是经过转发到达的，肯定有发起节点的地址，以便收到消息的节点可以响应消息。如果地址是本地，就是本地的用户发起的请求，直接读取分配给用户的角色的集合；否则，根据地址索取授权证书。有证书时，从证书中提取角色信息；没有证书时，执行授权，最终得到分配给用户的角色的集合。然后执行角色权限检查，从而检查用户是否有相应的权限。图 2 给出访问控制的工作流程。

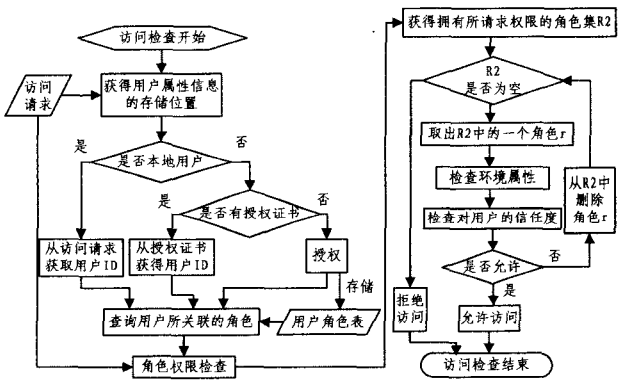

图 2 访问控制的工作流程

(1)从本地查询用户的角色。

从本地查询用户的角色，就是利用用户 ID 从用户角色表中检索用户关联的角色。

(2)检查授权证书。节点 i 给用户 j 的一个证书 C_j^i 的内容包括：

1)证书拥有者 ID，这是从节点 i 的角度对 j 的一个标识。

2)证书提供者，就是节点 i。

3)有效期。

4)证书提供者对前面内容的签名。

授权证书是授权后分配给其他节点上的用户的身份凭证。授权证书中记录了进行访问检查的节点为其他节点上的用户指定的一个唯一标识，这个唯一标识将作为证书拥有者 ID 保存在授权证书中。授权证书可以提供授权结果的重用。只要授权证书在有效期中，对用户进行访问检查时就可以直接提取证书拥有者 ID。将证书拥有者 ID 作为用户 ID，到用户角色表中查出这个用户 ID 对应的角色，就可以获得上次授权的结果，而不需要再次判断用户与角色的关联关系。这种做法是因为难以唯一标识来自其他节点的用户。如果没有授权证书或已经失效，就执行授权。

(3) 授权。

如果没有授权证书或已经失效，就执行授权。授权分 3 个阶段：一是从用户所在节点查询用户属性信息；二是利用授权模型为用户分配角色；三是制作授权证书。

1)从用户所在节点查询用户信息。所查询的用户信息是对用户特征的描述(user profile)。一个 user profile 应该包括与安全有关的用户特征，如用户 ID、用户所在节点的标识、用户的公钥、用户上一次认证的时间、用户所在节点的 IP 地址、用户在其所在节点的角色级别、用户的出生年份、专业、工作、学历等。在具体应用时要根据安全需求进行考察，决定 user profile 包含哪些用户特征。这些信息是用户第一次加入网络的时候记录下来的基本信息，由用户注册的节点进行维护。

2)利用授权模型为用户关联角色。对等网络中，资源节点往往不知道请求者的身份，而且资源保护政策也不关心请求者身份，而是针对其它一些用户属性进行控制。如政策规定“XX 学院的副教授可以读取、修改文件 A”，这样的政策只关心请求者隶属的部门和职称。授权模型使用用户属性来与角色进行联系，它将身份 ID 看作是一种属性，与其他属性是地位平等的。在获得了用户的属性信息后，可以得出与用户关联的角色。如果存在与用户关联的角色，节点会给用户命名一个用户 ID，用户 ID 和所关联的角色被存储在用户角色表中。节点为用户关联角色后，得到用户 ID，一方面可以用于制作授权证书，另一方面用于下一步查询用户所关联的角色。

3)制作授权证书。制作授权证书时，用户 ID 作为在授权证书中的证书拥有者 ID。生成的授权证书被发送给用户，在用户下一次访问请求时，利用授权证书来得到证书拥有者的 ID，将证书拥有者的 ID 作为用户 ID，到用户角色表中查出这个用户 ID 对应的角色，就得到了用户所关联的角色。

(4)查询用户所关联的角色。利用从上一步得到的用户 ID，在节点的用户角色表中查询用户所关联的角色，得到角色集 R1。

(5)角色权限检查。角色权限检查首先从访问请求中提取要进行访问检查的权限 P，再从上一步得到的角色集 R1。利用 R1 中的角色和权限 P 在角色权限表进行检索，得到用户所关联的角色中拥有权限 P 的角色，组成角色集 R2。如果 R2 为空就拒绝访问，否则就检查环境属性和对用户的信任度。

(6)检查环境属性和对用户的信任度。从 R2 中取出一个角色 *role*。提取当前的环境属性信息，如时间、日期等，然后检查用户的信任度和当前的环境属性信息是否符合角色的 URP 中的要求，符合则允许访问，否则就将角色 *role* 从 R2 中删除，再检查 R2 中的下一个角色。当遍历了所有 R2 中的角色后，仍然没有允许访问，就拒绝用户的访问请求。

结束语 (1)在无中心控制的情况下，TABAC 有效执行资源保护政策，弥补基于信任模型的访问控制的局限性。

无中心控制的环境下节点难以标识所有用户身份，因为用户信息分散存储在各个节点上，可能在本地存储，也可能在其它节点存储。对于后者，在全网没有中心控制的情况下，节点不知道用户的存在，难以确定标识用户身份。TABAC 依据用户属性、环境属性和节点对用户的信任度来建立用户角色指派关系，摆脱了基于用户身份的授权方式，适应无中心控制的环境。

TABAC 中建立用户角色关系，除了依据基于信任模型

(下转第 41 页)

制。由此实现通过检测系统传输环境的变化而自适应地改变窗口长度，从而实现比较理想的时延及吞吐量性能。

参 考 文 献

[1] Shah A M, ShamimAra S, Matsumoto M. An Improved Selective Repeat-ARQ Scheme for IrDA Links at High Bit Error Rate [J]. New Zealand: The HIT Lab NZ, University of Canterbury, 2005: 37-42

[2] Varthis E G, Fotiadis D I. A comparison of stop-and-wait and go-back-N ARQ schemes for IEEE 802. 11e wireless infrared networks[J]. Computer Communications, 2006, 29: 1015-1025

[3] Yao Yu-dong. An Effective Go-Back-N ARQ Scheme for Variable-Error-Rate Channels[J]. IEEE Transactions on communications, 1995, 43(1): 20-23

[4] Vojinovic R, Petrovic G. The analysis of the adaptive three-mode ARQ GBN scheme using retransmission cycles mechanism[J]. International Journal of Electronics and Communication, 2006, 60: 190-198

[5] 黎锁平，刘存明，何志鹏. 无线数据传输的 GBN-ARQ 和 SR-ARQ 系统时延性能研究[J]. 信号处理，2005，25(3)：384-388

[6] 黎锁平，刘存明. 带休假的返回 n-ARQ 系统时延性能研究[J]. 系统工程学报，2008，23(3)：367-371

[7] 黎锁平，刘存明. 基于噪声信道的 ARQ 系统时延性能及最小滑动窗口控制研究[J]. 信息与控制，2008，37(6)：697-702

(上接第 31 页)

的计算结果来建立用户角色指派关系，还要依据用户属性信息。不同节点利用信任模型计算出的用户信任度可能会不同。信任度具有主观性，并不是用户固有的特征，用它对用户进行分类不够准确。因此 TABAC 中考虑了用户属性(如年龄、学历、专业等)，这些属性是用户特征的表现，从多个角度说明用户的客观情况，依据用户属性和信任模型的计算结果一同来对用户进行分类，弥补基于信任和信誉模型来建立用户角色指派关系的局限性。

(2)用户增加时，TABAC 可以有效地对新增加用户的访问行为进行控制。

对等网络中节点动态地加入(退出)，由于节点上存放用户信息，因此导致用户的加入(退出)。对于用户的加入(退出)，其他节点是不知道的。当对等网络中一个节点上新增了用户，除非使用全网的消息投递，否则其他节点就不知道此用户的存在，而全网的消息投递代价太大。再者，如果每增加一个用户，节点都需要立即考虑为它建立授权关系，由于用户数目大，对于单个节点来说有许多用户是不会访问其资源的，因而不会使用到授权关系，于是建立授权关系所花费的开销就被浪费了。

(3)TABAC 的访问检查流程可以减少对新增用户的授权开销。

用户加入时，用户信息不存储在节点上，因此不必建立该用户的角色指派关系。在其访问资源时，才去建立用户角色指派关系。采用这样的工作流程，即使有许多用户加入对等网，但是只要没有实际访问资源，节点就不会考虑为其建立授权关系。这样能够适应 P2P 网络中节点的动态性。当用户退出时，如果此用户对应的用户角色指派关系过期，就自动撤销了授权。如果在有效期中，用户又加入了网络，产生了访问请求，那么可以继续拥有用户角色指派关系中对应的角色。

(4)下一步工作。本文在基于信任模型的角色访问控制的基础上通过引入用户属性、资源属性和环境属性实现对具有相同信任度的用户的细粒度访问控制。文中给出了模型的基本概念、授权规则和访问控制流程。在具体访问控制策略的实施中属性的选取、描述，不同节点上属性信息的获取、语义一致性分析、转换和映射，以及属性信息的引入有可能带来的时间复杂度是下一步值得深入研究的工作。

参 考 文 献

[1] 宋伟，卢正鼎，李瑞轩，等. 一种 Peer-to-Peer 环境下的分布式访问控制模型[J]. 计算机应用与软件，2006，23(12)：31-33

[2] Maruoka M, Nemati A G, Barolli V, et al. Role-based Access Control in Peer-to-Peer(P2P) Societies[C]// 22nd International Conference on Advanced Information Networking and Applications. IEEE Computer Society, 2008: 495-500

[3] Fenkam P, Dustdar S, Kirda E. Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments[C]// Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. IEEE Computer Society, 2002: 95-102

[4] Palomar E, Estevez-Tapiador J M, Hernandez-Castro J C, et al. Certificate-based Access Control in Pure P2P Networks[C]// Proceedings of the Sixth IEEE International Conference on Peer-to-Peer Computing. IEEE Computer Society, 2006: 177-184

[5] Berket K, Essiari A, Muratas A. PKI-based Security for Peer-to-Peer Information Sharing[C]// Proceedings of the Fourth International Conference on Peer-to-Peer Compu-ting. IEEE Computer Society, 2004: 45-52

[6] 张书钦，芦东昕，杨永田. 对等网络中基于信任的访问控制研究[J]. 计算机科学，2005，32(5)：31-33

[7] 张骞，张霞，刘积仁. 混合 P2P 环境下有效的访问控制机制[J]. 东北大学学报，2007，28(5)：643-647

[8] Wang Lei, Zhu Yanqin, Jin Lanfang, et al. Trust Mechanism in Distributed Access Control Model of P2P Networks[C]// Seventh IEEE/ACIS International Conference on Compu-ter and Information Science. IEEE Computer Society, 2008: 19-24

[9] Tran H, Hitchens M, Varadharajan V, et al. A Trust based Access Control Framework for P2P File-Sharing Systems[C]// Proceedings of the 38th Hawaii International Conference on System Sciences. IEEE Computer Society, 2005: 302c-302c

[10] Gummadi A, Yoon J P. Modeling Group Trust For Peer-to-Peer Access Control[C]// Proceedings of the 15th International Workshop on Database and Expert Systems Applications. IEEE Computer Society, 2004: 971-978

[11] Al-Kahtani M A, Sandhu R. A Model for Attribute-Based User-Role Assignment[C]// Proceedings of the 18th Annual Computer Security Applications Conference. Las Vegas, Nevada, IEEE Computer Society Press, 2002: 353-364

[12] Zhu Yi-qun, Li Jian-hua, Zhang Quan-hai. A General Attribute based RBAC Model for Web Service[C]// Proceedings of IEEE International Conference on Services Computing. 2007: 236-239