doi:10.11959/j.issn.1000-436x.2017027

P2P 网络中基于模糊理论的任务访问控制模型

刘浩[1]，张连明[2]，陈志刚[3]
（1. 湖南人文科技学院信息学院，湖南 娄底 417000；2. 湖南师范大学物理与信息科学学院，湖南 长沙 410081；
3. 中南大学信息科学与工程学院，湖南 长沙 410083）

摘 要：P2P 网络的开放性自组织等特性给系统带来一系列的安全风险，然而传统的访问控制模型并不能适用于 P2P 网络这样的分布式管理系统。针对该问题，给出一种基于模糊理论的任务访问控制模型，并对该模型进行形式化描述与分析。通过层次分析法和模糊评价模型，计算每次交互任务的风险值。该模型通过对任务访问控制模型进行扩展，依据交互任务的风险值对访问权限进行动态管理。分析与实验结果表明该模型能够抑制非合作节点的交互成功率，增大整个对等网络系统的交互成功率，提高了对等网络系统的安全性。

关键词：P2P 网络；模糊理论；风险评估；交互；任务；访问控制
中图分类号：TP393 **文献标识码**：A

Task-based access control mode of peer-to-peer network based on fuzzy theory

LIU Hao[1], ZHANG Lian-ming[2], CHEN Zhi-gang[3]
(1. Institute of Information, Hunan University of Humanities, Science and Technology, Loudi 417000, China;
2. College of Physics and Information Science, Hunan Normal University, Changsha 410081, China;
3. School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: The opening and self-organization features of P2P network brings a series of security risks, and the traditional access control model is not suitable for P2P network as it is a kind of distributed management system. Task-based access control mode of P2P network was proposed based on fuzzy theory. And the formalization description and analysis of the model was also proposed. The risk value of each transaction was calculated through hierarchy process analysis and fuzzy comprehensive evaluation. In this model, according to the risk value of each transaction, the dynamic management of access authority was realized by extending task-based access control model. The results show that this model can restrain the success of noncooperative nodes transaction and raise the success of the whole P2P network system transaction, thus improving the security of P2P network system.

Key words: peer-to-peer network, fuzzy theory, risk assessment, transaction, task, access control

1 引言

当前，作为一种分布式体系结构模型，P2P 网络（peer-to-peer network）强调资源的全面共享，无需依赖集中式服务器的支持，实际应用非常广泛[1]。相关研究表明基于 P2P 网络的各种应用在互联网上的重要性日益提高，用户数量也逐年增多[2,3]。然而，P2P 网络的开放性自组织等特性给系统带来一系列的安全风险，这严重制约了 P2P 网络应用的进一步发展[4]。访问控制是维护 P2P 网络系统安全、保护网络资源的重要手段之一[5]。近 30 年来，访问控制一直是国内外信息安全界的研究热点之一，先后出

收稿日期：2016-05-05；**修回日期**：2016-11-08
基金项目：国家自然科学基金资助项目（No.61571188）；湖南省教育厅科研优秀青年基金资助项目（No.15B125）；湖南省计算机应用技术重点建设学科基金资助项目
Foundation Items: The National Natural Science Foundation of China (No.61571188), The Outstanding Youth Scientific Research Foundation of Hunan Provincial Department of Education (No.15B125), The Key Construction Course of Computer Application Technology in Hunan Province

现了自主访问控制、强制访问控制、基于角色的访问控制和基于行为的访问控制等相关模型[6]。文献[7]借鉴了社会网络的信任评价机制，给出了一种对等网络的节点准入控制模型。文献[8]根据信任评价机制和多级安全策略，构造了一种 P2P 网络的访问控制模型。文献[9]给出了一种 P2P 网络环境中基于信誉的访问控制模型。针对传统的强制访问控制模型难以满足协作环境下的访问控制新需求的问题，文献[10]给出了一种支持协作的强制访问控制模型，该模型将主体—客体为中心的访问控制与任务为中心的访问控制相结合，通过控制主客体的安全标记，解决了符合安全策略的敏感信息的双向流动问题，使其更适合协作环境下的访问控制。为适应网构环境下应用系统主客体间访问集中控制的需要，文献[11]提出了一种基于动态情景网关的系统协同访问控制模型。但是，这些传统的访问控制模型都是从系统整体安全角度出发对信息资源进行保护，并没有把执行任务的操作环境（主体节点的脆弱性、目标节点的威胁以及共享资源的安全需求）考虑在内，也不能对主体节点所拥有的权限进行动态管理。因此，它们并不能完全适用于对等网络这样的分布式管理系统。

在信息系统中，通过风险分析可以有针对性地提出安全保护对策和措施，从根本上将风险控制在可接受的范围之内[12]。针对 P2P 网络中节点信息交换不可避免地会给系统带来安全隐患等问题，文献[13]运用信任评价与传统的风险计算相结合的方法来评估对等点信息交换中的风险。文献[14]给出了一种面向医疗大数据的风险自适应的访问控制模型，该模型通过分析医生的访问历史，监测和控制对于医疗记录的过度访问以及特殊情况下的访问请求，使用信息熵和 EM 算法量化医生侵犯隐私造成的风险，根据风险适应性地调整医生的访问能力，保护患者隐私。针对 P2P 文件共享系统中服务不可靠性和恶意节点带来的安全攻击风险，文献[15]给出了一种基于多项式主观逻辑与风险机制的信任模型。这些研究大多把风险作为信任的一种补充或忽略了风险的影响，这就导致了网络系统安全决策的主观性和片面性[16]。

Kwakernaak[17]于 1978 年首次提出了模糊随机变量的概念与模糊评价模型，而后模糊评价模型得到了国内外学者的普遍关注，文献[18~20]将模糊评价模型应用于系统安全状况的评价，并通过若干实例验证了该评价模型的有效性。基于任务的访问控制模型能将信息的机密性、完整性和可用性的访问控制限制在具体任务中，并将其结合在一起，保障信息系统的安全性[21,22]。在一定程度上，信息系统中某次交互任务的风险具有不确定性、模糊性，而在决策时是需要确定的策略，因此，模糊评价模型是良好候选解决方法之一。本文研究的基本思路是：根据模糊评价的基本原理和基于任务访问控制模型的相关理论，给出了一种基于模糊理论的任务访问控制模型，并对该模型进行了形式化描述与分析。该模型能够实现主体节点对目标节点访问权限的动态管理，从而达到网络系统安全的目标。本文的分析场景为 P2P 网络资源共享应用，为了描述方便，称该访问控制模型为 TACFT（task-based access control mode of peer-to-peer network based on fuzzy theory）。

2　TACFT 的体系结构与相关概念

TACFT 体系结构如图 1 所示。在 P2P 网络系统中：第 1 步，服务请求节点向服务提供节点发送服务请求；第 2 步，服务提供节点需要对本次交互任务（task）进行风险评估（图 1 中虚线框中的模块），包括资产识别、脆弱性识别和威胁识别；第 3 步，根据模糊评价与风险分析相关理论对风险进行量化，并计算出本次交互任务的风险值；第 4 步，访问控制决策模块根据风险值来决策访问控制的实施；第 5 步，访问控制实施模块确定服务提供节点是否与服务请求节点进行本次交互，以及服务请求节点具有哪些操作权限和操作权限的生命周期，审计模块主要是用来实现对操作的记录和跟踪；第 6 步，服务提供节点根据相关操作权限等策略为服务请求节点提供共享服务；第 7 步，服务提供节点将本次交互的情况反馈给访问控制实施模块；第 8 步，访问控制实施模块根据反馈情况建议访问控制决策模块完善其相关策略。

在 P2P 网络系统中，每一个节点既是客服机，又是服务器，节点之间的地位是对等的。节点之间的资源共享，不需要在集中服务器上进行身份认证和访问控制，而是每个节点都需要防止自己提供的资源被未授权的用户访问。TACFT 将交互任务的操作环境考虑在内，主体节点可根据自身的安全需求和访问控制策略对访问权限进行动态的管理。因此，它完全适用于对等网络这样的分布式系统。

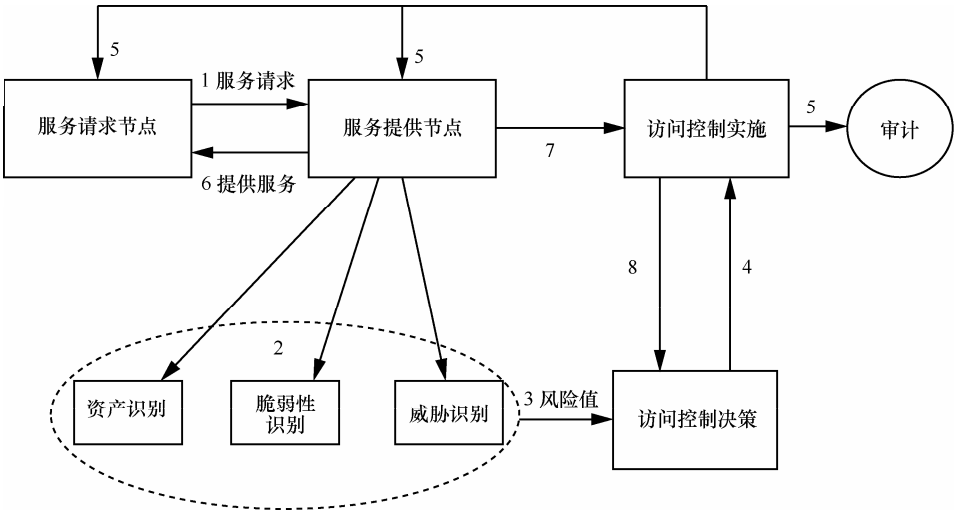


图 1 TACFT 体系结构

在文献[12,13,18,23]的基础上，下面给出一些相关的定义。

定义 1 资产（asset）。系统中具有价值的信息、资源或服务，是访问控制需要保护的对象，本文以 P2P 网络资源共享为分析场景，那么本文中所提及的“资源”概念均等价于“资产”。以 S 表示所有共享资源类别的集合，用 $s \in S$ 表示某一类具体的资源。

定义 2 服务提供节点，也称为主体节点（subject node）。系统中能够共享某一资源或提供服务的节点，用 Z_n 表示本次交互任务中的主体节点。

定义 3 服务请求节点，也称为目标节点（object node）。系统中需要得到某一资源或服务的节点，用 O_n 表示本次交互任务中的目标节点。

定义 4 脆弱性（vulnerability）。是主体节点 Z_n 的一种安全属性，它是服务提供节点本身所具有的漏洞，是可能被恶意节点所利用的缺陷，是主体节点被攻击可能性的重要属性。以 $AV(Z_n)$ 表示主体节点 Z_n 的脆弱性程度，是脆弱性识别的主要内容。

定义 5 威胁（threat）。是目标节点 O_n 的一种安全属性，它是目标节点使本次交互任务发生不安全事件内在或外在因素的综合。以 $T(O_n)$ 表示目标节点 O_n 产生威胁的可能性程度，是威胁识别的主要内容。

定义 6 风险(risk)。是本次交互任务中发生不安全事故，并造成破坏或资源受损的可能性。

3 TACFT 的模糊综合评价法

3.1 风险评估的函数因子

风险评估的目的就是对某一交互任务可能带来的风险进行分析，评估安全威胁的发生可能性及其影响程度，为安全策略的确定提供依据。影响风险评估的函数因子包括风险事件发生的可能性与风险事件发生所产生的后果[18,23]。风险事件产生的后果可用本次交互任务的资产价值（文件资源价值）来体现，而风险发生的可能性主要通过分析本次交互任务中主体节点的脆弱性和目标节点的威胁性来确定。

资源作为对等网络中最有价值的基本元素，是 TACFT 的第一评估要素。首先，对网络系统中的所有资源进行合理分类，分析其安全需求。这里的安全需求主要包括共享资源的机密性、完整性、可用性共 3 个方面。

定义 7 机密性(confidentiality)。是资源的一种安全属性，指资源所达到的未提供（未泄露）给非授权用户的程度，以 $C(s)$ 表示某一资源 s 的机密性。

定义 8 完整性(integrity)。是资源的一种安全属性，指资源不能被非授权篡改或破坏的属性，以 $I(s)$ 表示某一资源 s 的完整性。

定义 9 可用性(availability)。是资源的一种安全属性，指被授权用户按访问控制的要求可访问资源的程度，以 $A(s)$ 表示某一资源 s 的可用性。

定义 10 资源大小(asset scale)。是本次交互任务需要访问的文件资源大小，以 $Q(s)$ 表示某一资源 s 的大小。

定义 11 资源价值(asset value)。是资源一种重要程度的属性，它是资产（资源）识别的主要内容，以 $V(s)$ 表示某一资源 s 的价值。

那么，资源 s 价值 $V(s)$ 由资源的机密性、完整

性、可用性及其大小所确定。

根据前面的定义，脆弱性识别就是分析主体节点 Z_n 本身所具有的安全漏洞，评估主体节点发生不安全事故的内因。包括主体节点所采取保密机制的强度、其防火墙的安全性能高低以及前期发生安全事故的频率共 3 个方面。

定义 12　保密机制强度 P_Z。设主体节点 Z_n 所采取的保密机制强度为 P_Z。

定义 13　安全性能参数 F_Z。设主体节点 Z_n 防火墙的安全性能参数为 F_Z。

本文中，防火墙的安全性能参数 F_Z 是指主体节点 Z_n 能否阻挡或捕捉到恶意攻击和非法访问的成功率。

定义 14　频率 K_Z。设主体节点 Z_n 前期发生安全事故的频率为 K_Z。

威胁识别是目标节点使本次交互任务可能发生不安全事件内在或外在因素的综合。这里主要从 3 个方面来分析：1）目标节点的前期交互行为；2）目标节点的可靠性；3）其他节点对目标节点的评价。

定义 15　设来自目标节点前期交互行为的可能威胁为 $X(O_n)$。

定义 16　设来自目标节点可靠性的可能威胁为 $D(O_n)$。

定义 17　其他节点对目标节点的威胁评价 $\Psi(O_n)$。

通过分析[18,23]，将影响风险评估的函数因子分为 2 级，如表 1 所示。其中，表 1 是对各因素进行综合评价后才能得到的结果，显然不同的条件，其数值不同，为待定值，所以为空。

表 1　风险评估的函数因子

一层	二层	评语集				
		较低	低	一般	高	较高
资产价值 $V(s)$	$Q(s)$	待定	待定	待定	待定	待定
	$C(s)$	待定	待定	待定	待定	待定
	$I(s)$	待定	待定	待定	待定	待定
	$A(s)$	待定	待定	待定	待定	待定
脆弱性 $AV(Z_n)$	P_Z	待定	待定	待定	待定	待定
	F_Z	待定	待定	待定	待定	待定
	K_Z	待定	待定	待定	待定	待定
威胁 $T(O_n)$	$X(O_n)$	待定	待定	待定	待定	待定
	$D(O_n)$	待定	待定	待定	待定	待定
	$\Psi(O_n)$	待定	待定	待定	待定	待定

3.2　函数因子权重的确定

函数因子权重的确定采用层次分析法[23]，层次分析法就是对各评价因素相互间的重要性进行两两比较，在允许相容性范围内，根据综合重要性排出其评价顺序，并进行特征根计算。为了便于量化，引入 1~9 的标度来表示各评价因素之间比较强弱关系，如表 2 所示。

表 2　风险评估的函数因子

标度 a_{ij}	定义
1	因素 i 与因素 j 一样重要
3	因素 i 比因素 j 稍重要
5	因素 i 比因素 j 较重要
7	因素 i 比因素 j 非常重要
9	因素 i 比因素 j 绝对重要
2,4,6,8	因素 i 与因素 j 的重要性介于上述 2 个相邻等级之间
倒数 $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}$	因素 j 与因素 i 的比较 a_{ji} 得到 a_{ij} 的倒数，即 $a_{ji}=\frac{1}{a_{ij}}$

假设评价因素的个数为 m，对它们进行两两比较（在系统初始化时，根据安全性需求由所有节点投票决定），并按上述标度赋值，得到以下判断矩阵

$$\boldsymbol{A}=\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \tag{1}$$

其中，$a_{ii}=1$，$i=1,2,\cdots,m$；$a_{ji}=\frac{1}{a_{ij}}$，$i,j=1,2,\cdots,m$。

求判断矩阵 $\boldsymbol{A}$ 的最大特征根与所对应的权重向量，步骤如下。

1) 先求判断矩阵 $\boldsymbol{A}$ 的最大特征根 $\lambda_{\max}$ 与所对应的特征向量

$$\boldsymbol{W}=\begin{bmatrix} W_1 \\ \vdots \\ W_m \end{bmatrix} \tag{2}$$

2) 判断矩阵的一致性检验，所谓一致性是指判断思维的逻辑一致性。利用一致性指标 $CI=\frac{\lambda_{\max}-m}{m-1}$ 和一致性比率 CR 做一致性检验，其中，$CR=\frac{CI}{RI}$，随机一致性指标 RI 通过表 3 可查。

表 3 随机一致性指标 *RI* 标准值参考

矩阵阶数 m	RI
3	0.58
4	0.9
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45
10	1.49

3) 若 $CR \prec 0.1$ 或 $CI \prec 0.1$，则检验通过，则对特征向量 $\boldsymbol{W} = \begin{bmatrix} W_1 \\ \vdots \\ W_m \end{bmatrix}$ 进行归一化之后得到权重向量。

4) 否则，若检验没通过，需要调整函数因子之间两两比较的标度值，重新构造判断矩阵 $\boldsymbol{A}$，重复上述步骤。

对评语集进行量化，得到 $L=\{$较低，低，一般，高，较高$\}=\{0.1,0.3,0.5,0.7,1.0\}$。

3.3 模糊评价模型

模糊评价模型是一种对多因素影响的事件作出全面评价的决策模型。主要包括 4 个方面：因素集、评语集、单因素评价矩阵和权重分配向量。在复杂系统中，如果涉及的因素很多，并且因素之间还存在着不同的层次，那么就需要将评价因素集合进行分类，先对每一类进行综合评判，再对各类评判结果进行类之间的高层次综合评判。在本文中，风险事件产生的后果用本次交互任务的资产价值（文件资源价值）来体现，属于单层次模糊评价模型。而风险事件发生的可能性主要通过分析本次交互任务中主体节点的脆弱性和目标节点的威胁性来确定，因此属于二层次模糊评价模型。

风险事件产生的后果取决于以下因素集 $V=\{V(s)\}=\{V_1,V_2,V_3,V_4\}=\{Q(s),C(s),I(s),A(s)\}$。在系统初始化时，根据系统的安全需求，将所有的文件资源进行分类，对每类文件资源采用层次分析法确定因素集的权重向量 $\boldsymbol{A}'=\{a_1',a_2',a_3',a_4'\}$。根据量化后评语集 L，由主体节点根据以往的交互历史来对各因素进行评价（对于新加入系统的主体节点，主体节点可以通过向其邻居节点发送请求，获得其邻居节点与目标节点的交互历史，综合其邻居节点的交互历史，可对各因素进行评价），得到各因素模糊子集 $R_i'=\{r_{i1}',r_{i2}',r_{i3}',r_{i4}',r_{i5}'\}$ $(i=1,2,3,4)$。

$$\boldsymbol{R}'=\begin{Bmatrix} r_{11}',r_{12}',r_{13}',r_{14}',r_{15}' \\ r_{21}',r_{22}',r_{23}',r_{24}',r_{25}' \\ r_{31}',r_{32}',r_{33}',r_{34}',r_{35}' \\ r_{41}',r_{42}',r_{43}',r_{44}',r_{45}' \end{Bmatrix} \tag{3}$$

本次交互任务中风险事件产生后果的模糊评判矩阵 $\boldsymbol{B}'=\boldsymbol{A}'\boldsymbol{R}'$，对 $\boldsymbol{B}'$ 进行归一化处理得到 $\tilde{\boldsymbol{B}}'=\{b_1',b_2',b_3',b_4',b_5'\}$。

风险事件发生的可能性取决于以下因素集，$U=\{U_1,U_2\}=\{AV(Z_n),T(O_n)\}$，由主体节点通过层次分析法确定因素集中因素的权重，$W=\{w_1,w_2\}$。而对于每一因素子集 U_i $(i=1,2)$，采用单层次模糊评价模型评判。若各子因素的权重向量为 $\boldsymbol{A}_i$，其评判决策矩阵为 $\boldsymbol{R}_i$，则可以得到第 i 个子集的综合评判结果：$\boldsymbol{B}_i=\boldsymbol{A}_i\boldsymbol{R}_i=[b_{i1}\ \ b_{i2}\ \ b_{i3}]$。

对 U 进行综合评判，其评判决策矩阵为

$$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{B}_1\\ \boldsymbol{B}_2\end{bmatrix}=\begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23}\end{bmatrix} \tag{4}$$

最后，得到 U 的综合评判结果

$$\boldsymbol{\Omega}=\boldsymbol{W}\boldsymbol{B} \tag{5}$$

这也是 U 中所有因素的综合评判结果。对 $\boldsymbol{\Omega}$ 进行归一化处理得到 $\tilde{\boldsymbol{\Omega}}$。

4 风险计算

风险评估的最终目的就是要进行风险量化，或者说采用特定的方法以数量的形式将风险评估的结果表示出来。简而言之，就是得到风险值 R_t。风险值 R_t 既是风险事件发生的可能性 P 的函数，也是风险事件产生后果 C 的函数[18,23]，即

$$R_t=f(P,C) \tag{6}$$

假设 P 和 C 的域值为 $[0,1]$，并用下标 s、f 分别表示事件的成功与失败。则有

$$P_{\mathrm{f}}=1-P_{\mathrm{s}},\quad C_{\mathrm{f}}=1-C_{\mathrm{s}} \tag{7}$$

风险值 R_t 实际上是风险事件发生及其产生后果的似然估计。

$$\begin{aligned} R_t&=1-P_{\mathrm{f}}C_{\mathrm{f}}=1-(1-P_{\mathrm{s}})(1-C_{\mathrm{s}}) \\ &=P_{\mathrm{s}}+C_{\mathrm{s}}-P_{\mathrm{s}}C_{\mathrm{s}} \end{aligned} \tag{8}$$

其中，$P_s=\tilde{\boldsymbol{\Omega}}\boldsymbol{L}^{\mathrm{T}}$，$C_s=\tilde{\boldsymbol{B}}'\boldsymbol{L}^{\mathrm{T}}$。

5　访问控制模型

5.1　TACFT 的基本概念

本文对任务访问控制模型进行了扩展，从目标（服务请求）节点对资源访问的具体需求出发，并综合考虑了本次资源共享交互中服务提供节点和目标节点的各种内外因素，对本次交互任务进行风险评估，以实现灵活动态的授权机制，这种安全策略正好满足 P2P 网络分布式访问控制的安全需求。为了方便对 TACFT 进行形式化描述，先给出一些相关的概念。

定义 18　任务。就是节点间进行资源共享的一个逻辑单元，是可区分的对某一资源的动作。

定义 19　授权步（authorization step）。表示为 As，是指对某一资源的原子操作，一个任务可依次分为多个授权步来完成，其中，任何一个授权步的失败都将导致整个任务的失败。

授权步之间存在着相互依赖关系，包括顺序依赖、失败依赖、失败代理依赖、失败撤销依赖。顺序依赖是指在授权步 As_1 完成之后，As_2 才能被激活；失败依赖是指授权步 As_1 失败之后，As_2 才能被激活；失败代理依赖是指在授权步 As_1 失败之后，才能由 As_2 代理执行；失败撤销依赖是指授权步 As_1 失败之后，As_2 的授权被收回。

定义 20　条件（conditions）。目标节点执行授权步中许可操作的条件。

定义 21　许可集 $\boldsymbol{\Phi}=\{\phi_1,\phi_2,\cdots,\phi_n\}$，许可操作 $\phi_i=\{op,s,condition\}$。其中，$s$ 是访问控制的资源，操作 op 为作用在资源 s 上的一种访问方式，$condition\in conditions$ 表示在本次任务中被允许操作时的风险值应该小于预定的阈值 Π，其值域为[0,1]，一般可设 Π=0.5。

5.2　TACFT 的形式化描述

在 TACFT 中，授权可以用一个五元组表示为 $Au(O_n,S,\boldsymbol{\Phi},TTL,As)$。其中，$O_n$ 为目标节点（服务请求节点），S 表示所有共享资源的集合，$\boldsymbol{\Phi}$ 是许可集合，As 为授权步，TTL 为授权步 As 的生命周期。

下面对 TACFT 模型进行形式化描述。

1) 由任务 $Task$、授权步 As、目标节点 O_n 和许可集 $\boldsymbol{\Phi}$ 共 4 部分组成。

2) 每个任务由若干个授权步 As 组成，即 $Task=\{As_1,As_2,\cdots,As_n\}$，$As$ 之间存在关系 $As\times As\subseteq 2^{\Gamma}$，$\Gamma$ ={顺序依赖，失败依赖，失败代理依赖，失败撤销依赖}。

3) 任务风险评估映射：$R_t\rightarrow Task$，表示对某一特定的任务进行风险评估，即给某一任务赋予相应的风险评估值。

4) $As\rightarrow O_n$ 是从授权步到目标节点（服务请求节点）之间的一个映射，随时间变化而变化。

5) 目标节点执行许可集的激活函数：$init(As,\boldsymbol{\Phi})\rightarrow O_n$，表示目标节点 O_n 获得授权步 As 所对应的操作许可集合 $\boldsymbol{\Phi}$。

6) 操作权限回收函数 $Revoke(As,\phi_1)\rightarrow\boldsymbol{\Phi}'$，$\boldsymbol{\Phi}'=\boldsymbol{\Phi}-\phi_1$。

7) 撤销目标节点执行许可集的函数（也称为权限回收函数）：$destroy(As,\boldsymbol{\Phi},O_n)$。

只有当对任务的风险评估值小于预定的阈值 Π 时，以上的授权才有效，目标节点 O_n 开始拥有许可集中的操作权限，同时本次授权开始倒计时。当生命周期终止，本次授权失效，将被主体节点 Z_n 收回。任何一个任务需要若干个授权步的组合执行才能完成。同时，根据需要，授权步所对应的操作权限许可集可以动态的变化，如规定写操作权限只能使用 3 次，那么当某一任务使用了 3 次写操作权限后，写操作权限将从授权步许可集中剔除掉。通过授权步的生命期和对授权步操作集的动态管理，主体节点 Z_n 可以根据安全需求和访问控制策略进行动态的访问权限管理。

5.3　TACFT 的安全性能分析

通过对授权步的动态操作权限管理，TACFT 模型支持以下安全控制原则与功能。

1) 最小特权原则。在执行任务时，只给用户分配完成任务所需的权限，任务被终止或者已完成，用户将不再拥有所分配的操作权限，并且当某一权限不再使用时，授权步将自动收回该操作权限。

2) 职责分离原则。当一些敏感的任务需要不同的用户执行时，可通过将授权步分别授予不同的目标节点来实现。

3) 安全审计功能。它是识别与防止网络攻击行为、追查网络非法行为的重要手段之一。审计模块作为 TACFT 模型的重要组成部分，可以防止主体节点内部机密或敏感信息的非法泄露。

6　仿真实验与结果分析

在仿真实验中使用 P2Psim 作为系统模拟软件，通过它来构建 TACFT 的网络模型，以检验 TACFT 的有效性。本实验采用北京大学网络实验室提供的 Maze 文件共享系统的用户日志。利用 Maze 系统用户节点 5 天的上传和下载日志信息来构造实验环境，总共 120 000 个活动用户节点。系统将资源的机密性分为 5 级：P（公开），U（一般），C（秘密），Sc（机密），Ts（绝密）；并且其依次赋值为 0、0.25、0.5、0.75、1。对于某一资源，主体节点将根据该资源所属类别的机密程度指定相应的级别（对 $C(s)$ 赋值）。共享资源的完整性和可用性处理与取值方法类似。对这些节点的行为进行统计分析，大致可分为 3 类节点。

1) 优良节点（good node）。该类节点提供服务的质量优良、性能稳定，对别的节点评价客观。

2) 恶意节点（malicious node）。该类节点提供服务的质量低劣拒绝提供服务，对别的节点提供不真实的评价或对资源进行非法访问操作。

3) 低性能节点（low performance node）。该类节点性能不稳定、可靠性差。

再假设优良节点在网络系统中所占的比重为 P_{G}，其获得成功交互的概率为 SP_{G}；低性能节点在网络系统中所占的比重为 P_{L}，其获得成功交互的概率为 SP_{L}；恶意节点在网络系统中所占的比重为 P_{M}，其获得成功交互的概率为 SP_{M}。若在自然状态下，即没有引入访问控制机制，则一次随机交互获得成功的概率为 $P_{\mathrm{nature}} = SP_{\mathrm{G}} \times P_{\mathrm{G}} + SP_{\mathrm{M}} \times P_{\mathrm{M}} + SP_{\mathrm{L}} \times P_{\mathrm{L}}$。假设引入了 TACFT 机制后网络节点之间交互成功的概率为 P_{TACFT}，引入了文献[5]的访问控制机制后网络节点之间交互成功的概率为 P_{r_5}。现假设恶意节点和低性能节点在网络系统中所占的比重相等，即 $P_{\mathrm{M}} = P_{\mathrm{L}}$，当优良节点在系统中所占比重变化时，重复上面的实验 7 次，观察 P_{nature}、P_{r_5}、P_{TACFT} 的变化情况。实验结果如图 2 所示。

从图 2 可以看出，有 $P_{\mathrm{nature}} \leqslant P_{r_5} \leqslant P_{\mathrm{TACFT}}$ 成立，这说明在引入访问控制机制之后，网络系统中的交互成功率有了较大的提高，而且 TACFT 机制比文献[5]的访问控制机制更为有效。

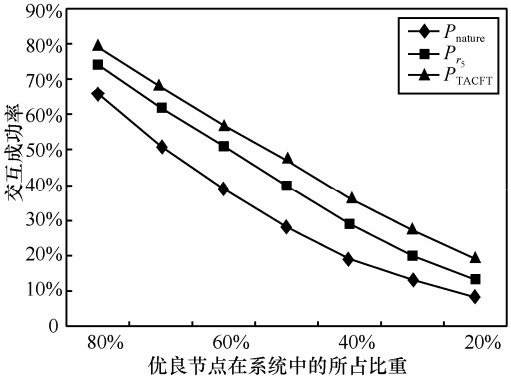


图 2　P_{nature}、P_{r_5}、P_{TACFT} 的变化比较

显然，优良节点的比率越高，整个系统的交互成功率越高，系统越稳定。为了系统的稳定性，不失一般性，不妨设优良节点在网络系统所占比重为 60%，恶意节点所占比重为 20%，低性能节点所占比重为 20%。在引入 TACFT 机制后，系统总共发起 30 000 次服务请求，考察 3 类节点的交互成功率，其实验结果如图 3 所示。

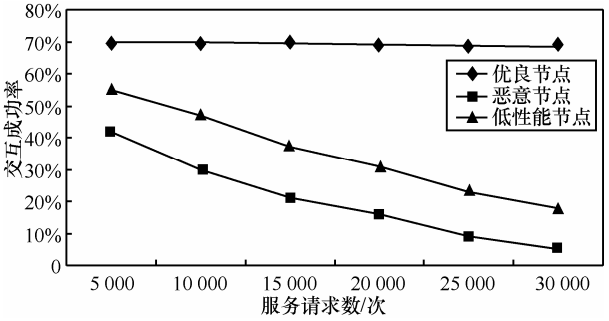


图 3　3 类节点的交互成功率比较

从图 3 可以看出，当服务请求次数增加时，优良节点交互的成功率基本保持在 70%左右，恶意节点和低性能节点的交互成功率快速下降，并且恶意节点的下降速度更快。

引入了 TACFT 机制后，每个节点每天发起 10 次服务请求，认为每个节点从自身安全考虑，会接受优良节点的服务请求，而拒绝恶意节点的服务请求，对于低性能节点，则根据其当前的行为表现决定。考察整个网络系统对 3 类节点判断的准确率，其实验结果如图 4 所示。

从图 4 可以看出，随着时间的延续，系统对低性能节点的判断准确率一直保持在 50%左右，对恶意节点和优良节点的判断准确率逐步上升，最终保持在 90%以上。

综上所述，访问控制模型能够有效地提高网络系统的安全性，达到了预期的设计目标。

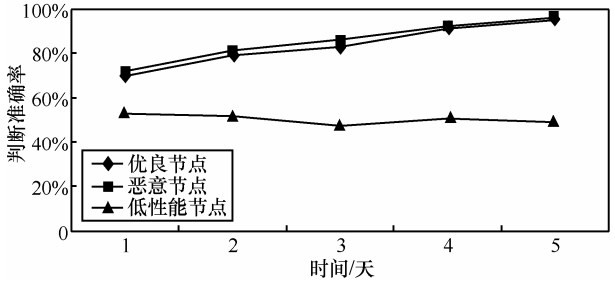


图 4　系统对 3 类节点判断的准确率比较

7　结束语

本文借鉴了模糊理论、风险评估的基本原理，给出了一种 P2P 网络环境下基于模糊理论的任务访问控制模型，给 P2P 网络访问控制模型的研究提供了新的研究思路。在现有的研究基础上，未来研究的工作重点包括在保证访问速度的前提下，以更为灵活的方式来提高访问控制粒度，或与基于角色的访问控制机制相结合，以提高 TACFT 的灵活性。

参考文献：

[1] 孙新, 李庆洲, 赵璞, 等. 对等网络中一种优化的副本分布方法[J]. 计算机学报, 2014,37(6): 1424-1434.
SUN X, LI Q Z, ZHAO P, et al. An optimized replica distribution method for peer-to-peer network[J]. Chinese Journal of Computers, 2014,37(6): 1424-1434.

[2] 闫佳, 应凌云, 刘海峰, 等. 结构化对等网测量方法研究[J]. 软件学报, 2014,25(6):1301-1315.
YAN J, YING L Y, LIU H F, et al. Research on network measurement of structured P2P network[J]. Journal of Software, 2014, 25(6): 1301-1315.

[3] 曾明霏, 余顺争. 使用虚拟参与人和博弈论的 P2P 网络信用系统模型[J]. 小型微型计算机系统, 2014,35(6): 1309-1314.
ZENG M F, YU S Z. A reputation system for peer-to-peer networks using game theory and virtual player[J]. Journal of Chinese Computer system, 2014,35(6): 1309-1314.

[4] 曹晓梅, 胡文捷. 基于动态角色属性的 MP2P 信任模型[J]. 计算机科学, 2015,42(8):106 -111.
CAO X M, HU W J. Dynamic role property based trust model for MP2P networks[J]. Computer Science, 2015,42(8):106 -111.

[5] 李勇军, 代亚非. P2P 文件共享系统中的一种基于商品市场模型的访问控制机制[J].计算机学报, 2012,35(8): 1675-1682.
LI Y J, DAI Y F. A kind of access control mechanism based on commodity market in P2P file sharing system[J]. Chinese Journal of Computers, 2012,35(8): 1675-1682.

[6] 李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016,37(5): 9-20.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control mode[J]. Journal on Communications, 2016,37(5): 9-20.

[7] LIU W, REN P, SUN D H, et al. TrustP2PNet: P2P social network with admission control model based on trust[J]. Aasri Procedia, 2013, 5(3): 281-286.

[8] WANG X. A study of P2P access control strategy based on trust and security grade [C]// CSSS Proceedings. 2011.

[9] LANG B. A computational trust model for access control in P2P [J]. Science China Information Sciences, 2010, 53(5): 896-910.

[10] 范艳芳, 蔡英. 支持协作的强制访问控制模型[J].计算机研究与发展, 2015, 52(10): 2411-2421.
FAN Y F, CAI Y. Cohabitation supported mandatory access control mode[J]. Journal of Computer Research and Development, 2015, 52(10): 2411-2421.

[11] 郭树行, 张禹. 基于动态情景网关的系统协同访问控制模型[J]. 通信学报, 2013, 34(z1): 142-145.
GUO S X, ZHANG Y. Dynamic situation gateway based system cooperation access gate model[J]. Journal on Communications, 2013, 34(z1): 142-145.

[12] 田俊峰, 杜瑞忠, 蔡红云, 等. 可信计算与信任管理[M]. 北京: 科学出版社, 2014.
TIAN J F, DU R Z, CAI H Y, et al. Trusted computing and trust management[M]. Beijing: Science Press, 2014.

[13] 李开, 章华娟, 卢正鼎. P2P 网络中基于信任的风险计算方法[J]. 计算机科学, 2010,37(10): 102-105.
LI K, ZHANG H J, LU Z D. Risk assessment approach based on trust in P2P network[J]. Computer Science, 2010,37(10): 102-105.

[14] 惠榛, 李昊, 张敏, 等. 面向医疗大数据的风险自适应的访问控制模型[J].通信学报, 2015,36(12): 190-199.
HUI Z, LI H, ZHANG M, et al. Risk-ablative access control model for big data in healthcare[J]. Journal on Communications, 2015,36(12): 190-199.

[15] TIAN J F, LI C, HE X M. Trust model based on the multinomial subjective logic and risk mechanism for P2P network of file sharing [J].Journal of Electronics, 2011,28(1): 108-117.

[16] 张润莲, 武小年, 周胜源, 等. 一种基于实体行为风险评估的信任模型[J].计算机学报, 2015, 36(12): 190-199.
ZHANG R L, WU X N, ZHOU S Y, et al. A trust model based on behaviors risk education[J]. Chinese Journal of Computers, 2015,36(12): 190-199.

[17] KWAKERNAAK H. An algorithm for rating multiple-aspect alternatives using fuzzy sets[J]. Automatica, 1979, 15(5): 615-616.

[18] 姜江, 李漩, 邢立宁, 等. 基于模糊证据推理的系统风险分析与评价[J].系统工程理论与实践, 2013, 33(2): 529-538.
JIANG J, LI X, XING L N, et al. System risk analysis and evaluation approach based on fuzzy evidential reasoning[J]. System Engineering-Theory & Practice, 2013,33(2): 529-538.

[19] 严斌宇, 刘方圆, 董敏坚. 一种基于风险评价的无线传感器网络信任模型[J]. 中南大学学报(自然科学版), 2011, 42(6): 1657-1661.
YAN B Y, LIU F Y, DONG M J. Trust model based on risk evaluation in wireless sensor networks[J]. Journal of Central South University(Science and Technology), 2011, 42(6): 1657-1661.

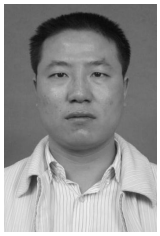
[20] 陈华喜, 郭有强, 姚保峰. 一种耦合赋权的网络安全评价模型[J]. 计算机工程, 2011, 37(22): 99-103.
CHEN H X, GUO Y Q, YAO B F, et al. Network security assessment model of coupling empowerment[J]. Computer Engineering, 2011, 37(22): 99-103.

[21] 赵勇, 刘吉强, 韩臻. 基于任务的访问控制模型研究[J].计算机工程, 2008,34(5): 28-30.
ZHAO Y, LIU J Q, HAN Z. Research on access control model based on task[J]. Computer Engineering, 2008,34(5): 28-30.

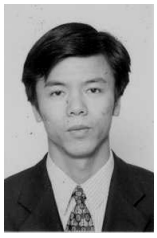
[22] 邓集波, 洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003,14(1):76-81.
DENG J B, HONG F. Task-based access control model[J]. Journal of Software, 2003,14(1):76-81.

[23] 谢季坚, 刘承平. 模糊数学方法及其应用[M].武汉: 华中科技大学出版社, 2000.
XIE J J, LIU C P. Fuzzy mathematics method and its application[M]. Wuhan: Huazhong University of Science & Technology Press, 2000.

作者简介：



刘浩（1977-），男，湖南邵阳人，湖南人文科技学院副教授，主要研究方向为并行计算、P2P 网络、信息安全等。



张连明（1972-），男，湖南邵阳人，湖南师范大学教授，主要研究方向为复杂网络与网络演算等。

陈志刚（1964-），男，湖南长沙人，中南大学教授、博士生导师，主要研究方向为计算机网络与分布式系统等。